LD3032

GPON OLT system

User Manual

Summary of Changes

Changes for : Issue 04

Chapter/Section	Reason for Update
3.1.2 Privileged EXEC Enable Mode	‘quote COMMAND’ command added.
3.2.2 Calling Command History	‘show cli history list' command added.
4.1.3.4 Creating System Account	‘user rename NAME_FROM NAME_TO' command added
4.1.9 Telnet Access	Telnet access related CLI added.
4.2.1 Displaying System Configuration	CLI about running configuration of the system updated.
4.2.2 Comparing Configuration Changes	‘show compare-config' comand added.
5.2.5 Displaying IUs Information	IUs information related CLI added
5.4.5 Displaying Interface	‘show ipv6 policy' command added.
5.5.3.7 IPv6 PBR Configuration	Configuring a route map for IPv6 PBR on an interface related CLI added.
5.5.4 Static Route and Default Gateway	Static Route related CLI added.
6.1.6.1 CPU Load	threshold of CPU load related CLI added.
6.1.9 SD Card	SD card information related CLI added.
6.1.10 Power Alarm Configuration	Alarm notification related CLI added.
6.1.11 Enabling FTP/TFTP Connection	FTP/TFTP connection related CLI added.
6.1.12 EQM Debugging	EQM debugging configuration added.
6.2.8 System Memory Information	System memory information related CLI updated. Configuring a debuggin for memory trace related CLI added.
6.2.9.1 Slowpath Filtering	‘show running-config slowpath-filter' command added.
6.2.18 Network Service Module (NSM) Informtaion	‘show nsm client' command added
6.2.19 Network Service Module (NSM) Daemon Debugging	NSM daemon debugging related CLI added.
7.1.1 SNMP Service	Enabling SNMP service related CLI added.
7.1.2 Restarting SNMP Deamon	‘restart snmpd' command added.

7.1.12 Displaying SNMP Configuration	Displaying SNMP OID related CLI added.
7.4.1 Syslog Output Level	Syslog output about SD card related CLI added.
7.4.3 Syslog index	‘syslog index snmp' command added.
7.4.7 Displaying Syslog Message	Received syslog message related CLI updated.
7.4.8 Uploading Syslog File	Uploading syslog files using FTP/TTP related CLI added.
7.7.2.2 Creating MEP	Assigning the configured MEP related CLI added.
7.7.20.11 Displaying Redundancy Sync-Module	‘show redundancy sync-module-list' command added.
7.12 MAC Table	‘show mac aging-time' command added.
7.15.2 SYN Configuration	‘ipv6 tcp syn-guard BANDWIDTH' command added.
7.17.7 Access List Entries Limit	Access list limitation related CLI added.
8.1.1.1 Registering ARP Table	Deleting the ARP entries related CLI added.
8.2.10.6 ND RA Guard	IPv6 RA Guard feature added.
8.2.13 Debugging Neighbor Discovery	IPv6 ND packet debugging related CLI added.
9.1.1.2 Adding a Member Port to VLAN Group	‘switchport trunk allowed vlan' related CLI added.
9.1.5 Displaying VLAN Information	Displaying VLAN information related CLI updated.
9.3.2.4 Class Creation	Displaying created class related CLI added.
9.3.6.1 Creating Admin Flow for packet classification	Displaying created admin flow related CLI added.
9.3.9 Displaying Policy Interface Configuration	Displaying policy interface configuration related CLI added.
9.4.4 Enabling STP Function	Enabling/disabling STP function on a interface CLI added.
9.4.11 Loop Back Detection	Error-disable recovery function related CLI added.
9.6.6.5 Appending Enterprise Number	‘policy append enterprise-number' command added.

9.6.11 Debugging DHCP	‘show debugging dhcp' command added.
9.7 Dynamic Host Configuration Protocol (DHCP) for IPv6	DHCP for IPv6 Chapter added.
9.7.1.3 DHCPv6 unique identifier (DUID)	DUID related CLI added.
9.8.1.2 Access to Associated IP Address	‘vip-access' CLI updated.
9.8.2.3 VRRP Debug	RRP debugging related CLI added.
9.10.4 Invalid Traffic Guard	Invalid Traffic Guard function description added.
9.14 Configuring PPPoE Tag Option Format	Configuring PPPoE Tag Option Chapter added.
10.1.2.1 IGMP Static Join	CLI modified.
10.2.2.4 IGMP Snooping R-APS	Enabling R-APS packet related CLI added.
10.2.3.8 TCN Multicast Flooding	Topology Change Notification(TCN) debugging related CLI added.
10.2.7.8 Displaying IGMP Proxy Information	Displaying IGMP proxy group membership information related CLI added.
10.3.1.1 Enabling Multicast Routing	Enabling Layer 3 multicast routing for IPv6 related CLI added.
10.3.1.5 Static Multicast Route Configuration	configuring mroute related CLI added.
10.3.1.7 Displaying RPF information	‘show ip rpf A.B.C.D' command added.
10.3.2.1 PIM Mode	‘clear ip pim sparse-mode packet' command added.
10.3.3.1 Rendezvous Point	Usinf anycast RP related CLI added.
10.3.3.6 Debugging PIM-SM	Debuggin PIM-SM related CLI added.
10.4 IP Multicast Interface	Displaying IP multicast interface configuration related CLI added.
11 IPv6 Multicast	IPv6 Multicast Chapter added.
11.1 Multicast Listener Discovery (MLD)	Multicast Listener Discovery (MLD) related CLI added.
11.2 IPv6 Multicast Functions	MLD snooping related CLI added.
11.3 IPv6 Multicast Routing	Multicast Routing related CLI added.
11.4 IPv6 Multicast Interface	Displaying IPv6 multicast interface configuration related CLI added.

11.1.7 Displaying MLD Information	‘show ipv6 mld-proxy' command added.
12.1.1.4 Enabling ASN Capabilities	‘bgp extended-asn-cap' command added.
12.1.1.6 IPv4 Unicast Address	‘bgp default ipv4-unicast' command added.
12.1.1.8 BGP Aggregation	‘bgp aggregate-nexthop-check' command added.
12.1.1.9 BGP Path Selection	RFC1771 configuration related CLI added.
12.1.3 BGP Autonomous System Number Formatting	CLI to change the default display and regular expression match format of BGP added. ‘bgp asnotation {dot | dotplus}' command added.
12.1.4 Enforcing the First AS Path Feature	‘bgp enforce-first-as’ command added.
12.1.5 External BGP Peering Session Reset	‘bgp fast-external-failover’ command added.
12.1.6 BGP Scan Time	‘bgp scan-time <0-60>' command added.
12.1.7 BGP Update Delay	‘bgp update-delay <1-3600>' command added.
12.1.9 Route Reflector	Displaying BGP network information related CLI added.
12.1.15 BGP Session Reset	Managing BGP network related CLI added and updated.
12.1.16 BGP AS-path Access List	Definong AS path access-list related CLI added.
12.1.20 BGP Network	Backdoor route and route-map related CLI added.
12.1.23 BGP Filtering through Prefix Lists	BGP Filtering through Prefix Lists Chapter added.
12.1.25 BGP Monitoring and Management	BGP configuration related CLI added.
12.2.17 Blocking Routing Information	‘distribute-list WORD in' command added.
12.2.19.1 Displaying OSPF Protocol Information	‘show ip protocols ospf ' command added.
12.3.6.2 Not So Stubby Area (NSSA)	NSSA cnfiguration related CLI added.
12.3.8 Graceful Restart Support	Restarting OSPFv3 protocol pcocessor related CLI added.
12.3.14 OSPFv3 Distance	OSPFv3 Distance configuration related CLI added.

12.3.15.1 Displaying OSPFv3 Information	‘show ipv6 protocols ospf ' related CLI added.
12.4.16 RIP Routing Metric Update as Cisco	Enabling/disabling the RIP routing metric update related CLI added.
12.4.17.1 Displaying RIP Protocol Information	Displaying RIP information related CLI added.
12.4.16 RIP Routing Metric Update as Cisco	‘cisco-metric-behavior ' command added.
12.5 Routing Information Protocol Next Generation (RIPng)	Routing Information Protocol Next Generation Chapter added.
12.7 Virtual Routing and Forwarding (VRF)	Virtual Routing and Forwarding Chapter added.
13.1.10 OLT Transceiver	OLT transceiver configuration related CLI added.
13.1.22 OMCI-DB Validation Check	Checking the OMCI ME information related CLI added.
13.1.23 OMCI MIB Upload Suppression	‘olt omci-mib-upload-sup enable’ Command added.
13.1.25 Flow Control Configuration	Configuring flow control on gpon interface related CLI added.
13.1.26.1 OLT Traffic Statistics	Displaying traffic statistics of an OLT related CLI added.
13.2.11.4 PPPoE Configuration	PPPoE of ONU related CLI added.
13.2.14 ONU Reset	ONU reset related CLI added.
13.2.22 Generic Status Portal (GSP)	GSP Configuration related CLI added.

Contents of update:

Changes made between issue 02 and issue 03

Chapter/Section	Reason for Update
4.1.3.3	“Login Password Recovery Process” added.

Changes made between issue 01 and issue 02

Chapter/Section	Reason for Update
4.1.9 Telnet Access	Telnet service connection related CLI added.

Issue History

Issue Number	Date of Issue	SW Release Version for Update
01	10/2015	Initial release
02	10/2015	Software Release NOS1.02
03	02/2016	Software Release NOS1.02
04	05/2016	Software Release NOS1.04

Contents

Illustrations

Tables

1 Introduction

1.1 Audience

This manual is intended for LD3032 multi-platform PON OLT system operators and maintenance personnel for providers of Gigabit passive optical network (GPON) and Ethernet services. This manual assumes that you are familiar with the following:

- Ethernet networking technology and standards
- Internet topologies and protocols
- PON technology and standards
- Usage and functions of graphical user interfaces.

1.2 Document Structure

Tab. 1.1 briefly describes the structure of this document.

Chapter	Description
1 Introduction	Introduces the overall information of the document.
2 System Overview	Introduces the LD3032 system. It also lists the features of the system.
3 Command Line Interface (CLI)	Describes how to use the Command Line Interface (CLI).
4 System Basic Configuration and Operation	Describes how to manage the system account and IP address.
5 Equipment/Interface Management	Descibes the slot assignment and how to configure the plug-in places of the chassis and replace the IUs.
6 System Environment	Describes how to configure the system environment and management functions.
7 Network Management	Describes how to configure the network management functions.
8 System Security	Describes how to configure the system security functions.
9 System Main Functions	Describes how to configure the system main functions.
10 IP Multicast	Describes how to configure the IP multicast functions.
12 IP Routing Protocol	Describes how to configure the IP routing protocols.
12 GPON Configuration	Describes how to configure the GPON functions.
14 System Software Upgrade	Describes how to upgrade the system software.
15 Abbreviations	Lists all abbreviations and acronyms which appear in this document.

Tab. 1.1 Overview of Chapters

1.3 Document Convention

This guide uses the following conventions to convey instructions and information.

Information

ℹ This information symbol provides useful information when using commands to configure and means reader take note. Notes contain helpful suggestions or references.

Warning

⚠ This warning symbol means danger. You are in a situation that could cause bodily injury or broke the equipment. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents by making quick guide based on this guide.

1.4 Document Notation

The following table shows commands used in guide book. Please be aware of each command to use them correctly.

Notation	Description
a	Commands you should use as is.
NAME, PROFILE, VALUE, …	Variables for which you supply values.
IFPORTS	For entry this variable, see Section 5.3.1.
[ ]	Commands or variables that appear within square brackets [ ] are optional.
< >	Range of number that you can use.
{ }	A choice of required keywords appears in braces { }. You must select one.
|	Optional variables are separated by vertical bars |.

Tab. 1.2 Command Notation of Guide Book

1.5 Virus Protection

⚠ To prevent a virus infection you may not use any software other than that which is released for the Operating System (OS based on Basis Access Integrator), Local Craft Terminal (LCT) and transmission system.

Even when exchanging data via network or external data media(e.g. floppy disks) there is a possibility of infecting your system with a virus. The occurrence of a virus in your system may lead to a loss of data and breakdown of functionality.

⚠ The operator is responsible for protecting against viruses, and for carrying out repair procedures when the system is infected.

You have to do the following:

- You have to check every data media (used data media as well as new ones) for virus before reading data from it.
- You must ensure that a current valid virus scanning program is always available. This program has to be supplied with regular updates by a certified software.
- It is recommended that you make periodic checks against viruses in your OS.
- At the LCT it is recommended to integrate the virus scanning program into the startup sequence.

1.6 Declaration of CE Conformity

The CE declaration of the product will be fulfilled if the construction and cabling is undertaken in accordance with the manual and the documents listed there in, e.g. mounting instructions, cable lists where necessary account should be taken of project-specific documents.

Deviations from the specifications or unstipulated changes during construction, e.g. the use of cable types with lower screening values can lead to violation of the CE requirements. In such cases, the conformity declaration is invalidated and the responsibility passes to those who have caused the deviations.

⚠ This is a class A product. In a domestic environment, this product may cause radio reference in which case the user may be required to take adequate measures.

1.7 GPL/LGPL Warranty and Liability Exclusion

Furukawa’s, LD3032, contains both proprietary software and “Open Source Software”. The Open Source Software is licensed to you at no charge under the GNU General Public License (GPL) and the GNU Lesser General Public License (LGPL). This Open Source Software was written by third parties and enjoys copyright protection. You are entitled to use this Open Source Software under the conditions set out in the GPL and LGPL licenses indicated above. In the event of conflicts between Furukawa license conditions and the GPL or LGPL license conditions, the GPL and LGPL conditions shall prevail with respect to the Open Source portions of the software.

The GPL can be found under the following URL:
http://www.gnu.org/copyleft/gpl.html

The LGPL can be found under the following URL:
http://www.gnu.org/copyleft/lgpl.html

In addition, if the source code to the Open Source Software has not been delivered with this product, you may obtain the source code (including the related copyright notices) by sending your request.

You will, however, be required to reimburse Furukawa Electric Latam for its costs of postage and copying. Any source code request made by you must be sent within 3 years of your purchase of the product. Please include a copy of your sales receipt when submitting your request. Also please include the exact name and number of the devices and the version number of the installed software.

The use of Open Source Software contained in this product in any manner other than the simple running of the program occurs at your own risk, that is, without any warranty claims against Furukawa Electric Latam. For more information about the warranties provided by the authors of the Open Source Software contained in this product, please consult the GPL and LGPL.

You have no warranty claims against Furukawa Electric Latam when a defect in the product is or could have been caused by changes made by you in any part of the software or its configuration. In addition, you have no warranty claims against Furukawa Electric Latam when the Open Source Software infringes the intellectual property rights of a third party.

Furukawa Electric Latam provides no technical support for either the software or the Open Source Software contained therein if either has been changed.

2 System Overview

The LD3032 is a 2RU height chassis GPON Optical Line Termination (OLT) which supports up to 32-Port GPON interfaces per chassis. You can insert or pull out the plug-in units to/from the chassis in easy and safe way.

The LD3032 provides 7 slots for the plug-in units. Each type of interface unit contains different number of ports. The two slots are reserved for the SFU cards for management/switching. And two slots are reserved for the SIU for providing up to 32 GPON subscriber interfaces (SIU_GPON16) per chassis. Each SFU contains four 1G/10G ports (SFP/SFP+) as the uplink interfaces, and the remaining three slots are reserved for two power supply modules and fan unit. A console interface for CLI accesses as well as a RJ45 interface for out-of-band management is provided on the SFU's front panel. The two slots are reserved for the modular DC type power supply units to provide power redundancy and flexibility in various operating environments.

The LD3032 is comprised of two GPON service modular units to deliver a wide range of full-featured and high-performance over FTTx applications. It is a high-density chassis system that supports up to 4,096 residential and business subscribers (ONTs) with 32 GPON ports (1:128 split ratio). The system also provides simultaneous services of GPON and Gigabit Ethernet. The LD3032 features flexible and high capacity GPON access and 10GbE uplinks, scalability and line rate performance with 320Gbps non-blocked switch fabric.

The LD3032 guarantees equipment-level reliability with full redundancy design concept of SFU/Power/GPON ports. Continuous traffic forwarding to the core network without failure is a substantial factor for aggregation switches to perform. The PON technology adds new features and functionality targeted at improving performance and interoperability. In addition adds support for new applications, services, and deployment scenarios. Among these changes are improvements in data rate and reach performance, diagnostics, and stand-by mode.

Fig.2.1 shows the product view of the LD3032.

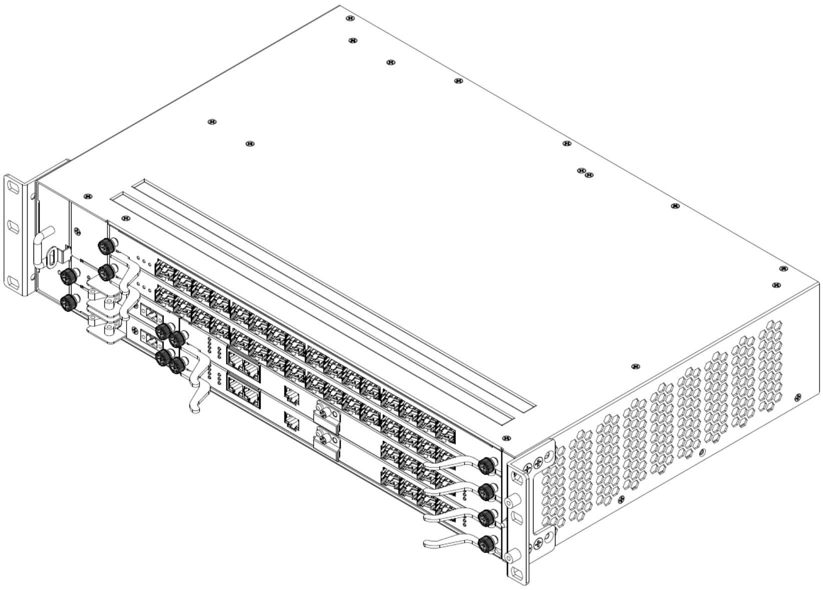


Fig. 2.1 Front View of the LD3032

2.1 System Features

This section introduces the main features of the LD3032 GPON OLT system which provides Layer 3 switching, Ethernet switching and GPON functionalities.

Virtual Local Area Network (VLAN)

Virtual local area network (VLAN) is made by dividing one network into several logical networks. Packets cannot be transmitted between different VLANs. Therefore it can prevent needless packets accumulating and strengthen security. The LD3032 recognizes 802.1Q tagged frame and supports maximum 4096 VLANs. Port-based, protocol-based, MAC-based, and subnet-based VLANs are supported in the LD3032.

Quality of Service (QoS)

For the LD3032, QoS-based forwarding sorts traffic into a number of classes and marks the packets accordingly. Thus, different quality of service is provided to each class, which the packets belong to. The rich QoS capabilities enable network managers to protect mission-critical applications and support differentiated level of bandwidth for managing traffic congestion. The LD3032 support ingress and egress (shaping) rate limiting, and different scheduling type such as Strict Priority (SP), Weighted Round Robin (WRR) and Deficit Round Robin (DRR).

IP Multicast

Because broadcasting in a LAN is restricted if possible, multicasting could be used instead of broadcasting by forwarding multicast packets only to the member hosts who joined multicast group. The LD3032 provides IGMPv2, IGMP snooping and PIM-SM for host membership management and multicast routing.

SNMP

Simple Network Management Protocol (SNMP) is to manage network elements using TCP/IP protocol. The LD3032 supports SNMPv1, 2, 3 and Remote Monitoring (RMON). Network operator can use MIB also to monitor and manage the LD3032.

IP Routing

The LD3032 is Layer 3 switch, which has routing table and IP address as router. Therefore, it supports static routing, RIPv1/v2, OSPFv2 and BGPv4 for unicast routing.

Dynamic Host Configuration Protocol (DHCP)

The LD3032 supports Dynamic Host Configuration Protocol (DHCP) server that automatically assigns IP address to clients accessed to network. That means it has IP address pool, and operator can effectively utilize limited IP source by leasing temporary IP address. In Layer 3 network, DHCP request packet can be sent to DHCP server via DHCP relay and option 82 function.

Spanning Tree Protocol (STP)

To prevent loop and preserve backup route in Layer 2 network, the LD3032 supports Spanning Tree Protocol (STP) defined in IEEE 802.1D. Between STP enabled switches, a root bridge is automatically selected and the network remains in tree topology. However, the recovery time in STP is very slow (about 30 seconds), Rapid Spanning Tree Protocol (RSTP) is also provided. IEEE 802.1W defines the recovery time as 2 seconds. If there is only one VLAN in the network, traditional STP works. However, in more than one VLAN network, STP cannot work per VLAN. To avoid this problem, the LD3032 supports Multiple Spanning Tree Protocol (MSTP).

Link Aggregation (Trunking)

The LD3032 aggregates several physical interfaces into one logical port (aggregate port). Port trunk aggregates interfaces with the standard of same speed, same duplex mode, and same VLAN ID. According to IEEE 802.3ad, the LD3032 can configure maximum 8 aggregate ports and up to 12 trunk groups.

Link Aggregation Control Protocol (LACP)

The LD3032 supports Link Aggregation Control Protocol (LACP), complying with IEEE 802.3ad, which aggregates multiple links of equipments to use more enlarged bandwidth.

System Management based on CLI

It is easy for users who administer system by using telnet or console port to configure the functions for system operating through CLI. CLI is easy to configure the needed functions after looking for available commands by help menu different with UNIX.

Storm Control

Broadcast storm control is, when too much of broadcast packets are being transmitted to network, a situation of network timeout because the packets occupy most of transmit capacity. The LD3032 supports broadcast and multicast storm control, which disuses flooding packet, that exceed the limit during the time configured by user.

SLA (Service Level Agreement)

Service level agreement (SLA) is a bilateral, legal agreement between network provider and customer to specify the quality of service. The major aspects of a quality of service agreement where network and service parameters are specified are the bandwidth, the availability, the network capacity, and the network quality. The purpose of SLA is on reducing expenditure by adapting standardized rating criteria for network service. To set target for the service quality, standard values for availability, transaction time, failure rate for connection and so forth are specified. With this, the minimum network speed is to be assured, and handling network troubles is to be prepared to improve service quality and user efficiency.

Profile-based Management

With profile function, each OLT can be configured and managed. By creating several profiles to have some configurations, if an OLT is assigned to use an appropriate profile of the profiles, the assigned profile will be automatically applied to the OLT. So the use of profile provides easy and efficient manageability for the OLT conforming policies and service environments of users.

Outband Management Interface

The LD3032 can connect to equipments at remote place by assigning IP address to MGMT interface. Since MGMT interface is operated regardless of status of service port, it is still possible to configure and manage equipment at remote place even though problem such as link disconnection is occurred.

RADIUS and TACACS+

The LD3032 supports client authentication protocol, that is RADIUS (Remote Authentication Dial-In User Service) and TACACS+ (Terminal Access Controller Access Control System Plus). Not only user IP and password registered in switch but also authentication through RADIUS server and TACACS+ server are required to access. So security of system and network management is strengthened.

Secure Shell (SSH)

Network security is getting more important because the access network has been generalized among numerous users. However, typical FTP and telnet service have big weakness for their security. Secure shell (SSH) is a network protocol that allows establishing a secure channel between a local and a remote computer. It uses public-key cryptography to authenticate the remote computer and to allow the remote computer to authenticate the user.

3 Command Line Interface (CLI)

The LD3032 enables system administrators to manage the LD3032 by providing the command line interface (CLI). This user-friendly CLI provides you with a more convenient management environment.

To manage the system with the CLI, a management network environment is required. The LD3032 can connect to the management network either directly (outband) or through the access network (inband). It can even connect using a combination of the two; for example, a cascaded LD3032 connects inband to the cascading switch, and then from the cascading switch to the management network through the outband interface.

The LD3032 also provides the RS232 console interface to simply access the system with a provided RJ45-to-DB9 cable.

This chapter describes a basic instruction for using the command line interface (CLI) which is used for managing the LD3032 system.

- Configuration Mode
- Useful Tips

3.1 Configuration Mode

You can configure and manage the LD3032 with the CLI via a management network environment or the console interface.

- The CLI provides the following command modes:
  - Privileged EXEC View Mode
  - Privileged EXEC Enable Mode
  - Global Configuration Mode
  - DHCP Pool Configuration Mode
  - DHCP Option Configuration Mode
  - DHCP Option 82 Configuration Mode
  - Interface Configuration Mode
  - Rule Configuration Mode
  - RMON Configuration Mode
  - Router Configuration Mode
  - Route-Map Configuration Mode
  - GPON Configuration Mode

3.1.1 Privileged EXEC View Mode

When you log in to the switch, the CLI will start with *Privileged EXEC View* mode which is a read-only mode. In this mode, you can see a system configuration and information with several commands.

Tab. 3.1 shows main command of *Privileged EXEC View* mode.

Command	Description
enable	Opens *Privileged EXEC Enable* mode.
exit	Logs out the switch.
show	Shows a system configuration and information.

Tab. 3.1 Main Command of *Privileged EXEC View* Mode

3.1.2 Privileged EXEC Enable Mode

To configure the switch, you need to open *Privileged EXEC Enable* mode with the **enable** command, then the system prompt will changes from SWITCH> to SWITCH#.

Command	Mode	Description
enable	View	Opens *Privileged EXEC Enable* mode.

You can set a password to *Privileged EXEC Enable* mode to enhance security. Once setting a password, you should enter a configured password, when you open *Privileged EXEC Enable* mode.

Tab. 3.2 shows main commands of *Privileged EXEC Enable* mode.

Command	Description
clock	Sets a system time and date.
configure terminal	Opens *Global Configuration* mode.
reload	Reboots the system.
telnet	Connects to a remote host through telnet.
terminal length	Configures the number of lines of the current terminal.
traceroute	Traces a packet route.
where	Displays users accessing the system via telnet or console.

Tab. 3.2 Main Command of *Privileged EXEC Enable* Mode

In *Privileged EXEC Enable* mode, you can send a subcommand to an FTP server by using the **quote** *COMMAND commands*.

Command	Mode	Description
quote *COMMAND*	Enable	Sends a command to the Linux. COMMAND: external command

3.1.3 Global Configuration Mode

In *Global Configuration* mode, you can configure general functions of the system. You can also open another configuration mode from this mode.

To open *Global Configuration* mode, enter the **configure terminal** command, and then the system prompt will be changed from SWITCH# to SWITCH(config)#.

Command	Mode	Description
configure terminal	Enable	Opens *Global Configuration* mode.

Tab. 3.3 shows main commands of *Global Configuration* mode.

Command	Description
access-list	Configures an access list.
dns	Sets a DNS server.
dot1x	Configures 802.1X authentication.
exec-timeout	Sets an auto log-out timer.
help	Shows a description of the interactive help system.
hostname	Sets a host name of the system.
interface	Opens *Interface Configuration* mode to configure a specified interface.
mvr	Configures MVR.
ntp	Configures NTP.
passwd	Sets a system password.
qos	Configures QoS.
rmon-alarm	Opens *RMON Configuration* mode to configure RMON alarm.
route-map	Opens *Route-map Configuration* mode.
snmp	Configures SNMP.
ssh	Configures SSH.
syslog	Configures a syslog.
threshold	Sets a system threshold.

Tab. 3.3 Main Command of *Global Configuration* Mode

3.1.4 Interface Configuration Mode

The *Interface Configuration* mode configures the switch at the physical interface level. In a particular interface mode, you can use the commands configure specific IP interface settings, including bridge-group, description, etc.

The following table shows several types of interfaces.

Interface Type	Internal i/f Name (Abbreviation)	Configuration (CLI)	Description

gpon	GPON	`SWITCH(config)#` **`interface gpon`** *`1/1`*
		`SWITCH(config-if[GPON1/1])#`
			G.984.x GPON

gigabitethernet	GE	`SWITCH(config)#` **`interface gigabitethernet`** *`1/1`*
		`SWITCH(config-if[GE1/1])#`
			Gigabit Ethernet IEEE 802.3z

tengigabitethernet	XE	`SWITCH(config)#` **`interface tengigabitethernet`** *`0/1`*
		`SWITCH(config-if[XE1/1])#`
			10-Gigabit Ethernet IEEE 802.3an

management	mgmt	`SWITCH(config)#` **`interface management`**
		`SWITCH(config-if[mgmt])#`
			Management interface

channelgroup	CG	`SWITCH(config)#` **`interface channelgroup`** *`GROUP-ID`*
		`SWITCH(config-if[CG#])#`
			Link aggregation

vlan	br	`SWITCH(config)#` **`interface vlan`** *`1`*
		`SWITCH(config-if[1])#`
			Virtual LAN

loopback	lo	`SWITCH(config)#` **`interface loopback`**
		`SWITCH(config-if[lo])#`
			Loopback interface

3.1.4.1 Ethernet Interface Mode

The Ethernet Interface mode contains commands for configuring the 1GE or 10GE interface. You can open this *Interface Configuration* mode when at least one SFU_10GE4 module is installed in the LD3032 chassis.

To open *Ethernet Interface Configuration* mode, enter the **interface gigabitethernet**/**tengigabitethernet** command, then the system prompt will be changed from SWITCH(config)# to SWITCH(config-if[GE])# or SWITCH(config-if[XE])#.

Command	Mode	Description
interface {**gigabitethernet** | **tengigabitethernet**} *IFPORT*	Global	Enters the *Interface Configuration* mode to configure an 1G/10G Ethernet type interface. IFPORT: physical interface port number (SLOT#/PORT#, e.g. 0/1, 0/2) IFPORT-RANGE: list of valid ports per Ethernet interface unit. Use a hyphen to designate a range of ports. (e.g. 0/1-4 or 0/1-0/4)
interface range {**gigabitethernet** | **tengigabitethernet**} *IFPORT-RANGE*		

3.1.4.2 GPON Interface Mode

The GPON Interface mode contains commands for configuring the GPON interface. You can open this *Interface Configuration* mode when at least one SIU_GPON16 module is installed in the LD3032 chassis.

To open *GPON Interface Configuration* mode, enter the **interface gpon** command, then the system prompt will be changed from SWITCH(config)# to SWITCH(config-if[GPON])#.

Command	Mode	Description
interface gpon *IFPORT*	Global	Enters the *Interface Configuration* mode to configure an GPON type interface. IFPORT: physical interface port number (SLOT#/PORT#, e.g. 1/1, 2/1) IFPORT-RANGE: list of valid ports per GPON interface unit. Use a hyphen to designate a range of ports. (e.g. 1/1-16 or 1/1-1/16)
interface range gpon *IFPORT-RANGE*		

3.1.4.3 Management (MGMT) Interface Mode

You can configure the system to be accessed remotely by Telnet. Firstly, you have to install the SFU module in the central slot of the chassis. The LD3032 has a management port (MGMT) and console port on the front panel of SFU module.

To open *Interface MGMT Interface Configuration* mode, enter the **interface management** command, then the system prompt will be changed from SWITCH(config)# to SWITCH(config-if[mgmt])#.

Command	Mode	Description
interface management	Global	Opens *MGMT Interface Configuration* mode to specify an IP address.

3.1.4.4 VLAN Database Mode

To create a VLAN, the VLAN Database mode contains the commands. To open *VLAN Database* mode, enter the **vlan database** command, then the system prompt will be changed from SWITCH(config)# to SWITCH(config-vlan)#.

Command	Mode	Description
vlan database	Global	Opens *VLAN Database* mode.
vlan *VLANS*	VLAN Database	Creates a VLAN by assigning VLAN ID: VLANS: VLAN ID (2-4094, multiple entries possible)

When a VLAN ID is created in the VLAN Database mode, you can enter the VLAN Interface mode. To open *VLAN Interface* mode, enter the **interface vlan** command, then the system prompt will be changed from SWITCH(config)# to SWITCH(config-if[*VLANS*])#.

Command	Mode	Description
interface vlan *VLANS*	Global	Opens *VLAN Interface* mode. VLANS: an existing VLAN ID

3.1.4.5 Channel Group Mode

The Channel Group mode contains commands for configuring Link Aggregation Groups (LAG) or Trunk.

To open *Channel Group* mode, enter the **interface channelgroup** command, then the system prompt will be changed from SWITCH(config)# to SWITCH(config-if[CG#])#.

Command	Mode	Description
interface channelgroup *GROUP-ID*	Global	Opens *Channel Group* mode. GROUP-ID: an existing channel-group number IFPORT-RANGE: list of valid channel-group numbers to add.
interface range channelgroup *GROUP-ID-RANGE*		

3.1.5 DHCP Pool Configuration Mode

In *DHCP Pool Configuration* mode, you can configure general functions of DHCP per each DHCP pool. The LD3032 supports multiple DHCP environments with this pool-based DHCP configuration.

To open *DHCP Pool Configuration* mode, enter the **ip dhcp pool** command, then the system prompt will be changed from SWITCH(config)# to SWITCH(config-dhcp[POOL])#.

Command	Mode	Description
ip dhcp pool *POOL*	Global	Opens *DHCP Pool Configuration mode* to configure DHCP.

⚠ To open *DHCP Pool Configuration* mode, use the **service dhcp** command in the *Global Configuration* mode first!

Tab. 3.4 shows main commands of *DHCP Pool Configuration* mode.

Command	Description
default-router	Configures the default gateway of the pool.
dns-server	Configures a DNS server.
range	Configures the range of IP addresses.

Tab. 3.4 Main Command of *DHCP Pool Configuration* Mode

3.1.6 DHCP Option Configuration Mode

In *DHCP Option Configuration* mode, you can configure DHCP option. You can define DHCP options that are carried in the DHCP communication between DHCP server and client or relay agent. A specific DHCP option can be defined by its format type, length and value.

To open *DHCP Option Configuration* mode, use the command. Then the system prompt will be changed from SWITCH(config)# to SWITCH(dhcp-opt[NAME])#.

Command	Mode	Description
ip dhcp option format *NAME*	Global	Opens *DHCP Option Configuration* mode to configure DHCP options.

The following is the main command of *DHCP Option Configuration* mode.

Command	Description
attr	Configures the attribute for option field in the DHCP packet.

Tab. 3.5 Main Command of *DHCP Option Configuration* Mode

3.1.7 DHCP Option 82 Configuration Mode

In *DHCP Option 82 Configuration* mode, you can configure DHCP option 82 for DHCP relay agent. This feature enables network administrators to manage IP resources more efficiently.

To open *DHCP Option 82 Configuration* mode, enter the **ip dhcp option82** command, then the system prompt will be changed from SWITCH(config)# to SWITCH(config-opt82)#.

Command	Mode	Description
ip dhcp option82	Global	Opens *DHCP Option 82 Configuration* mode to configure DHCP option 82.

To open *DHCP Option 82 Configuration* mode, use the **service dhcp** command in the *Global Configuration* mode first!

Tab. 3.6 is the main commands of *DHCP Option 82 Configuration* mode.

Command	Description
policy	Configures the policy for option 82 field in the DHCP packet.
system-remote-id	Configures a system remote ID.
system-circuit-id	Configures a system circuit ID.

Tab. 3.6 Main Command of *DHCP Option 82 Configuration* Mode

3.1.8 Rule Configuration Mode

Rule configuration is classified by three different modes according to its roles for Rule mechanism. You can configure a rule for incoming or outgoing packets. Using the function, you can handle packets classified by the rule.

To open *Rule Configuration* mode, enter the **flow, policer and policy** commands, then the system prompt will be changed from SWITCH(config)# to SWITCH(config-flow[NAME])#, SWITCH(config-policer[NAME])# and SWITCH(config-policy[NAME])# .

Command	Mode	Description
flow *NAME* **create**	Global	Opens *Flow Configuration* mode.
policer *NAME* **create**		Opens *Policer Configuration* mode.
policy *NAME* **create**		Opens *Policy Configuration* mode.

Tab.3.7 shows main commands of *Rule Configuration* mode.

Command	Description
cos	Classifies an IEEE 802.1p priority.
mac	Classifies a MAC address.
action match	Configures a rule action for classified packets.
rate-limit	Comfigures a rate-limit of classified packets
priority	Configures a rule priority of specified policy.

Tab. 3.7 Main Command of *Rule Configuration* Mode

3.1.9 RMON Configuration Mode

In *RMON Configuration* mode, you can configure RMON alarm, RMON event and RMON history. The LD3032 provides three different configuration modes to configure each type of RMON.

Command	Mode	Description
rmon-alarm <1-65535>	Global	Opens *RMON Configuration* mode. 1-65535: index number
rmon-event <1-65535>		
rmon-history <1-65535>		

Tab. 3.8 shows main commands of *RMON Configuration* mode.

Command	Description
active	Activates RMON.
owner	Shows the subject which configures each RMON and uses relevant information.

Tab. 3.8 Main Command of *RMON Configuration* Mode

3.1.10 Router Configuration Mode

In *Router Configuration* mode, you can configure IP routing protocols and VRRP. The LD3032 provides three IP routing protocols such as RIP v2, BGPv4 and OSPFv2.

To open *Rule Configuration* mode, enter the **router** command, then the system prompt will be changed from SWITCH(config)# to SWITCH(config-router)#.

Command	Mode	Description
router {*IP-PROTOCOL* | **vrrp**}	Global	Opens *Router Configuration* mode to configure IP routing protocols and VRRP.

Tab. 3.9 shows main commands of *Router Configuration* mode.

Command	Description
distance	Configures distance value to find better route.
neighbor	Configures neighbor router.
network	Configures network to operate each routing protocol.
redistribute	Registers transmitted routing information to another router’s table.
associate	Configures associated IP address same with virtual router.
authentication	Configures password of virtual router group.
preempt	Activates/deactivates preempt.
vr-priority	Assigns priority to virtual router.
vr-timers	Configures advertisement time, which means the interval that master router distributes its information to another virtual router.

Tab. 3.9 Main Command of *Router Configuration* Mode

3.1.11 Route-Map Configuration Mode

In *Route-map Configuration* mode, you can configure to transmit routing information with various options.

To open *Route-map Configuration* mode, enter the **route-map** command, then the system prompt will be changed from SWITCH(config)# to SWITCH(config-route-map)#.

Command	Mode	Description
route-map *NAME* {**permit** | **deny**} <0-65535>	Global	Opens *Route-map Configuration* mode.

Tab. 3.10 shows main commands of *Route-map Configuration* mode.

Command	Description
match	Classifies routing information to permit or deny.
set	Configures routing information options.

Tab. 3.10 Main Command of *Route-map Configuration* Mode

3.1.12 GPON Configuration Mode

There are two *GPON Configuration* mode; onu-profile, dba-profile. You can configure GPON-related functions. To open *PON Configuration* mode, enter the following command, then the system prompt will be changed from SWITCH(config)# to SWITCH(config-onu-profile[*profile-name*])# / SWITCH(config-dba-profile[*profile-name*])# .

Command	Mode	Description
onu-profile *NAME* **create**	Global	Opens *ONU-profile Configuration* mode.
dba-profile *NAME* **create**		Opens *DBA-profile Configuration* mode.

Tab. 3.11 shows main commands of *ONU profile Configuration* mode.

Command	Description
dba-profile	Applies the DBA profile to ONU profile.
dhcp-opt254-append	Adds DHCP option 254 fileld for ONU.
igmp-snooping	Configures an ONU’s Ethernet port-related function.

Tab. 3.11 Main Command of *ONU profile Configuration* Mode

Tab. 3.12 shows main commands of *DBA profile Configuration* mode.

Command	Description
link-sla	Configures SLA link state.
queue-sla	Configures SLA queue value.
sr-report-interval	Configures the interval for SR reporting.

Tab. 3.12 Main Command of *DBA profile Configuration* Mode

3.2 Useful Tips

This section describes useful tips for operating the LD3032 with a CLI.

- Listing Available Command
- Calling Command History
- Using Abbreviation
- Using Command of Privileged EXEC Enable Mode
- Exit Current Command Mode

3.2.1 Listing Available Command

To list available commands, input question mark <**?**> in the current mode. When you input the question mark <**?**>, you can see available commands used in this mode and variables following after the commands.

The following is the available commands on *Privileged EXEC Enable* mode of the LD3032.

```
SWITCH# ?
Exec commands:
  clear           Reset functions
  clock           Manually set the system clock
  configure       Enter configuration mode
  copy            Copy from one file to another
  debug           Debugging functions
  default-os      Select default OS
  disconnect      Disconnect user connection
  enable          Turn on privileged mode command
  erase           Erase saved configuration
  exit            End current mode and down to previous mode
  halt            Halt process
  help            Description of the interactive help system
  no              Negate a command or set its defaults
  ping            Send echo messages
  quote           Execute external command
  rcommand        Management stacking node
  release         Release the acquired address of the interface

(Omitted)

SWITCH#
```

i

Question mark <**?**> will not be shown in the screen and you do not need to press <**ENTER**> key to display the command list.

If you need to find out the list of available commands of the current mode in detail, use the following commands.

Command	Mode	Description
show list	All	Shows available commands of the current mode.
show cli		Shows available commands of the current mode with tree structure.

The following is an example of displaying the list of available commands of *Privileged EXEC Enable* mode.

```
SWITCH# show list
  clear arp
  clear arp IFNAME
  clear ip arp inspection log
  clear ip arp inspection statistics (vlan VLAN_NAME|)
  clear ip bgp *
  clear ip bgp * in
  clear ip bgp * in prefix-filter
  clear ip bgp * ipv4 (unicast|multicast) in
  clear ip bgp * ipv4 (unicast|multicast) in prefix-filter
  clear ip bgp * ipv4 (unicast|multicast) out
  clear ip bgp * ipv4 (unicast|multicast) soft
  clear ip bgp * ipv4 (unicast|multicast) soft in
  clear ip bgp * ipv4 (unicast|multicast) soft out
  clear ip bgp * out
  clear ip bgp * soft
  clear ip bgp * soft in
  clear ip bgp * soft out
  clear ip bgp * vpnv4 unicast in
  clear ip bgp * vpnv4 unicast out
  clear ip bgp * vpnv4 unicast soft
  clear ip bgp * vpnv4 unicast soft in
  clear ip bgp * vpnv4 unicast soft out
  clear ip bgp <1-65535>
  clear ip bgp <1-65535> in
  clear ip bgp <1-65535> in prefix-filter
-- more --
```

Press the <**ENTER**> key to skip to the next list.

In case that the LD3032 installed command shell, you can find out commands starting with a specific alphabet. Input the first letter and question mark without space. The following is an example of finding out the commands starting “**s**” in *Privileged EXEC Enable* mode of the LD3032.

```
SWITCH# s?
show          Show running system information
ssh           Configure secure shell

SWITCH# s
```

In addition, it is possible to view variables you should input following commands. After inputting the command you need, make one space and input a question mark. The following is an example of viewing variables after the **write** command. Please note that you must input one space between the command and question mark.

```
SWITCH# write ?
memory        Write to NV memory
terminal      Write to terminal

SWITCH# write
```

The LD3032 also provides the simple instruction of calling the help string with the **help** command. You can see the instruction using the command regardless of the configuration mode.

To display the instruction of calling the help string for using CLI, use the following command.

Command	Mode	Description
help	All	Shows the instruction of calling the help string for using CLI.

The following is the actual output of the **help** command.

```
SWITCH# help
Furukawa Electric LatamCLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

SWITCH#
```

3.2.2 Calling Command History

In case of installed command shell, you do not have to enter the command you entered before. When you need to reuse the commands you did, use this arrow key <↑>. When you press the arrow key, the commands will be displayed in the latest order.

The following is an example of calling command history after using several commands. After using these commands in order: **show clock** → **configure terminal** → **interface** *1* → **exit**, press the arrow key <↑> and then you will see the commands from latest one: **exit** → **interface** *1* → **configure terminal** → **show clock**.

```
SWITCH(config)# exit
SWITCH# show clock
Mon, 5 Jan 1970 23:50:12 +0000
SWITCH# configure terminal
SWITCH(config)# interface 1
SWITCH(config-if)# exit
SWITCH(config)# exit
SWITCH# (press the arrow key ↑)
SWITCH# exit (press the arrow key ↑)
SWITCH# interface 1 (press the arrow key ↑)
SWITCH# configure terminal (press the arrow key ↑)
SWITCH# show clock (press the arrow key ↑)
```

To save the command history in non-volatile memory, use the following command.

Command	Mode	Description
history non-volatile [<10-2000>]	Global	Saves a command history. 10-2000: history recording max. count (default:2000)
history non-volatile sdcard {**cli** | **snmp**}		Enables the system to store CLI/SNMP log history in a local SD card.

To delete the non-volatile command history, use the following command.

Command	Mode	Description
no history non-volatile	Global	Deletes the command history.
no history non-volatile sdcard {**cli** | **snmp**}		Disables the system to store CLI/SNMP log history in a local SD card.
remove history user *NAME*		Deletes the command history of specified user. NAME: user name
clear history non-volatile sdcard {**cli** | **snmp**}	Enable Global	Clears all CLI/SNMP log history stored in a local SD card.

To display the command history, use the following command.

Command	Mode	Description
show history	Enable	Shows a command history.
show cli history list		Shows a command hisroty list.
show history non-volatile [<1-2000>]	Enable Global	Shows a command history. non-volatile: reserves the command history. 1-2000: line number to be displayed
show history non-volatile user *NAME* [<1-2000>]		Shows the command history of specified user. NAME: user name 1-2000: line number to be displayed
show history non-volatile sdcard {**cli** | **snmp**}		Shows the recent CLI/SNMP log files stored in a local SD card.
show history non-volatile sdcard {**cli** | **snmp**} {*FILENAME* | **file-list** }		Shows the specified CLI/SNMP log files stored in a local SD card.

To enable/disable the command history logging, use the following command.

Command	Mode	Description
command-history-log enable [**default**]	Enable Global	Enables the command history logging.
command-history-log disable [**default**]		Disables the command history logging.

To display the configured status of command history logging, use the following command.

Command	Mode	Description
show command-history-log status	Enable Global	Shows the command history logging status.

3.2.3 Using Abbreviation

Several commands can be used in the abbreviated form. The following table shows some examples of abbreviated commands.

Command	Abbreviation
clock	cl
exit	ex
show	sh
configure terminal	con te

Tab. 3.13 Command Abbreviation

3.2.4 Using Command of Privileged EXEC Enable Mode

You can execute the commands of *Privileged EXEC Enable* mode as **show**, **ping**, **telnet**, **traceroute**, and so on regardless of which mode you are located on.

To execute the commands of *Privileged EXEC Enable* mode on different mode, use the following command.

Command	Mode	Description
do *COMMAND*	All	Executes the commands of *Privileged EXEC Enable* mode.

3.2.5 Exit Current Command Mode

To exit to the previous command mode, use the following command.

Command	Mode	Description
exit	All	Exits to the previous command mode.
end		Exits to *Privileged EXEC Enable* mode.

If you use the **exit** command in *Privileged EXEC Enable* mode or *Privileged EXEC View* mode, you will be logged out!

4 System Basic Configuration and Operation

4.1 Basic Configuration

After installing the system, the LD3032 is supposed to examine that each port is correctly connected to network and management PC. You can connect to the system to configure and manage the LD3032. This section provides instructions how to change password for system connection and how to connect to the system through telnet.

4.1.1 Connecting to the Console Port

To begin setup, you must connect the Console to the RJ45 Console port. To connect the cable, perform the following steps:

Step 1 Attach the RJ45 connector on the cable to the RJ45 connector on the console port of the LD3032.

Step2 Connect the other end of the cable to one of the serial ports on your workstation.

Step3 Open your terminal emulation software and configure the COM port settings to which you have connected the cable. The settings should be set to match the default settings for the switch, which are:

- 9600 bps
- 8 data bits
- 1 stop bit
- No parity
- No flow control

4.1.2 System Login

After installing the LD3032, finally make sure that each port is correctly connected to PC for network and management. Then, turn on the power and boot the system as follows.

Step 1 When you turn on the switch, booting will be automatically started and login prompt will be displayed.

```
SWITCH login:
```

Step 2 When you enter a login ID at the login prompt, the password prompt will be displayed, and then enter the proper password to log in the system. By default setting, the login ID is configured as *admin* with no password.

```
SWITCH login: admin
Password:
SWITCH>
```

Step 3 In *Privileged EXEC View* mode, you can check only the configuration for the switch. To configure and manage the switch, you should begin *Privileged EXEC Enable* mode. The following is an example of beginning *Privileged EXEC Enable* mode.

```
SWITCH> enable
SWITCH#
```

4.1.3 Configuring System Login Information

4.1.3.1 Password for Privileged EXEC Enable Mode

You can configure a password to enhance the security for *Privileged EXEC Enable* mode. To configure a password for *Privileged EXEC Enable* mode, use the following command.

Command	Mode	Description
passwd enable *PASSWORD*	Global	Configures a password to begin *Privileged EXEC Enable* mode.
passwd enable 8 *PASSWORD*		Configures an encrypted password.

password enable does not support encryption at default value. Therefore it shows the string (or password) as it is when you use the **show running-config** command. In this case, the user's password is shown to everyone and has unsecured environment.

To encrypt the password which will be shown at running-config, you should use the **service password-encryption** command. And to represent the string (password) is encrypted, input **8** before the encrypted string.

When you use the **password enable** command with **8** and "the string", you will make into *Privileged EXEC Enable* mode with the encrypted string. Therefore, to log in the system, you should do it with the encrypted string as password that you configured after **8**. In short, according to using the **8** option or not, the next string is encrypted or not.

The following is an example of configuring the password in *Privileged EXEC Enable* mode as *testpassword*.

```
SWITCH# configure terminal
SWITCH(config)# passwd enable testpassword
SWITCH(config)#
```

The following is an example of accessing after configuring a password.

```
SWITCH login: admin
Password:
SWITCH> enable
Password:
SWITCH#
```

To delete the configured password, use the following command.

Command	Mode	Description
no passwd enable	Global	Deletes the password.

The created password can be displayed with the **show running-config** command. To encrypt the password not to be displayed, use the following command.

Command	Mode	Description
service password-encryption	Global	Encrypts the system password.

To disable password encryption, use the following command.

Command	Mode	Description
no service password-encryption	Global	Disables password encryption.

4.1.3.2 Changing Login Password

To configure a password for created account, use the following command.

Command	Mode	Description
passwd	Global	Configures a password.
passwd *USER*		Configures a password for created account. USER: user's name to change a password

The following is an example of changing the current password.

```
SWITCH(config)# passwd
Changing password for admin
Enter the new password (maximum of 32 characters)
Please use a combination of upper and lower case letters and numbers.
Enter new password:junior95
Re-enter new password:junior95
Password changed.
SWITCH(config)#
```

⚠ The password you are entering will not be shown in the screen, so please be careful not to make a mistake.

4.1.3.3 Login Password Recovery Process

To recovery login password to default, perform the following step-by-step instruction:

Step 1
After the LD3032 is manually restarted, the booting messages are shown up. Keep on pressing [**Space Bar**] key right after "[Loading OS1 image ...]" is shown up on the screen.

Step 2
Enter "**password**" and press [**Enter**] key when displaying a blinking cursor after "[Image OK OS1]"

Step 3
Verify the "`password restore to default...`" messages.

```
***********************************************************
*                                                         *
*              Boot Loader Version 01.48.0002             *
*                   FURUKAWA ELECTRIC LATAM               *
*                                                         *
***********************************************************
Press 's' key to go to Boot Mode:  0
[Loading OS1 image . . .]
            ____________________ Step 1 (Space Bar)
[Image OK  :  os1]
                 password ------ Step 2

INIT: version 2.85 booting
Extracting configuration
password restore to default... --Step 3

Thu, 28 Jan 2016 16:01:51 +0900
INIT: Entering runlevel: 3
INIT: Start UP

SWITCH login: admin
Password:
SWITCH>
```

The password of “admin” is restored to the factory default password (no password) if the operator has not created any user accounts.

The screen image above may differ from the actual. (default: OS1 image)

4.1.3.4 Creating System Account

For the LD3032, the administrator can create a system account. In addition, it is possible to set the security level from 0 to 15 to enhance the system security.

To create a system account, use the following command.

Command	Mode	Description
user add *NAME DESCRIPTION*	Global	Creates a system account. NAME: user name up to 32 characters
user add *NAME* **level** <0-15> *DESCRIPTION*		Creates a system account with a security level.

The account of level 0 to level 14 without any configuring authority only can use **exit** and **help** in *Privileged EXEC View* mode and cannot access to *Privileged EXEC Enable* mode. The account with the highest level 15 has a read-write authority.

To change the name of the created account, user the following command.

Command	Mode	Description
user rename *NAME_FROM NAME_TO* **[***DESC***]**	Global	Changes a created account NAME_FROM: user name to change (from) NAME_TO: user name to be changed (to) DESC: user description

To delete the created account, use the following command.

Command	Mode	Description
user del *NAME*	Global	Delete the created account.

To display a created account, use the following command.

Command	Mode	Description
show user	Enable Global	Shows a created account.

4.1.3.5 Login Banner

It is possible to set system login and log-out banner. Administrator can leave a message to other users with this banner.

To set system login and log-out banner, use the following command.

Command	Mode	Description
banner	Global	Sets a banner before login the system.
banner login		Sets a banner when successfully log in the system.
banner login-fail		Sets a banner when failing to login the system.

To restore a default banner, use the following command.

Command	Mode	Description
no banner	Global	Restores a default banner.
no banner login		
no banner login-fail		

To display a current login banner, use the following command.

Command	Mode	Description
show banner	Enable Global	Shows a current login banner.

4.1.3.6 Setting Auto Log-out Time

For security reasons of the LD3032, if no command is entered within the configured inactivity time, the user is automatically logged out of the system. Administrator can configure the inactivity timer. To enable auto log-out function, use the following command.

Command	Mode	Description
exec-timeout <1-35791> [<0-59>]	Global	Enables auto log-out function for its current session. 1-35791: time unit in minutes (by default 10 minutes) 0-59: time unit in seconds
exec-timeout 0		Disables auto log-out.

To display a configuration of auto-logout function, use the following command.

Command	Mode	Description
show exec-timeout	Enable Global	Shows a configuration of auto-logout function.

4.1.3.7 Security Level

For the LD3032, it is possible to configure the security level from 0 to 15 for a system account. The level 15, as the highest level, has a read-write authority. The administrator can configure from level 0 to level 14. The administrator decides which level user uses which commands in which level. As the basic right from level 0 to level 14, it is possible to use **exit** and **help** command in *Privileged EXEC View* mode and it is not possible to access to *Privileged EXEC Enable* mode.

To define the security level and its authority, use the following command.

Command	Mode	Description
privilege view level <0-15> {*COMMAND* | **all**}	Global	Uses the specific command of *Privileged EXEC View* mode in the level.
privilege enable level <0-15> {*COMMAND* | **all**}		Uses the specific command of *Privileged EXEC Enable* mode in the level.
privilege configure level <0-15> {*COMMAND* | **all**}		Uses the specific command of *Global Configuration* mode in the level.
privilege interface level <0-15> {*COMMAND* | **all**}		Uses the specific command of *Interface Configuration* mode in the level.
privilege vrrp level <0-15> {*COMMAND* | **all**}		Uses the specific command of *VRRP Configuration* mode in the level.
privilege rip level <0-15> {*COMMAND* | **all**}		Uses the specific command of *RIP Configuration* mode in the level.
privilege bgp level <0-15> {*COMMAND* | **all**}		Uses the specific command of *BGP Configuration* mode in the level.
privilege ospf level <0-15> {*COMMAND* | **all**}		Uses the specific command of *OSPF Configuration* mode in the level.
privilege flow level <0-15> {*COMMAND* | **all**}		Uses the specific command of *Flow Configuration* mode in the level.

privilege policer level <0-15> {*COMMAND* | **all**}		Uses the specific command of *Policer Configuration* mode in the level.
privilege policy level <0-15> {*COMMAND* | **all**}		Uses the specific command of *Policy Configuration* mode in the level.
privilege {**rmon-alarm level**| **rmon-event**| **rmon-history**} <0-15> {*COMMAND* | **all**}		Uses the specific command of *RMON Configuration* mode in the level.
privilege dhcp-pool level <0-15> {*COMMAND* | **all**}		Uses the specific command of *DHCP Pool Configuration* mode in the level.
privilege dhcp-pool-class level <0-15> {*COMMAND* | **all**}		Uses the specific command of *DHCP Pool Class Configuration* mode in the level.
privilege dhcp-option82 level <0-15> {*COMMAND* | **all**}		Uses the specific command of *DHCP Option 82 Configuration* mode in the level.
privilege dhcp-class level <0-15> {*COMMAND* | **all**}		Uses the specific command of *DHCP Class Configuration* mode in the level.
privilege route-map level <0-15> {*COMMAND* | **all**}		Uses the specific command of *Route-map Configuration* mode in the level.

The commands that are used in low level can be also used in the higher level. For example, the command in level 0 can be used in from level 0 to level 14.

The commands should be input same as the displayed commands by **show list**. Therefore, it is not possible to input the commands in the bracket separately.

```
SWITCH# show list
  clear arp
  clear arp IFNAME
  clear ip arp inspection statistics (vlan VLAN_NAME|)
  clear ip bgp * in
  clear ip bgp * in prefix-filter
  clear ip bgp * ipv4 (unicast|multicast) in
  clear ip bgp * ipv4 (unicast|multicast) in prefix-filter
  clear ip bgp * ipv4 (unicast|multicast) out
  clear ip bgp * ipv4 (unicast|multicast) soft
  clear ip bgp * ipv4 (unicast|multicast) soft in
  clear ip bgp * ipv4 (unicast|multicast) soft out
  clear ip bgp * out
  clear ip bgp * soft
  clear ip bgp * soft in
(Omitted)
```

It is not possible to input **clear ip bgp * ipv4 unicast in**. You should input like **clear ip bgp * ipv4** {**unicast | multicast**} **in**. The commands starting with the same character are applied by inputting only the starting commands. For example, if you input **show**, all the commands starting with **show** are applied.

To delete a configured security level, use the following command.

Command	Mode	Description
no privilege	Global	Deletes all configured security levels.
no privilege view level <0-15> {*COMMAND* | **all**}		Delete a configured security level on each mode.
no privilege enable level <0-15> {*COMMAND* | **all**}		
no privilege configure level <0-15> {*COMMAND* | **all**}		
no privilege interface level <0-15> {*COMMAND* | **all**}		
no privilege flow level <0-15> {*COMMAND* | **all**}		
no privilege vrrp level <0-15> {*COMMAND* | **all**}		
no privilege policer level <0-15> {*COMMAND* | **all**}		
no privilege policy level <0-15> {*COMMAND* | **all**}		
no privilege rip level <0-15> {*COMMAND* | **all**}		
no privilege bgp level <0-15> {*COMMAND* | **all**}		
no privilege ospf level <0-15> {*COMMAND* | **all**}		
no privilege rmon-alarm level <0-15> {*COMMAND* | **all**}		
no privilege rmon-event level <0-15> {*COMMAND* | **all**}		
no privilege rmon-history level <0-15> {*COMMAND* | **all**}		
no privilege dhcp-pool level <0-15> {*COMMAND* | **all**}		
no privilege dhcp-pool-class level <0-15> {*COMMAND* | **all**}		
no privilege dhcp-option82 level <0-15> {*COMMAND* | **all**}		
no privilege dhcp-class level <0-15> {*COMMAND* | **all**}		
no privilege route-map level <0-15> {*COMMAND* | **all**}		

To display a configured security level, use the following command.

Command	Mode	Description
show privilege	Enable Global	Shows a configured security level.
show privilege now		Shows a security level of current mode.

The following is an example of creating the system account *test0* having a security level 10 and *test1* having a security level 1 with no password.

```
SWITCH(config)# user add test0 level 0 level0user
Changing password for test0
Enter the new password (maximum of 32 characters)
Please use a combination of upper and lower case letters and numbers.
Enter new password:(Enter)
Bad password: too short.

Warning: weak password (continuing).
Re-enter new password: (Enter)
Password changed.
SWITCH(config)# user add test1 level 1 level1user
Changing password for test1
```

```
Enter the new password (maximum of 32 characters)
Please use a combination of upper and lower case letters and numbers.
Enter new password: (Enter)
Bad password: too short.

Warning: weak password (continuing).
Re-enter new password: (Enter)
Password changed.
SWITCH(config)# show user
====================================================
 User name            Description       Level
====================================================
test0                level0user          0
test1                level1user          1
SWITCH(config)#
```

The following is an example of configuring an authority of the security level 0 and 1.

```
SWITCH(config)# privilege view level 0 enable
SWITCH(config)# privilege enable level 0 show
SWITCH(config)# privilege enable level 1 configure terminal
SWITCH(config)# show privilege

 Command Privilege Level Configuration
 -----------------------------------------------

 Node         All   Level   Command
 EXEC(ENABLE)         1     configure terminal
 EXEC(VIEW)           0     enable
 EXEC(ENABLE)         0     show

 3 entry(s) found.

SWITCH(config)#
```

In the above configuration, as level 0, it is possible to use only show command in *Privileged EXEC Enable* mode; however as level 1, it is possible to use not only the commands in level 1 but also time configuration commands in *Privileged EXEC Enable* mode and accessing commands to *Global Configuration* mode.

4.1.3.8 Limiting Number of Users

For the LD3032, you can limit the number of users accessing the switch through telnet. In case of using the system authentication with RADIUS or TACACS+, a configured number includes the number of users accessing the switch via the authentication server. To set the number of users accessing the switch, use the following command.

Command	Mode	Description
login connect <1-8>	Global	Sets the number of users accessing the switch. 1-8: the number of user (default: 8)
no login connect		Deletes a configured value.

4.1.4 System Rebooting

4.1.4.1 Manual System Rebooting

When installing or maintaining the system, some tasks require rebooting the system by various reasons. Then you can reboot the system with a selected system OS.

To restart the system manually, use the following command.

Command	Mode	Description
reload [**os1** | **os2**]	Enable	Restarts the system.
reload mate [**os1** | **os2**]		Restarts the system OS of the standby SFU if the switch is running in redundant mode.

i The **reload mate** command can be used to upgrade the system OS; the downloaded OS can be performed on the standby SFU for system reliability test.

The following is an example of restarting the system with the **reload** command.

```
SWITCH# reload
Do you want to save the system configuration? [y/n]
Do you want to reload the system? [y/n]
```

If you reboot the system without saving new configuration, new configuration will be deleted. So, you have to save the configuration before rebooting. Not to make that mistake, the LD3032 is supported to print the following message to ask if user really wants to reboot and save configuration.

Please, press <**y**> key when you would like to save the configurations. Then, press <**y**> key, if you want to continue to reboot the system, press <**y**> key.

4.1.5 Configuring Host Name and Time

4.1.5.1 Host Name

Host name displayed on prompt is necessary to distinguish each device connected to network. To set a new host name, use the following command.

Command	Mode	Description
hostname *NAME*	Global	Creates a host name of the switch, enter the name.
no hostname [*NAME*]		Deletes a configured host name, enter the name.

The following is an example of changing host name to *TEST*.

```
SWITCH(config)# hostname TEST
TEST(config)#
```

4.1.5.2 Time and Date

To set system time and date, use the following command.

Command	Mode	Description
clock *DATETIME*	Enable	Sets system time and date.
show clock	Enable Global	Shows system time and date.

The LD3032 can be configured to observe the daylight saving time in specified area. It means that whenever the system time is updated using a time server located in a different time area, it will be automatically corrected with the local daylight saving time offset.

To set daylight saving time, use the following command.

Command	Mode	Description
clock summer-time *TIMEZONE* **date** [*DATE MONTH YEAR HH:MM DATE MONTH YEAR HH:MM* <1-1440>]	Global	Adjusts the system time to daylight saving time during the specified time. 1-1440: daylight saving time offset (unit: minutes, default: Mar 10 2:00-Nov 10 2:00, offset : 60 minutes)
clock summer-time *TIMEZONE* **recurring** [*WEEK DAY MONTH YEAR HH:MM WEEK DAY MONTH YEAR HH:MM* <1-1440>]		Configures daylight saving time during the period date for every year. 1-1440: daylight saving time offset (unit: minutes, default: Mar 10 2:00-Nov 10 2:00, offset : 60 minutes)
no clock summer-time		Deletes the configured daylight saving time.

To display the configured daylight saving time, use the following command.

Command	Mode	Description
show clock summer-time	Enable Global	Shows the configured summer time.

The following example sets system time from 12:00, August 18, 2011 to 12:00, August 20, 2011.

```
SWITCH(config)# time-zone GMT+9
SWITCH(config)# clock summer-time GMT+9 date 18 8 2011 12:00 20 8 2011 12:00
60
SWITCH(config)# show clock summer-time

=============================================
Summer time is set. But not running.
---------------------------------------------
Summer time type : this year only
---------------------------------------------
Start time : 2011 aug 18 12:00
Stop  time : 2011 aug 20 12:00
=============================================
SWITCH(config)#
```

4.1.5.3 Time Zone

The LD3032 provides three kinds of time zone, GMT, UCT and UTC. The time zone of the switch is predefined as GMT (Greenwich Mean Time). You can also set the time zone where the network element belongs.

To set the time zone, use the following command.

Command	Mode	Description
time-zone *TIMEZONE*	Global	Sets the time zone (refer to the below table).
clear time-zone		Clears a configured time zone.

To display the world time zone, use the following command.

Command	Mode	Description
show time-zone	Enable Global	Shows the world time zone map.

The following table shows the world time zone.

Time Zone	Country/City	Time Zone	Country/City
GMT-12	International Date Line West	**GMT+12**	Wellington, Fiji
GMT-11	Midway Island, Samoa, Pago Pago	**GMT+11**	Magadan, New Caledonia
GMT-10	Hawaii, Honolulu	**GMT+10**	Sydney, Brisbane, Hobart
GMT-9:30	Taiohae	**GMT+9:30**	Darwin
GMT-9	Anchorage, Gambier Islands	**GMT+9**	Seoul, Tokyo, Osaka
GMT-8	LA, Seattle, Vancouver	**GMT+8**	Beijing, Hong Kong, Singapore
GMT-7	Edmonton, Phoenix, Denver	**GMT+7**	Bangkok, Hanoi, Jakarta
GMT-6	Guatemala, Mexico City, New Orleans, Chicago, Houston	**GMT+6:30**	Yangon
		GMT+6	Almaty, Dhaka
GMT-5	New York, Miami, Boston, Ottawa, Havana, Toronto, Washington DC	**GMT+5:45**	Kathmandu
		GMT+5:30	Mumbai, New Delhi, Kolkata
GMT-4:30	Caracas	**GMT+5**	Karachi, Tashkent, Lahore
GMT-4	Santo Domingo, La Paz, San Juan	**GMT+4:30**	Kabul
GMT-3:30	St.John’s	**GMT+4**	Dubai
GMT-3	Atlantic Time(DST), Brasillia	**GMT+3:30**	Tehran
GMT-2	Mid-Atlantic, Rio de Janeriro	**GMT+3**	Baghdad, Moscow, Riyadh
GMT-1	Azores, Praia	**GMT+2**	Cairo, Athens, Minsk, Helsinki
GMT / GMT0	London, Lisbon, Dublin, Casablanca	**GMT+1**	Berlin, Rome, Paris, Stockholm
UTC/ UCT/ Universal / Zulu /Greenwich		London, Lisbon, Dublin, Casablanca	

Tab. 4.1 World Time Zone

⚠ To see a configured time zone, use the **show clock** command.

4.1.5.4 Network Time Protocol (NTP)

The network time protocol (NTP) provides a mechanism to synchronize time on computers across an internet. The specification for NTP is defined in RFC 1119.

To enable/disable the NTP function, use the following command.

Command	Mode	Description
ntp server *SERVER1* [*SERVER2*] [*SERVER3*]	Global	Enables NTP function with a specified NTP server. SERVER: server IP address (maximum 3 servers)
no ntp server *SERVER1* [*SERVER2*] [*SERVER3*]		Deletes a specified NTP server. SERVER: server IP address
no ntp		Disables the NTP function.

To display a configured NTP, use the following command.

Command	Mode	Description
show ntp	Enable Global	Shows a configured NTP function.

To synchronize the system clock, the system periodically sends the NTP message to the NTP server. You can configure the system to bind the IP address to the message which allows the NTP server to recognize your system.

To bind the IP address to the NTP message, use the following command.

Command	Mode	Description
ntp bind-address *A.B.C.D*	Global	Specifies the IP address to be bound to the NTP message.
no ntp bind-address		Deletes a specified IP address.

To specify the polling interval for the time synchronization with the NTP server, use the following command.

Command	Mode	Description
ntp poll-interval <6-17>	Global	Sets the NTP polling interval. (default: 16 (2^16=65535, 18Hour))
no ntp poll-interval		Deletes the configured NTP polling interval.

4.1.5.5 Simple Network Time Protocol (SNTP)

NTP (Network Time Protocol) and SNTP (Simple Network Time Protocol) are the same TCP/IP protocol in that they use the same UDP time packet from the Ethernet Time Server message to compute accurate time. The basic difference in the two protocols is the algorithms being used by the client in the client/server relationship.

The NTP algorithm is much more complicated than the SNTP algorithm. NTP normally uses multiple time servers to verify the time and then controls the rate of adjustment or slew rate of the PC which provides a very high degree of accuracy. The algorithm determines if the values are accurate by identifying time server that doesn’t agree with other time servers. It then speeds up or slows down the PC's drift rate so that the PC's time is always correct and there won't be any subsequent time jumps after the initial correction. Unlike NTP, SNTP usually uses just one Ethernet Time Server to calculate the time and then it "jumps" the system time to the calculated time. However, it can have back-up Ethernet Time Servers in case one is not available.

To configure the switch in SNTP, use the following commands.

Command	Mode	Description
sntp *SERVER1* [*SERVER2*] [*SERVER3*]	Global	Enables SNTP function with a specified SNTP server. SERVER: server IP address (maximum 3 servers)

no sntp *SERVER1* [*SERVER2*] [*SERVER3*]		Deletes a specified SNTP server.
no sntp		Disables SNTP function.

i

You can configure up to 3 servers so that you use second and third servers as backup use in case the first server is down.

To display SNTP configuration, use the following command.

Command	Mode	Description
show sntp	Enable Global	Show SNTP configuration.

4.1.6 DNS Server

To set a DNS server, use the following command.

Command	Mode	Description
dns server {*A.B.C.D* | *X:X::X:X*}	Global	Sets a DNS server. A.B.C.D: DNS server IPv4 address X:X::X:X: DNS server IPv6 address
no dns server {*A.B.C.D* | *X:X::X:X*}		Removes a DNS server.

To display a configured DNS server, use the following command.

Command	Mode	Description
show dns	Enable Global	Shows a configured DNS server.

If a specific domain name is registered instead of IP address, user can do telnet, FTP, TFTP and ping to the hosts on the domain with domain name.

To search domain name, use the following command.

Command	Mode	Description
dns search *DOMAIN*	Global	Searches a domain name.
no dns search *DOMAIN*		Removes a domain name.

It is possible to delete DNS server and domain name at the same time with the below command.

Command	Mode	Description
no dns	Global	Deletes DNS server and domain name.

4.1.7 FTP Server

The LD3032 provides the FTP server feature, which is enabled by default. For security reason, however, the FTP server may need to be disabled to block an illegal access.

To enable/disable the FTP server on the system, use the following command.

Command	Mode	Description
ftp server enable	Global	Enables/disables the FTP server on the system. (default: enable)
ftp server disable		

If the FTP server is disabled, the system software upgrade cannot be done via FTP server!

4.1.8 Auto Log-out

For security reasons of the LD3032, if no command is entered within the configured inactivity time, the user is automatically logged out of the system. Administrator can configure the inactive session timeout.

To enable auto log-out function, use the following command.

Command	Mode	Description
exec-timeout <1-35791> [<0-59>]	Global	Enables auto log-out. 1-35791: time unit in minutes (by default 10 minutes) 0-59: time unit in seconds
exec-timeout 0		Disables auto log-out.

To display a configuration of auto-logout function, use the following command.

Command	Mode	Description
show exec-timeout	Enable Global	Shows a configuration of auto-logout function.

The LD3032 uses the global auto log-out function to determine how long to manage state information for a session and to determine when to drop sessions that do not become fully established. These global auto log-out timeouts apply globally to all sessions.

To enable auto log-out function for all sessions, use the following command.

Command	Mode	Description
global-timeout <1-35791> [<0-59>]	Global	Enables auto log-out for all sessions. 1-35791: timeout value in minutes 0-59: timeout in seconds
global-timeout 0		Disables auto log-out for all sessions.

4.1.9 Telnet Access

To activate/deactivate the connection to a remote host via telnet, use the following command.

Command	Mode	Description
service telnet	Global	Activates the telnet service.
no service telnet		Deactivates the telnet service.
show service	Enable/Global	Shows the status of network connection services (telnet/ssh/ftp/tftp/snmp).

To connect to a remote host via telnet, use the following command.

Command	Mode	Description
telnet {*A.B.C.D* | **ipv6** *X:X::X:X*}	Enable	Connects to a remote host via telnet. A.B.C.D | X:X::X:X: IPv4/IPv6 address or host name of a remote system
telnet *A.B.C.D* [*TCP-PORT*]		Connects to a remote host via telnet. A.B.C.D | X:X::X:X: IPv4/IPv6 address or host name of a remote system TCP-PORT: TCP port number

⚠ In case of telnet connection, you need to wait for the **[OK]** message, when you save a system configuration. Otherwise, all changes will be lost when the telnet session is disconnected.

```
SWITCH# write memory
[OK]
SWITCH#
```

The system administrator can disconnect users connected from remote place. To disconnect a user connected through telnet, use the following command.

Command	Mode	Description
disconnect *TTY-NUMBER*	Enable	Disconnects a user connected through telnet.

The following is an example of disconnecting a user connected from a remote place.

```
SWITCH# where
admin at ttys0 from console for 4 days 22 hours 15 minutes 24.88 seconds
admin at ttyp0 from 10.0.1.4:1670 for 4 days 17 hours 53 minutes 28.76 seconds
admin at ttyp1 from 147.54.140.133:49538 for 6 minutes 34.12 seconds
SWITCH# disconnect ttyp0
SWITCH# where
admin at ttys0 from console for 4 days 22 hours 15 minutes 34.88 seconds
admin at ttyp1 from 147.54.140.133:49538 for 6 minutes 44.12 seconds
SWITCH#
```

4.2 System Configuration Management

4.2.1 Displaying System Configuration

To display the current running configuration of the system, use the following command.

Command	Mode	Description
show running-config	All	Shows a configuration of the system.
show running-config { **access-list** | **admin-flow** | **admin-policy** | **arp** | **as-path access-list** | **bgp** | **community-list** | **dhcp** | **dhcp6** | **dns** | **flow** [*NAME*] | **full** | **hostname** | **ip mroute** | **ip multicast** | **key chain** | **ip route** | **login** | **policer** | **policy** | **ip** | **ipv6** | **pppoe** | **router** | **rmon-alarm** | **rmon-event** | **rmon-history** | **route-map** | **router** {**bgp** | **rip** | **ospf** } | **router ipv6** {**ospf| rip**}| **router-id** | **snmp** | **syslog** | **time-zone**}		Shows a configuration of the system with the specific option.
show running-config interface {**management** | **vlan** *VLANS* | **loopback** | **gigabitethernet** *IFPORT* | **tengigabitethernet** *IFPORT* | **gpon** *IFPORT* | **channelgroup** *GROUP*}		
show running-config { gpon | dba-profile [*NAME*]**|** **onu-profile** [*NAME*] **| extended-vlan-tagging-operation** [*NAME*] **| tdm-pw-profile** [*NAME*] **| traffic-profile** [*NAME*]**| voip-profile** [*NAME*]**| pw-maintenance-profile**[*NAME*]**}**		Shows the configurations of the system with the GPON option.

4.2.2 Comparing Configuration Changes

To display the different configuration between startup-config and running-config, use the following command.

Command	Mode	Description
show compare-config	Enable	Shows configuration compared with startup-config and running-config.

4.2.3 Writing System Configuration

If you change the configuration of the system, you need to save the changes in the system flash memory. To write a current running configuration, use the following command.

Command	Mode	Description
write memory	All	Writes a current running configuration in the system flash memory.
write terminal	Enable	Shows a current running configuration on the terminal. (alias to the **show running-config** command)

When you use the **write memory** command, make sure there is no key input until **[OK]** message appears.

4.2.4 Auto-Saving

The LD3032 supports the auto-saving feature, allowing the system to save the system configuration automatically. This feature prevents the loss of unsaved system configuration by unexpected system failure. To allow the system to save the system configuration automatically, use the following command.

Command	Mode	Description
write interval <10-1440>	Global	Enables auto-saving with a given interval as a multiple of 10. 10-1440: time interval (unit: minute)
no write interval		Disables auto-saving.

4.2.5 System Configuration File

To copy a system configuration file, use the following command.

Command	Mode	Description
copy running-config {*FILENAME* | **startup-config**}	Enable	Copies a running configuration file. FILENAME: configuration file name startup-config: startup configuration file
copy startup-config *FILENAME*		Copies a startup configuration file to a specified file name.
copy *FILENAME* **startup-config**		Copies a specified configuration file to the startup configuration file.
copy *FILENAME1 FILENAME2*		Copies a specified configuration file to another configuration file.

To back up a system configuration file using FTP or TFTP, use the following command.

Command	Mode	Description
copy {**ftp** | **tftp**} **config upload** {*FILE-NAME* | **startup-config**}	Enable	Uploads a file to FTP or TFTP server with the name configured by user.
copy {**ftp** | **tftp**} **config download** {*FILE-NAME* | **startup-config**}		Downloads a config file from FTP or TFTP server with the name configured by user.
copy {**ftp** | **tftp**} **fpga download**		Downloads a FPGA image file from FTP or TFTP server.
copy {**ftp** | **tftp**} **history non-volatile sdcard** {**cli** |**snmp** } **upload** *FILE-NAME*		Uploads the command history of CLI/SNMP logs from SD card to FTP/TFTP server. FILE-NAME: all log file
copy {**ftp** | **tftp**} **history-log upload** *FILE-NAME*		Uploads a CLI history log file to FTP/ TFTP server FILE-NAME: CLI history log file name

i

To access FTP to back up the configuration or use the backup file, you should know FTP user ID and the password. To back up the configuration or use the file through FTP, you can recognize the file transmission because hash function is automatically turned on.

To delete a system configuration file, use the following command.

Command	Mode	Description
erase config *FILENAME*	Enable Global	Deletes a specified configuration file. FILENAME: configuration file name
erase startup-config	Enable	Deletes a startup configuration file.

To display a system configuration file, use the following command.

Command	Mode	Description
show startup-config	Enable Global	Shows a current startup configuration.
show config-list		Shows a list of configuration files.

4.2.6 Restoring Default Configuration

To restore a default configuration of the system, use the following command.

Command	Mode	Description
restore factory-defaults	Enable	Restores a factory default configuration.
restore layer2-defaults		Restores an L2 default configuration.

After restoring a default configuration, you need to restart the system to initiate.

4.2.7 Core Dump File

A core dump file contains the memory image of a particular process, or the memory images of parts of the address space of that process, along with other information such as the values of processor registers. The LD3032 can be configured to generate core dumps and save them in ramdisk for useful debugging aids in several situations such as accesses to non-existent memory, segmentation errors. To configure a core dump, use the following command.

Command	Mode	Description
generate coredump *PID*	Enable Global	Generates a core dump file and save it with a name. PID: process ID
clear coredump *PID*		Deletes the specific core dump file.

To back up a core dump file using FTP or TFTP, use the following command.

Command	Mode	Description
copy {**ftp** | **tftp**} **coredump upload**	Enable	Uploads a core dump file to FTP or TFTP server.

To display a core dump file, use the following command.

Command	Mode	Description
show coredump [*NAME*]	Enable Global	Shows a current status of core dump file NAME: process name

5 Equipment/Interface Management

5.1 Slot Assignment

The LD3032 is a shelf based modular multi-platform L3 switch. It features highly flexible hardware configurations with multiple GPON units with 10G Ethernet ports, so that user can fully customize it for PON OLT and fiber to the premises network can be achieved.

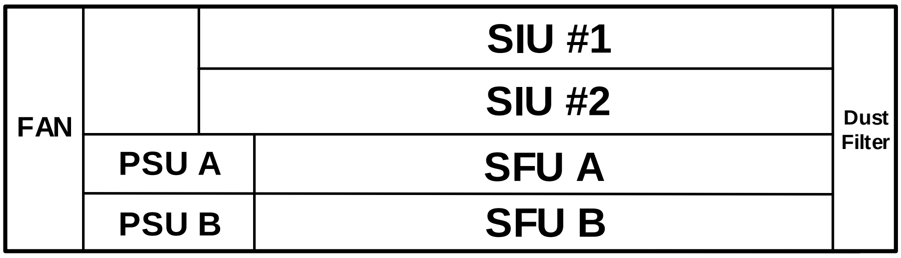


Fig. 5.1 Slot Assignment of LD3032

Tab. 5.1 shows the port indices and slot assignment.

System	Slot number	Module type	Interface type
LD3032 Shelf	1 to 2	SIU	SIU_GPON16

Tab. 5.1 Port Indices and Slot Assignment

The LD3032 has the reserved 2 slots for SIUs.

5.2 IUs Management

In LD3032 shelf, there are 2 slots for SIUs. By default, all of IU slots are in admin ‘locked’ state that IUs are unable to operate normally even though they are properly inserted into the shelf with power-up. To activate a specific IU, you have to change the admin state of a slot from ‘locked’ to ‘unlocked’ by the command. This means that a subscriber/network service card can only be active when its slot is configured with a planned IU type and changed to ‘unlock’ state by the command.

It is possible to configure the plug-in slots of the shelf with a specific IU type before module equipping. If the module will be equipped later, the system checks whether the module equipping is valid or not. If it is invalid, an IU can not be activated in the system.

5.2.1 Registering IUs

After installing in the LD3032 chassis, perform the following steps for each IU to be properly operated.

Step 1 Configure a slot for the specified IU type, use the following command.

Command	Mode	Description
slot planning iu *SLOT_NUMBER* {**siu-gpon16** | **sfu-10ge4**}	Global	Specifies an IU type in a slot. SLOT_NUMBER : the slot number of IU (e.g. X | X-Y)

⚠ If a slot was configured with a specified IU type, and the system has detected that a different type of IU is physically inserted in this slot, the equipped IU cannot be activated in the system.

Step 2 Change the admin state to ‘unlock’ for each slot to activate the equipped IU.

Command	Mode	Description
slot unlock iu *SLOT_NUMBER*	Global	Unlocks a particular slot. SLOT_NUMBER : the slot number of IU (e.g. X | X-Y)

To lock a particular slot for preventing the abnormal operation, use the following command.

Command	Mode	Description
slot lock iu *SLOT_NUMBER*	Global	Locks a particular slot. (default) SLOT_NUMBER : the slot number of IU (e.g. X | X-Y)

5.2.2 IUs Replacement

The procedures in this section replace IU to another one. The configuration of IU’s replacement is a five-step process:

Step 1 Lock the existing IU in a slot that you want to replace.

To lock a particular slot, use the following command.

Command	Mode	Description
slot lock iu *SLOT_NUMBER*	Global	Locks a particular slot. (default) SLOT_NUMBER : the number of IU slot (e.g. X | X-Y)

Step 2 Remove the existing IU from the slot, use the following command.

Command	Mode	Description
no slot planning iu *SLOT_NUMBER*	Global	Removes the registered IU from the slot.

Step 3 Register new IU in the slot.

Command	Mode	Description
slot planning iu *SLOT_NUMBER* {**siu-gpon16** | **sfu-10ge4**}	Global	Specifies an IU type in a slot.

Step 4 Replace the old IU with the new IU. Insert new IU into the intended slot.

Step 5 Change the admin state to ‘unlock’ for specified slot number with **slot unlock siu** command to make IU activating in the system

5.2.3 Rebooting IUs

To restart the specified IU, use the following command.

Command	Mode	Description
slot restart iu *SLOT_NUMBER*	Global	Restarts an interface module in the specified slot number.

To turn the power on/off of a specific IU, use the following command.

Command	Mode	Description
slot power iu *SLOT_NUMBER* {**on** |**off** }	Global	Powers on/off an interface module in the specified slot number.

5.2.4 Default OS of IUs

To set the default OS of the IU, use the following command.

Command	Mode	Description
slot default-os iu *SLOT_NUMBER* {**os1** | **os2**}	Global	Sets the default OS of the IU. (default: os1)

5.2.5 Displaying IUs Information

To display information of the specified slot, use the following command.

Command	Mode	Description
show slot cpuload iu {*SLOT_NUMBER* | **all**}	Enable Global	Shows the specified slot information.
show slot memory iu {*SLOT_NUMBER* | **all**}		
show slot nos iu {*SLOT_NUMBER* | **all**}		
show slot status iu {*SLOT_NUMBER* | **all**}		
show slot system all		
show slot system iu {*SLOT_NUMBER* | **all**}		
show slot system sfu [mate]		

5.3 Interface Basic

In this chapter, you can find the instructions for the basic interface type and port numbering scheme. Please read the following instructions carefully before you configure an interface in the LD3032.

5.3.1 IU Interface Port Numbering Scheme

The LD3032 provides 2 service slots for GPON interface unit (SIU_GPON16). Each type of interface unit contains 16 ports, which means the LD3032 provides maximum 32 physical ports.

When specifying the port number for the OLT ID for SIU_GPON16 in the CLI, you can simply put the number in the form of *SLOT*/*PORT* such as **1/1**, **1/2**, **1/3**, …, **2/16**. Multiple input is also possible, e.g. **1/1-1/8**.

The following table shows the interface numbering scheme according to its IU types.

System	Slot #	IU Type	Interface Port Number (Slot# / Port#)
LD3032 Shelf	1	SIU_GPON16 (siu-gpon16)	1/1, 1/2, 1/3, 1/4, 1/5, …1/14, 1/15, 1/16
	2		2/1, 2/2, 2/3, 2/4, 2/5,… 2/14, 2/15, 2/16
	0	SFU (sfu-10ge4) 4 x 10G ports	0/1, 0/2, 0/3, 0/4

Tab. 5.2 Interface Numbering Scheme according to SIU types

Regarding to the type of the interface, the port number is specified in the same form.

5.4 Configuring Interface

5.4.1 Opening Interface Configuration Mode

You can configure parameters for a specific interface/port by entering interface configuration mode. After you configure an interface, configuration changes applied to the port-based interface apply to all the physical interfaces assigned to the port interface. Configuration changes applied to the physical interface affect only the interface where you apply the configuration. To change the parameters of all ports in a specific IU, open *Interface Configuration* mode using **interface range** command.

To display a status of slot information, use the following command.

Command	Mode	Description
show slot status iu {*SLOT_NUMBER* | **all**}	Enable Global	Shows the slot information.

To configure an interface, you need to open *Interface Configuration* mode first. To enter *Interface Configuration* mode per Interface Unit (IU), use the following command.

Command	Mode	Description
interface {**gigabitethernet** | **tengigabitethernet** | **gpon** } *IFPORT*	Global	Opens *Ethernet/GPON Interface Configuration* mode to configure a specified interface. IFPORT: SLOT/PORT
interface channelgroup *GROUP-ID*		Opens *Channel Group Interface Configuration* mode.
interface range {**gigabitethernet** | **tengigabitethernet** | **gpon** } *IFPORT-RANGE*		Opens *Ethernet/GPON Interface Configuration* mode to configure multiple interface ports per Interface Unit (IU). IFPORT-RANGE: multiple interface port number (e.g. 1/1-8 or 1/1-1/8)

i

To display if an interface is enabled, use the **show running-config** command.

To open *Interface Configuration* mode per MGMT port/VLAN/Loopback interface, use the following command.

Command	Mode	Description
interface {**management** | **loop-back** | **vlan** *VLANS*}	Global	Opens *Interface Configuration* mode to configure a specified interface.

5.4.2 Enabling an Interface

To enable/disable an interface, use the following command.

Command	Mode	Description
no shutdown	Interface	Enables an interface.
shutdown		Disables an interface.

The following is an example of enabling the tengigabitethernet interface 8/1.

```
SWITCH# configure terminal
SWITCH(config)# interface tengigabitethernet 8/1
SWITCH(config-if[XE8/1])# no shutdown
SWITCH(config-if[XE8/1])#
```

i

To display if an interface is enabled, use the **show running-config** command.

5.4.3 Interface Description

To specify a description on an interface, use the following command.

Command	Mode	Description
description *LINE*	Interface	Specifies a description on an interface.
no description		Deletes a specified description.

5.4.4 Interface Traffic Statistics

5.4.4.1 Packet Statistics

To display the traffic statistics of an Ethernet port, use the following command.

Command	Mode	Description
show interface statistics {**avg** | **interface** | **rmon** | **5min**} **all**	Enable Global	Shows the traffic statistics of the average packet for a specified Ethernet port. IFPORTS: interface port number (1/1, 1/2, 1/3, …) Interface: interface MIB counters rmon: RMON MIB counters
show interface statistics {**avg** | **interface** | **rmon** | **5min**} {**gigabitethernet** | **tengigabitethernet** | **gpon** } *IFPORTS*		
show interface statistics avg-type {**gigabitethernet** | **tengigabitethernet** | **gpon** } *IFPORTS*		Shows the pps statistics per packet type for a specified interface.

To delete all collected statistics for an Ethernet/GPON port, use the following command.

Command	Mode	Description
clear interface statistics all	Enable Global	Deletes all collected statistics. IFPORTS: port number (1/1, 1/2, 2/1, …)
clear interface statistics {**gigabitethernet** | **tengigabitethernet** | **gpon** } *IFPORTS*		
clear interface statistics cpu		Clears all collected interface statistics from CPU.

5.4.5 Displaying Interface

To display an interface status and configuration, use the following command.

Command	Mode	Description
show interface	Enable Global	Shows an interface status and configuration. INTERFACE: interface name
show interface {**management** | **loopback** | **vlan** *VLANS*}		
show interface {**gigabitethernet** | **tengigabitethernet** | **gpon** | **channelgroup**} *IFPORTS*		

To display the interface status and information, use the following command.

Command	Mode	Description
show interface-status [{**gigabitethernet** | **tengigabitethernet** | **gpon** | **channelgroup**} *IFPORTS*]	Enable Global	Shows a current port status, enter a port number. PORTS: port number (1/1, 1/2, 2/1, …)

Command	Mode	Description
show interface status [{**gigabitethernet** | **tengigabitethernet** | **gpon** | **channelgroup**} *IFPORTS*]		
show interface description		Shows the description of an interface.
show interface module-info [{**gigabitethernet** | **tengigabitethernet** | **gpon** | **channelgroup**} *IFPORTS*]		Shows optical module (SFP) information.

5.4.6 Interface Identifier

To specify a identifier on an interface, use the following command.

Command	Mode	Description
identifier hex *LINE*	Interface [XE/GE/CG/br/GPON	Sets interface identifier. LINE: Interface identifier of max 8byte value (e.g. ffeac3c434f20a00)

5.4.7 Interface Alias Name

To set alias name for interface, use the following command.

Command	Mode	Description
alias *WORD*	Interface [XE/GE/CG/br/GPON	Sets alias name of the interface. WORD: name

5.5 Assigning an IP Address

The Layer 2 switches only see the MAC address in an incoming packet to determine where the packet needs to come from/to and which ports should receive the packet. The Layer 2 switches do not need IP addresses to transmit packets. However, if you want to access to the LD3032 from a remote place with TCP/IP through SNMP or telnet, it requires an IP address.

You can enable the interface to communicate with another network device on the network by assigning an IP address.

5.5.1 Enabling MGMT/VLAN Interface

To assign an IP address to an interface, you need to enable the interface first. If the interface is not enabled, you cannot access it from a remote place, even though an IP address has been assigned.

To configure an interface, you need to open *Interface Configuration* mode first. To open *Interface Configuration* mode, use the following command.

Command	Mode	Description
interface { **management** | **vlan** *VLAN* | **loopback**}	Global	Opens *Interface Configuration* mode to specify an IP address.

To enable/disable an interface, use the following command.

Command	Mode	Description
no shutdown	Interface	Enables an interface.
shutdown		Disables an interface.

The following is an example of enabling the MGMT interface.

```
SWITCH# configure terminal
SWITCH(config)# interface management
SWITCH(config-if[mgmt])# no shutdown
SWITCH(config-if[mgmt])#
```

To display if an interface is enabled, use the **show running-config** command.

5.5.2 Assigning IP Address to Network Interface

After enabling an interface, assign an IP address. To assign an IP address to a network interface, use the following command.

Command	Mode	Description
ip address *A.B.C.D/M*	Interface	Assigns an IP address to an interface.

ip address *A.B.C.D/M* **primary**	[MGMT/VLAN/LO]	Assigns a primary IP address to an interface.
ip address *A.B.C.D/M* **secondary**		Assigns a secondary IP address to an interface.
ip address dhcp		Assigns an IP address from a DHCP server.
no ip address		Clears an IP address assigned to an interface.
no ip address *A.B.C.D/M*		
no ip address *A.B.C.D/M* **secondary**		Clears a secondary IP address assigned to an interface.
no ip address dhcp		Stops assigning an IP address from a DHCP server.

The **ip address dhcp** command is for configuring an interface as a DHCP client. For the detail of configuring a DHCP client, see Section 9.6.9.

To display an assigned IP address, use the following command.

Command	Mode	Description
show ip	Interface [MGMT/VLAN/LO]	Shows an IP address assigned to an interface.

5.5.3 Assigning an IPv6 Address

IPv6 is designed as an evolutionary step from IPv4. IPv6 runs well on high performance networks like Gigabit Ethernet, ATM, and others, as well as low bandwidth networks.

The main changes from IPv4 to IPv6 are summarized as follows:

- **Expanded addressing capability and auto configuration mechanism**
  IPv6 128bits address size solves the problem of the limited address space of IPv4 and offers a deeper addressing hierarchy and simpler configuration.

- **Simplification of the header format**
  The IPv6 header has a fixed length of 40 bytes. It actually accommodates only an 8-byte header plus two 16-byte IP address (source and destination address). The packets can be handled faster with lower processing costs.

- **Improved support for extensions and options**
  With IPv6, the options are handled as Extension headers. Extension headers are optional and only inserted between the IPv6 header and the payload, if necessary. Forwarding IPv6 packets is much more efficient than IPv4.

IPv6 Header

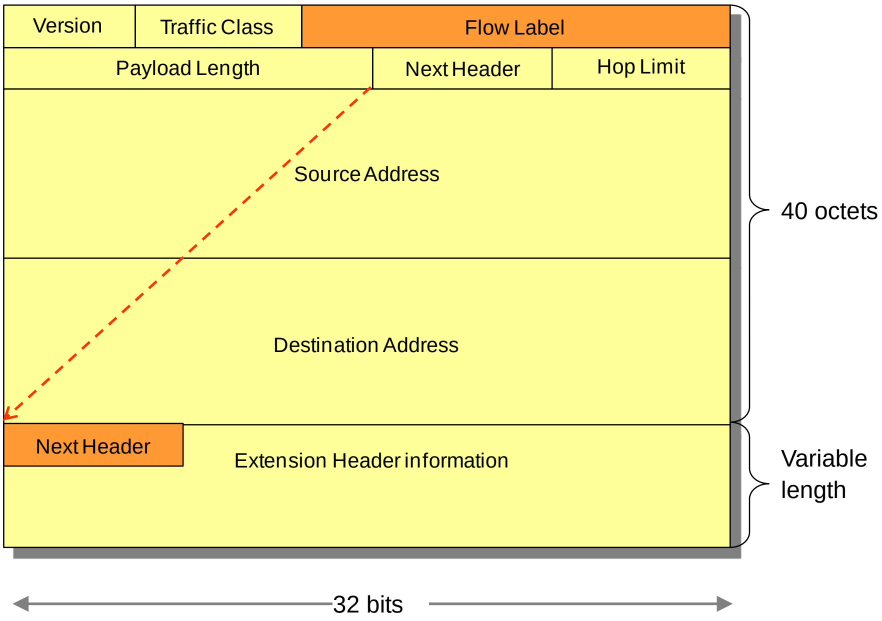


Fig. 5.2 Structure of IPv6 Header

Tab.4.1 provides an overview of the IPv6 header fields.

Field	Description
Version	Version of the protocol (4 Bits)
Priority	This field replaces the Type of Service field in IPv4. This field is used by sending nodes and forwarding routers to identify and distinguish between different classes or priorities of IPv6 packets. (1 Byte)
Flow label	This field distinguishes packets that require the same treatment, in order to facilitate the handling of real-time traffic. (20 Bits)
Payload Length	This field specifies the length of data carried after the IP header. Extension headers are considered part of the payload and are therefore included in the calculation. (2 Bytes)
Next Header	This field contains a protocol number or a value for an extension header. (1 Byte)
Hop limit	The value indicates a number of hops. Every forwarding node decrements the number by one. (1 Byte)
Source Address	This field contains the IP address of the originator of the packet.
Destination Address	This field contains the IP address of the intended recipient of the packet.

Tab. 5.3 Overview of IPv6 Header Fields

IPv6 Addressing

A typical IPv6 address consists of three parts-the global routing prefix, the subnet ID, and the interface ID. An IPv6 address has 128 bits, or 16 bytes. The address is divided into eight, 16-bit hexadecimal blocks, separated by colons.

```
FE80 : 0000 : 0000 : 0000 : 0202 : BA3FF : FE1E : 3210

FE80 : 0 : 0 : 0 : 202 : BA3FF : FE1E : 3210

FE80 :: 202 : BA3FF : FE1E : 3210
```

Some abbreviations are possible to make the IPv6 address easier. As above 3 examples are same IPv6 addresses. For instance, leading zeros in a 16-bit block can be omitted. Sequences of 16 bit blocks containing only zeros are replaced with two colons :: (not more than once per address).

IPv6 Prefix Notation

The prefix length specifies how many left-most bits of the address specify the prefix. The prefix is used to identify the subnet that an interface belongs to and is used by routers for forwarding.

IPv6 Address Types

IPv6 uses multicast addresses instead of the broadcast address. An IPv6 address can be classified into one of three categories, which Unicast, Multicast and Anycast address. The Anicast address, a new type of address introduced with RFC 1546, is now used with IPv6. An anycast address is assigned to multiple interfaces. A packet sent to an anycast address is delivered to only one of these interfaces, usually the nearest one.

IPv6 Special Addresses

There are some special addresses without prefix.
- **Unspecified address** : the unspecified address for IPv6

```
0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 (or ::)
```

- **Localhost address** : the special address for the loopback interface.

```
0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0001 (or ::1)
```

- **Link local address** : It is assigned automatically to an interface when IPv6 is enabled. The link local address is used only on local links for link communication purposes. These addresses typically begin with `fe80`.

- **Site local address** : These addresses typically begin with `fec0` and are used within a site. They are not for global use.

- **Multicasting addresses** : Multicast capability is formally added into the IPv6 protocol. The multicasting addresses begin with `ff0x`, where `x` is any hexadecimal number. An example of multicast address is `ff02::1`. This stands for all nodes of an address.

You can enable the interface to communicate with another network device on the network by assigning an IPv6 address as follows:

- Assigning IPv6 Address to Network Interface
- Assigning Link Local Address to Network Interface
- Static Route and Default Gateway
- Displaying IPv6 interface

5.5.3.1 Assigning IPv6 Address to Network Interface

After enabling an interface, assign an IPv6 global address. To assign an IPv6 address to a network interface, use the following command.

Command	Mode	Description
ipv6 address *X:X::X:X/M*	Interface [MGMT/VLAN/LO]	Assigns an IPv6 global address to an interface. X:X::X:X/M: IPv6 address/prefix-length
ipv6 address *X:X::X:X/M* **anycast**		Assigns an IPv6 anycast address to an interface.

To disable an assigned IPv6 address, use the following command.

Command	Mode	Description
no ipv6 address [*X:X::X:X/M*]	Interface	Clears an IP address assigned to an interface.

	[MGMT/VLAN/LO]	

The IPv6 address is automatically learned and based upon the received Router Advertisement from its upstream service provider router.

To enable/disable automatic configuration of IPv6 addresses using stateless auto configuration on an interface, use the following command.

Command	Mode	Description
ipv6 address autoconfig	Interface [MGMT/VLAN/LO]	Enables automatic configuration of IPv6 addresses using stateless autoconfiguration.
no ipv6 address autoconfig		Disables automatic configuration of IPv6 addresses using stateless autoconfiguration.

To enable the interface to acquire an IPv6 address from the DHCPv6 server, use the following command.

Command	Mode	Description
ipv6 address dhcp [**rapid-commit**]	Interface [XE/GPON/ MGMT/VLAN/ LO]	Acquires an IPv6 address on an interface from the DHCPv6 server. rapid-commit: allows the two-message exchange method for address allocation, the client includes the rapid-commit option in a solicit message if it is enabled
no ipv6 address dhcp		Removes the IPv6 address from the interface.

To configure dynamic IPv6 address allocation to a network interface, use the following command.

Command	Mode	Description
ipv6 address *PREFIX X:X::X:X/M*	Interface [XE/GPON/ MGMT/VLAN/ LO]	Configures IPv6 address which is dynamically changeable according to the prefix name. PREFIX: prefix name X:X::X:X/M : IPv6 prefix of sub host.
no ipv6 address *PREFIX X:X::X:X/M*		Disables a dynamic IPv6 address allocation using the prefix name and sub-host address.

5.5.3.2 Assigning Link Local Address to Network Interface

The link-lcal address used between directly connected nodes on a single network link. To assign an IPv6 link-local address to a network interface, use the following command.

Command	Mode	Description
ipv6 address link-local *X:X::X:X*	Interface [MGMT/VLAN/	Assigns a link-local address on the interface. X:X::X:X: IPv6 address using MAC address accord-

	LO]	ing to its EUI-64 format

To disable an assigned IPv6 link-local address, use the following command.

Command	Mode	Description
no ipv6 address link-local	Interface [MGMT/VLAN/ LO]	Clears a link-local address assigned to an interface.

5.5.3.3 Static Route and Default Gateway

The static route is a predefined route to a specific network and/or device such as a host. Packets are transmitted to destination through static route. Static route includes destination address, neighbor router to receive packet, number of routes that packets have to go through. To configure a static route, use the following command.

Command	Mode	Description
ipv6 route *X:X::X:X/M* {*GATEWAY* | *INTERFACE*} [<1-255>]	Global	Configures a static route. X:X::X:X/M: destination IPv6 prefix GATEWAY: IPv6 gateway address INTERFACE: IPv6 gateway interface name or pseudo interface null 1-255: distance value for this prefix
ipv6 route *X:X::X:X/M INTERFACE* [<1-255>]		

To delete a configured static route, use the following command.

Command	Mode	Description
no ipv6 route *X:X::X:X/M* [{*GATEWAY* | *INTERFACE*}]	Global	Deletes a configured static route.
no ipv6 route *X:X::X:X/M GATEWAY INTERFACE*		

The following is an example of configuring a static route to reach three destinations, which are not directly connected.

```
SWITCH(config)# ipv6 route 4000::/16 br101
SWITCH(config)# ipv6 route 3000:3::/64 br103
SWITCH(config)# ipv6 route 3000:2::/64 br102
```

To display a configured static route, use the following command.

Command	Mode	Description
show ipv6 route [**bgp** | **connected** | **kernel** | **ospf** | **rip** |**static** | *X:X::X:X* | *X:X::X:X/M* | **summary**]	Enable Global	Shows configured routing information.
show ipv6 route database [**bgp** |		Shows configured routing information with IP routing

connected | **kernel** | **ospf** | **rip** | **static**]		table database.

To remove all kernel IPv6 route caches, use the following command.

Command	Mode	Description
clear ipv6 route kernel	Enable	Removes all kernel IPv6 route caches

5.5.3.4 Enabling IPv6 Processing

To enable/disable the IPv6 processing on an interface, use the following command.

Command	Mode	Description
ipv6 enable	Interface [MGMT/VLAN/LO]	Enables the IPv6 processing on an interface.
no ipv6 enable		Disables the IPv6 processing on an interface.

To enable/disable global IPV6 forwarding between all interfaces, use the following command.

Command	Mode	Description
ipv6 forwarding	Global	Enables global IPv6 packet forwarding function on the system. (Default)
no ipv6 forwarding		Disables global IPv6 packet forwarding function.

To display the status of global IPv6 forwarding, use the following command.

Command	Mode	Description
show ipv6 forwarding	Enable Global	Shows the IPv6 status of forwarding mode.

5.5.3.5 IPv6 Interface Mode

You can configure the interface for router mode or host mode. The router mode allows the switch to receive Router Solicitation(RS) messages or send Router Advertisement (RA) messages to the network within this interface. In case of host mode, it functions as an IPv6 host. The interface can not send RA messages to other devices.

To specify the IPv6 interface mode on an interface, use the following command.

Command	Mode	Description
ipv6 mode host	Interface [MGMT/VLAN/LO]	Configures the interface for host mode. The interface can not send RA messages to the network.
ipv6 mode router		Configures the interface for router mode. The interface receives RS messages and send RA messages to the

		network.
no ipv6 mode		Deletes the configured IPv6 interface mode.

5.5.3.6 Displaying IPv6 interface

To display an assigned IPv6 address, use the following command.

Command	Mode	Description
show ipv6	Interface	Shows the IPv6 addresses assigned to an interface.

To display an interface status and configuration, use the following command.

Command	Mode	Description
show ipv6 interface	Enable Global	Shows all configured interfaces and their configurations.
show ipv6 interface {**gigabitethernet** | **tengigabitethernet** | **gpon** | **channelgroup**} *IFPORTS*		Shows the specified IPv6 interface information. INTERFACE: IPv6 interface name
show ipv6 interface {**gigabitethernet** | **tengigabitethernet** | **gpon** | **channelgroup**} *IFPORTS* **brief**		Shows a brief summary of IPv6 interface status and configuration.
show ipv6 interface brief		

5.5.3.7 IPv6 PBR Configuration

To identify a route map to use for IPv6 PBR(Policy-based Routing) on an interface, use the following command.

Command	Mode	Description
ipv6 policy route-map *WORD*	Interface [XE/br/CG/GPON]	Configures a route map for IPv6 policy on the interface. WORD: route map name

To display the IPv6 policy-based routing (PBR) configuration, use the following command.

Command	Mode	Description
show ipv6 policy	Enable Global	Shows IPv6 policy route maps attached to interface.

5.5.4 Static Route and Default Gateway

The static route is a predefined route to a specific network and/or device such as a host. Unlike a dynamic routing protocol, *static routes* are not automatically updated and must be manually reconfigured if the network topology changes. Static route includes destination address, neighbor address, and etc. To configure a static route, use the following command.

Command	Mode	Description
ip route *A.B.C.D SUBNET-MASK* {*GATEWAY* | **null** | *INTERFACE*} [<1-255>]	Global	Configures a static route. A.B.C.D: destination IP prefix A.B.C.D/M: destination IP prefix with mask SUBNET-MASK*:* IP destination prefix mask (A.B.C.D) GATEWAY: gateway address INTERFACE: IP gateway interface name 1-255: distance value for this route src: binding source IP address
ip route *A.B.C.D/M* {*GATEWAY* | **null** | *INTERFACE*} [<1-255> | **src** *A.B.C.D*]		

To delete a configured static route, use the following command.

Command	Mode	Description
no ip route *A.B.C.D SUBNET-MASK* {*GATEWAY* | **null**} [<1-255>]	Global	Deletes a configured static route.
no ip route *A.B.C.D/M* {*GATE-WAY* | **null** | *INTERFACE*} [<1-255>]		

To configure a default gateway, use the following command.

Command	Mode	Description
ip route default {*GATEWAY* | **null**} [<1-255>]	Global	Configures a default gateway.

To delete a configure default gateway, use the following command.

Command	Mode	Description
no ip route default {*GATEWAY* | **null**} [<1-255>]	Global	Deletes a default gateway.

To display a configured static route, use the following command.

Command	Mode	Description
show ip route [**database**]	Enable Global	Shows all IP routing table
show ip route [**bgp** | **connected** | **kernel** | **ospf** | **rip** | **static** | *A.B.C.D* | *A.B.C.D/M* | **summary | performance | pbr**]		Shows configured routing information.
show ip route database [**bgp** | **connected** | **kernel** | **ospf** | **rip** | **static**]		Shows configured routing information with IP routing table database.

To clear IPv4 stale kernel routes form FIB, use the following command.

Command	Mode	Description
clear ip route [**kernel**]	Enable Global	Clears IPv4 stale routes.

5.5.5 Displaying IP Address Assignment

To display an assigned IP address of interface, use the following command.

Command	Mode	Description
show ip	Interface	Shows the brief information of IP address assignment.
show ip interface {**brief** | **vlan** *VLANS*}	Enable Global	
show ip interface {**gigabitethernet** | **tengigabitethernet** | **gpon** | **channelgroup**} *IFPORTS*		

5.5.6 Initial Management Access and IP Address Assignment

You can configure the system to be accessed remotely by Telnet. Firstly, you have to install the SFU module in the central slot of the chassis. The LD3032 has a management port (MGMT) and console port on the front panel of SFU module.

After the LD3032 is plugged an Ethernet cable directly from your network into the management (MGMT) port for remotely access into the switch, it is operational.

To access the system remotely via management interface, follow these steps.

1. Connect to the console port is used for direct local configuration and management. The console port settings are:
   - 9600 baud rate
   - 8 data bits
   - 1 stop bit
   - No parity
   - No flow control
2. Connect a terminal or PC with terminal-emulation software to the console port on the SFU module. At your terminal, booting will be automatically started and login prompt will be displayed. By default setting, the user name is configured as ***admin***. At the password prompt, press [**ENTER**].
3. Open the *MGMT Interface Configuration* Mode. And assign an IP address and subnetwork mask for the management interface.
4. Configure a management route to the network from which you are accessing the system.
5. Save the IP settings so that they will be in effect after the next system reboot by **reload** command.
6. Once you have completed the proper hardware installation and initial software

configuration for the LD3032, you can access the system remotely by Telnet.

The following is an example of accessing the system remotely.

```
SWITCH login: admin
Password:
SWITCH> enable
SWITCH# configure terminal
SWITCH(config)# interface management
SWITCH(config-if[mgmt])# ip address 10.55.192.161/24
SWITCH(config-if[mgmt])# no shutdown
SWITCH(config-if[mgmt])# write memory
[OK]
SWITCH(config-if[mgmt])# exit
SWITCH(config)# ip route 10.55.0.0/16 10.55.192.254
SWITCH(config)# write memory
[OK]
SWITCH(config)# show ip interface brief

Interface       Status            Protocol  Primary IP      Secondary IP
------------------------------------------------------------------------------
mgmt             up                up       10.55.192.161    unassigned
SWITCH(config)# exit
SWITCH# reload
```

5.6 SFU Redundancy

The LD3032 meets carrier's requirements for high reliability, which is a substantial factor for aggregation switches to perform traffic forwarding to core network without failure. It provides equipment-level reliability including Switching Fabric Unit (SFU) redundancy and power redundancy.

Switching Fabric Interface Redundancy

There are two slots for SFU in the rear of the LD3032 base chassis. A redundant SFU could be equipped into either slot. This switch can perform normal switching operation with a single SFU, but also can accommodate dual SFUs to ensure stable operation.

When dual SFUs are used, the system decides the running mode of SFUs between active and standby. The first inserted and booted SFU runs in active mode and the other SFU that follows runs in standby mode. The following diagram illustrates SFU redundancy scheme used for the LD3032. Both SFUs are internally linked to IUs. They receive traffic from IUs and update their own Forwarding Database (FDB) in the same manner so that they can keep identical data to make a forwarding decision. However, only the active SFU can send traffic back to the OIUs; the standby SFU can just receive traffic for address learning.

In a redundancy scenario, only the active SFU is working in the system and contains user configurations via SNMP or CLI and dynamically-learned state information such as DHCP snooping, IGMP snooping, L3 protocols, STP states, etc. But the standby SFU doesn't have that information. Thus, there is a mechanism to synchronize between the active SFU and standby SFU. The active SFU periodically sends state information to the standby SFU through an interlinked 100MB channel between them.

5.6.1 Automatic Switchover

Software or hardware failure and accident can cause an automatic switchover from active SFU to standby SFU. Also, a static switchover by network operator could be made due to software upgrade, equipment exchange, or network construction. If the switchover happens, the standby SFU can start working without a service break.

To change the board's role between an active SFU and standby SFU, use the following command.

Command	Mode	Description
switchover [**force**]	Enable	Changes the standby SFU to be active. Then the active SFU become a standby state after system reset. force: force doing switchover even though the system is performing important task like software upgrade.

To display the status of SFU, use the following command.

Command	Mode	Description
show redundancy status	Enable Global	Shows boards' role, active and standby, and board operating mode. The switch runs in redundant mode if in use of dual SFUs and runs in standalone mode for a single SFU.
show redundancy sync-module-list		Shows

5.6.2 Fault Monitoring Function

You can also configure the LD3032 to monitor the fault of the SFU daemons for automatic SFU switchover for a connection failure.

If a certain daemon (eqmd, swchd, nsm, snmpd, ripd, updated, etc.) is terminating abnormally or no response is received from the daemon, you can define the action. To define what action should be taken if there is a SFU failure in operation or no response, use the following command.

Command	Mode	Description
fault-monitor daemon *NAME* **admin-status** {**enable** | **disable**}	Global	Enables/disables the fault monitoring function per daemon. (default: enable) NAME: daemon name (eqmd, swchd, nsm, snmpd, ripd, updated, ospfd, bgpd, pimd, vrrpd, dhcpd, eapd, imi, ocmd)
fault-monitor inspect-interval <3-86400>		Defines the inspection interval value for fault monitoring. 3-86400: inspection interval value (default: 10 seconds)
fault-monitor startup-threshold <100-1000>		Defines the startup-threshold value after the daemon's fault detection. 100-1000: startup-threshold value (default: 100 seconds)
fault-monitor daemon *NAME* **fault-type crash action** {**switchover** | **log** | **restart**}		Configures the action to be taken if a particular daemon is crashed down. switchover: makes a switchover to the standby SFU. In a standalone mode, it restarts the system instead. log: generates the syslog messages. restart: restarts the daemon (default)
fault-monitor daemon *NAME* **threshold** <1-10>		Specifies the timeout until it receives a response from the daemon during the fault monitoring period. 1-10: threshold value (default:10 seconds)
fault-monitor daemon *NAME* **fault-type timeout action** {**switchover** | **log** | **restart**}		Configures the action to be taken if a particular daemon brings no response for a given time. switchover: makes a switchover to the standby SFU. In standalone mode, it restarts the system instead. log: generates the syslog messages restart: restarts the daemon (default)

To remove the configured actions, use the following command.

Command	Mode	Description
no fault-monitor daemon *NAME* **fault-type** {**crash** | **timeout**} **action**	Global	Deletes the configured actions.
no fault-monitor daemon *NAME* **threshold**		Deletes the configured threshold value and returns to the default setting.
no fault-monitor inspect-interval		Deletes the configured interval for inspection and returns to the default setting.
no fault-monitor startup-threshold		Deletes the configured startup-threshold and returns to the default setting..

To display the current fault monitoring status of all daemons, use the following command.

Command	Mode	Description
show fault-monitor	Global	Shows the current fault monitoring status of all daemons.

5.6.3 Data Synchronization between SFUs

If there are dual SFUs in LD3032 chassis, the currently saved configuration data of active SFU can be copied and moved to standby SFU. To synchronize the configuration data between SFUs for redundancy control, use the following command.

Command	Mode	Description
copy configsync all	Enable	Copies the entire configuration files of active SFU and send them to the standby SFU.
copy configsync partial *FILENAME*		Copies a configuration file to a specified file name. FILENAME: configuration file name

The user can not set any configuration on the standby SFU by default. To enable/disable a standby SFU to be configured by CLI, use the following command.

Command	Mode	Description
red-config-standby enable	Enable	Enables a standby SFU to be configured by CLI.
red-config-standby disable		Disables a standby SFU to be configured by CLI.

5.7 Configure External Alarm LEDs

The LD3032 supports the monitoring function by its alarm LED status indication by mapping between SNMP alarm severity of system and alarm LED level on the front panel of SFU.

You can configure SNMP alarms so that the system generates a trap message when an event corresponding to one of the alarms occurs. After configuring an alarm consists of enabling the alarm and setting the severity level at which a trap is generated. A trap is sent only when the severity of the alarm matches the severity specified for the trap.

In addition, LD3032 can monitor the external alarm LEDs on the switch fabric unit (SFU) card using SNMP alarm severity settings or alarm LED level setting. If you set the critical severity of the SNMP alarm, the system will generate trap messages and turn on the CRIT alarm LED when corresponding events occur.

The following table shows the mappings between SNMP alarm severity and SFU alarm LEDs:

SNMP Alarm Severity	SFU Alarm Level
critical	CRIT (critical) LED
major	MAJ (major) LED
minor, warning, intermediate	MIN (minor) LED

To activate an alarm LED operation mode and set the level of the alarm LEDs when corresponding event occurs, use the following command.

Command	Mode	Description
alarm-led level all {**critical** | **major** | **minor**}	Global	Sets the level of the alarm LEDs when any event occurs.
alarm-led level fan-fail {**critical** | **major** | **minor**}		Sets the level of the alarm LEDs when fan failure occurs.
alarm-led level fan-remove {**critical** | **major** | **minor**}		Sets the level of the alarm LEDs when the fan is removed.
alarm-led level power-fail {**critical** | **major** | **minor**}		Sets the level of an alarm LED in case of power failure.
alarm-led level power-remove {**critical** | **major** | **minor**}		Sets the level of an alarm LED when power module is removed.
alarm-led level temperature {**critical** | **major** | **minor**}		Sets the level of an alarm LED when temperature exceeds the threshold.

To deactivate an alarm LED operation mode and the level of the alarm LED settings, use the following command.

Command	Mode	Description
alarm-led clear {**fan-fail** | **fan-remove** | **power-fail** | **power-remove** | **temperature** }	Global	Deactivates an alarm LED operation mode

To block/unblock the alarm LED configurations according to the level of alarm LEDs, use the following command.

Command	Mode	Description
alarm-led block {**all** | **critical** | **major** | **minor**}	Global	Blocks the alarm LED configuration.
alarm-led unblock {**all** | **critical** | **major** | **minor**}		Unblocks the alarm LED configuration.

To display the status of alarm-led operation, use the following command.

Command	Mode	Description
show alarm-led	Enable Global	Shows the status of alarm-led settings.

5.8 IU Firmware Upgrade

5.8.1 Manually Upgrading SFU

To upgrade the system software of the switch, use the following command.

Command	Mode	Description
copy {**ftp** | **tftp**} **os download** {**os1** | **os2**}	Enable	Upgrades the system software of the switch via FTP or TFTP. os1 | os2: the area where the system software is stored

⚠ To upgrade the system software, FTP or TFTP server must be set up first! Using the **copy** command, the system will download the new system software from the server.

⚠ To reflect the downloaded system software, the system must restart using the **reload** command! For more information, see Section 4.1.4.1.

5.8.2 Upgrading IUs

To select IU upgrade mode to upgrade IU, use the following command.

Command	Mode	Description
slot upgrade-mode iu *SLOT_NUMBER* **auto**	Global	Enables IU auto upgrade mode. SLOT_NUMBER : 1 to 2
slot upgrade-mode iu *SLOT_NUMBER* **manual**		Enable IU manual upgrade mode.

To manually upgrade the system software of a specific module, perform the following step-by-step instruction:

To download the system software image of IU, use the following command.

Command	Mode	Description
copy {**ftp** | **tftp**} **iu download**	Enable	Downloads the system software of the Interface unit from FTP/TFTP server.

To select an IU in the specified slot and uploads the new system software using the following command.

Command	Mode	Description
slot upgrade iu *SLOT_NUMBER*	Global	Select a slot number of IU and performs the upgrade.

To restart a specific IU in the slot using the following command.

Command	Mode	Description
slot restart iu *SLOT_NUMBER*	Global	Resets an interface module in the specified slot number.

To display the new system software using the following command.

Command	Mode	Description
show slot nos iu {**all** | *SLOT_NUMBER*}	Enable Global	Shows the system software of each slot.

5.8.3 Manually SFU Firmware Uploading

To upload the system software of the switch, use the following command.

Command	Mode	Description
copy {**ftp** | **tftp**} **os upload** {**os1** | **os2**}	Enable	Uploads the system software image of the switch to FTP or TFTP os1 | os2: the area where the system software is stored

5.9 Ethernet Port Configuration

Depending on the type of the interface units (Ethernet, GPON), the number of chassis' physical ports can be changed. It features highly flexible hardware configurations with multiple 1 or 10 Gigabit Ethernet components. In this chapter, you can find the instructions for the basic port configuration such as auto-negotiation, flow control, transmit rate, etc. Please read the following instructions carefully before you configure a port in the LD3032.

5.9.1 Enabling Ethernet Port

The Ethernet Interface mode contains commands for configuring the 1GE or 10GE interface. You can open this *Interface Configuration* mode when at least one SFU_10GE4 module is installed in the LD3032 chassis.

To open *Ethernet Interface Configuration* mode, enter the **interface gigabitethernet**/**tengigabitethernet** command, then the system prompt will be changed from SWITCH(config)# to SWITCH(config-if[GE])# or SWITCH(config-if[XE])#.

Command	Mode	Description
interface {**gigabitethernet** | **tengigabitethernet**} *IFPORT*	Global	Enters the *Interface Configuration* mode to configure an 1G/10G Ethernet type interface. IFPORT: physical interface port number (SLOT#/PORT#, e.g. 1/1, 1/2) IFPORT-RANGE: list of valid ports per Ethernet interface unit. Use a hyphen to designate a range of ports. (e.g. 1/1-8 or 1/1-1/8)
interface range {**gigabitethernet** | **tengigabitethernet**} *IFPORT-RANGE*		

To enable/disable the Ethernet interface, use the following command.

Command	Mode	Description
no shutdown	Interface [XE/GE]	Enables an 1G or 10G Ethernet interface.
shutdown		Disables an 1G or 10G Ethernet interface.

5.9.2 Auto-Negotiation

Auto-negotiation is a mechanism that takes control of the cable when a connection is established to a network device. Auto-negotiation detects the various modes that exist in the network device on the other end of the

wire and advertises it own abilities to automatically configure the highest performance mode of interoperation. As a standard technology, this allows simple, automatic connection of devices that support a variety of modes from a variety of manufacturers.

To enable/disable the auto-negotiation on an Ethernet port, use the following command.

Command	Mode	Description
nego {**on** | **off**}	Interface [XE/GE]	Enables/disables the auto-negotiation on a specified port, enter a port number. (default: on)

⚠ Auto-negotiation operates only on 10/100/1000Base-T interface. You cannot enable this function on 1000Base-X or 10GbE optical interface.

5.9.3 Transmit Rate

To set the transmit rate of a 10G Ethernet port, use the following command.

Command	Mode	Description
speed {**1000** | **10000**}	Interface [XE]	Sets the transmit rate of a specified port to 1000/10000 Mbps.
no speed		Deletes the configured port speed.

5.9.4 Link Monitoring Timer

The link debounce time is the amount time that an interface waits to notify the link down state of a physical Ethernet port. When link debounce timer is enabled, port's link down detection is delayed, resulting in a loss of traffic during the debounce period.

To enable/disable the debounce timer on an Ethernet port, use the following command.

Command	Mode	Description
link-debounce-time <10-5000>	Interface [XE/GE]	Enables the debounce timer and specify the time for an Ethernet interface. 10-5000: timer value (in milliseconds, default: 0)
no link-debounce-time		Disables the debounce timer on the specified interface.

To display the debounce timer information, use the following command.

Command	Mode	Description
show link-debounce-time	Enable Global Interface [XE/GE]	Shows the configured link debounce time value.

To configure the interval for link monitoring on the Ethernet port, use the following command.

Command	Mode	Description
link-check-timer <20-1000>	Interface [XE/GE]	Specifies the time interval for checking the link of Ethernet interface. 20-1000: interval value (in milliseconds, default: 500ms)
no link-check-timer		Disables the link checking timer on the specified interface.

5.9.5 Network Service Port

To change a service port number that is in use by a different network service, use the following command.

Command	Mode	Description
service port {**ftp** | **ftp-data** | **ssh** | **telnet**} <1-65535>	Global	Chages the default port number for FTP/FTP-data/SSH/Telnet service. 1-65535: port number (Default port number: FTP (21), FTP-data (20), SSH (22), Telnet (23))
no service port {**ftp**| **ftp-data** | **ssh** | **telnet**}		Deletes the configured service port number and returns to the default port number for network service.

5.9.6 L2 Port Bridge

The L2 port bridge feature allows the port to forward the packets that the outgoing interface in the MAC address entry is the same as the incoming interface where the packet arrived. If one port is enabled with L2 port bridge feature, it forwards the packets to its destination port when the MAC address is found in the L2 table. The switch can have multiple MAC addresses associated with the same port.

To enable/disable the L2 port bridge feature, use the following command.

Command	Mode	Description
switchport port-bridge	Interface [XE/GE]	Enables L2 port bridge feature on the interface.
no switchport port-bridge		Disables L2 port bridge feature. (default)

5.9.7 Flow Control

In Ethernet networking, the flow control is the process of adjusting the flow of data from one network device to another to ensure that the receiving device can handle all of the incoming data. For this process, the receiving device normally sends a PAUSE frame to the sending device when its buffer is full. The sending device then stops sending data for a while. This is particularly important where the sending device is capable of sending data much faster than the receiving device can receive it.

To enable the flow control on an Ethernet port, use the following command.

Command	Mode	Description
flowcontrol both	Interface [XE/GE]	Enables the IEEE802.3x flow control function on a specified interface.
flowcontrol receive {**on** | **off**}		Enables/disables the IEEE802.3x flow control function of RX packets.
flowcontrol send {**on** | **off**}		Enables/disables the IEEE802.3x flow control function of TX packets.

To disable the flow control on an Ethernet port, use the following command.

Command	Mode	Description
no flowcontrol	Interface [XE/GE]	Disables the flow control on a specified interface.

To display the flow control information, use the following command.

Command	Mode	Description
show flowcontrol	Enable	Shows a current flow control status.
show flowcontrol interface {**gigabitethernet** | **tengigabitethernet** } *IFPORTS*		

6 System Environment

6.1 Environment Configuration

You can configure a system environment of the LD3032 with the following items:

6.1.1 Terminal Configuration

By default, the LD3032 is configured to display 24 lines composed by 80 characters on console terminal. You can change the number of displaying lines by using the **terminal length** command. The maximum line displaying is 512 lines.

To set the number of the lines displaying on terminal screen, use the following command.

Command	Mode	Description
terminal length <0-512>	Enable	Sets the number of the lines displaying on a terminal screen, enter the value.
no terminal length		Restores a default line displaying.

6.1.2 Fan Operation

For the LD3032, it is possible to control fan operation. To control fan operation, use the following command.

Command	Mode	Description
fan operation full	Global	Operates the fans at full-speed.
fan operation auto		Controls the fan operation based on the configured threshold value.

It is possible to configure to start and stop fan operation according to the system temperature. To configure this, see Section 6.1.6.3.

To display fan status and the temperature for fan operation, use the following command.

Command	Mode	Description
show status fan	Enable Global	Shows the fan status and the temperature for the fan operation.

6.1.3 Disabling Daemon Operation

You can disable the daemon operation unnecessarily occupying CPU. To disable certain daemon operation, use the following command.

Command	Mode	Description
halt *PID*	Enable	Disables the daemon operation.

You can display the PID of each running processes with the **show process** command.

```
SWITCH# show process
USER     PID  %CPU  %MEM    VSZ   RSS  TTY   STAT   START  TIME   COMMAND
admin      1   0.2   0.2   1448   592  ?     S      Feb23  0:05   init [3]
admin      2   0.0   0.0      0     0  ?     S      Feb23  0:00   [keventd]
admin      3   0.0   0.0      0     0  ?     SN     Feb23  0:00   [ksoftirqd_CPU0]
admin      4   0.0   0.0      0     0  ?     S      Feb23  0:00   [kswapd]
admin      5   0.0   0.0      0     0  ?     S      Feb23  0:00   [bdflush]
admin      6   0.0   0.0      0     0  ?     S      Feb23  0:00   [kupdated]
admin      7   0.0   0.0      0     0  ?     S      Feb23  0:00   [mtdblockd]
admin      8   0.0   0.0      0     0  ?     S<     Feb23  0:00   [bcmDPC]
admin      9   0.0   0.0      0     0  ?     S<     Feb23  0:29   [bcmCNTR.0]
admin     16   0.0   0.0      0     0  ?     SN     Feb23  0:00   [jffs2_gcd_mtd0]
admin     81   0.0   2.0  10524  5492  ?     S      Feb23  0:53   /usr/sbin/swchd
admin     83   0.0   1.5   6756  3756  ?     S      Feb23  0:53   /usr/sbin/nsm

(Omitted)

SWITCH#
```

6.1.4 FTP Bind Address

When used as an FTP client, the LD3032 connects to an FTP server via the interface toward that server, which means the FTP client uses the IP address configured in that interface as a source IP address. However, an interface of the LD3032 may have multiple IP addresses. In such a multiple-IP environment, a primary IP address is normally used. You can configure the LD3032 to use one of the secondary IP addresses as a source IP of an FTP client.

To use a specific IP address as a source IP of an FTP client, use the following command.

Command	Mode	Description
ftp bind-address *A.B.C.D*	Global	Specifies a source IP address of an FTP client. A.B.C.D: one of the secondary IP addresses configured in an interface
no ftp bind-address		Deletes a specified source IP address.

This configuration is also applicable to a TFTP client.

6.1.5 Enable DDM Function

If you insert an SFP module including Digital Diagnostic Monitoring (DDM) function into ports, you can monitor the operating parameters of the SFP module, including the transceiver type, length, connector type, and vendor information. However, you might not want to see DDM polling information because it may result in CPU overload to collect DDM data via I^{2}C interface. To enable or disable the DDM function of SFP mouldes, use the following command.

Command	Mode	Description
module ddm {**enable** | **disable**} **all**	Global	Specifies whether to collect DDM information from all SFP modules.
module ddm {**enable** | **disable**}	Interface [GE/XE/GPON]	Specifies whether to collect DDM information from SFP modules in the specified interface.

This **module ddm** function is enabled by default. Thus, if you don't want to get DDM information, configure this setting as disable.

To display the status of DDM function, use the following command.

Command	Mode	Description
show module ddm	Enable Global	Displays the status of DDM function.

You can monitor the DDM information of the SFP ports when using the **show interface module-info** command.

6.1.5.1 SFP Module Operation

The system module will operate depending on monitoring type of temperature, RX/TX power, voltage or Txbias. To set the threshold of module, use the following command.

Command	Mode	Description
threshold module {**rxpower** | **txpower**} {**alarm** | **warning**} *START-VALUE STOP-VALUE* {**sfp**|**system**}	Interface [GE/XE/GPON]	Sets the Diagnostics threshold of SFP module by RX/TX power and monitors the module. The range of RX/TX power: -40～8.1647 dBm
threshold module temper {**alarm** | **warning**} *START-VALUE STOP-VALUE* {**sfp**|**system**}		Sets the Diagnostics threshold of SFP module depending on temperature and monitors the module The range of temperature: -128～127.99℃
threshold module txbias {**alarm** | **warning**} *START-VALUE STOP-VALUE* {**sfp**|**system**}		Sets the Diagnostics threshold of SFP module depending on txbias and monitors the module. The range of txbias: 0～ 131 mA
threshold module voltage {**alarm** | **warning**} *START-VALUE STOP-VALUE* {**sfp**|**system**}		Sets the Diagnostics threshold of SFP module depending on voltage and monitors the module. The range of voltage: 0～ 6.5535 V

To delete the threshold of module operation depending on specified monitoring type, use the following command.

Command	Mode	Description
no threshold module {**rxpower** | **voltage** | **txbias** | **txpower** | **temper**} {**alarm** | **warning**}	Interface [GE/XE/GPON]	Deletes the configured threshold of SFP module.

6.1.6 System Threshold

You can configure the system with various kinds of the system threshold such as CPU load, traffic, temperature, etc. Using this threshold, the LD3032 generates syslog messages, sends SNMP traps, or performs a relevant procedure.

6.1.6.1 CPU Load

To set the threshold of CPU load, use the following command.

Command	Mode	Description
threshold cpu <21-100> {**5** | **60** | **600**} [<20-100> {**5** | **60** | **600**}]	Global	Sets the threshold of CPU load in the unit of percent (%). 21-100: CPU load high (default: 70) 20-100: CPU load low (default: 30) 5 | 60 | 600: time interval (unit: second / default:60)
threshold cpu iu *SLOT_NUM* <21-100> {**5** | **60** | **600**} [<20-100> {**5** | **60** | **600**}]		Sets the threshold of IU’s CPU load in the unit of percent (%). 21-100: CPU load high (default: 70) 20-100: CPU load low (default: 30) 5 | 60 | 600: time interval (unit: second / default:60)
no threshold cpu		Deletes the configured threshold of CPU load.
no threshold cpu iu *SLOT_NUM*		Deletes the configured threshold of IU’s CPU load.

To display the configured threshold of CPU load, use the following command.

Command	Mode	Description
show cpuload	Enable Global	Shows the configured threshold and average of CPU load.
show cpu-trueload		Shows the CPU load history during the last 10 minutes in the time slots of every 5 seconds.

6.1.6.2 Port Traffic

To set the threshold of port traffic, use the following command.

Command	Mode	Description
threshold *THRESHOLD* {**5** | **60** | **600**} {**rx** | **tx**}	Interface [GE/XE/GPON]	Sets the threshold of port traffic. PORTS: port number (1/1, 1/2, 2/1, …) THRESHOLD: threshold value (unit: kbps) 5 | 60 | 600: time interval (unit: second)
no threshold port *PORTS* {**rx** | **tx**}		Deletes the configured threshold of port traffic.

i The threshold of the port is set to the maximum rate of the port by default.

You can also set the blocking timer. When incoming traffic via a given port exceeds a configured threshold, the port will discard that traffic during a specified time.

To set the blocking timer, use the following command.

Command	Mode	Description
threshold block timer <10-3600>	Interface [GE/XE/GPON]	Sets the blocking timer. 10-3600: blocking time (unit: second)
no threshold block		Disables the blocking timer

To display the configured threshold of port traffic, use the following command.

Command	Mode	Description
show interface threshold	Enable Global	Shows the configured threshold of port traffic.

6.1.6.3 Fan Operation

The system fan will operate depending on measured system temperature. To set the threshold of fan operation, use the following command.

Command	Mode	Description
threshold fan *RUN-VALUE STOP-VALUE*	Global	Sets the threshold of chassis temperature for fan operation in the unit of Celsius (°C). RUN-VALUE : sets system temperature for running fans (-30~ 100°C, default: 50°C) STOP-VALUE : sets system temperature for stopping fans (-30~ 100°C, default: 10°C)
no threshold fan		Deletes the configured threshold.

! When you set the threshold of fan operation, *FULL-VALUE* must be higher than *HALF-VALUE*.

To display the configured threshold of fan operation, use the following command.

Command	Mode	Description
show status fan	Enable/Global	Shows the status and configured threshold of fan operation.

6.1.6.4 System Temperature

To set the threshold of system temperature, use the following command.

Command	Mode	Description
threshold temp *HIGH_VALUE LOW_VALUE*	Global	Sets the threshold of system temperature(°C). HIGH_VALUE: overload system temperature (-40 to 100°C) LOW_VALUE: underload system temperature (-40 to 100°C)
threshold temp iu *NUMBER HIGH_VALUE LOW_VALUE*		Sets the threshold of IU temperature(°C). NUMBER : a slot number of IU HIGH_VALUE: overload system temperature (-40 to 100°C) LOW_VALUE: underload system temperature (-40 to 100°C)
no threshold temp		Deletes the configured threshold of system/IU temperature.
no threshold temp iu *NUMBER*		

To enable/disable the system/IU shut down due to over-temperature event that can lead to serious system problems, use the following command.

Command	Mode	Description
threshold power iu *SLOT_NUMBER VALUE*	Global	Sets the over-temperature threshold value of interface unit. VALUE: temperature threshold for IU power-off (60 to 90°C, default: 80°C)
threshold power system *VALUE*		Sets the over-temperature threshold value of chassis system. VALUE: temperature threshold for system shut-down (80 to 120°C, default: 110°C)
threshold power system { **enable** | **disable** }		Enables/disables the system shut down in the over-temperature event.
no threshold power iu *SLOT_NUMBER*		Deletes the configured over-temperature threshold value of IU/system.
no threshold power system		

To display the configured threshold of system temperature, use the following command.

Command	Mode	Description
show status temp	Enable Global	Shows the status and configured threshold of system temperature.

6.1.6.5 System Memory

To set the threshold of system memory in use, use the following command.

Command	Mode	Description
threshold memory <20-100>	Global	Sets the threshold of system memory in the unit of percent (%). 20-100: system memory in use
no threshold memory		Deletes the configured threshold of system memory.

6.1.7 MAC Learning Mode

The LD3032 supports two methods of MAC learning that are CPU-based learning (CML) and the switching fabric-based learning (SML). You can choose the way how to learn MAC addresses by CLI.

The following table shows the functional performance of CML mode and SML mode.

Functions	CML	SML
MAC learning	Slow(default)	Fast
CPU load during MAC learning	High	Low
Interval of Chip calling	Depending on the number of packets	Periodically
Interconnection with CPU	Accurate	Delay
Security Policy	Accurate	Delay
ERP enabled port	Disable	Enable

Tab. 6.1 CML and SML Capability Comparison

To specify MAC learning mode in the system, use the following command.

Command	Mode	Description
mac-learning mode {**cml** | **sml**}	Global	Specifies MAC learning mode in the system. cml: CPU managed-learning (default) sml: switching fabric managed-learning

6.1.8 The Utilization and Aging-time of L3 Table

To display the urtilization of packets in use on L3 interface, host entries, LPM entries and L3 ECMP entries, use the following command.

Command	Mode	Description
show ip tables summary	Enable Global	Shows the usage of L3 interface, host, LPM, ECMP entries.

To specify the L3 table aging time, use the following command.

Command	Mode	Description
ip tables aging-time <10-4294967295>	Global	Specifies the L3 table aging time (default: 300 seconds).

6.1.9 SD Card

To display SD card information, use the following command.

Command	Mode	Description
show sdcard information	Enable Global	Shows the fan status and the temperature for the fan operation.

The sdcard can be safely unmounted/mounted by using the following command.

Command	Mode	Description
umount sdcard	Enable Global	Unmounts a SD card from the SFU.
mount sdcard		Mounts a SD memory card to the SFU.

6.1.10 Power Alarm Configuration

To enable the alarm notification when detecting an error of power (PSU), use the following command.

Command	Mode	Description
alarm {**0**|**1**} {**0**|**1**} {**0**|**1**}	Enable	Enables the alarm notification using trap message when an error occurs in a power supply unit. 0 | 1 : select PSU A (0) or PSU B (1) 0 | 1 : select alarm-out YES (1) or NO (0) 0 | 1 : send tram message YES (1) or NO (0)

6.1.11 Enabling FTP/TFTP Connection

To enable/disable the connection via FTP, use the following command.

Command	Mode	Description
service ftp	Global	Enables/ disables the connection via FTP.
no service ftp		

To enable/disable the connection via TFTP, use the following command.

Command	Mode	Description
service tftp	Global	Enables/ disables the connection via TFTP.
no service tftp		

To display the status of network connection services, use the following command.

Command	Mode	Description
show service	Enable/Global/Bridge	Shows the status of network connection services (telnet/ssh/ftp/tftp/snmp).

6.1.12 EQM Debugging

To configure a debugging for EQM module, use the following command.

Command	Mode	Description
debug eqm all	Enable	Enables the debugging for EQM module used to manage the equipment.
no debug eqm all		Disables the debugging for EQM module used to manage the equipment.

6.2 System Management

When there is any problem in the system, you must find what the problem is and its solution. Therefore, you should not only be aware of a status of the system but also verify if the system is correctly configured.

6.2.1 Network Connection

To verify if your system is correctly connected to the network, use the **ping** command. For IP network, this command transmits a message to Internet Control Message Protocol (ICMP). ICMP is an internet protocol that notifies fault situation and provides information on the location where IP packet is received. When the ICMP echo message is received at the location, its replying message is returned to the place where it came from.

To perform a ping test to verify network status, use the following command.

Command	Mode	Description
ping [*A.B.C.D*]	Enable	Performs a ping test to verify network status.
ping ipv6 *X:X::X:X* [{**gigabitethernet** | **tengigabitethernet** | **gpon** | **channelgroup**} *IFPORTS*]		Performs a ping test to verify IPv6 network status.

The followings are the available options to perform the **ping** command.

Items	Description
Protocol [ip]	Supports ping test. The default is IP.
Target IP address	Sends ICMP echo message by inputting IP address or host name of destination in order to verify network status.
Repeat count [5]	Sends ICMP echo message as many as count. The default is 5.
Datagram size [100]	Ping packet size. The default is 100 bytes.
Timeout in seconds [2]	It is considered as successful ping test if reply returns within the configured time interval. The default is 2 seconds.
Extended commands [n]	Adds the additional options. The default is no.

Tab. 6.2 Options for Ping

The following is an example of ping test 5 times to verify network status with IP address 10.55.193.110.

```
SWITCH# ping
Protocol [ip]: ip
Target IP address: 10.55.193.110
Repeat count [5]: 5
Datagram size [100]: 100
Timeout in seconds [2]: 2
Extended commands [n]: n
PING 10.55.193.110 (10.55.193.110) 100(128) bytes of data.
108 bytes from 10.55.193.110: icmp_seq=1 ttl=255 time=0.058 ms
108 bytes from 10.55.193.110: icmp_seq=2 ttl=255 time=0.400 ms
108 bytes from 10.55.193.110: icmp_seq=3 ttl=255 time=0.403 ms
```

```
108 bytes from 10.55.193.110: icmp_seq=4 ttl=255 time=1.63 ms
108 bytes from 10.55.193.110: icmp_seq=5 ttl=255 time=0.414 ms

--- 10.55.193.110 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 8008ms
rtt min/avg/max/mdev = 0.058/0.581/1.632/0.542 ms
SWITCH#
```

When multiple IP addresses are assigned to the switch, sometimes you need to verify the connection status between the specific IP address and network status.

In this case, use the same process as ping test and then input the followings after extended commands. It is possible to verify the connection between specific IP address and network using the following command.

The following is the information to use ping test for multiple IP addresses.

Items	Description
Source address or interface	Designates the address where the relative device should respond in source IP address.
Type of service [0]:	The service filed of QoS (Quality Of Service) in Layer 3 application. It is possible to designate the priority for IP packet.
Data pattern [0xABCD]	Configures the data pattern to be used for pinging. Default is 0xABCD.

Tab. 6.3 Options for Ping for Multiple IP Addresses

The following is to verify network status between 10.45.239.203 and 10.55.193.110 when IP address of the switch is configured as 10.45.239.203.

```
SWITCH# ping
Protocol [ip]:ip
Target IP address: 10.55.193.110
Repeat count [5]: 5
Datagram size [100]: 100
Timeout in seconds [2]: 2
Extended commands [n]: y
Source address or interface: 10.45.239.203
Type of service [0]: 0
Data pattern [0xABCD]: 0xABCD
PATTERN: 0xabcd
PING 10.55.193.110 (10.55.193.110) from 10.45.239.203 : 100(128) bytes of data.
108 bytes from 10.55.193.110: icmp_seq=1 ttl=255 time=30.4 ms
108 bytes from 10.55.193.110: icmp_seq=2 ttl=255 time=11.9 ms
108 bytes from 10.55.193.110: icmp_seq=3 ttl=255 time=21.9 ms
108 bytes from 10.55.193.110: icmp_seq=4 ttl=255 time=11.9 ms
108 bytes from 10.55.193.110: icmp_seq=5 ttl=255 time=30.1 ms

--- 10.55.193.110 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 8050ms
rtt min/avg/max/mdev = 11.972/21.301/30.411/8.200 ms
SWITCH#
```

6.2.2 IP ICMP Source Routing

If you implement PING test to verify the status of network connection, ICMP request arrives at the final destination as the closest route according to the routing theory.

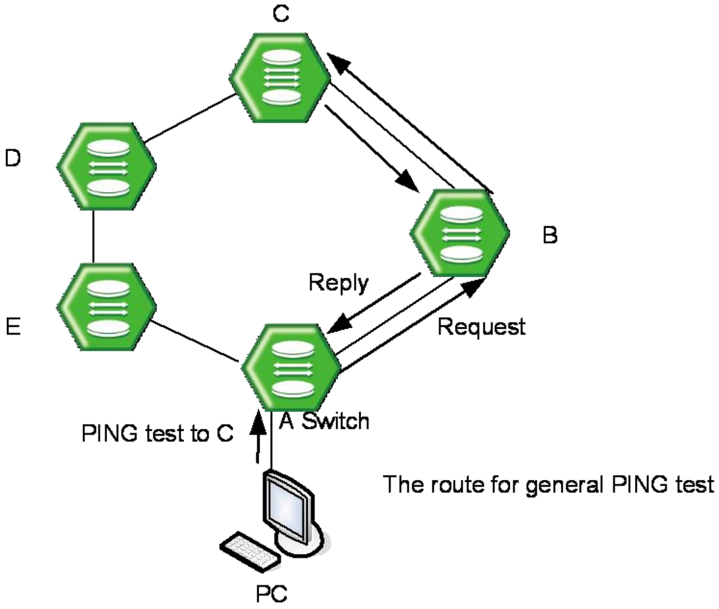


Fig. 6.1 Ping Test for Network Status

In Fig. 6.2, if you perform ping test from PC to C, it goes through the route of **A→B→C**. This is the general case. But, the LD3032 can enable to perform ping test from PC as the route of **A→E→D→C**.

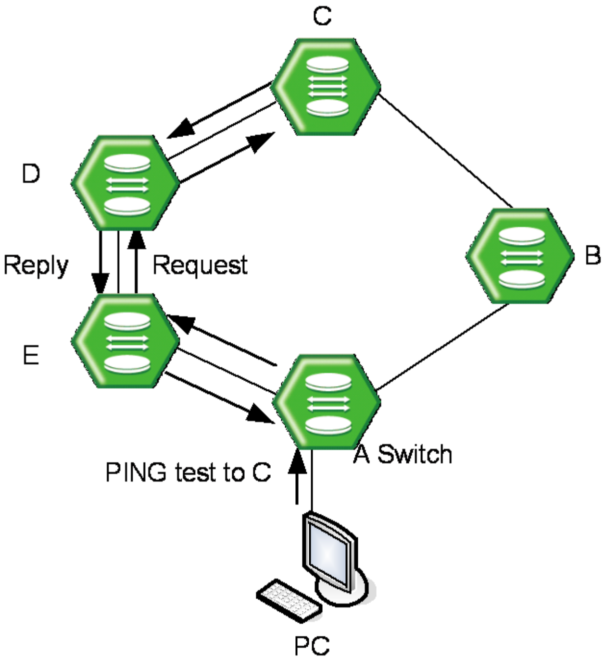


Fig. 6.2 IP Source Routing

To perform ping test as the route which the manager designated, use the following steps.

Step 1 Enable IP source-routing function from the equipment connected to PC which the PING test is going to be performed.

To enable/disable IP source-routing in the LD3032, use the following command.

Command	Mode	Description
ip icmp source-route	Global	Enable IP source-routing function.
No ip icmp source-route		Disable IP source-routing function.

Step 2 Perform the ping test from PC as the designate route with the **ping** command.

6.2.3 Tracing Packet Route

You can discover the routes that packets will actually take when traveling to their destinations. To do this, the **traceroute** command sends probe datagrams and displays the round-trip time for each node.

If the timer goes off before a response comes in, an asterisk (*) is printed on the screen.

Command	Mode	Description
traceroute [*DESTINATION*]	Enable	Traces packet routes through the network. WORD: destination IP address or host name A.B.C.D: destination IP address X:X::X:X: IPv6 address to be traced
traceroute ip *A.B.C.D*		
traceroute ipv6 *X:X::X:X*		

The followings are the configurable options to trace the routes.

Items	Description
Protocol [ip]	Supports ping test. Default is IP.
Target IP address	Sends ICMP echo message by inputting IP address or host name of destination in order to check network status with relative.
Source address	Source IP address which other side should make a response.
Numeric display [n]	Hop is displayed the number instead of indications or statistics.
Timeout in seconds [2]	It is considered as successful ping test if reply returns within the configured time interval. Default is 2 seconds.
Probe count [3]	Set the frequency of probing UDP packets.
Maximum time to live [30]	The TTL field is reduced by one on every hop. Set the time to trace hop transmission (The number of maximum hops). Default is 30 seconds.
Port Number [33434]	Selects general UDP port to be used for performing to trace the routes. The default is 33434.

Tab. 6.4 Options for Tracing Packet Route

The following is an example of tracing packet route sent to 10.55.193.104.

```
SWITCH# traceroute 10.55.193.104
traceroute to 10.55.193.104 (10.55.193.104), 30 hops max, 40 byte packets
 1  10.45.239.254 (10.45.239.254)  2.459 ms  1.956 ms  1.781 ms
 2  10.45.191.254 (10.45.191.254)  1.114 ms  2.112 ms  1.786 ms
 3  10.45.1.254 (10.45.1.254)  2.723 ms  2.604 ms  1.767 ms
 4  10.55.1.1 (10.55.1.1)  2.532 ms  2.522 ms  1.793 ms
 5  10.55.1.1 (10.55.1.1)  1.623 ms  0.879 ms  1.755 ms
 6  10.55.193.104 (10.55.193.104)  9.375 ms  3.817 ms  2.514 ms
SWITCH#
```

6.2.4 Displaying User Connecting to System

To display current users connecting to the system from a remote place or via console interface, use the following command.

Command	Mode	Description
where	Enable	Shows current users connecting to the system from a remote place or via console interface.

The following is an example of displaying current users connecting to the system.

```
SWITCH# where
admin at ttyp0 from 10.20.1.32:2196 for 30 minutes 35.56 seconds
admin at ttyS0 from console for 28 minutes 10.90 seconds
SWITCH#
```

6.2.5 MAC Table

To display MAC table recorded in specific port, use the following command.

Command	Mode	Description
show mac	Enable Global Interface-all	Shows MAC table. PORTS: port number
show mac interface {**channelgroup** | **gpon** | **gigabitethernet** | **tengigabitethernet** | **vlan** } *IFPORTS*		

6.2.6 System Running Time

To display the system running time, use the following command.

Command	Mode	Description
show uptime	Enable Global	Shows the system running time.

The following is an example of displaying the system running time.

```
SWITCH# show uptime
10:41am up 15 days, 10:55, 0 users, load average: 0.05, 0.07, 0.01
SWITCH#
```

6.2.7 System Information

To display the system information, use the following command.

Command	Mode	Description
show system	Enable Global	Shows the system information.

The following is an example of displaying the system information of the LD3032.

```
SWITCH(config)# show system

SysInfo(System Information)

    Model Name         : LD3032_SFU
    Main Memory Size    : 2048 MB
    Flash Memory Size    : 8 MB(SPANSION 29GL064), 64 MB(SPANSION 29GL512), 64
MB(SPANSION 29GL512)
    H/W Revision       : DS-TN-24V-A0
    H/W Address        : 00:d0:cb:00:0e:c0
    Serial Number      : N/A
    NOS Version        : 1.01
    B/L Version        : 4.76
    PLD Version        : 0x10
```

```
        Manufacturer       : ALPHA in China
        Manufacture Data   : N/A, N/A

    SWITCH(config)#
```

6.2.8 System Memory Information

To display a system memory status, use the following command.

Command	Mode	Description
show memory [**all**]	Enable Global	Shows system memory information.
show memory {**bgp** | **dhcp** | **eqm** | **free** | **gpon** | **hwmon** | **imi** | **ipv6** | **lib** | **nsm** | **ospf** | **pim** | **pim6** | **pppoe** | **recp** | **rip** | **sfpmon** | **summary** | **swch**}		Shows system memory information with a specific option.

To configure a debugging for dynamic memory trace, use the following command.

Command	Mode	Description
debug memory mtrace *DAEMON* { **start** | **end**}	Enable	Enables/disables the debugging for dynamic memory trace of the specified daemon. DAEMON: daemon name
show debug memory mallinfo *DAEMON*		Displays the debugging of dynamic memory allocation information.

6.2.9 CPU Packet Limit

If the CPU of the system processes too many packets during the operation, it may cause the performance decrease. To prevent the CPU overload, you can manually limit the number of the packets handled by CPU.

To limit the number of the packets handled by CPU, use the following command.

Command	Mode	Description
cpu packet limit <100-20000>	Global	Limits the number of the packets handled by CPU. 100-20000: incoming packets per second to CPU (defulat : 3500)
cpu packet limit <0-7> <100-20000>		Limits the number of the packets handled by CPU. 0-7 : Queue number 100-20000: incoming packets per second to CPU (defulat : unlimited)
no cpu packet limit [<0-7>]		Deletes the configured numbers of incoming packets per second to CPU.

To display the configured CPU packet limit, use the following command.

Command	Mode	Description
show cpu packet limit	Enable Global	Shows the configured CPU packet limit.

The LD3032 provides CPU storm control feature for mass ARP, DHCP, and IGMP packet. Generally, wrong network configuration, hardware malfunction, virus and so on cause these kinds of mass packets. The packet storm occupies most of the bandwidth of the network, and that causes the network very unstable.

To enable/disable the CPU storm control, use the following command.

Command	Mode	Description
cpu-storm {**arp** | **dhcp** | **igmp** | **pim**} **rate** <2-2000>	Global	Enables ARP, DHCP or IGMP packet storm control respectively in CPU with a user defined rate. 2-2000: Bandwidth in steps of 1 packet per second (unit: pps)
no cpu-storm {**arp** | **dhcp** | **igmp** | **pim**}		Disables ARP, DHCP or IGMP packet storm control in CPU.

To display the configuration of the CPU storm control, use the following command.

Command	Mode	Description
show cpu-storm	Global	Displays the configuration of the CPU storm control.

6.2.9.1 Slowpath Filtering

The LD3032 provides a slowpath packet filtering feature for incoming/outgoing traffic management to/from CPU. You have to create a filter first and set the packet classification criteria and the policy. You can use physical port ID, 802.1p priority (CoS), VLAN ID, 802.1q tag, and so on to classify the CPU packets. After applying the CPU packet filter, it classifies the packets, and processes the traffic according to user-defined policies.

To open *Slowpath Packet Filtering Configuration* mode, use the following command.

Command	Mode	Description
slowpath-filter *FILTER_NAME*	Global	Creates a slowpath packet filter. FILTER_NAME: slowpath packet filter name
no slowpath-filter { *NAME* | **all** }		Deletes the configured slowpath packet filter.

After entering slowpath packet filtering mode, the prompt changes from SWITCH(config)# to SWITCH(slowpath-filt[*NAME*])#.

After entering *Slowpath Packet Filtering Configuration* mode, the filtering parameters can be configured by user. The filter match, filter priority, filter action, stage and policy can be configured for each slowpath packet filter.

To configure one or more packet filter match pattern(s), use the following command.

Command	Mode	Description
match vid <1-4094> [**tag-position** <1-8>]	SP-Filter	Classifies a VLAN ID. VLAN: VLAN ID
match cos <0-7>		Classifies a queue of CPU RX/TX packets. 0-7: CoS queue number
match interface {**management** | **vlan** *VLANS* | **loopback** | **gigabitethernet** *IFPORT* | **tengigabitethernet** *IFPORT* | **gpon** *IFPORT* | **channelgroup** *GROUP*}		Classifies an interface.
match 802dot1q tpid { - | *TPID* } **pcp** { - | <0-7> } **vid** { - | <1-4094> } [**tag-position** <1-8>]		Classifies an 802.1q tag. tpid: tag protocol ID TPID: tag protocol ID (ex: 8100) pcp: priority code point tag-position: VLAN tag position -: any
match offset <0-127> **data** *HEX* [{ **desc** *DESC* | **mask** *MASK* [**desc** *DESC*]}]		Classifies an offset. 0-127: begin position, max 127 bytes HEX: hex value (ex: ffaa, up to 16 bytes) MASK: hex value (ex: f0f0) DESC: description up to 16 bytes
match offset <0-127> **length** <1-16> **data** *HEX* [**mask** *MASK*]		
match ethertype { **ip** | **arp** | *ETHERTYPE*}		Classifies a protocol based VLAN Ethernet type. ETHERTYPE: selects Ethernet type (hex digit: 0806)
match protocol { **icmp** | **igmp** [**reportv2** | **reportv1** | **leave** | **query**]}		Classifies an IGMP/ICMP packet.
Match protocol { **tcp** | **udp**} [{**srcport** *PORT* | **dstport** *PORT*}]		Classifies an TCP/UDP packet.

To delete the configured slow path filter match pattern(s), use the following command.

Command	Mode	Description
no match vid <1-4094> [**tag-position** <1-8>]	SP-Filter	Deletes a specified packet-classifying pattern for each option.
No match cos <0-7>		
no match interface {**management** | **vlan** *VLANS* | **loopback** | **gigabitethernet** *IFPORT* | **tengigabitethernet** *IFPORT* | **gpon** *IFPORT* | **channelgroup** *GROUP*}		
no match 802dot1q tpid { - | *TPID* } **pcp** { - | <0-7> } **vid** { - | <1-4094>} [**tag-position** <1-8>]		
no match offset <0-127> **data** *HEX* [**mask** *MASK*]		
no match ethertype { **ip** | **arp** | *ETHERTYPE*}		

Command	Mode	Description
no match protocol { **icmp** | **igmp**}		
no match protocol { **tcp** | **udp**} [{**srcport** *PORT* | **dstport** *PORT*}]		

To specify the action policy of slowpath packet filter for the packets matching the configured match patterns, use the following command.

Command	Mode	Description
action {**permit** | **drop**}	SP-Filter	Specifies a drop or permit statement of the CPU packet filter with the configured match pattern. permit: permits the traffic of entries drop: discards the traffic of entries
action {**802dot1q** | **802dot1q-attach**} **tpid** { - | *TPID* } **pcp** { - | <0-7> } **vid** { - | <1-4094> } [**tag-position** <1-8>]		Configures the action to be taken according to the 802.1q tag. 802dot1q: translates 802.1q tag 802dot1q-attach: attaches 802.1q tag 802dot1q-detach: detaches 802.1q tag tpid: tag protocol ID TPID: tag protocol ID (ex: 8100) pcp: priority code point VLAN: VLAN ID, 1 to 4094 tag-position: VLAN tag position -: any
action 802dot1q-detach [**tag-position** <1-8>]		
action rate-limit <1-1000> **burst-size** <1-1000>		Sets the bandwidth for classified packets belonging to specified CPU packet filter 1-1000: permits the number of packets per second 1-1000: size that can be store token

If two or more created slow packet filters match the same packet then the filter having a higher priority will be processed first. To specify a priority of the slow packet filter, use the following command.

Command	Mode	Description
priority <1-65535>	SP-Filter	Sets the priority for the slowpath packet filter. 1-65535: value of priority

To choose the direction of packets to be applied by the configured slowpath packet filter, use the following command.

Command	Mode	Description
stage {**cpu-tx** | **cpu-rx** | **vid-assigned**}	SP-Filter	Selects a type of slowpath packets to be applied by the user-defined filtering policy. cpu-tx: filtering for outgoing packets from CPU cpu-rx: filtering for incoming packets to CPU vid-assigned: filtering for the incoming packets after matching VLAN ID assigned

apply		Saves and applies the configured slowpath packet filter

To display the configured slowpath packet filter, use the following command.

Command	Mode	Description
show slowpath-filter [*NAME*]	Enable Global SP-Filter	Shows the configured slowpath packet filter.
show running-config slowpath-filter		Shows the running configuration for slowpath packet filter.

To clear the collected statistics counter of slowpath packet filter, use the following command.

Command	Mode	Description
clear slowpath-filter stats [*NAME*]	Global SP-Filter	Resets the collected statistics counters of slowpath packet filter.

6.2.9.2 CPU Statistics

To display the statistics of the traffic handled by CPU, use the following command.

Command	Mode	Description
show cpu statistics avg-pkt [{**gigabitethernet** | **tengigabitethernet** | **gpon** } *IFPORTS*]	Enable Global	Shows the statistics of the traffic handled by CPU per packet type.
Show cpu statistics total [{**gigabitethernet** | **tengigabitethernet** | **gpon** } *IFPORTS*]		Shows the traffic statistics of the average packet handled by CPU.
Show cpu counters [{**gigabitethernet** | **tengigabitethernet** | **gpon** | **channelgroup**} *IFPORTS* | **vlan** *VLAN*]		Shows the incoming traffic statistics to CPU according to protocol types.
Show cpu counters avg [{**gigabitethernet** | **tengigabitethernet** | **gpon** | **channelgroup**} *IFPORTS* | **vlan** *VLAN*]		Shows the incoming traffic statistics average to CPU according to protocol types.

To delete the collected statistics of the traffic handled by CPU, use the following command.

Command	Mode	Description
clear cpu statistics [{**gigabitethernet** | **tengigabitethernet** | **gpon** } *IFPORTS*]	Global	Deletes the collected statistics of the traffic handled by CPU.

The LD3032 can be configured to generate a syslog message when the number of the packets handled by CPU exceeds a specified value. This function allows system administrators to monitor the switch and network status more effectively. To configure the switch to generate a syslog message according to the number of the packets handled by CPU, use the following command.

Command	Mode	Description
cpu statistics-limit {**unicast** | **multicast** | **broadcast**} <10-100>	Interface [XE/GE/GPON]	Generates a syslog message according to the specified number of the packets handled by CPU. This is configurable for each packet type and physical port. unicast | multicast | broadcast: packet type 10-100: packet count (actual value: 1000-10000)

To disable the switch to generate a syslog message according to the number of the packets handled by CPU, use the following command.

Command	Mode	Description
no cpu statistics-limit {**unicast** | **multicast** | **broadcast** | **all**}	Interface [XE/GE/GPON]	Disables the switch to generate a syslog message according to the number of the packets handled by CPU for each packet type. all: all physical ports

To display a configured value to generate a syslog message according to the number of the packets handled by CPU, use the following command.

Command	Mode	Description
show cpu statistics-limit	Enable Global	Shows a configured value to generate a syslog message according to the number of the packets handled by CPU.

6.2.10 Running Process

The LD3032 provides a function that shows information of the running processes. The information with this command can be very useful to manage the switch.

To display information of the running processes, use the following command.

Command	Mode	Description
show process	Enable Global	Shows information of the running processes.

The following is an example of displaying information of the running processes.

```
SWITCH# show process
USER     PID  %CPU  %MEM     VSZ   RSS  TTY   STAT   START  TIME  COMMAND
```

```
admin     1  0.2  0.2   1448   592  ?    S     20:12  0:05  init [3]
admin     2  0.0  0.0      0     0  ?    S     20:12  0:00  [keventd]
admin     3  0.0  0.0      0     0  ?    SN    20:12  0:00  [ksoftirqd_CPU0]
admin     4  0.0  0.0      0     0  ?    S     20:12  0:00  [kswapd]
admin     5  0.0  0.0      0     0  ?    S     20:12  0:00  [bdflush]
admin     6  0.0  0.0      0     0  ?    S     20:12  0:00  [kupdated]
admin     7  0.0  0.0      0     0  ?    S     20:12  0:00  [mtdblockd]
admin     8  0.0  0.0      0     0  ?    SW<   20:12  0:00  [bcmDPC]
admin     9  1.4  0.0      0     0  ?    SW<   20:12  0:29  [bcmCNTR.0]
admin    10  1.4  0.0      0     0  ?    SW<   20:12  0:29  [bcmCNTR.1]
admin    17  0.0  0.0      0     0  ?    SWN   20:12  0:00  [jffs2_gcd_mtd3]
admin   149  0.0  0.3   1784   776  ?    S     Jan01  0:00  /sbin/syslogd -m
admin   151  0.0  0.2   1428   544  ?    S     Jan01  0:00  /sbin/klogd -c 1
admin   103  2.6  2.0  20552  5100  ?    S     20:12  0:53  /usr/sbin/swchd

(Omitted)

SWITCH#
```

6.2.11 Displaying System Software

To display a current system software version, use the following command.

Command	Mode	Description
show version	Enable Global	Shows a version of system software.

To display a size of the current system software, use the following command.

Command	Mode	Description
show os-size	Enable Global	Shows a size of system software.

6.2.12 Displaying Installed OS

To display the current usage of the system flash memory, use the followng command.

Command	Mode	Description
show flash	Enable Global	Shows the current usage of the system flash memory.

6.2.13 Default OS

The LD3032 supports the dual OS feature. You can verify the running OS in the flash memory with the **show flash** command. When two system Oss are installed, you can set one of those as the default OS.

To set the default OS of the system, use the following command.

Command	Mode	Description

default-os {**os1** | **os2**}	Enable	Sets the default OS of the system. (default: os1)

6.2.14 Switch Status

To display the temperature of switch, power status, and fan status, use the following command.

Command	Mode	Description
show status fan	Enable Global	Shows the fan status of the switch.
show status power		Shows the current power status.
show status temp		Shows the current temperature of the switch.
show environment		Shows fan status and temperature of switch.
show status alarm		Shows the alarm-IN/OUT status.

6.2.15 Forwarding Information Base (FIB) Table

The FIB is a table that contains a mirror image of the forwarding information in the IP routing table. When routing or topology changes occur in the network the route processor updates the IP routing table and the information updates the FIB. Because there is a one-to-one correlation between FIB entries and routing table entries, the FIB contains all known routes and eliminates the need for route cache maintenance that is associated with switching paths, such as fast switching and optimum switching. FIB is used for making IP destination prefix-based switching decisions and maintaining next-hop address information based on the information in the IP routing table.

The forwarding information base (FIB) table contains information that the forwarding processors require to make IP forwarding decisions.

The forwarding information base (FIB) is the group of the information to forward traffic in Layer 3, which is created from Routing Information Base (RIB) on the CPU. You can verify the forwarding entries in the FIB table with the **show ip route fib** command. To specify the time to retain the forwarding entries information in the FIB table, use the following command.

Command	Mode	Description
fib retain forever	Global	Retains the forwarding entries in the FIB constantly.
fib retain time <1-65535>		Retains the forwarding entries in the FIB for specific seconds: 1-65535: time value in second

To delete the specified time for retaining the forwarding entries information, use the following command.

Command	Mode	Description
no fib retain forever	Global	Deletes the specified time to retain the forwarding entries in the FIB.
no fib retain time <1-65535>		

To display the forwarding entries in the FIB table on the switching fabric, use the following command.

Command	Mode	Description
show ip route fib	Enable Global	Shows the forwarding entries in the FIB table.

To set the multipath numbers installed to FIB, use the following command.

Command	Mode	Description
ip maximum-paths <1-8>	Global	Sets multipath numbers that installed to the Forwarding Information Base(FIB) 1-8: the numbers of multipath supported (default:4)

6.2.16 Tech Support Information

For various reason, a system error may occur. Once the system error occurs, system engineers try to examine the internal system information such as a system configuration, log data, memory dump, and so on to solve the problem.

To reduce the effort to acquire the detail informtation of the system for a technical suppport, the LD3032 provides the function that generates all the system information reflecting the current state. Using this function, you can verify all the details on a console screen or even in the remote place via FTP/TFTP.

To generate the tech-support information, use the following command.

Command	Mode	Description
tech-support {**all** | **crash-info**} **console**	Enable	Generates the tech-support information on a console screen.
tech-support {**all** | **crash-info**} **remote** *A.B.C.D* {**ftp** | **tftp**}		Generates the tech-support information in the remote place via FTP or TFTP. The name of the generated information file is **a.info**. (This is not changeable.)

In case of generating the tech-support information on a console screen, the contents will be displayed without the screen pause regardless of your terminal configuration.

6.2.17 System Boot Information

To display the information of the last system boot, use the following command.

Command	Mode	Description
show boot-info	Enable Global	Shows the information of the last system boot.

6.2.18 Network Service Module (NSM) Informtaion

To display the information of the NSM Client, use the following command.

Command	Mode	Description
show nsm client	Enable Global	Shows the information of the NSM client.

6.2.19 Network Service Module (NSM) Daemon Debugging

To enable NSM daemon debugging, use the following command.

Command	Mode	Description
debug nsm [**all**]	Enable	Enables NSM debugging. all: all NSM debugging
debug nsm {**events** | **kernel**}		Enables NSM events/kernel debugging.
debug nsm packet {**send** | **recv**} [**detail**]		Enables NSM packets debugging. packet: NSM packets send: outgoing packets recv: incoming packets detail: detailed information
debug nsm packet [**detail**]		

To disable NSM debugging, use the following command.

Command	Mode	Description
no debug nsm [**all**]	Enable	Disables NSM debugging.
no debug nsm {**events** | **kernel**}		
no debug nsm packet {**send** | **recv**} [**detail**]		
no debug nsm packet [**detail**]		

To display the debugging information, use the following command.

Command	Mode	Description
show debugging nsm	Enable Global	Shows the debugging information of NSM.

To disable all debugging, use the following command.

Command	Mode	Description
no debug all [ipv6 | nsm | ospf | rip]	Enable	Disables all debugging.

6.2.20 Protocol Statistics Information

To enables/disables the system to collect the statistics of the protocols, use the following command.

Command	Mode	Description
protocol statistics {**enable** | **disable**} [**arp** | **icmp** | **ip** | **tcp** | **udp**]	Global	Enables/disables the system to collect the statistics of the protocols. (ARP, ICMP, IP, TCP, UDP)

To display the statistics of the protocol, use the following command.

Command	Mode	Description
show protocol statistics avg-pkt [{**channelgroup** | **gpon** | **gigabitethernet** | **tengigabitethernet** | **vlan** } *IFPORT*]	Enable Global	Shows the statistics of the protocol for average packets.
show protocol statistics total [{**channelgroup** | **gpon** | **gigabitethernet** | **tengigabitethernet** | **vlan** } *IFPORT*]		Shows the traffic statistics of the protocol for total packets.

To delete the collected statistics of the protocol, use the following command.

Command	Mode	Description
clear protocol statistics [{**channelgroup** | **gpon** | **gigabitethernet** | **tengigabitethernet** | **vlan** } *IFPORT*]	Global	Deletes the collected statistics of the protocol.

7 Network Management

7.1 Simple Network Management Protocol (SNMP)

The simple network management protocol (SNMP) is an application-layer protocol designed to facilitate the exchange of management information between network devices. SNMP consists of three parts: an SNMP manager, a managed device and an SNMP agent. SNMP provides a message format for sending information between SNMP manager and SNMP agent. The agent and MIB reside on the switch. In configuring SNMP on the switch, you define the relationship between the manager and the agent. According to community, you can give right only to read or right to both read and write. The SNMP agent has MIB variables to reply to requests from SNMP administrator. In addition, SNMP administrator can obtain data from the agent and save data in the agent. The SNMP agent gets data from MIB, which saves information on system and network.

SNMP agent sends a trap to administrator for specific cases. Trap is a warning message to alert network status to SNMP administrator.

The LD3032 enhances access management of SNMP agent and limits the range of OID opened to agents.

7.1.1 SNMP Service

To enable/disable SNMP service, use the following command.

Command	Mode	Description
service snmp	Global	Enables SNMP service.
no service snmp		Disables SNMP service. (default)

7.1.2 Restarting SNMP Deamon

To restart SNMP Deamon service, use the following command.

Command	Mode	Description
restart snmpd	Enable	Restarts SNMP deamon.

7.1.3 SNMP Community

Only an authorized person can access SNMP agent by configuring SNMP community with a community name and additional information.

To configure SNMP community to allow an authorized person to access, use the following command.

Command	Mode	Description
snmp community {**ro** | **rw**} *COMMUNITY* [*A.B.C.D*] [*OID*]	Global	Creates SNMP community. COMMUNITY: community name
no snmp community {**ro** | **rw**}		Deletes created community.

COMMUNITY		

You can configure up to 3 SNMP communities for each read-only and read-write.

To display configured SNMP community, use the following command.

Command	Mode	Description
show snmp community	Enable Global	Shows created SNMP community.

The following is an example of creating 2 SNMP communities.

```
SWITCH(config)# snmp community ro public
SWITCH(config)# snmp community rw private
SWITCH(config)# show snmp community

Community List
Type  Community        Source             OID
-----------------------------------------------
ro    public
rw    private

SWITCH(config)#
```

7.1.4 Information of SNMP Agent

You can specify the basic information of SNMP agent as administrator, location, and address that confirm its own identity.

To set the basic information of the SNMP agent, use the following command.

Command	Mode	Description
snmp contact *NAME*	Global	Sets the name of the administrator.
snmp location *LOCATION*		Sets the location of the SNMP agent.
snmp agent-address *A.B.C.D*		Sets an IP address of the SNMP agent.
no snmp contact		Deletes the specified basic information for each item.
no snmp location		
no snmp agent-address		

The following is an example of specifying basic information of SNMP agent.

```
SWITCH(config)# snmp contact Brad
SWITCH(config)# snmp location Germany
SWITCH(config)#
```

To display the basic information of the SNMP agent, use the following command.

Command	Mode	Description
show snmp contact	Enable	Shows the name of the administrator.

show snmp location	Global	Shows the location of the SNMP agent.
show snmp agent-address		Shows the IP address of the SNMP agent.

7.1.5 SNMP Com2sec

SNMP v2 authorizes the host to access the agent according to the identity of the host and community name. The **com2sec** command specifies the mapping from the identity of the host and community name to security name.

To configure an SNMP security name, use the following command.

Command	Mode	Description
snmp com2sec *SECURITY* {*IP-ADDRESS* | *IP-ADDRESS/M*} *COMMUNITY*	Global	Specifies the mapping from the identity of the host and community name to security name, enter security and community name. SECURITY: security name COMMUNITY: community name
no snmp com2sec *SECURITY*		Deletes a specified security name, enter the security name. SECURITY: security name
show snmp com2sec	Enable Global	Shows a specified security name.

The following is an example of configuring SNMP com2sec.

```
SWITCH(config)# snmp com2sec TEST 10.1.1.1 PUBLIC
SWITCH(config)# show snmp com2sec

Com2Sec List
SecName          Source             Community
------------------------------------------------
TEST             10.1.1.1           PUBLIC

SWITCH(config)#
```

7.1.6 SNMP Group

You can create an SNMP group that can access SNMP agent and its community that belongs to a group.

To create an SNMP group, use the following command.

Command	Mode	Description
snmp group *GROUP* {**v1** | **v2c** | **v3**} *SECURITY*	Global	Creates SNMP group, enter the group name. GROUP: group name SECURITY: security name
no snmp group *GROUP* [{**v1** | **v2c** | **v3**} [*SECURITY*]]		Deletes SNMP group, enter the group name. GROUP: group name
show snmp group	Enable Global	Shows a created SNMP group.

7.1.7 SNMP View Record

You can create an SNMP view record to limit access to MIB objects with object identity (OID) by an SNMP manager.

To configure an SNMP view record, use the following command.

Command	Mode	Description
snmp view *VIEW* {**included** | **excluded**} *OID* [*MASK*]	Global	Creates an SNMP view record. VIEW: view record name included: includes a sub-tree. excluded: excludes a sub-tree. OID: OID number
no snmp view *VIEW* [*OID*]		Deletes a created SNMP view record. VIEW: view record name

To display a created SNMP view record, use the following command.

Command	Mode	Description
show snmp view	Enable Global	Shows a created SNMP view record.

The following is an example of creating an SNMP view record.

```
SWITCH(config)# snmp view TEST included 410
SWITCH(config)# show snmp view

View List
ViewName         Type      SubTree / Mask
-------------------------------------------
TEST             included  410

SWITCH(config)#
```

7.1.8 Permission to Access SNMP View Record

To grant an SNMP group to access to a specific SNMP view record, use the following command.

Command	Mode	Description
snmp access *GROUP* {**v1** | **v2c**} *READ-VIEW WRITE-VIEW NOTIFY-VIEW*	Global	Grants an SNMP group to access a specific SNMP view record. GROUP: group name
snmp access *GROUP* **v3** {**no-auth** | **auth** | **priv**} *READ-VIEW WRITE-VIEW NOTIFY-VIEW*		Grants an SNMP version 3 group to access a specific SNMP view record. GROUP: group name
no snmp access *GROUP*		Deletes a granted SNMP group to access a specific SNMP view record.

To display a granted SNMP group to access to a specific SNMP view record, use the following command.

Command	Mode	Description
show snmp access	Enable Global	Shows a granted SNMP group to access to a specific SNMP view record.

7.1.9 SNMP Version 3 User

In SNMP version 3, you can register an SNMP agent as user. If you register an SNMP version 3 user, you should configure it with the authentication key.

To create/delete an SNMP version 3 user, use the following command.

Command	Mode	Description
snmp user *USER* {**md5** | **sha**} *AUTH_KEY* [**des** *PRIVATE_KEY*]	Global	Creates an SNMP version 3 user.
no snmp user *USER*		Deletes a registered SNMP version 3 user.

To display a current SNMP version 3 user, use the following command.

Command	Mode	Description
show snmp user	Enable Global	Displays an SNMP version 3 user.

7.1.10 SNMP Trap

SNMP trap is an alert message that SNMP agent notifies SNMP manager about certain problems. If you configure the SNMP trap, the system transmits pertinent information to network management program. In this case, trap message receivers are called a trap host.

7.1.10.1 SNMP Trap Mode

To select the SNMP trap mode, use the following command.

Command	Mode	Description
snmp trap-mode {**alarm-report** | **event**}	Global	Selects the SNMP trap mode. alarm-report: alarm report based trap event: event based trap (default)

7.1.10.2 SNMP Trap Host

To set an SNMP trap host, use the following command.

Command	Mode	Description

snmp trap-host *A.B.C.D* [*COMMUNITY*]	Global	Specifies an SNMP trap v1 host.
snmp trap2-host *A.B.C.D* [*COMMUNITY*]		Specifies an SNMP trap v2 host.
snmp inform-trap-host *A.B.C.D* [*COMMUNITY*]		Specifies an SNMP inform trap host.

To delete a specified SNMP trap host, use the following command.

Command	Mode	Description
no snmp trap-host *A.B.C.D*	Global	Deletes a specified SNMP trap v1 host.
no snmp trap2-host *A.B.C.D*		Deletes a specified SNMP trap v2 host.
no snmp inform-trap-host *A.B.C.D*		Deletes a specified SNMP inform trap host.

You can set maximum 16 SNMP trap hosts with inputting one by one.

The following is an example of setting an SNMP trap host.

```
SWITCH(config)# snmp trap-host 10.1.1.3
SWITCH(config)# snmp trap-host 20.1.1.5
SWITCH(config)# snmp trap-host 30.1.1.2
SWITCH(config)#
```

7.1.10.3 Enabling SNMP Trap

The system provides various kind of SNMP trap, but it may inefficiently work if all these trap messages are sent very frequently. Therefore, you can select each SNMP trap sent to an SNMP trap host.

- **auth-failure** is shown to inform wrong community is input when user trying to access to SNMP inputs wrong community.
- **cold-start** is shown when SNMP agent is turned off and restarts again.
- **link-up/down** is shown when network of port specified by user is disconnected, or when the network is connected again.
- **mem-threshold** is shown when memory usage exceeds the threshold specified by user. When memory usage falls below the threshold, the trap message will be shown to notify it.
- **cpu-threshold** is shown when CPU utilization exceeds the threshold specified by user. When CPU load falls below the threshold, trap message will be shown to notify it.
- **port-threshold** is shown when the port traffic exceeds the threshold configured by user. When port traffic falls below the threshold, trap message will be shown.
- **temp-threshold** is shown when the system temperature exceeds the thresh-old configured by user. when system temperature falls below the threshold, trap message will be shown.
- **dhcp-lease** is shown when no more IP address is left in the DHCP pool. Even if this

occurs only in one DHCP pool of several pools, this trap message will be shown.

- **fan/power/module** is shown when there is any status-change of fan, power, and module.

The system is configured to send all the SNMP traps by default.

To enable the SNMP trap, use the following command.

Command	Mode	Description
snmp trap auth-fail	Global	Configures the system to send SNMP trap when SNMP authentication is fail.
snmp trap cli-history		Configures the system to send SNMP trap of CLI history log.
snmp trap cold-start		Configures the system to send SNMP trap when SNMP agent restarts.
snmp trap cpu-threshold		Configures the system to send SNMP trap when CPU load exceeds or falls below the threshold.
snmp trap dhcp-lease		Configures the system to send SNMP trap when no more IP address is left in the DHCP pool.
snmp trap fan		Configures the system to send SNMP trap when the fan begins to operate or stops.
snmp trap link-threshold		Configures the system to send SNMP trap when interface link exceeds or falls below the threshold.
snmp trap linkstatus		Configures the system to send SNMP trap when there is any problem in link.
snmp trap mem-threshold		Configures the system to send SNMP trap when memory usage exceeds or falls below the threshold.
snmp trap module		Configures the system to send SNMP trap when there is any problem in module.
snmp trap power		Configures the system to send SNMP trap when any problem occurs in power.
snmp trap pps-control		Configures the system to send SNMP trap when the number of packets per second exceeds or falls below the PPS threshold.
snmp trap temp-threshold		Configures the system to send SNMP trap when system temperature exceeds or falls below the threshold.

7.1.10.4 Disabling SNMP Trap

To disable the SNMP trap, use the following command.

Command	Mode	Description
no snmp trap {**auth-fail** | **cli-history** | **cold-start** |	Global	Disables each SNMP trap.

link-threshold | **linkstatus** | **mem-threshold** | **cpu-threshold** | **temp-threshold** | **dhcp-lease** | **fan** | **power** | **pps-control** | **module**}		

7.1.10.5 Displaying SNMP Trap

To display the configuration of the SNMP trap, use the following command.

Command	Mode	Description
show snmp trap	Enable Global	Shows the configuration of SNMP trap.
show snmp alarm-report		Shows a collected alarm report based trap.

7.1.11 SNMP Alarm

The LD3032 provides an alarm notification function. The alarm will be sent to a SNMP trap host whenever a specific event in the system occurs through CLI. You can also set the alarm severity on each alarm and make the alarm be shown only in case of selected severity or higher. This enhanced alarm notification allows system administrators to manage the system efficiently.

7.1.11.1 Alarm Notify Activity

Normally the LD3032 is supposed to generate an alarm only when a pre-defined event has occurred such as the fan fail, system restart, temperature high, etc. However, you can additionally configure the system to generate an alarm when any configuration parameter has been changed via CLI.

To enable/disable the alarm notify activity, use the following command.

Command	Mode	Description
snmp notify-activity {**enable** | **disable**}	Global	Enables/disables the alarm notify activity. (default: disable)

7.1.11.2 Alarm Severity Criterion

You can set an alarm severity criterion to make an alarm be shown only in case of selected severity or higher. For example, if an alarm severity criterion has been set to **major**, you will see only an alarm whose severity is **major** or **critical**.

To set an alarm severity criterion, use the following command.

Command	Mode	Description
snmp alarm-severity criteria {**critical** | **major** | **minor** | **warning** | **intermediate**}	Global	Sets an alarm severity criterion. (default: warning)

i The order of alarm severity is **critical** > **major** > **minor** > **warning** > **intermediate**.

7.1.11.3 Default Alarm Severity

To set default alarm severity, use the following command.

Command	Mode	Description
snmp alarm-severity default {**critical** | **major** | **minor** | **warning** | **intermediate**}	Global	Sets default alarm severity. (default: minor)

7.1.11.4 Generic Alarm Severity

To set generic alarm severity, use the following command.

Command	Mode	Description
snmp alarm-severity fan-fail {**critical** | **major** | **minor** | **warning** | **intermediate**}	Global	Sets severity of an alarm for system fan failure.
snmp alarm-severity cold-start {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for system cold restart.
snmp alarm-severity broadcast-over {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for too much broadcast.
snmp alarm-severity cpu-load-over {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for CPU load high.
snmp alarm-severity dhcp-lease {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for no more IP address left in the DHCP pool.
snmp alarm-severity dhcp-illegal {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for illegal DHCP entry.
snmp alarm-severity fan-remove {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for system fan removed.
snmp alarm-severity ip-conflict {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for IP address conflict.
snmp alarm-severity memory-over {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for system memory usage high.
snmp alarm-severity mfgd-block {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for MAC flood guard block.
snmp alarm-severity pim-group-filter {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for pim group filtering.
snmp alarm-severity port-link-down {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for Ethernet port link down.
snmp alarm-severity port-remove {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for Ethernet port removed.
snmp alarm-severity port-thread-over {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for port thread over.
snmp alarm-severity power-fail {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for system power failure.
snmp alarm-severity power-remove {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for system power removed.

snmp alarm-severity rmon-alarm-rising {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for RMON alarm rising.
snmp alarm-severity rmon-alarm-falling {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for RMON alarm falling.
snmp alarm-severity system-restart {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for system restart.
snmp alarm-severity module-remove {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for module removed.
snmp alarm-severity temperature-high {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for system temperature high.

To delete configured alarm severity, use the following command.

Command	Mode	Description
no snmp alarm-severity fan-fail	Global	Deletes configured alarm severity.
no snmp alarm-severity cold-start		
no snmp alarm-severity broadcast-over		
no snmp alarm-severity cpu-load-over		
no snmp alarm-severity dhcp-lease		
no snmp alarm-severity dhcp-illegal		
no snmp alarm-severity fan-remove		
no snmp alarm-severity ip-conflict		
no snmp alarm-severity memory-over		
no snmp alarm-severity mfgd-block		
no snmp alarm-severity pim-group-filter		
no snmp alarm-severity port-link-down		
no snmp alarm-severity port-remove		
no snmp alarm-severity port-thread-over		
no snmp alarm-severity power-fail		
no snmp alarm-severity power-remove		
no snmp alarm-severity rmon-alarm-rising		
no snmp alarm-severity rmon-alarm-falling		
no snmp alarm-severity system-restart		
no snmp alarm-severity module-remove		
no snmp alarm-severity temperature-high		

7.1.11.5 ADVA Alarm Severity

To set ADVA alarm severity, use the following command.

Command	Mode	Description
snmp alarm-severity adva-fan-fail {**critical** | **major** | **minor** | **warning** | **intermediate**}	Global	Sets ADVA severity of an alarm for system temperature high.

snmp alarm-severity adva-if-misconfig {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets ADVA severity of an alarm for wrong configuration.
snmp alarm-severity adva-if-opt-thres {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets ADVA severity of an alarm for traffic threshold over for an Ethernet optical interface.
snmp alarm-severity adva-if-rcv-fail {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets ADVA severity of an alarm for failure to receive packets.
snmp alarm-severity adva-if-trans-fault {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets ADVA severity of an alarm for failure to transmit packets.
snmp alarm-severity adva-if-sfp-mismatch {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets ADVA severity of an alarm for SFP module mismatched.
snmp alarm-severity adva-psu-fail {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets ADVA severity of an alarm for PSU failure.
snmp alarm-severity adva-temperature {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets ADVA severity of an alarm for system temperature high.
snmp alarm-severity adva-voltage-high {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets ADVA severity of an alarm for input voltage high.
snmp alarm-severity adva-voltage-low {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets ADVA severity of an alarm for input voltage low.

To delete configured ADVA alarm severity, use the following command.

Command	Mode	Description
no snmp alarm-severity adva-fan-fail	Global	Deletes configured ADVA alarm severity.
no snmp alarm-severity adva-if-misconfig		
no snmp alarm-severity adva-if-opt-thres		
no snmp alarm-severity adva-if-rcv-fail		
no snmp alarm-severity adva-if-sfp-mismatch		
no snmp alarm-severity adva-if-trans-fault		
no snmp alarm-severity adva-psu-fail		
no snmp alarm-severity adva-temperature		
no snmp alarm-severity adva-voltage-high		
no snmp alarm-severity adva-voltage-low		

7.1.11.6 STP Guard Alarm Severity

To set severity of an alarm for STP guard, use the following command.

Command	Mode	Description
snmp alarm-severity stp-bpdu-guard {**critical** | **major** | **minor** | **warning** | **intermediate**}	Global	Sets severity of an alarm for BPDU guard disabled.
snmp alarm-severity stp-root-		Sets severity of an alarm for root guard disabled.

guard {**critical** | **major** | **minor** | **warning** | **intermediate**}		

To delete configured severity of alarm for STP guard, use the following command.

Command	Mode	Description
no snmp alarm-severity stp-bpdu-guard	Global	Deletes configured severity of an alarm for STP guard.
no snmp alarm-severity stp-root-guard		

7.1.11.7 Displaying SNMP Alarm

To display a collected alarm, use the following command.

Command	Mode	Description
show snmp alarm-severity	Enable Global	Shows a configured alarm severity.
show snmp alarm-history		Shows a collected alarm history.
show snmp alarm-report		Shows a collected alarm report.

To delete a collected alarm in the system, use the following command.

Command	Mode	Description
snmp clear alarm-history	Global	Deletes a collected alarm history in the system.
snmp clear alarm-report		Deletes a collected alarm report in the system.

7.1.12 Displaying SNMP Configuration

An SNMP OID is assigned to an individual object within a Management Information Base (MIB). To search the available SNMP OID, use the following command.

Command	Mode	Description
show snmp-mib-registry {all | bgp | dhcp | eap | eqm | gpon | hwmon | imi | nsm | ospf | ospf6 | pim | rip | sflow | sfpmon | snmp | swch | vrrp }	Enable	Shows the available SNMP OID value.

To display a history about SetRequest of SNMP, use the following command.

Command	Mode	Description
show snmp history	Global	Shows a collected setrequest history in the system.
clear snmp history		Deletes a collected setrequest history in the system.

7.1.13 Disabling SNMP

To disable SNMP, use the following command.

Command	Mode	Description
no snmp	Global	Disables SNMP.

⚠ When you use the **no snmp** command, all configurations of SNMP will be lost.

7.2 Link Layer Discovery Protocol (LLDP)

Link Layer Discovery Protocol (LLDP) is the function of transmitting data for network management for the switches connected in LAN according to IEEE 802.1ab standard.

7.2.1 LLDP Operation

The LD3032 supporting LLDP transmits the management information between near switches. The information carries the management information that can recognize the network elements and the function. This information is saved in internal Management Information Base (MIB).

When LLDP starts to operate, the switches send their information to near switches. If there is some change in local status, it sends their changed information to near switch to inform their status. For example, if the port status is disabled, it informs that the port is disabled to near switches. And the switch that receives the information from near switches processes LLDP frame and saves the information of the other switches. The information received from other switches is aged.

7.2.2 Enabling LLDP

To enable/disable LLDP, use the following command.

Command	Mode	Description
lldp enable	Interface [XE/GPON]	Enables LLDP function on a port.
lldp disable		Disables LLDP function.

7.2.3 LLDP Operation Type

If you activated LLDP on a port, configure LLDP operation type.

Each LLDP operation type works as one of the followings:

- **both** sends and receive LLDP frame.
- **tx_only** only sends LLDP frame.
- **rx_only** only receives LLDP frame.
- **disable** does not process any LLDP frame.

To configure how to operate LLDP, use the following command.

Command	Mode	Description
lldp adminstatus {**both** | **tx_only** | **rx_only** | **disable**}	Interface [XE/GPON]	Configures LLDP operation type. (default: both)

7.2.4 Basic TLV

LLDP is transmitted through TLV. There are mandatory TLV and optional TLV. In optional TLV, there are basic TLV and organizationally specific TLV. Basic TLV must be in the switch where LLDP is realized, specific TLV can be added according to the feature of the switch.

For the LD3032, the administrator can enable and disable basic TLV by selecting it. To enable basic TLV by selecting it, use the following command.

Command	Mode	Description
lldp { **portdescription** | **sysname** | **sysdescription** | **syscap**}	Interface [XE/GPON]	Selects basic TLV that to be sent in the port. portdescription: port description sysname: system name sysdescription: system description syscap: system capability
no lldp { **portdescription** | **sysname** | **sysdescription** | **syscap**}		Disables basic TLV configured to be sent in the port.

To specify an IP management address to be used in the LLDP management type, length, and TLV, use the following command.

Command	Mode	Description
lldp mgmtaddr *A.B.C.D*	Interface [XE/GPON]	Specifies an IP management address to be used in the LLDP. mgmtaddr: management address
no lldp mgmtaddr *A.B.C.D*		Deletes the specified IP management address.

7.2.5 LLDP Message

For the LD3032, it is possible to configure the interval time and times of sending LLDP message. To configure the interval time and times of LLDP message, use the following command.

Command	Mode	Description
lldp msg txinterval <5-32768>	Global	Configures the interval of sending LLDP message. The unit is second. (default: 30)
lldp msg txhold <2-10>		Configures the periodic times of LLDP message. (default: 4)

7.2.6 Reinitiating Delay

To configure the interval time of enabling LLDP frame after configuring LLDP operation type, use the following command.

Command	Mode	Description
lldp reinitdelay <1-10>	Global	Configures the interval time of enabling LLDP frame from the time of configuring not to process LLDP frame. (default: 2)

To configure delay time of transmitting LLDP frame, use the following command.

Command	Mode	Description
lldp txdelay <1-8192>	Global	Configures delay time of transmitting LLDP frame. (default: 2)

7.2.7 Displaying LLDP Configuration

To display LLDP configuration, use the following command.

Command	Mode	Description
show lldp config	Enable Global	Shows LLDP configuration.
show lldp remote		Show statistics for remote entries.
show lldp statistics		Shows LLDP operation and statistics.

To delete an accumulated statistics on the port, use the following command.

Command	Mode	Description
clear lldp statistics [*PORTS*]	Enable Global	Deletes an accumulated statistics on the port.

7.3 Remote Monitoring (RMON)

Remote Monitoring (RMON) is a function to monitor communication status of devices connected to Ethernet at remote place. While SNMP can give information only about the device mounting an SNMP agent, RMON gives network status information about overall segments including devices. Thus, user can manage network more effectively. For instance, in case of SNMP it is possible to be informed traffic about certain ports but through RMON you can monitor traffics occurred in overall network, traffics of each host connected to segment, and the current status of traffic between hosts.

Since RMON processes quite lots of data, its processor share is very high. Therefore, administrator should take intensive care to prevent performance degradation and not to overload network transmission caused by RMON. There are nine RMON MIB groups defined in RFC 1757: Statistics, History, Alarm, Host, Host Top N, Matrix, Filter, Packet Capture and Event. The LD3032 supports two MIB groups of them, most basic ones: Statistics (only for uplink ports) and History.

7.3.1 RMON History

RMON history is periodical sample inquiry of statistical data about each traffic occurred in Ethernet port. Statistical data of all ports are pre-configured to be monitored at 30-minute interval, and 50 statistical data stored in one port. It also allows you to configure the time interval to take the sample and the number of samples you want to save.

To open *RMON Configuration* mode, use the following command.

Command	Mode	Description
rmon-history <1-65535>	Global	Opens *RMON Configuration* mode. 1-65535: index number

The following is an example of opening *RMON Configuration* mode with index number 5.

```
SWITCH(config)# rmon-history 5
SWITCH(config-rmonhistory[5])#
```

Input a question mark <**?**> at the system prompt in *RMON Configuration* mode if you want to list available commands.

The following is an example of listing available commands in *RMON Configuration* mode.

```
SWITCH(config-rmonhistory[5])# ?
RMON history configuration commands:
  active              Activate the history
  data-source         Set data source name for the ethernet port
  do                  To run exec commands in config mode
  exit                End current mode and down to previous mode
  help                Description of the interactive help system
  interval            Define the time interval for the history
  owner               Assign the owner who define and is using the history
                      resources
  requested-buckets   Define the bucket count for the interval
  show                Show running system information
  write              Write running configuration to memory or terminal

SWITCH(config-rmonhistory[5])#
```

7.3.1.1 Source Port of Statistical Data

To specify a source port of statistical data, use the following command.

Command	Mode	Description
data-source *NAME*	RMON	Specifies a data object ID: NAME: enters a data object ID. (ex. ifindex.n1/port1)

7.3.1.2 Subject of RMON History

To identify a subject using RMON history, use the following command.

Command	Mode	Description
owner *NAME*	RMON	Identifies subject using relevant data, enter the name (max. 32 characters).

7.3.1.3 Number of Sample Data

To configure the number of sample data of RMON history, use the following command.

Command	Mode	Description
requested-buckets <1-65535>	RMON	Defines a bucket count for the interval, enter the number of buckets. 1-65535: bucket number (default: 50)

7.3.1.4 Interval of Sample Inquiry

To configure the interval of sample inquiry in terms of second, use the following command.

Command	Mode	Description
interval <1-3600>	RMON	Defines the time interval for the history (in seconds), enter the value. (default: 1800)

1 sec is the minimum time which can be selected. But the minimum sampling interval currently is 30 sec, i.e., all intervals will be round up to a multiple of 30 seconds.

7.3.1.5 Activating RMON History

To activate RMON history, use the following command.

Command	Mode	Description
active	RMON	Activates RMON history.

Before activating RMON history, check if your configuration is correct. After RMON history is activated, you cannot change its configuration. If you need to change configuration, you need to delete the RMON history and configure it again.

7.3.1.6 Deleting Configuration of RMON History

When you need to change a configuration of RMON history, you should delete an existing RMON history. To delete an RMON history, use the following command.

Command	Mode	Description
no rmon-history <1-65535>	Global	Deletes the RMON history of specified number, enter the value for deleting.

7.3.1.7 Displaying RMON History

To display an RMON history, use the following command.

Command	Mode	Description
show running-config rmon-history	All	Shows a configured RMON history.

Always the last values will be displayed but no more than the number of the granted buckets.

The following is an example of displaying RMON history.

```
SWITCH(config-rmonhistory[5])# show running-config rmon-history
!
rmon-history 5
 owner test
 data-source ifindex.hdlc1
 interval 60
 requested-buckets 25
 active
!
SWITCH(config-rmonhistory[5])#
```

7.3.2 RMON Alarm

You need to open *RMON Alarm Configuration* mode first to configure RMON alarm.

Command	Mode	Description
rmon-alarm <1-65535>	Global	Opens *RMON Alarm Configuration* mode. 1-65535: index number

7.3.2.1 Subject of RMON Alarm

You need to configure RMON alarm and identify subject using many kinds of data from alarm. To identify subject of alarm, use the following command.

Command	Mode	Description
owner *NAME*	RMON	Identifies subject using relevant data, enter the name (max. 32 characters).

7.3.2.2 Object of Sample Inquiry

To assign object used for sample inquiry, use the following command.

Command	Mode	Description
sample-variable *MIB-OBJECT*	RMON	Assigns MIB object used for sample inquiry.

7.3.2.3 Absolute and Delta Comparison

There are two ways to compare with the threshold: absolute comparison and delta comparison.

- **Absolute Comparison**
  Comparing sample data with the threshold at configured interval, if the data is more than the threshold or less than it, alarm is occurred
- **Delta Comparison**
  Comparing difference between current data and the latest data with the threshold, if the data is more than the threshold or less than it, alarm is occurred.

To compare object selected as sample with the threshold, use the following command.

Command	Mode	Description
sample-type absolute	RMON	Compares object with the threshold directly.

To configure delta comparison, use the following command.

Command	Mode	Description
sample-type delta	RMON	Compares difference between current data and the latest data with the threshold.

7.3.2.4 Upper Bound of Threshold

If you need to occur alarm when object used for sample inquiry is more than upper bound of threshold, you have to configure the upper bound of threshold. To configure upper bound of threshold, use the following command.

Command	Mode	Description
rising-threshold *VALUE*	RMON	Configures upper bound of threshold. VALUE: 0-2147483647

After configuring upper bound of threshold, configure to generate RMON event when object is more than configured threshold. Use the following command.

Command	Mode	Description
rising-event <1-65535>	RMON	Configures to generate RMON event when object is more than configured threshold. 1-65535: event index

7.3.2.5 Lower Bound of Threshold

If you need to occur alarm when object used for sample inquiry is less than lower bound of threshold, you should configure lower bound of threshold.

To configure lower bound of threshold, use the following command.

Command	Mode	Description
falling-threshold *VALUE*	RMON	Configures lower bound of threshold.

After configuring lower bound of threshold, configure to generate RMON event when object is less than configured threshold. Use the following command.

Command	Mode	Description
falling-event <1-65535>	RMON	Configures to generate RMON alarm when object is less than configured threshold.

7.3.2.6 Standard of the First Alarm

It is possible for users to configure standard when alarm is first occurred. User can select the first point when object is more than threshold, or the first point when object is less than threshold, or the first point when object is more than threshold or less than threshold.

To configure the first RMON alarm to occur when object is less than lower bound of threshold first, use the following command.

Command	Mode	Description
startup-type falling	RMON	Configures the first RMON Alarm to occur when object is less than lower bound of threshold first.

To configure the first alarm to occur when object is firstly more than upper bound of threshold, use the following command.

Command	Mode	Description
startup-type rising	RMON	Configures the first Alarm to occur when object is firstly more than upper bound of threshold.

To configure the first alarm to occur when object is firstly more than threshold or less than threshold, use the following command.

Command	Mode	Description
startup-type rising-and-falling	RMON	Configures the first Alarm to occur when object is firstly more than threshold or less than threshold.

7.3.2.7 Interval of Sample Inquiry

The interval of sample inquiry means time interval to compare selected sample data with upper bound of threshold or lower bound of threshold in terns of seconds.

To configure interval of sample inquiry for RMON alarm, use the following command.

Command	Mode	Description
sample-interval <0-65535>	RMON	Configures interval of sample inquiry. (unit: second)

7.3.2.8 Activating RMON Alarm

After finishing all configurations, you need to activate RMON alarm. To activate RMON alarm, use the following command.

Command	Mode	Description
active	RMON	Activates RMON alarm.

7.3.2.9 Deleting Configuration of RMON Alarm

When you need to change a configuration of RMON alarm, you should delete an existing RMON alarm.

To delete RMON alarm, use the following command.

Command	Mode	Description
no rmon-alarm <1-65535>	Global	Deletes RMON history of specified number, enter the value for deleting.

7.3.3 RMON Event

RMON event identifies all operations such as RMON alarm in the switch. You can configure event or trap message to be sent to SNMP management server when sending RMON alarm. You need to open *RMON Event Configuration* mode to configure RMON event.

Command	Mode	Description
rmon-event <1-65535>	Global	Opens *RMON Event Configuration* mode. 1-65535: index number

7.3.3.1 Event Community

When RMON event is happened, you need to input community to transmit SNMP trap message to host. Community means a password to give message transmission right. To configure community for trap message transmission, use the following command.

Command	Mode	Description
community *NAME*	RMON	Configures password for trap message transmission right. NAME: community name

7.3.3.2 Event Description

It is possible to describe event briefly when event is happened. However, the description will not be automatically made. Thus administrator should make the description. To specify a description about the current RMON event, use the following command.

Command	Mode	Description
description *DESCRIPTION*	RMON	Specifies the description of the current RMON event.

7.3.3.3 Subject of RMON Event

You need to configure event and identify subject using various data from event. To identify subject of RMON event, use the following command.

Command	Mode	Description
owner *NAME*	RMON	Identifies subject of event. You can use maximum 126 characters and this subject should be same with the subject of RMON event.

7.3.3.4 Event Type

When RMON event is happened, you need to configure event type to arrange where to send event. To configure event type, use the following command.

Command	Mode	Description
type log	RMON	Configures event type as log type. Event of log type is sent to the place where the log file is made.
type trap		Configures event type as trap type. Event of trap type is sent to SNMP administrator and PC.
type log-and-trap		Configures event type as both log type and trap type.
type none		Configures none event type.

7.3.3.5 Activating RMON Event

After finishing all configurations, you should activate RMON event. To activate RMON event, use the following command.

Command	Mode	Description
active	RMON	Activates RMON event.

7.3.3.6 Deleting Configuration of RMON Event

Before changing the configuration of RMON event, you should delete RMON event of the number and configure it again.

To delete RMON event, use the following command.

Command	Mode	Description
no rmon-event <1-65535>	Global	Delete RMON event of specified number.

7.3.4 Simple RMON Event Configuration

You can simply monitor specified event variables, such as total number of received packets on a port during the sample interval. To define what packet types are monitored, the value of parameters' thresholds (falling and rising thresholds) during the sampling interval to generate the syslog message of event, use the following command.

Command	Mode	Description
rmon-simple { **crc-align-error** | **jabber** | **oversize-packets** | **undersize-packets** | **fragments** | **drop-events** } <1-65535> *FALLING_THRESHOLD RISING_THRESHOLD*	Interface [XE/GE /GPON]	Configures what packet types are monitored, the value of parameters' thresholds (falling and rising thresholds) to generate the syslog messages of event. PORT : port number 1-65535: sample interval crc-align-error: number of packets received that were from 64 to 1518 octets long, but had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error) jabber: number of occurrences of corrupted data or useless signals the port has encountered oversize-packets: number of received packets that exceeded the maximum size (1518 bytes) undersize-packets: number of frames that were less than the minimum length (64 bytes) fragments: number of undersized frames with alignment errors, and frames with frame check sequence (FCS) errors drop-events: the total number of events in which packets were dropped by the RMON probe due to lack of resources FALLING_THRESHOLD: When the value of the moni-

		tored variable is smaller than or equal to the falling threshold, a falling event is triggered. (1-2147483647) RISING_THRESHOLD: When the value of the monitored variable is greater than or equal to the rising threshold, a rising event is triggered. (1-2147483647)
no rmon-simple { **crc-align-error** | **jabber** | **oversize-packets** | **undersize-packets** | **fragments** | **drop-events** }		Deletes the configured simple RMON event monitoring function.

7.4 Syslog

The syslog is a function that allows the network element to generate the event notification and forward it to the event message collector like a syslog server. This function is enabled as default, so even though you disable this function manually, the syslog will be enabled again.

7.4.1 Syslog Output Level

Syslog Output Level without a Priority

To set a syslog output level, use the following command.

Command	Mode	Description
syslog output {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info** | **debug**} **console**	Global	Generates a syslog message of selected level or higher and forwards it to the console.
syslog output {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info** | **debug**} **local** {**volatile** | **non-volatile**}		Generates a syslog message of selected level or higher in the system memory. volatile: deletes a syslog message after restart. non-volatile: reserves a syslog message.
syslog output {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info** | **debug**} **external sdcard** {**sfu l slot** *SLOT_NUMBER*}		Generates a syslog message of selected level or higher and forwards it to the SDcard. SLOT_NUMBER: slot number
syslog output {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info** | **debug**} **remote** *A.B.C.D*		Generates a syslog message of selected level or higher and forwards it to a remote host.

To disable a specified syslog output, use the following command.

Command	Mode	Description
no syslog output {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info** | **debug**} **console**	Global	Deletes a specified syslog output.
no syslog output {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info** | **debug**} **local** {**volatile** | **non-volatile**}		
no syslog output {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info** | **debug**} **remote** *A.B.C.D*		

Syslog Output Level with a Priority

To set a user-defined syslog output level with a priority, use the following command.

Command	Mode	Description

syslog output priority {**auth** | **authpriv** | **kern** | **local0** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7** | **syslog** | **user**} {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info**} **console**	Global	Generates a user-defined syslog message with a priority and forwards it to the console.
syslog output priority {**auth** | **authpriv** | **kern** | **local0** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7** | **syslog** | **user**} {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info**} **local** {**volatile** | **non-volatile**}		Generates a user-defined syslog message with a priority in the system memory. volatile: deletes a syslog message after restart. non-volatile: reserves a syslog message.
syslog output priority {**auth** | **authpriv** | **kern** | **local0** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7** | **syslog** | **user**} {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info**} **remote** *A.B.C.D*		Generates a user-defined syslog message with a priority and forwards it to a remote host.

To disable a user-defined syslog output level, use the following command.

Command	Mode	Description
no syslog output priority {**auth** | **authpriv** | **kern** | **local0** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7** | **syslog** | **user**} {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info**} **console**	Global	Deletes a specified user-defined syslog output level with a priority.
no syslog output priority {**auth** | **authpriv** | **kern** | **local0** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7** | **syslog** | **user**} {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info**} **local** {**volatile** | **non-volatile**}		
no syslog output priority {**auth** | **authpriv** | **kern** | **local0** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7** | **syslog** | **user**} {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info**} **remote** *A.B.C.D*		

The order of priority is **emergency** > **alert** > **critical** > **error** > **warning** > **notice** > **info** > **debug**. If you set a specific level of syslog output, you will receive only a syslog message for selected level or higher. If you want receive a syslog message for all the levels, you need to set the level to **debug**.

The following is an example of configuring syslog message to send all logs higher than notice to remote host 10.1.1.1 and configuring local1.info to transmit to console.

```
SWITCH(config)# syslog output notice remote 10.1.1.1
SWITCH(config)# syslog output priority local1 info console
SWITCH(config)# show syslog
System logger on running!

info                local volatile
info                local non-volatile
notice              remote 10.1.1.1
local1.info         console
SWITCH(config)#
```

Syslog Output Level on the SD card

If the SD card is mounted in the LD3032 chassis, you can save the syslog logs to the SD card instead of local/remote memory. To store a system logs on the SD card and set its syslog output level, use the following command.

Command	Mode	Description
syslog output {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info** | **debug**} **sdcard**	Global	Generates a syslog message of selected level or higher and forwards it to a SD card.
no syslog output {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info** | **debug**} **sdcard**		Deletes a specified user-defined syslog message.

To display the syslog messages on the SD card, use the following command.

Command	Mode	Description
show syslog external sdcard slot *SLOT_NUMBER* **{|file** *FILE-NAME***} {|**<1-4294967295> **| reverse {|**<1-4294967295>**}}**		Shows the information of syslog messages written on the SD card. <1-4294967295>: line number SLOT_NUMBER: FILE-NAME: log file name STARTDATE: YYYY/MM/DD (ex. 2000/01/01) STARTTIME: HH:MM:SS (ex. 13:01:01) ENDDATE: YYYY/MM/DD (ex.) ENDTIME: HH:MM:SS (ex. 13:01:01)
show syslog external sdcard slot *SLOT_NUMBER* **{|file** *FILE-NAME***) date from** *STARTDATE* **{|***STARTTIME***} {|to** *ENDDATE* **| to** *ENDDATE ENDTIME***} {|<**1-4294967295**> | reverse {|<**1-4294967295**>}}**		
show syslog external sdcard slot *SLOT_NUMBER* **{|file** *FILE-NAME***} date to** *ENDDATE* **{|***ENDTIME***} {|<**1-4294967295**> | reverse {|<**1-4294967295**>}}**		
show syslog external sdcard slot *SLOT_NUMBER* **file-list**		
show syslog external sdcard sfu {|file *FILENAME***} {|**<1-		

4294967295> **|** **reverse** **{|**<1-4294967295>**)}**		
show syslog external sdcard sfu {|file *FILENAME***}** **date from** *STARTDATE* **{|***STARTTIME***}** **{|to** *ENDDATE* **|** **to** *ENDDATE ENDTIME***}** **{|<**1-4294967295**>** **|** **reverse {|<**1-4294967295**>}}**		
show syslog external sdcard sfu {|file *FILENAME***}** **date to** *ENDDATE* **{|***ENDTIME***}** **{|<**1-4294967295**>** **|** **reverse** **{|<**1-4294967295**>}}**		
show syslog external sdcard sfu file-list		

7.4.2 Facility Code

You can set a facility code of the generated syslog message. This code make a syslog message distinguished from others, so network administrator can handle various syslog messages efficiently.

To set a facility code, use the following command.

Command	Mode	Description
syslog local-code <0-7>	Global	Sets a facility code.
no syslog local-code		Deletes a specified facility code.

The following is an example of configuring priority of all syslog messages which is transmitted to remote host 10.1.1.1, as the facility code 0.

```
SWITCH(config)# syslog output err remote 10.1.1.1
SWITCH(config)# syslog local-code 0
SWITCH(config)# show syslog
System logger on running!

info                 local volatile
info                 local non-volatile
err                  remote 10.1.1.1
local_code           0
SWITCH(config)#
```

7.4.3 Syslog index

To set a user-defined syslog message index level with a priority, use the following command.

Command	Mode	Description
syslog index {**system** | **physical-**	Global	Generates a user-defined syslog message index with a

entity | **dhcp** | **filter** | **rmon** | **gpon** | **loop-detect** **|** **snmp**} *INDEX* **priority** {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info** | **debug**}		priority
no syslog index {**system** | **physical-entity** | **dhcp** | **filter** | **rmon** | **gpon** | **loop-detect** } *INDEX*		Deletes a specified user-defined syslog message index level with a priority.

To display the configuration of the syslog index, use the following command.

Command	Mode	Description
show syslog index	Enable Global	Shows the information of syslog message index
show syslog index {**system** | **physical-entity** | **dhcp** | **filter** | **rmon** | **gpon** | **loop-detect**} [*INDEX*]		Shows the syslog index information of each parameter

The order of priority is **emergency** > **alert** > **critical** > **error** > **warning** > **notice** > **info** > **debug**. If you set a specific level of syslog output, you will receive only a syslog message for selected level or higher. If you want receive a syslog message for all the levels, you need to set the level to **debug**.

7.4.4 Syslog Bind Address

You can specify an IP address to attach to the syslog message for its identity. To specify the IP address to bind to a syslog message, use the following command.

Command	Mode	Description
syslog bind-address *A.B.C.D*	Global	Specifies the IP address to bind to a syslog message.
no syslog bind-address		Deletes a specified IP address.

7.4.5 Debug Message for Remote Terminal

To display a syslog debug message to a remote terminal, use the following command.

Command	Mode	Description
terminal monitor	Enable	Enables the terminal monitor function.
no terminal monitor		Disables the terminal monitor function.

This function is not operational in the local console.

7.4.6 Disabling Syslog

To disable the syslog, use the following command.

Command	Mode	Description
no syslog	Global	Disables the syslog.

The syslog is enabled by default.

7.4.7 Displaying Syslog Message

To display the received syslog message in the system memory, use the following command.

Command	Mode	Description
show syslog local {**volatile** | **non-volatile**} [*NUMBER*]	Enable Global	Shows the received syslog messages. volatile: removes the syslog messages after restart. non-volatile: reserves the syslog messages. NUMBER: shows the last N syslog messages.
show syslog local {**volatile** | **non-volatile**} **reverse**		Shows the received syslog messages in the reverse order.
show syslog external sdcard slot *SLOT_NUMBER* **{|file** *FILE-NAME***} {|**<1-4294967295> **| reverse {|**<1-4294967295>**}}**		Shows the received syslog messages from external output file. <1-4294967295>: line number SLOT_NUMBER: FILE-NAME: log file name STARTDATE: YYYY/MM/DD (ex. 2000/01/01) STARTTIME: HH:MM:SS (ex. 13:01:01) ENDDATE: YYYY/MM/DD (ex.) ENDTIME: HH:MM:SS (ex. 13:01:01)
show syslog external sdcard slot *SLOT_NUMBER* **{|file** *FILE-NAME***) date from** *STARTDATE* **{|***STARTTIME***} {|to** *ENDDATE* **| to** *ENDDATE ENDTIME***} {|<**1-4294967295**> | reverse {|<**1-4294967295**>}}**		
show syslog external sdcard slot *SLOT_NUMBER* **{|file** *FILE-NAME***} date to** *ENDDATE* **{|***ENDTIME***} {|<**1-4294967295**> | reverse {|<**1-4294967295**>}}**		
show syslog external sdcard slot *SLOT_NUMBER* **file-list**		
show syslog external sdcard sfu {|file *FILENAME***} {|**<1-4294967295> **| reverse {|**<1-4294967295>**)}**		
show syslog external sdcard sfu {|file *FILENAME***} date from** *STARTDATE* **{|***STARTTIME***} {|to**		

ENDDATE **| to** *ENDDATE ENDTIME***}** **{|<**1-4294967295**>** **| reverse {|<**1-4294967295**>}}**		
show syslog external sdcard sfu {|file *FILENAME***}** **date to** *ENDDATE* **{|***ENDTIME***}** **{|<**1-4294967295**>** **| reverse {|<**1-4294967295**>}}**		
show syslog external sdcard sfu file-list		

To clear the syslog message in the system memory, use the following command.

Command	Mode	Description
clear syslog local {**volatile** | **non-volatile**}	Enable Global	Removes the received syslog messages.
clear syslog external sdcard sfu		
clear syslog external sdcard slot *SLOT_NUMBER*		

7.4.8 Uploading Syslog File

To upload a syslog file of the external output using FTP or TFTP, use the following command.

Command	Mode	Description
copy {**ftp** | **tftp**} **syslog external sdcard sfu upload** [*FILENAME*]	Enable	Uploads a syslog file to FTP or TFTP server with the name configured by user. FILENAME: log file name NUM: slot number
copy {**ftp** | **tftp**} **syslog external sdcard slot** *NUM* **upload** [*FILENAME*]		

7.4.9 Displaying Syslog Configuration

To display the configuration of the syslog, use the following command.

Command	Mode	Description
show syslog [**status**]	Enable Global	Shows the configuration of the syslog.
show syslog {**volatile** | **non-volatile**} **information**		Shows the usage of the area where the received syslog messages are stored. volatile: the area for volatile syslog messages non-volatile: the area for non-volatile syslog messages

7.5 Operation, Administration and Maintenance (OAM)

In the enterprise, Ethernet links and networks have been managed via Simple Network Management Protocol (SNMP). Although SNMP provides a very flexible management solution, it is not always efficient and is sometimes inadequate to the task.

First, using SNMP assumes that the underlying network is operational because SNMP relies on IP connectivity; however, you need management functionality even more when the underlying network is non-operational. Second, SNMP assumes every device is IP accessible. This requires provisioning IP on every device and instituting an IP overlay network even if the ultimate end-user service is an Ethernet service. This is impractical in a carrier environment. For these reasons, carriers look for management capabilities at every layer of the network. The Ethernet layer has not traditionally offered inherent management capabilities, so the IEEE 802.3ah Ethernet in the First Mile (EFM) task force and Y.1731 added the Operations, Administration and Maintenance (OAM) capabilities to Ethernet like interfaces. These management capabilities were introduced to provide some basic OAM function on Ethernet media. OAM is complementary, not competitive, with SNMP management in that it provides some basic management functions at Layer 2, rather than using Layer 3 and above as required by SNMP over an IP infrastructure.

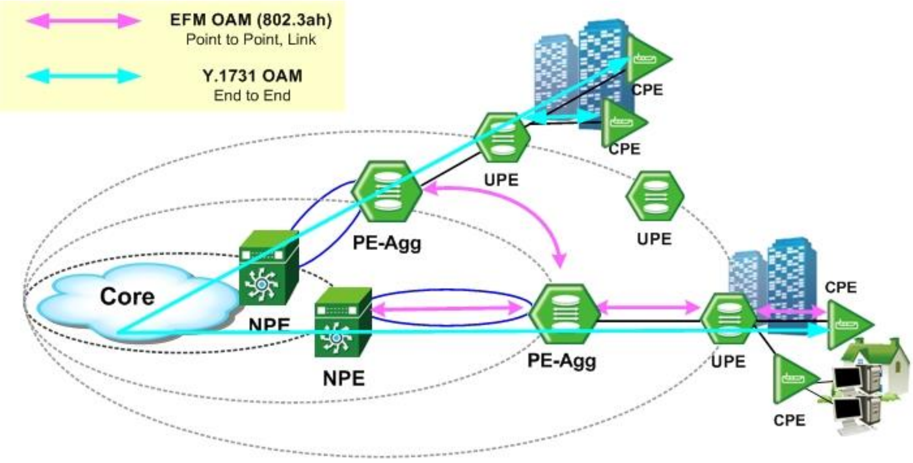


Fig. 7.1 OAM Deployment Scenario

OAM is responsible for monitoring and troubleshooting individual Ethernet links or end-to-end Ethernet instances.

EFM OAM provides mechanisms for remote fault detection and loopback controls. It provides single-hop functionality in that it works only between two directly connected Ethernet stations, called local Data Terminal Equipment (DTE) and a remote DTE. OAMPDUs are interchanged between local DTE and remote DTE. A local DTE manages a remote DTE by referring to OAMPDUs containing the information of critical link events or faults with its remote DTE.

ITU-T Y.1731 OAM is used for the per-customer and per-service granularity required Maintenance Association End/Intermediate Point (MEP/MIP) on a per-domain, per-VLAN, or per-port. It is the standard for Layer 2 ping, Layer 2 traceroute, and end-to-end connectivity check of the Ethernet network. ITU-T Y.1731 OAM detects, verifies and isolates connectivity failures in Bridged VLANs. And Y.1731 provides functions for performance monitoring and it is focusing on the services aspect of Ethernet.

7.6 EFM OAM

EFM OAM capabilities are a need for Ethernet subscriber access link monitoring in L2, remote loopback and remote failure indication. EFM OAM uses a slow protocol frame which is called OAM Protocol Data Units (OAMPDUs). Using OAMPDUs, local DTE manages the remote DTE.

There are five EFM OAM operations for local DTE to manage remote DTE.

- **OAM Discovery**
  Local DTE exchanges OAM status information with remote DTE using OAMPDUs.
- **Remote Loopback**
  Local DTE diagnoses the connection of remote DTE using loopback control.
  - Enables the loopback status of remote DTE using OAMPDUs from local DTE.
  - Monitors the link condition by loopback function when local DTE receives back every packet it sends to remote DTE.
- **Link Monitoring**
  Local DTE monitors and informs remote DTE of the event notifications related to the link faults.
- **Remote Failure Indication**
  Local DTE indicates a loss of signal (Link Fault), unrecoverable errors (Dying Gasp) and undefined critical errors (Critical Event)
- **Variable Retrieval**
  Local DTE sends a variable request OAMPDU and gets a value of MIB variable for information retrieval of remote OAM port.

7.6.1 Enabling EFM OAM

To enable/disable EFM OAM function, use the following command.

Command	Mode	Description
oam efm enable *PORTS*	Global	Enables EFM OAM.
oam efm disable *PORTS*		Disables EFM OAM.

To configure an interval of EFM OAMPDUs which are exchanged between local DTE and remote DTE, use the following command.

Command	Mode	Description
oam efm hello-interval <100-5000>	Global	Configures the interval between OAMPDUs. (default: 1000ms, step: 100ms)
oam efm keepalive-interval <500-10000>		Configures the remote DTE aging interval. (default: 5000ms, step: 100ms)

7.6.2 OAM Link Monitoring

To enable/disable the link monitoring function, use the following command.

Command	Mode	Description
oam efm link-monitor enable *PORTS*	Global	Enables link monitoring function.
oam efm link-monitor disable *PORTS*		Disables link monitoring function.

To specify an errored window size and threshold according to the event type, use the following command.

Command	Mode	Description
oam efm link-monitor frame window <10-600> **threshold** <0-65535> *PORTS*	Global	Specifies the window size and threshold in case of frame event. 10-600: window size (unit: 100msec, default:1 second) 0-65535: threshold value (default:1)
oam efm link-monitor frame-period window <1000-200000000> **threshold** <0-65535> *PORTS*		Specifies the window size and threshold in case of frame-period event. 1000-200000000: window size (default: 1000000 pkts) 0-65535: threshold value (default:1)
oam efm link-monitor symbol-period window <1-1000000> **threshold** <0-65535> *PORTS*		Specifies the window size and threshold in case of symbol-period event. 1-1000000: window size (default: 625 million) 0-65535: threshold value (default:1)
oam efm link-monitor frame-seconds-summary window <10-900> **threshold** <0-900> *PORTS*		Specifies the window size and threshold in case of frame-seconds-summary error event. 10-900: window size (default: 60 seconds) 0-900: threshold value (default:1)

To clear the collected statistics of EFM OAM link monitoring, use the following command.

Command	Mode	Description
clear oam efm link-monitor stats *PORTS*	Global	Clears the collected statistics of EFM OAM link monitoring.

To configure how to handle the event notifications that the switch is received, use the following command.

Command	Mode	Description
oam efm link-monitor action syslog *PORTS*	Global	Generates a syslog message when event notifications are received.
oam efm link-monitor action snmp-trap *PORTS*		Generates a snmp trap message when event notifications are received.

7.6.3 EFM OAM Mode

To configure EFM OAM mode, use the following command.

Command	Mode	Description
oam efm mode {**active** | **passive**} *PORTS*	Global	Configures the mode of EFM OAM.

i Both request and loopback can be available in the EFM OAM active mode. However, request or loopback is not available in the OAM passive mode.

7.6.4 OAM Loopback

For OAM loopback function, both the switch and the host should support OAM function. OAM loopback function enables Loopback function from the user's device to the host which connected to the user's device and operates it.

To enable/disable the remote loopback mode, use the following command.

Command	Mode	Description
oam efm remote-loopback permit *PORTS*	Global	Receives the loopback control commands from its remote peer switch.
oam efm remote-loopback deny *PORTS*		Ignores the loopback control commands from its remote peer switch. (Default)

To configure loopback function of the host connected to the switch, use the following command.

Command	Mode	Description
oam efm remote-loopback enable *PORTS*	Global	Enables loopback function of peer device.
oam efm remote-loopback disable *PORTS*		Disables loopback function of peer device.
oam efm remote-loopback test <1-100> *PORTS*		Starts to perform the test of loopback operation. 1-100: the number of test packets

7.6.5 OAM Unidirection

When RX is impossible in OAM, it is possible to send the information by using TX. To enable/disable the function, use the following command.

Command	Mode	Description
oam efm unidir enable *PORTS*	Global	Sends the information by using TX.
oam efm unidir disable *PORTS*		Disables to transmit the information by using TX.

7.6.6 Displaying EFM OAM Configuration

To display OAM configuration, use the following command.

Command	Mode	Description
show oam efm	Enable Global	Shows EFM OAM configuration.
show oam efm link-monitor {**local** | **remote**} *PORTS*		Shows the link monitoring status and remote statistics on the port.
show oam efm local *PORTS*		Shows local OAM configuration.
show oam efm remote *PORTS*		Shows remote OAM configuration.
show oam efm variable <0-255> <0-65535> *PORTS*		Shows remote OAM variable. 0-255: branch number 0-65535: leaf number

7.7 Ethernet (ITU-T Y.1731) OAM

The ITU-T Y.1731 fault management functions feature provides new functions for fault and performance management to serve the needs of service providers in large networks. It is designed to support point-to-point connections and multipoint connectivity in the Ethernet layer. The ITU-T Recommendation Y.1731 specifies OAM mechanisms to operate and maintain the network and service aspects of ETH layer.

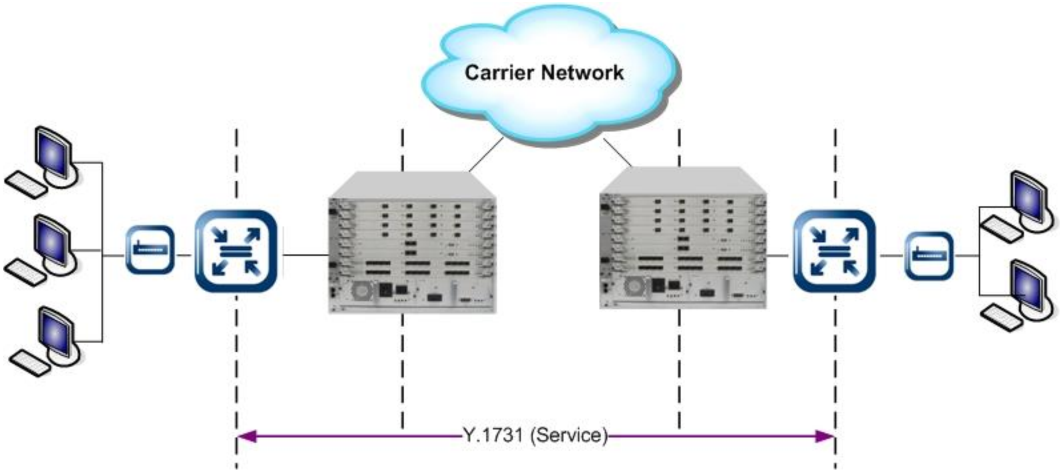


Fig. 7.2 CFM and Y.1731 OAM for end-to-end visibility

Y.1731 OAM Elements

You need to know conceptual information of Y.1731 OAM. There are several definitions of the Y.1731, they are in total agreement between each standard. However, Y.1731 adds functions for performance monitoring and it is focusing on the services aspect of Ethernet.

Y.1731 OAM consists of the following management elements.

- **Maintenance Entity (ME)**
  An entity that requires management. It is a relationship between two Maintenance entity group end points.
- **Maintenance Entity Group (MEG)**
  ME group includes different MEs that satisfy the following conditions:
  - MEs in the same administrative boundary
  - MEs have the same MEG level
  - MEs belong to the same point-to-point ETH connection or multipoint ETH connectivity.
- **MEG End Point (MEP)**
  A marked end point of an ETH MEG that can initiate/terminate proactive OAM frames for fault management and performance monitoring. The OAM frames are distinct from the transit ETH flows. Each MEP has a unique MEPID.
- **MEG Intermediate Point (MIP)**
  An intermediate point passively receives some OAM frames and responds back to the originating MEP.
- **MIP Half Function (MHF)**
  A MIP is comprised of two MHFs, which are up MHF and down MHF. MHF enables Y.1731 OAM to manage MIP CCM database as well as MEP CCM database.

MEG Level

Eight MEG levels are available to accommodate different network deployment scenarios. There are two cases based upon ETH layer encapsulation:

- **Shared MEG Levels**: Customer, provider, and operator share the MEG levels.
  - Customer role: Level 7, 6, 5
  - Provider role: Level 4, 3
  - Operator role: Level 2, 1
- **Independent MEG Levels**: Customer and provider do not share the MEG levels but provider and operator share the MEG levels.
  - Provider bridge: C-Tag, S-Tag

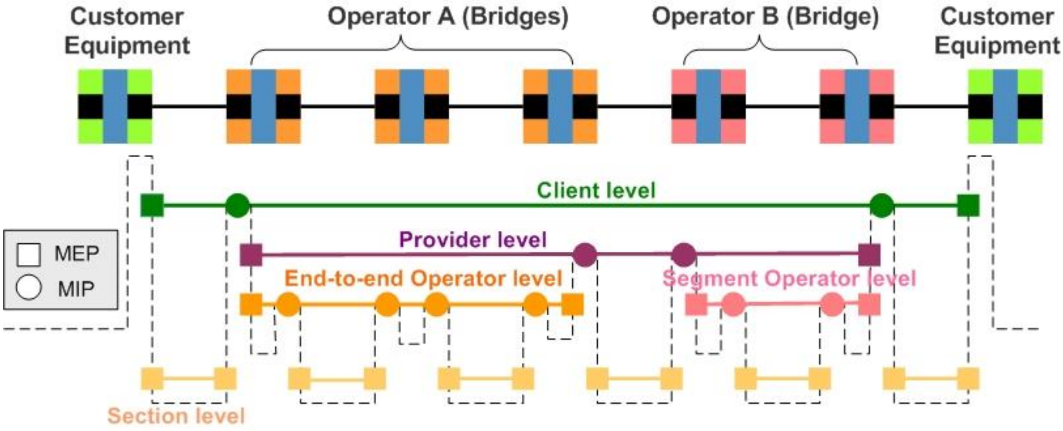


Fig. 7.3 Shared MEG Levels

Y.1731 Functions for Fault management

ITU-T Y.1731 OAM supports the following functions for fault management:

- **Ethernet Continuity Check (ETH-CC)**
  Each MEP sends periodic CCMs to other MEPs with a multicast destination address. The loss of CCMs that ride along the data path would indicate a connectivity failure.
- **Ethernet Loopback (ETH-LB)**
  A LBM is sent to a unicast destination MAC address. MEP at the destination MAC address responds to the LBM with an LBR. These messages are useful for verifying connectivity with a specific L2 destination.
- **Ethernet Link Trace (ETH-LT)**
  ETH-LT function is used to retrieve adjacency relationship between a MEP and a remote MEP or MIP.
- **Ethernet Alarm Indication Signal (ETH-AIS)**
  ETH-AIS is used to suppress alarms at the client layer following detection of defect conditions at the server layer. Upon detecting a defect condition, the MEP start transmitting periodic AIS frames at a configured client MEG level.
- **Ethernet Locked Signal (ETH-LCK)**
  ETH-LCK is used to communicate the administrative locking of a server layer MEP and consequential interruption of data traffic forwarding towards the MEP expecting the traffic.

- **Ethernet Test Signal (ETH-TEST)**
  When ETH-TEST function is enabled, it performs diagnostics tests to verify bandwidth throughput, frame loss, bit errors, etc.

Y.1731 Functions for Performance Monitoring

ITU-T Y.1731 OAM supports the following functions for performance monitoring:

- **Frame Loss Measurement (ETH-LM)**
  Using the frame with ETH-LM information, the switch collects counter values applicable for ingress and egress service frames where the counters maintain a count of transmitted and received data frames between a pair of MEPs.
- **Frame Delay Measurement (ETH-DM)**
  Frame delay and frame delay variation measurements are performed by exchanging frames with ETH-DM information between MEPs.

7.7.1 Enabling Y.1731 OAM

To enable/disable ITU-T Y.1731 OAM function globally, use the following command.

Command	Mode	Description
ethernet oam enable	Global	Enables ITU-T Y.1731 OAM function.
ethernet oam disable		Disables ITU-T Y.1731 OAM function.

7.7.2 Creating Y.1731 Entity

ITU-T Y.1731 uses the entities that are managed and the management functional components. An ME is an entity that requires management. A MEG includes a set of MEs that satisfy the some conditions. To implement Y.1731 OAM, you should create MEG and specify its level.

7.7.2.1 Creating MEG

To create a MEG name and specify its level, use the following command.

Command	Mode	Description
ethernet oam meg *NAME* **level** <0-7> [**primary-vlan** *VLAN*]	Global	Creates a MEG name and specifies MEG's level NAME: MEG's name 0-7: MEG's level to use (default: 0) VLAN: MEG' vlan ID
no ethernet oam meg *NAME*		Deletes the configured MEG with a unique name.

7.7.2.2 Creating MEP

To determine a MEG End Point (MEP) with MEP ID for a specific MEG and configure MEP's direction, use the following command.

Command	Mode	Description
ethernet oam mep mepid <1-8191> **meg** *MEG-AME*	Global	Configures a MEP ID on a port of specific MEG. 1-8191: source MEP ID for OAM PDU to send MEG-NAME: MEG name
no ethernet oam mep mepid <1-8191> **meg** *MEG-NAME*		Deletes the configured MEP.

To create MEP, you need to create MEG first.

To assign the MEP and MEP's direction, use the following command.

Command	Mode	Description
ethernet oam mep assign mepid <1-8191> **meg** *MEG-NAME* **direction up**	Interface [XE/GE/CG]	Assigns the configured MEP.
ethernet oam mep assign mepid <1-8191> **meg** *MEG-NAME* **direction down**		

7.7.2.3 Creating MIP

To determine a MEG Intermediate Point (MIP) and specify its level, use the following command.

Command	Mode	Description
ethernet oam mip level <0-7>	Interface [XE/GE/CG]	Configures a MIP on an interface port and specifies MIP's level. 0-7: MIP's level to use
no ethernet oam mip		Deletes the configured MIP.

To configure a default MEG with its level or MHF use, use the following command.

Command	Mode	Description
ethernet oam default-meg default level <0-7>	Global	Creates a default MEG and specifies MEG's level 0-7: the level to be created dynamic MHF
ethernet oam default-meg default mhf-creation default		Creates a default MEG with MHF.
ethernet oam default-meg de-		Creates a default MEG with MHF only if there is a MEP

fault mhf-creation explicit		at the next lower level.
ethernet oam default-meg default mhf-creation none		Creates a default MEG without MHF.

To delete a configured MHF, use the following command.

Command	Mode	Description
no ethernet oam default-meg default {**mhf-creation** | **level**}	Global	Deletes a default MEG, its level, and MHF.

A MEG should have a unique name across entire networks. Several MEGs can have same level. But one single MEG cannot have serveral levels.

7.7.2.4 Creating RMEP

To select the static or dynamic method for creating a remote MEP, use the following command.

Command	Mode	Description
ethernet oam rmep-creation {**static** | **dynamic**}	Global	Selects the method to create a remote MEP.
no ethernet oam rmep-creation		Deletes the configured remote MEP creation method.

To specify a remote MEP ID in the static method, use the following command.

Command	Mode	Description
ethernet oam rmep rmepid <1-8191> **meg** *NAME*	Interface [XE/GE/CG]	Configures a remote MEP ID on the port of specific MEG.
no ethernet oam rmep rmepid <1-8191> **meg** *NAME*		Deletes the configured remote MEP.

7.7.3 Enabling Y.1731 Entity

To enable ITU-T Y.1731 function for MEPs, use the following command.

Command	Mode	Description
ethernet oam mep enable meg *NAME* [**mepid** <1-8191>]	Global	Enables Y.1731 OAM for MEPs. NAME: MEG’s name

To disable ITU-T Y.1731 function for MEPs, use the following command.

Command	Mode	Description
ethernet oam mep disable meg	Global	Disables Y.1731 OAM for MEPs

NAME [**mepid** <1-8191>]		

7.7.4 Fault Alarm Detection

To configure parameters for detecting and notifying its faults, use the following command.

Command	Mode	Description
ethernet oam fault-detect meg *NAME* [**mepid** <1-8191>] {**priority** <1-8> | **keep-time** <0-1023> | **clear-time** <0-1023>}	Global	Specifies a value of each parameter for detecting and notifying its faults. NAME: MEG's name 1-8: priority for notifying the faults (default: 2) 0-1023: the time for the operation to verify the detected faults. (default: 250=2.5seconds) 0-1023: the time for the operation to verify the deleted faults. (default: 1000=10 seconds)
no ethernet oam fault-detect meg *NAME* [**mepid** <1-8191>] {**priority** | **keep-time** | **clear-time**}		Deletes a specified value of parameters and returns to the default setting.

7.7.5 Y.1731 OAM on Trunk Port

Enable/disable ITU-T Y.1731 OAM on the trunk port, use the following command.

Command	Mode	Description
ethernet oam trunk *PORT* **meg** *NAME*	Global	Enables Y.1731 OAM on a trunk port. PORT: a port number of bridge NAME: MEG's name
no ethernet oam trunk *PORT*		Disables Y.1731 OAM on a trunk port. PORT: a port number of bridge

7.7.6 Sender ID TLV

To add/delete the sender ID TLV to OAM PDUs, use the following command.

Command	Mode	Description
ethernet oam tlv-permission sender-id	Global	Adds the sender ID TLV to OAM PDUs.
no ethernet oam tlv-permission sender-id		Deletes the sender ID TLV.

7.7.7 MEG Cross-check

To enable/disable Y.1731 cross-check function for a MEG, use the following command.

Command	Mode	Description
ethernet oam cross-check enable meg *NAME*	Global	Enables Y.1731 cross-check for a specific MEG.
ethernet oam cross-check disable meg *NAME*		Disables Y.1731 crosscheck for a specific MEG.

To configure a waiting time for remote MEPs to perform the cross-check function, use the following command.

Command	Mode	Description
ethernet oam cross-check start-delay <1-65535>	Global	Sets a waiting time that the switch waits for remote MEPs until performing the cross-check function. 1-65535: the delay time for cross-check (default: 30s)
no ethernet oam cross-check start-delay		Deletes the configured waiting time before the cross-check function is started.

To create and specify a remote MEP that is added in the static list of expected remote MEPs for cross-check, use the following command.

Command	Mode	Description
ethernet oam cross-check rmep-id <1-8191> **meg** *NAME*	Global	Specifies a remote MEP for the cross-check. 1-8191: the remote MEP ID NAME: the name of MEG
no ethernet oam cross-check rmepid <1-8191> **meg** *NAME*		Clears the configured remote MEP for the cross-check.

To display the configured Y.1731 OAM crosscheck function, use the following command.

Command	Mode	Description
show ethernet oam remote mep cross-check [**meg** *NAME*]	Global	Shows the list of remote MEPs for the cross-check.

7.7.8 Ethernet Continuity Check (ETH-CC)

Ethernet Continuity Check function is used to detect loss of continuity between any pair of MEPs in a MEG. ETH-CC supports fault detection through Continuity Check Messages (CCMs) that allow end-points to detect an interruption in service. To enable/disable ETH-CC transmission in a MEG, use the following command.

Command	Mode	Description
ethernet oam cc enable meg *NAME* [**mepid** <1-8191>]	Global	Enables MEPs to send Continuity Check messages.
ethernet oam cc disable meg *NAME* [**mepid** <1-8191>]		Disables MEPs to send Continuity Check messages.

To enable/disable unicast CC transmission, use the following command.

Command	Mode	Description
ethernet oam cc unicast enable meg *NAME* **mepid** <1-8191> **rmac** *MACADDR*	Global	Enables unicast ETH-CC transmission in a MEG. 1-8191: MEP's ID MACADDR: the remote MEP's MAC address
ethernet oam cc unicast disable meg *NAME* **mepid** <1-8191> [**rmac** *MACADDR*]		Disables unicast ETH-CC transmission in a MEG.

To identify the priority of frame with ETH-CC information, use the following command.

Command	Mode	Description
ethernet oam cc meg *NAME* **priority** <0-7>	Global	Specifies a priority of CCM frames. <0-7>: priority of CCM frames (default: 7)
no ethernet oam cc meg *NAME* **priority**		Deletes a specified priority and returns to the default setting.

To specify an interval for sending periodic continuity check messages, use the following command.

Command	Mode	Description
ethernet oam cc meg *NAME* **interval** *TIME*	Global	Configures the interval of CCMs. TIME: 3.3ms, 10ms, 100ms, 1s(default), 10s, 1min, 10min
no ethernet oam cc meg *NAME* **interval**		Deletes a specified interval and returns to the default setting.

The following table shows CCM interval field encoding for ITU-T Y.1731 OAM.

Interval Field	Period Value	Transmission Rate
2	10 ms	100 frames per second
3	100 ms	10 frames per second (default transmission period for performance monitoring application)
4	1 s	1 frames per second (default transmission period for fault management application)
5	10 s	6 frames per minute
6	1 min	1 frames per minute
7	10 min	6 frames per hour

Tab. 7.1 ETH-CCM Interval Field Encoding

i

Even through 6 different values are specified for transmission period, the default values are recommended based on the application area for which ETH-CC is being used.

The consecutive number of the CCMs losses indicates that a remote MEP has gone down or not. To set the threshold of CCMs that are consecutively lost, use the following command.

Command	Mode	Description
ethernet oam cc meg *NAME* **loss-threshold** <2-255>	Global	Configures the loss threshold of continuity check messages. (default : 3)
no ethernet oam cc meg *NAME* **loss-threshold**		Deletes a specified loss threshold and returns to the default setting.

MEP can send CCM PDU with the pseudo MEG's name and receive CCM PDU from a remote MEP of pseudo MEG. To specify a MEP to communicate with a remote MEP of pseudo MEG, use the following command.

Command	Mode	Description
ethernet oam cc meg *NAME* **mepid** <1-8191> **pseudo-meg** *NAME*	Global	Specified a MEP to communicate with a remote MEP of pseudo MEG. NAME: MEG name 1-8191: MEP's ID NAME: pseudo MEG name for CCM
no ethernet oam cc meg *NAME* **mepid** <1-8191> **pseudo-meg**		Deletes a specified remote MEP of pseudo MEG.

To change the format of CCM PDU from Y.1731's to CFM OAM's, use the following command.

Command	Mode	Description
ethernet oam pdu-to-cfm	Global	Changes the format of CCM PDU from Y.1731 to CFM.
no ethernet oam pdu-to-cfm		Returns to the default Y.1731 format of CCM PDU.

Before the list of remote MEPs that cannot receive the continuity check messages is removed from the database, this data is kept for the configured hold time. To configure a hold time that MEP data is kept before it is removed from the database, use the following command.

Command	Mode	Description
ethernet oam meg *NAME* **archive-hold-time** <1-65535>	Global	Configures the time that missing MEP data is kept before it is removed from the database. (default: 100 minutes)
no ethernet oam meg *NAME* **archive-hold-time**		Deletes a specified hold time and returns to the default setting.

In Y.1731, the concept of MD is not defined, but a maintenance entity group (MEG) is defined in Y.1731 is the same as the MA, an MEG level is the same as the MD level. If the LD3032 receives Continuity Check (CC) message of Connectivity Fault Management (CFM) OAM, it can handle this message using the configured MD.

To specify a MD name, use the following command.

Command	Mode	Description
ethernet oam meg *NAME* **md** *NAME*	Global	Specifies a MD name for CC operation of CFM OAM.
no ethernet oam meg *NAME* **md** *NAME*		Deletes the configured MD name.

7.7.8.1 SNMP Server Traps

CCM frames with ETH-CC information allow detection of different defect conditions, which include:

- **Remote Detect Indication Condition**
  The **rdi** trap is shown when a MEP detects RDI with it receives a CCM frame with the RDI field set.
- **Loss of Continuity (LOC) Condition**
  The **loc** trap is shown if no CCM frames from a peer MEP are received within the interval equal to 3.5 times the receiving CCM transmission period.
- **Mismerge Condition**
  The **mmg** trap is shown when a CCM frame with same MEG level but with a MEG ID different than the receiving MEP’s own MEG ID is received.
- **Unexpected MEP Condition**
  The **unm** trap is shown when a CCM frame with an incorrect MEP ID, including receiving MEP’s own MEP ID, is received.
- **Unexpected MEG Level Condition**
  The **uml** trap is shown when a CCM frame with a MEG level lower than the receiving MEP’s MEG level is received.
- **Unexpected Period Condition**
  The **unp** trap is shown when a CCM frame is received with a period field value different than the receiving MEP’s own CCM transmission period.

To generate SNMP traps when detecting one of the defect conditions, use the following command.

Command	Mode	Description
ethernet oam snmp-server traps {**rdi** | **loc** | **unp** | **unm** | **mmg** | **unl**}	Global	Generates SNMP trap when a defect condition error occurs. rdi: remote defect indication error loc: loss of continuity error unp: unexpected period error unm: unexpected MEP error mmg: mismerge error unl: unexpected MEG level error

no ethernet oam snmp-server traps { **rdi** | **loc** | **unp** | **unm** | **mmg** | **unl**}		Disables SNMP trap generation by a specific defect condition.

7.7.9 Ethernet Loopback (ETH-LB)

Ethernet Loopback function supports fault verification through Loopback Messages (LBM) and Loopback Reply (LBR). These messages are used during initial set-up or after a fault has been detected to verify that the fault has occurred between two end points. Y.1731 allows both unicast and multicast loopback.

To configure unicast or multicast ETH-LB function, use the following command.

Command	Mode	Description
ethernet oam ping meg *NAME* **mepid** <1-8191> **multicast** [**timeout** <1-1000> **priority** <0-7>]	Global	Sends LBM frames with multicast ETH-LB information. 1-8191: source MEP ID for LBMs to send 1-1000: the waiting time for expected reception of LBRs (default: 5 seconds) 0-7: the priority of CCM or LTM messages (default:7)
ethernet oam ping meg *NAME* **mepid** <1-8191> **unicast** {**rmepid** <1-8191> | **rmac** *MACADDR*} [<1-6000> <100-60000> <1-1000> <0-7> <5-1480>]		Sends LBM frames with uniicast ETH-LB information to the configured remote MEP. 1-8191: source/destination MEP ID for LBMs to send MACADDR: MAC address of a remote MEG 1-6000: the number of LBMs to be transmitted (default:1) 100-60000: interval for sending OAM PDUs (default: 1000ms) 1-1000: the waiting time for receiving the expected response OAM PDUs (default: 5 seconds) 0-7: the priority of CCM or LTM messages (default:7) 5-1480: the length of data TLV (default:5)

7.7.10 Ethernet Link Trace (ETH-LT)

ETH-LT function is used to retrieve adjacency relationship between a MEP and a remote MEP or MIP. And it is also used for fault localization. The LD3032 sends LinkTrace Message (LTM) frames to discover a path for a link trace.

To generate LTM frames, use the following command.

Command	Mode	Description
ethernet oam traceroute meg *NAME* **mepid** <1-8191> {**rmepid** <1-8191> | **rmac** *MACADDR*} [**ttl** <1-64> **priority** <0-7>] [**use-fdb-only**]	Global	Sends LTM frames for a linktrace route. 1-8191: source/destination MEP ID to send LTMs MACADDR: destination MAC address to send LTMs 1-64: LTM's TTL (default: 64) 0-7: LTM message priority (default: 7)
ethernet oam traceroute meg *NAME* **mepid** <1-8191> {**rmepid** <1-8191> | **rmac** *MACADDR*} **use-fdb-only** [**ttl** <1-64> **priority** <0-7>]		

		use-fdb-only: only MAC address learned in FDB, not MPDB is to be used to determine the egress port

To set a maximum Y.1731 traceroute cache hold time that cache entries will be retained, use the following command.

Command	Mode	Description
ethernet oam traceroute cache hold-time <1-65535>	Global	Configures a hold time of traceroute cache entries. (default: 100 minutes)
no ethernet oam traceroute cache hold-time		Deletes a specified hold time of traceroute cache entries and returns to the default setting.

A traceroute cache size is the number of entries which are stored in cache table. To set a traceroute cache size in number of entry, use the following command.

Command	Mode	Description
ethernet oam traceroute cache size <1-4095>	Global	Configures the maximum numbers of entries in the traceroute cache table. (default: 100)
no ethernet oam traceroute cache size		Deletes a specified numbers of traceroute cache entries and returns to the default setting.

To display Y.1731 traceroute cache information, use the following command.

Command	Mode	Description
show ethernet oam traceroute-cache [**transaction** *TRANSACTION_ID*]	Enable Global	Shows the information of the traceroute cache.

To delete Y.1731 traceroute cache entries, use the following command.

Command	Mode	Description
clear ethernet oam traceroute-cache	Enable Global	Removes the traceroute cache entries.

7.7.11 Ethernet Alarm Indication Signal (ETH-AIS)

ITU-T Y.1731 supports fault notification through Alarm Indication Signal (AIS). Ethernet AIS is used to suppress alarms following detection of defect conditions at the server layer.

ETH-AIS implementation of the LD3032 has the following restriction, so you should keep in mind that before configuring ETH-AIS.

⚠

- ETH-AIS function can not be enabled with STP. When STP is already enabled in the system, ETH-AIS function can not be enabled.

7.7.11.1 Enabling ETH-AIS Function

To enable/disable ETH-AIS function, use the following command.

Command	Mode	Description
ethernet oam ais enable meg *NAME* [**mepid** <1-8191>]	Global	Enables ETH-AIS function. NAME: MEG’s name
ethernet oam ais disable meg *NAME* [**mepid** <1-8191>]		Disables ETH-AIS function

i ETH-AIS function can not be used within STP environments. ETH-AIS can be enabled when STP is disabled in the system.

To enable/disable a transmission of frame with ETH-AIS information on a MEP, use the following command.

Command	Mode	Description
ethernet oam ais transmit enable meg *NAME* [**mepid** <1-8191>]	Global	Enables ETH-AIS frame transmission on a MEP. NAME: MEG’s name
ethernet oam ais transmit disable meg *NAME* [**mepid** <1-8191>]		Disables ETH-AIS frame transmission on a MEP.

To enable/disable Unicast AIS frame transmission from the configured MEPs, use the following command.

Command	Mode	Description
ethernet oam ais unicast enable meg *NAME* **mepid** <1-8191> **rmac** *MACADDR*	Global	Enables Unicast AIS frame transmission from the MEPs.
ethernet oam ais unicast disable meg *NAME* **mepid** <1-8191> [**rmac** *MACADDR*]		Disables Unicast AIS frame transmission from the MEPs.

7.7.11.2 ETH-AIS Client MEG Level

Upon detecting a defect condition the MEP can immediately start transmitting periodic frames with ETH-AIS information at a configured client MEG level.

To specify the level of AIS frames, use the following command.

Command	Mode	Description
ethernet oam ais meg *NAME* **level** <1-7>	Global	Specifies an AIS frame’s level. 1-7: AIS frame’s level (default: 7)

no ethernet oam ais meg *NAME* **level**		Deletes a configured AIS frame's level and returns to the default setting.

7.7.11.3 Configuring AIS Frames

To determine an AIS transmission period, use the following command.

Command	Mode	Description
ethernet oam ais meg *NAME* **interval** {**one-second** | **one-minute**}	Global	Determines transmission periodicity of frames with ETH-AIS information. (default: one-second)
no ethernet oam ais meg *NAME* **interval**		Deletes a configured transmission period and returns to the default setting.

To specify the priority of frames with ETH-AIS information, use the following command.

Command	Mode	Description
ethernet oam ais meg *NAME* **priority** <0-7>	Global	Specifies a priority of ETH-AIS frames. <0-7>: priority of AIS frames (default: 7)
no ethernet oam ais meg *NAME* **priority**		Deletes the configured priority and returns to the default setting.

7.7.12 Ethernet Locked Signal (ETH-LCK)

Ethernet Locked Signal function (ETH-LCK) is used to communicate the administrative locking of a server (sub) layer MEP and consequential interruption of data traffic forwarding towards the MEP expecting this traffic.

7.7.12.1 Enabling ETH-LCK Function

To enable/disable MEPs to communicate using LCK frames, use the following command.

Command	Mode	Description
ethernet oam lck enable meg *NAME* [**mepid** <1-8191>]	Global	Enables LCK function of MEPs. NAME: MEG's name
ethernet oam lck disable meg *NAME* [**mepid** <1-8191>]		Disables LCK function of MEPs

To enable/disable MEPs for sending LCK frames to its peer MEP ID, use the following command.

Command	Mode	Description
ethernet oam lck transmit enable meg *NAME* [**mepid** <1-8191>]	Global	Enables MEPs for sending LCK frames. NAME: MEG's name
ethernet oam lck transmit disable meg *NAME* [**mepid** <1-8191>]		Disables LCK frame transmission of MEPs

To enable/disable MEPs with LCK frames, use the following command.

Command	Mode	Description
ethernet oam lck unicast enable meg *NAME* **mepid** <1-8191> **rmac** *MACADDR*	Global	Transmits the frames with unicast ETH-LCK information to a specified remote MEP.
ethernet oam lck unicast disable meg *NAME* **mepid** <1-8191> [**rmac** *MACADDR*]		Disables the transmission of frames with unicast ETH-LCK information. .

7.7.12.2 ETH-LCK Client MEG Level

To specify the level of LCK frames, use the following command.

Command	Mode	Description
ethernet oam lck meg *NAME* **level** <1-7>	Global	Specifies a LCK frame's level. 1-7: LCK frame's level (default: 7)
no ethernet oam lck meg *NAME* **level**		Deletes a configured LCK frame's level and returns to the default setting.

7.7.12.3 Configuring LCK Frames

To determine an LCK transmission period, use the following command.

Command	Mode	Description
ethernet oam lck meg *NAME* **interval** {**one-second** | **one-minute**}	Global	Determines transmission periodicity of frames with ETH-LCK information. (default: one-second)
no ethernet oam lck meg *NAME* **interval**		Deletes a configured transmission period.

To specify the priority of frames with ETH-LCK information, use the following command.

Command	Mode	Description
ethernet oam lck meg *NAME* **priority** <0-7>	Global	Specifies a priority of LCK frames. <0-7>: priority of frames (default: 7)
no ethernet oam lck meg *NAME* **priority**		Deletes a specified priority and returns to the default setting.

7.7.13 Ethernet Test Signal (ETH-TEST)

A MEP sends an OAM message that includes test data, which can be used to test throughput, measure bit errors, or detect frames delivered out of sequence.

7.7.13.1 Enabling/Disabling ETH-Test

When out-of-service ETH-Test function is performed, client data traffic except for LBM or TST frames is disrupted in the diagnosed entity. To configure a MEG for the out-of-service test, use the following command.

Command	Mode	Description
ethernet oam out-of-service meg *NAME* [**mepid** <1-8191>]	Global	Performs an out-of-service ETH-Test function.
no ethernet oam out-of-service meg *NAME* [**mepid** <1-8191>]		Performs an in-service ETH-Test function.

7.7.13.2 One-way ETH-Test

To enable one-way ETH-Test function for receiving TST frames from a peer MEP, use the following command.

Command	Mode	Description
ethernet oam tst one-way receive meg *NAME* **mepid** <1-8191> [<5-6000>]	Global	Receives TST frames for a diagnostic test.

To enable one-way ETH-Test function for transmitting TST frames, use the following command.

Command	Mode	Description
ethernet oam tst one-way transmit meg *NAME* **mepid** <1-8191> **multicast** [<5-6000> <100-60000> <0-7> <5-1480> <0-3>]	Global	Transmits the frames with multicast ETH-TEST information. 1-8191: source MEP ID for TST frames to send 5-6000: duration to send OAM PDU (default: 5 sec.) 100-60000: interval for sending TST frames (default: 1000ms) 0-7: the priority of TST frames (default:7) 5-1480: length of test TLV (default: 5) 0-3: pattern of test TLV used for diagnostics test (default: 0)
ethernet oam tst one-way transmit meg *NAME* **mepid** <1-8191> **unicast rmepid** <1-8191> [<5-6000> <100-60000> <0-7> <5-1480> <0-3>]		Transmits the frames with unicast ETH-TEST information to a configured remote MEP. 1-8191: source/destination MEP ID for TST frames to send

7.7.13.3 Two-way ETH-Test

To enable two-way ETH-Test function between the configured two MEPs for performing bidirectional diagnostics tests, use the following command.

Command	Mode	Description
ethernet oam tst two-way meg *NAME* **mepid** <1-8191> **rmepid** <1-8191> | [<5-6000> <100-60000> <1-1000> <0-7> <5-1480> <0-3>]	Global	Performs bidirectional diagnostics tests using the frames with ETH-TEST information between MEPs. 1-8191: source/destination MEP ID for TST frames to send MACADDR: destination MAC address 5-6000: duration to send OAM PDU (default: 5 sec.) 100-60000: interval for sending TST frames (default: 1000ms) 1-1000: the waiting time for receiving the expected response OAM PDUs (default: 5 sec) 0-7: the priority of TST frames (default:7) 5-1480: length of test TLV (default: 5) 0-3: pattern of test TLV used for diagnostics test (default: 0)

7.7.14 Ethernet Frame Loss Measurement (ETH-LM)

Ethernet Frame Loss Measurement (ETH-LM) function is used for performance monitoring. Frame Loss Ratio (FLR) is defined as a ratio, expressed as a percentage, of the number of service frames no delivered by the total number of service frames during time interval. There are two types of FLR measurement, dual-ended LM and single-ended LM. Dual-ended LM is accomplished by exchanging CCM OAM frames that include appropriate counts of frames transmitted and received. Single-ended LM is accomplished by exchanging LMM and LMR OAM frames that include appropriate counts of frames transmitted and received.

i

Dual-ended LM enables the proactive measurement of both near end and far end FLR at each end of a MEG. But single-ended LM only provides near end and far end FLR at the end that initiated the LM Request.

7.7.14.1 Single-ended Loss Measurement

To enable/disable each MEP for sending periodic single-ended frames with ETH-LM information to its peer MEP, use the following command.

Command	Mode	Description
ethernet oam lmm meg *NAME* **mepid** <1-8191> **unicast rmepid** <1-8191> [<5-6000> <100-60000> <1-1000> <0-7>]	Global	Transmits the frames with unicast ETH-LM information. 1-8191: source/destination MEP ID to send LMMs 5-6000: the duration of LMMs to be transmitted (default: 5 seconds) 100-60000: the interval for sending LMMs (default: 100ms) 1-1000: the waiting time for receiving the expected response LLMs (default: 5s)

		0-7: LMM message priority (default: 7)
ethernet oam lmm meg *NAME* **mepid** <1-8191> **multicast** [<5-6000> <100-60000> <1-1000> <0-7>]		Transmits the frames with multicast ETH-LM information.

7.7.14.2 Dual-ended Loss Measurement

To enable/disable each MEP for sending periodic dual-ended frames with ETH-LM information to its peer MEP, use the following command.

Command	Mode	Description
ethernet oam dlm enable meg *NAME* **mepid** <1-8191> **rmepid** <1-8191>	Global	Enables a MEP to send dual-ended frames with ETH-LM information.
ethernet oam dlm disable meg *NAME* **mepid** <1-8191>		Disables a MEP to send dual-ended frames with ETH-LM information.

Dual-ended LM counts do not include OAM frames at the MEPs ME level.

To display the configuration of dual-ended frame loss measurement, use the following command.

Command	Mode	Description
show ethernet oam dlm [**meg** *NAME* [**mepid** <1-8191>]]	Global	Shows a configured dual-ended frame loss measurement.

7.7.15 Ethernet Frame Delay Measurement (ETH-DM)

To measure frame delay and frame delay variation, ETH-DM can be used for OAM. By sending/receiving periodic frames with ETH-DM information to/from the peer MEP, each MEP performs frame delay and frame delay variation measurement.

7.7.15.1 One-way ETH-DM

Each MEP sends frame with one-way ETH-DM information to its peer MEP. 1DM PDU is used to support one-way ETH-DM.

To transmit/receive 1DM frames to/from the peer MEP, use the following command.

Command	Mode	Description
ethernet oam 1dm receive meg *NAME* **mepid** <1-8191> [<5-6000>]	Global	Receives 1DM frames from a peer MEP. 1-8191: source MEP ID to receive 1DMs 5-6000: the duration (default: 5 s)
ethernet oam 1dm transmit meg *NAME* **mep-**		Transmits 1DM frames with multicast

id <1-8191> **multicast** [<5-6000> <100-60000> <0-7>]		ETH-DM information. 100-60000: the interval for sending OAM PDUs (default: 100ms) 0-7: the OAM PDU priority value (default: 7)
ethernet oam 1dm transmit meg *NAME* **mep-id** <1-8191> **unicast rmepid** <1-8191> [<5-6000> <100-60000> <0-7>]		Transmits 1DM frames with unicast ETH-DM information to a remote MEP.

Dual-ended LM counts do not include OAM frames at the MEPs ME level.

7.7.15.2 Two-way ETH-DM

A MEP sends frames with ETH-DM request information to its peer MEP and receives frames with ETH-DM reply information from its peer MEP. DMM is used to support two-way ETH-DM request.

To carry out two-way frame delay & frame delay variation measurements for a MEP, use the following command.

Command	Mode	Description
ethernet oam dmm meg *NAME* **mepid** <1-8191> **unicast rmepid** <1-8191> [<5-6000> <100-60000> <1-1000> <0-7>]	Global	Performs two-way ETH-DM using unicast transmission of DMM frames. 5-6000: the duration (default: 5 s) 100-60000: the interval for sending OAM PDUs (default: 100ms) 1-1000: the waiting time for receiving the expected response OAM PDUs (default: 5s) 0-7: the OAM PDU priority value (default: 7)
ethernet oam dmm meg *NAME* **mepid** <1-8191> **multicast** [<5-6000> <100-60000> <1-1000> <0-7>]		Performs two-way ETH-DM using multicast transmission of DMM frames. 5-6000: the duration (default: 5 s) 100-60000: the interval for sending OAM PDUs (default: 100ms) 1-1000: the waiting time for receiving the expected response OAM PDUs (default: 5s) 0-7: the OAM PDU priority value (default: 7)

7.7.16 Throughput Measurement

RFC2544 specifies measuring the throughput by sending frames at increasing rate, graphing the percentage of frames received, and reporting the rate at which frames start being dropped. In general this rate is dependent on the frame size. Unicast ETH-LB and ETH-Test can be used for performing the throughput measurement.

A MEP can insert TST frames or LBM frames with configured size, pattern, etc. at a rate to exercise the throughput and make one-way or two-way measurement.

To make one-way throughput measurement by receiving TST frames from a peer MEP, use the following command.

Command	Mode	Description
ethernet oam tm one-way receive meg *NAME* **mepid** <1-8191> [<5-6000>]	Global	Receives TST frame for one-way throughput measurement. 5-6000: duration to send OAM PDU (default: 5s)

To make one-way throughput measurement of unicast or multicast transmission of TST frames, use the following command.

Command	Mode	Description
ethernet oam tm one-way transmit meg *NAME* **mepid** <1-8191> **multicast** [<5-6000> <1-5> <100-1000> <100-1000> <0-7> <5-1480> <0-3>]	Global	Makes one-way throughput measurement of multicast transmission of TST frames. NAME: MEG's name 5-6000: duration to send OAM PDU (default: 5s) 1-5: part duration of OAM PDU to be transmitted at the same transmission rate (default: 1) 100-1000: the number of OAM PDUs to be transmitted per second at first time (default: 100) 100-1000: the increment of number of OAM PDUs to be transmitted (default: 200) 0-7: OAM PDU priority (default: 7) 5-1480: the length of Test TLV (default: 5) 0-3: the pattern of Test TLV used for diagnostics test (default: 0)
ethernet oam tm one-way transmit meg *NAME* **mepid** <1-8191> **unicast rmepid** <1-8191> [<5-6000> <1-5> <100-1000> <100-1000> <0-7> <5-1480> <0-3>]		Makes one-way throughput measurement of unicast transmission of TST frames. 1-8191: source/destination MEP IDs

To make two-way throughput measurement by LBM frames, use the following command.

Command	Mode	Description
ethernet oam tm two-way meg *NAME* **mepid** <1-8191> **rmepid** <1-8191> [<5-6000> <1-5> <100-1000> <100-1000> <1-1000> <0-7> <5-1480> <0-3>]	Global	Makes two-way throughput measurement by LBM frames

7.7.17 Displaying Y.1731 OAM Information

To display the information of Y.1731 OAM, use the following command.

Command	Mode	Description
show ethernet oam meg [*NAME*]	Global	Shows information of Y.1731 maintenance entity group.
show ethernet oam config-error		Shows the Y.1731 configuration errors of a specific

vlan *VLAN* [**port** *PORT*]		VLAN ID.
show ethernet oam config-error [**port** *PORT*]		Shows the Y.1731 configuration errors of a specific port.
show ethernet oam error [**meg** *NAME*]		Shows the errors of connection between MEPs newly registered.

To display the information of MEPs configured on a switch, use the following command.

Command	Mode	Description
show ethernet oam local mep [**meg** *NAME*]	Global	Shows the information of Y.1731 local MEPs configured on a switch.
show ethernet oam local mep detail meg *NAME* **mepid** <1-8191>		Shows details of a local MEP in the Y.1731 database.
show ethernet oam remote mep [**meg** *NAME* [**mepid** <1-8191>]]		Shows information of a remote MEP in the Y.1731 database.
show ethernet oam remote mep detail meg *NAME* **mepid** <1-8191> **rmepid** <1-8191>		Shows details of a remote MEP in the Y.1731 database.

To display the entries in the maintenance domain intermediate points (MIPs) CCM database, use the following command.

Command	Mode	Description
show ethernet oam mip [**port** *PORT*]	Global	Shows the entries in the MIPs
show ethernet oam mip-ccdb		Shows the entries in the MIPs CCM database.

7.7.18 Deleting Y.1731 Database

To delete the Y.1731 OAM information, use the following command.

Command	Mode	Description
clear ethernet oam remote mep [**meg** *NAME*]	Enable Global	Deletes the data of remote MEP stored in MEP.
clear ethernet oam mip-ccdb		Deletes all of entries in the MIP CCM database.
clear ethernet oam error [**meg** *NAME*]		Deletes the errors of connection between MEPs. NAME: MEG name

7.7.19 Ring Automatic Protection Switching (R-APS)

The ITU-T Recommendation G.8032 specifies Ring Automatic Protection Switching (R-APS) as a network protection mechanism for Ethernet ring topology to prevent frequent operation of the protection switch due to an intermittent defect. An Ethernet ring consists of R-APS nodes. Each node (switch) is configured as a Ring Protection Link (RPL) owner node or a normal node. They exchange R-APS frames through ring ports. RPL-owner node blocks one of the ring ports to ensure that there is no loop formed for the Ethernet traffic. There is only one RPL-owner node in a ring. The normal nodes are responsible to inform their ring's owner node of Link failures/recovery. RPL is a single ring topology to be controlled by R-APS mechanism.

Both RPL-owner node and normal node have a west and east port for R-APS operation. Firstly, you should specify RPL ports, which are directly connected to the RPL link within an Ethernet ring. One of ring ports of RPL-owner node is blocked as unused link for traffic while it runs without the link failure detection. You should configure a west or east port to be blocked.

R-APS Messages

There are three types of R-APS messages of concern to the RPL-owner node-Normal node interaction in ring as shown below:

- **Normal Node messages**
  The following messages are sent by the normal nodes to inform RPL-owner node of their link changes.
  – **Signal Fail (SF)**: A normal node sends Signal Fail fames detecting its link failure.
  – **No Request (NR)**: A normal node sends No Request frames detecting its link recovery.

- **RPL-owner Node messages**
  An RPL-owner node is in charge of protecting the Ethernet ring. It sends periodic No Request frames to normal nodes and receives Signal fail/No Request frame from those nodes to detect the link failure or recovery.
  – **Signal Fail**: A RPL-owner node sends Signal Fail fames detecting its link failure.
  – **No Request and RPL Blocked**: This is used to inform the normal nodes of re-blocking status of its RPL port caused by link recovery.

R-APS implementation of the LD3032 has the following restrictions, so you should keep in mind those before configuring R-APS.

- R-APS can not be configured with STP. For enabling R-APS in the system, STP might be manually disabled.
- A west and east port number of RPL-owner node should be different.
- R-APS mechanism should be used for Ethernet Ring topology only.

If the link failure occurs, the nodes adjacent (Node A & B) to the failure detect their state and send Signal Fail (SF) frames. If an intermediate node (Node C) between RPL-owner node and a node adjacent to link failure receives SF frame, it starts to perform Forwarding Database (FDB) Flushing. FDB Flushing consists in erasing in the forwarding database of the switch all MAC entries that are forwarded to the ports. The Flushing of FDB is always followed by a period with MAC learning disabled. To prevent wrong MAC learning due to the remaining packets in the buffer, a node does not learn MAC addresses during a configured guard time.

After RPL-owner node receives SF frames from other nodes, it unblocks its RPL port for traffic transmission with Node B directly connected to the RPL port. RPL-owner node sends NR-RB (No Request and RPL Blocked) frame and informs the other nodes that its RPL port begins forwarding the traffic.

The following figure shows an example of R-APS operation in case of a link failure and a ring protection.

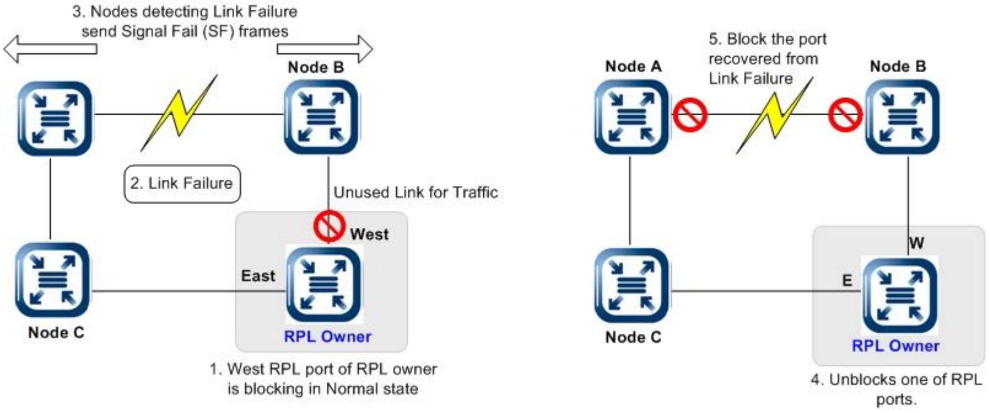


Fig. 7.4 Ring Protection in case of Link Failure

If Node A and Node B detect the link failure being recovered, they send No Request (NR) frames to RPL owner. But these nodes keep the blocking status of the link recovered ports. After RPL owner receives the frames, it blocks its own west RPL port. The RPL owner sends RPL Blocked frame that informs other nodes the blocking status of its RPL port. By receiving the frame, the nodes unblocks the ring ports which are detected a Link Failure recovery. The Ethernet ring is back to normal (Idle) state. RPL-owner node sends NR-RB (No Request and RPL Blocked) frame in idle state.

The following figure shows an example of a Link Failure and Ring Recovery operation.

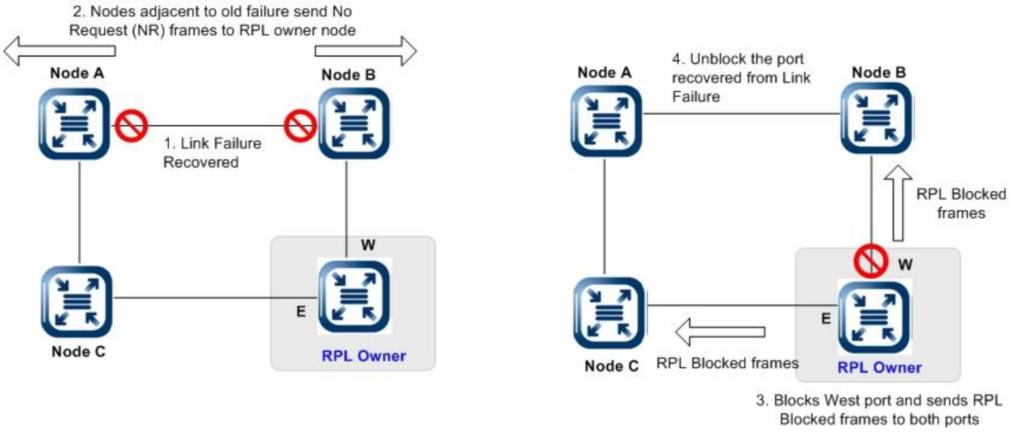


Fig. 7.5 Ring Recovery Procedure

The LD3032 supports G.8032v2 Ethernet ring protection switching. Version 2 of G.8032 introduced many additional features, such as:

- Multiple rings/ladder network support
- Revertive/Non-revertive mode after condition, that is causing the switch, is cleared
- Administrative commands: Forced Switch (FS), Manual Switch (MS) for blocking a particular ring port
- Flush FDB (Filtering database) Logic, which significantly reduces amount of flush FDB operations in the ring
- Support of multiple ERP instances on a single ring

7.7.19.1 Enabling R-APS Node

To operate the switches with R-APS configurations, you should enable RPL node. To enable/disable the R-APS configurations, use the following command.

Command	Mode	Description
ethernet oam r-aps <1-255> **enable**	Global	Enables R-APS node. 1-255: R-APS ring ID
ethernet oam r-aps <1-255> **disable**		Disables R-APS node.

! R-APS function must be disabled before the parameters are configured.

7.7.19.2 RPL Port State

To configure ring ports of R-APS node, use the following command.

Command	Mode	Description
ethernet oam r-aps <1-255> **ringports east** *E-PORT* **west** *W-PORT*	Global	Configures west port and east port. 1-255: R-APS ring ID NAME: MEG name
no ethernet oam r-aps <1-255> **ringports**		Deletes the configured RPL ports.

i West port and east port can not use same port number.

The RPL-owner node has east and west ring ports. One of ring port should be blocked as unused link for traffic while the ring runs without any link failure and the other port forwards the traffic to normal nodes. But you can determine an RPL port either West or East port to be blocked for the network management.

To manually configure a west or east port as an unused link that should be blocked traffic for Ethernet ring management, use the following command.

Command	Mode	Description
ethernet oam r-aps <1-255> **rpl** {**east** | **west**} {**owner** | **neighbour** | **next-neighbour**}	Global	Configures a west or east port as an unused link of RPL port. owner: responsible for blocking traffic over the RPL so that no loops are formed in the Ethernet traffic neighbor: an Ethernet ring node adjacent to the RPL next-neighbor: an Ethernet ring node adjacent to an RPL owner node or RPL neighbor node
no ethernet oam r-aps <1-255> **rpl** {**east** | **west**}		Deletes a configured RPL port of owner node.

i

There can be only one RPL owner node in a ring.

To create an R-APS ring node, use the following command.

Command	Mode	Description
ethernet oam r-aps <1-255> **level** <0-7> **vlan** *VLAN* [**sub-ring**] [**traffic-vlan** *VLAN*]	Global	Creates an R-APS ring node with ring ID, level and VLAN ID. 1-255: R-APS ring ID 0-7: R-APS ring node’s level VLAN: control VLAN ID of R-APS ring node

7.7.19.3 RPL Port State Switch

To move the blocking role of the RPL by blocking a ring link and unblocking the RPL temporarily, use the following command.

Command	Mode	Description
ethernet oam r-aps <1-255> **forced-switch** {**east | west**}	Global	Allows the operator to forcefully block a particular ring port.
ethernet oam r-aps <1-255> **manual-switch** {**east | west**}		Allows the operator to manually block a particular ring port.
ethernet oam r-aps <1-255> **clear-switch**		Cancels an existing forced-switch or manual-switch command on the ring port. And if its role is the RPL owner, the Wait-to-Restore and Wait-to-Block timers expire by this command.

i

Note the following points about forced-switch command.
- Effective even if there is an existing signal failure (SF) condition
- Multiple forced-switch commands for ring are supported
- May be used to allow immediate maintenance operations

i

Note the following points about manual-switch command.
- Ineffective in an existing forced-switch or signal failure (SF) condition
- Overridden by new forced-switch or SF conditions
- Multiple manual-switch commands cancel all manual-switch commands

In revertive operation, when the failure is recovered, the traffic channel resumes the use of the recovered ring link only after the traffic channel has been blocked on the RPL. On the other hand, in non-revertive operation, the traffic channel remains blocked on the recovered ring link and unblocked on the RPL even if the failure is recovered.

To specify a non-revertive or revertive mode, use the following command.

Command	Mode	Description
ethernet oam r-aps <1-255> **non-revertive**	Global	Specifies a non-revertive mode.
no ethernet oam r-aps <1-255> **non-revertive**		Specifies a revertive mode.

7.7.19.4 Hold Off Time

When a link failure occurs, the nodes start Hold off timer. The nodes do not change its link state until a hold off timer expires, to ensure that while the fault still exists, a link failure state is maintained. After the timer expires, they send the Signal Fail (SF) frames. The ring state is not changed from idle to protection state during the hold off time.

To specify hold-off time, use the following command.

Command	Mode	Description
ethernet oam r-aps <1-255> **hold-off-time** <0-10000>	Global	Configures hold-off time 0-10000: hold-off time (default: 100ms, unit: millisecond)

To configure hold-off time as default, use the following command.

Command	Mode	Description
no ethernet oam r-aps <1-255> **hold-off-time**	Global	Configures hold-off time as default value

7.7.19.5 Guard Time

If Node A and Node B detect the link failure being recovered, they send No Request (NR) frames to RPL owner and starts a guard timer to keep the blocking status of the link recovered ports. To prevent ring nodes from receiving out dated R-APS messages, RPL port of these nodes does not receive any frames from the external switches until this timer has expired.

To configure a Guard Time, use the following command.

Command	Mode	Description
ethernet oam r-aps <1-255> **guard-time** <10-2000>	Global	Configures guard time 10-2000: guard time (unit: millisecond, default: 500ms)

To delete the configured a Guard Time, use the following command.

Command	Mode	Description
no ethernet oam r-aps <1-255> **guard-time**	Global	Configures guard time as default value

7.7.19.6 Wait-to-Restore Time

If a port's link failure is recovered on the normal node, the blocked port should be changed to the forwarding status. However, the loop may occur when this port start to forward the traffic before a port of RPL-owner node is blocked. To prevent frequent operation of the protection switch due to an intermittent defect, the RPL-owner node starts a wait-to-restore timer. If there is no link failure until the timer has expired, RPL-owner blocks RPL port and starts FDB flushing. To specify a wait-to-restore time, use the following command.

Command	Mode	Description
ethernet oam r-aps <1-255> **wait-to-restore** <1-12>	Global	Configures wait-to-restore time. 1-12: Wait to restore time in minute (default:5 minutes)

To delete the configured wait-to-restore time, use the following command.

Command	Mode	Description
no ethernet oam r-aps <1-255> **wait-to-restore**	Global	Deletes the configured wait-to-restore time.

7.7.19.7 Wait-to-Block Time

After a force switch or a manual switch command is issued, a Wait-to-Block (WTB) timer is used to verify that no background condition exists. To specify a wait-to-block time, use the following command.

Command	Mode	Description
ethernet oam r-aps <1-255> **wait-to-block** <5-7>	Global	Configures wait-to-block time. 5-7: Wait to block time in minute (default:5 minutes)

To delete the configured wait-to-block time, use the following command.

Command	Mode	Description
no ethernet oam r-aps <1-255> **wait-to-block**	Global	Deletes the configured wait-to-block time.

i Wait-to-Block timer may be shorter than the Wait-to-Restore timer.

7.7.19.8 Interconnection Node

G.8032 specifies support for a network of interconnected rings. An interconnection node is an Ethernet ring node which is common to two or more Ethernet ring or to a sub-ring and an interconnected network. At each interconnection node there may be one or more Ethernet rings that can be accessed through a single ring port and not more than one Ethernet ring that is accessed by two ring ports. If the interconnecting node is used to connect a set of sub-ring to another network, then there is no Ethernet ring accessed by two ring ports.

The special node for ring interconnection is called an interconnection node, and links between them are called shared links. To specify the ring port of R-APS interconnection node, use the following command.

Command	Mode	Description
ethernet oam r-aps <1-255> **interconnection** {**east** | **west**} [{ **primary** | **secondary**}]	Global	Specifies the ring port type of R-APS interconnection node. primary | secondary: indicates the primary/secondary node for the minimization of the segmentation.
no ethernet oam r-aps <1-255> **interconnection**		Deletes the configured ring ports of R-APS interconnection node.

7.7.19.9 R-APS Virtual Channel

The R-APS virtual channel is the R-APS channel connection between two Interconnecting nodes of a sub-ring in other Ethernet ring(s) or network(s). For sub-rings, the two interconnection nodes may exchanges via a special virtual R-APS channel on the shared links.

- Sub-ring with R-APS virtual channel option, R-APS messages are encapsulated and transmitted over an R-APS virtual channel configured on the major ring.
- Sub-ring without R-APS virtual channel option, R-APS messages are terminated at the interconnection nodes but not blocked at RPL of the sub-ring.

To enable/disable a dedicated VLAN ID, use the following command.

Command	Mode	Description
ethernet oam r-aps <1-255> **virtual-channel**	Global	Configure R-APS channel of sub-ring with R-APS virtual channel.
no ethernet oam r-aps <1-255> **virtual-channel**		Configure R-APS channel of sub-ring without R-APS virtual channel.

7.7.19.10 Topology Change Propagation

To enable/disable the topology change propagation, use the following command.

Command	Mode	Description
ethernet oam r-aps <1-255> **propagate-tc**	Global	Enables the topology change propagation.
no ethernet oam r-aps <1-255> **propagate-tc**		Disables the topology change propagation.

7.7.19.11 Multiple Failure

In some cases, ring segmentation occurs due to multiple failures. To enable/disable the minimization of segmentation in case of multiple failures, use the following command.

Command	Mode	Description
ethernet oam r-aps <1-255> **multiple-failure** { **primary** | **secondary**}	Global	Enables the minimization of segmentation in case of multiple failures. primary | secondary: the primary/secondary node for the minimization of the segmentation
no ethernet oam r-aps <1-255> **multiple-failure**		Disables the minimization of segmentation in case of multiple failures.

7.7.19.12 Flooding Block

To enable/disable a flooding block, use the following command.

Command	Mode	Description
ethernet oam r-aps flooding-block enable	Global	Enables the flooding block state of R-APS node.
ethernet oam r-aps flooding-block disable		Disables the flooding block state of R-APS node.

7.7.19.13 Displaying R-APS Configuration

To display a configuration of R-APS, use the following command.

Command	Mode	Description
show ethernet oam r-aps	Global	Shows the information of R-APS
show ethernet oam r-aps detail <1-255>		Shows the R-APS node information. NAME: MEG name
show ethernet oam r-aps pkt statistics [<1-255>]		Shows the number of events and R-APS messages received for an ERP instance.

To clear the collected R-APS packet statistics, use the following command.

Command	Mode	Description
clear ethernet oam r-aps pkt statistics [<1-255>]	Global	Clears the R-APS packet statistics.

7.7.20 Uplink Redundancy

The OAM CCM-based uplink redundancy network consists of master node and slave node that are connected to uplink network. Each nodes are has communication ports and the ring topology consists of a primary and a secondary path (channel).

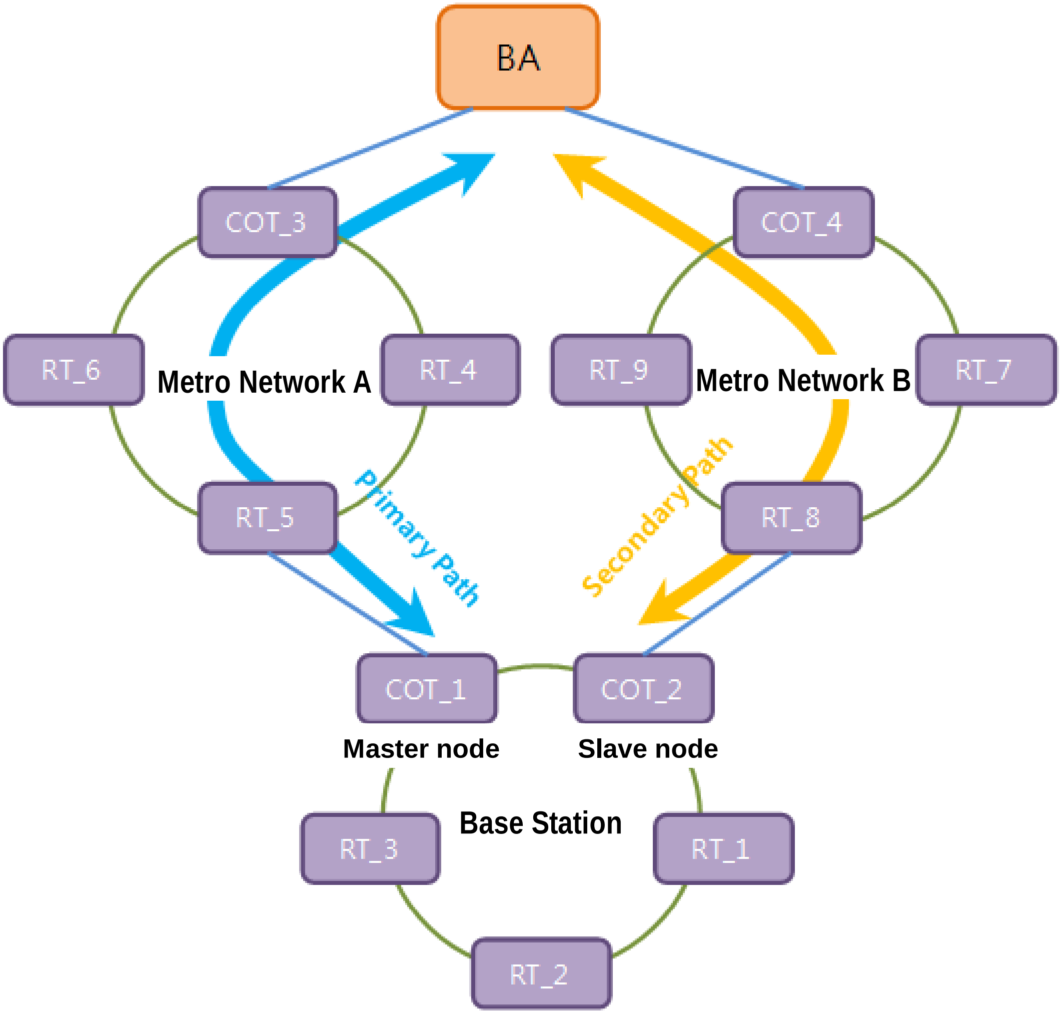


Fig. 7.6 Uplink Redundancy Deployment Scenario

The uplink redundancy feature is implemented on the base station network. COT_1 is a master node and COT_2 is a slave node for uplink redundancy operation. Both mater and slave nodes' uplink ports are connected to the metro/core network. The uplink path of master node is called as primary path, the slave node's uplink path is called as secondary path.

Uplink redundancy implementation of the LD3032 has the following restrictions/conditions, so you should keep in mind those before configuring uplink redundancy

- A single master node and slave node should be configured on the network.
- A master node should be connected to a slave node in order to transmit the OAM packets each other. OAM function must be enabled on the LD3032.
- A master node and slave node communicate with each other using tagged packets through the configured control VLAN ID. The appropriate VLAN port membership should be configured.

7.7.20.1 Enabling/disabling Uplink Redundancy

To enable/disable the uplink redundancy for the specified MEG, use the following command.

Command	Mode	Description
ethernet oam uplink-redundancy enable meg *NAME*	Global	Enables the uplink redundancy for specified MEG ID. NAME: MEG name
ethernet oam uplink-redundancy disable meg *NAME*		Disables the uplink redundancy for specified MEG ID.

7.7.20.2 Master / Slave Node

To specify an uplink redundancy port of master / slave node, use the following command.

Command	Mode	Description
ethernet oam uplink-redundancy meg *NAME* { **master** | **slave**} **port** *PORT*	Global	Specifies the port of master/slave node for uplink redundancy.
no ethernet oam uplink-redundancy meg *NAME* { **master** | **slave**}		Deletes the configured port of master/slave node for uplink redundancy.

A secondary path of slave node is supposed to be blocked as unused uplink link for traffic while uplink redundancy runs without any link failure or loss of OAM CCM message. While a primary path of master node is forwarded the uplink traffic. But you can configure the uplink port of master node (primary path) to be manually blocked. An uplink port of slave node (secondary path) is automatically changed to forward the traffic.

To manually change to the blocking state of the master node’s uplink port, use the following command.

Command	Mode	Description
ethernet oam uplink-redundancy meg *NAME* **manual-switch**	Global	Blocks the uplink port of master node. If the link failure occurs on the uplink port of slave node, the forwarding state of mater node does not change to blocking state.

To forcefully change to the blocking state of the master node's uplink port, use the following command.

Command	Mode	Description
ethernet oam uplink-redundancy meg *NAME* **forced-switch**	Global	Allows the operator to forcefully block the uplink port of master node. If the link failure occurs on the uplink port of slave node, both uplink ports of slave and mater node are blocked.
no ethernet oam uplink-redundancy meg *NAME* **forced-switch**		Cancels an existing forced-switch command on the uplink port.

7.7.20.3 Control VLAN

For uplink redundancy operation, there are one master node and the other slave node. To communicate each other, it needs to transmit the control packets through the control VLAN ID.

To enable/disable a control VLAN ID for communication between a master node and slave node, use the following command.

Command	Mode	Description
ethernet oam uplink-redundancy meg *NAME* **control-vlan** *VLAN*	Global	Specifies a control VLAN ID.
no ethernet oam uplink-redundancy meg *NAME* **control-vlan**		Deletes the configured control VLAN ID.

7.7.20.4 Ring Topology Monitoring

The LD3032 provides uplink redundancy feature with G.8032 (ERPS) ring topology. If the communication between the master and slave node is not available because of the internal error of ring, the uplink ports of master/slave node should be changed to the forwarding state. To monitor the connectivity of ring ports via OAM CCM, use the following command.

Command	Mode	Description
ethernet oam uplink-redundancy meg *NAME* **cc meg** *NAME* **primary-mepid** <1-8191>	Global	Enables a single ring port to monitor connectivity between uplink ports of the master and slave node using OAM CCM.
ethernet oam uplink-redundancy meg *NAME* **cc meg** *NAME* **secondary-mepid** <1-8191>		Enables two ring ports to monitor connectivity between uplink ports of the master and slave node using OAM CCM.
no ethernet oam uplink-redundancy meg *NAME* **cc meg** *NAME* **primary-mepid**		Disables a single ring port to monitor connectivity between uplink ports of the master and slave node using OAM CCM.
no ethernet oam uplink-redundancy meg *NAME* **cc meg** *NAME* **secondary-mepid**		Disables two ring ports to monitor connectivity between uplink ports of the master and slave node using OAM CCM.

7.7.20.5 Traffic VLAN

By default, the uplink redundancy function is protected by entire VLAN IDs. However, this function can be performed per VLAN ID using the traffic VLAN ID. If a traffic VLAN is enabled and the scope of protection VLAN is limited to a single VLAN with uplink redundancy operation.

To enable/disable a traffic VLAN ID, use the following command.

Command	Mode	Description
ethernet oam uplink-redundancy meg *NAME* **traffic-vlan**	Global	Enables a traffic VLAN.
no ethernet oam uplink-redundancy meg *NAME* **traffic-vlan**		Disables a traffic VLAN.

7.7.20.6 Non-revertive Mode

If the uplink traffic is transmitted using secondary path (channel) due to the link failure of primary path,

- In revertive operation, when the primary path's failure is recovered, the traffic channel changes from secondary to primary.
- In non-revertive operation, the traffic remains on the secondary path (channel) even if the primary path's failure is recovered.

To specify a non-revertive or revertive mode, use the following command.

Command	Mode	Description
ethernet oam uplink-redundancy meg *NAME* **non-revertive**	Global	Specifies a non-revertive mode of master node.
no ethernet oam uplink-redundancy meg *NAME* **non-revertive**		Specifies a revertive mode.

7.7.20.7 Trust Member Port Count

If a port of uplink redundancy is a link or several links aggregated as a trunk, you can configure a link aggregation member port to perform the uplink link failure detection/recovery using the trust member port count value. This count is the number of member ports without any failure detection. If the number of normal member ports is less than the given value, it perceives that any failure is detected.

If the number of member ports is larger than or equal to the configured value, it perceives that any failure is not detected.

To configure the trust LOC count at link aggregation port, use the following command.

Command	Mode	Description
ethernet oam uplink-redundancy meg *NAME* **trust-member-count** *COUNT*	Global	Configures the trust LOC count at link aggregation port. COUNT: the trust member port count value
no ethernet oam uplink-redundancy meg *NAME* **trust-member-count**		Deletes the configured trust LOC count.

7.7.20.8 Hold Off Time

When a link failure occurs, the nodes start Hold off timer. The nodes do not change their uplink link state until a hold off timer expires, to ensure that while the fault still exists, a link failure state is maintained. To specify hold-off time, use the following command.

Command	Mode	Description
ethernet oam uplink-redundancy meg *NAME* **hold-off-time** <0-10000>	Global	Configures the hold-off time 0-10000: hold-off time (default: 100ms, unit: millisecond)

To configure hold-off time as the default, use the following command.

Command	Mode	Description
no ethernet oam uplink-redundancy meg *NAME* **hold-off-time**	Global	Configures the hold-off time as default value

7.7.20.9 Wait-to-Restore Time

If an uplink port's link failure is recovered on the revertive mode, the forwarding/blocking status of uplink ports is not changed right after the recovery, the nodes wait the given wait-to-restore time.

To specify a wait-to-restore time, use the following command.

Command	Mode	Description
ethernet oam uplink-redundancy meg *NAME* **wait-to-restore** <10-720>	Global	Configures wait-to-restore time. 10-720: Wait to restore time in second (default:5s)

To delete the configured wait-to-restore time, use the following command.

Command	Mode	Description
no ethernet oam uplink-redundancy meg *NAME* **wait-to-restore**	Global	Deletes the configured wait-to-restore time.

7.7.20.10 Displaying Uplink Redundancy Configuration

To display the configuration of uplink redundancy, use the following command.

Command	Mode	Description
show ethernet oam uplink-redundancy	Global	Shows the information of uplink redundancy.
show ethernet oam uplink-redundancy detail meg *NAME*		Shows detailed information of uplink redundancy. NAME: MEG name

7.7.20.11 Displaying Redundancy Sync-Module

To display a list of the redundancy sync-module, use the following command.

Command	Mode	Description
show redundancy sync-module-list	Enable	Shows a list of redundancy sync module.

7.8 NetBIOS Filtering

NetBIOS (Network Basic Input/Output System) is a program that allows applications on different computers to communicate within a local area network (LAN). NetBIOS is used in Ethernet, included as part of NetBIOS Extended User Interface (NetBEUI). Resource and information in the same network can be shared with this protocol.

However, the more computers are used recently, the more strong security is required. To secure individual customer’s information and prevent information leakages in the LAN environ-men, the LD3032 provides NetBIOS filtering function.

Without NetBIOS filtering, customer’s data may be opened to each other even though the data should be kept. To keep customer’s information and prevent sharing information in the above case, NetBIOS filtering is necessary.

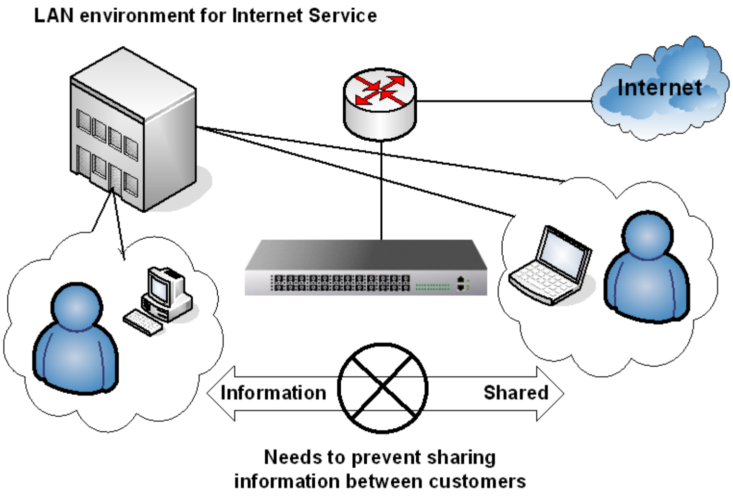

LAN environment for Internet Service
Internet
Information
Shared
Needs to prevent sharing
information between customers

Fig. 7.7 NetBIOS Filtering

To enable/disable NetBIOS filtering, use the following command.

Command	Mode	Description
netbios-filter on	Interface [GE/XE/GPON]	Configures NetBIOS filtering to a specified port.
netbios-filter off		Disables NetBIOS filtering from a specified port.

To display a configuration of NetBIOS filtering, use the following command.

Command	Mode	Description
show netbios-filter	Enable Global Interface[GE/XE/GPON]	Shows a configuration of NetBIOS filtering.

7.9 Martian Filtering

It is possible to block packets, which trying to bring different source IP out from same network. If packet brings different IP address, not its source IP address, then it is impossible to know it makes a trouble. Therefore, you would better prevent this kind of packet outgoing from your network. This function is named as Martian filter.

To enable/disable a Martian filtering, use the following command.

Command	Mode	Description
ip martian-filter	Interface [VLAN]	Blocks packets which bring different source IP address from the specified VLAN interface. INTERFACE: enter the interface name.
no ip martian-filter		Disables a configured Martian filter. INTERFACE: enter an interface name.

QoS and Martian filter cannot be used together.

7.10 Port Mirroring

Port mirroring is the function of monitoring a designated port. Here, one port to monitor is called monitor port and a port to be monitored is called mirrored port. Traffic transmitted from mirrored port are copied and sent to monitor port so that user can monitor network traffic.

The following is a network structure to analyze the traffic by port mirroring It analyzes traffic on the switch and network status by configuring Mirrored port and Monitor port connecting the computer, that the watch program is installed, to the port configured as Monitor port.

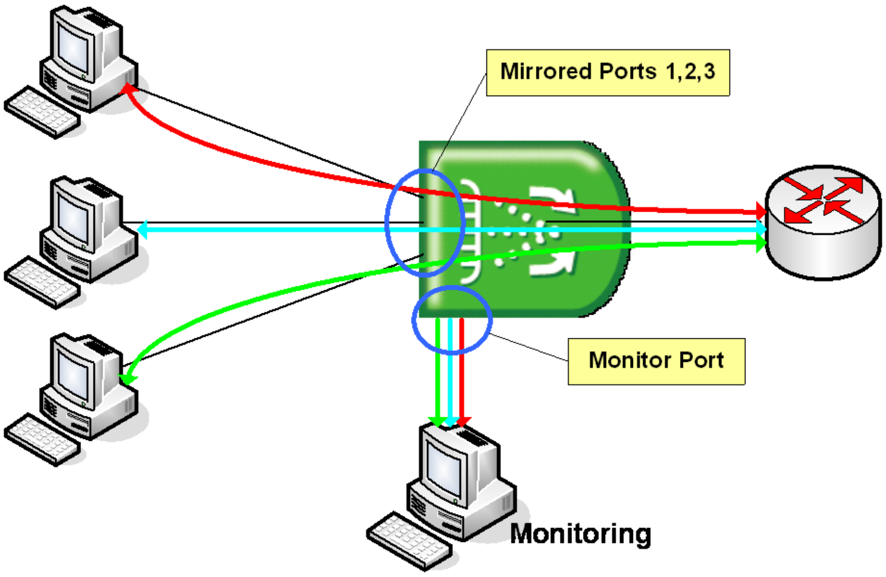


Fig. 7.8 Port Mirroring

To configure port mirroring, designate mirrored ports and monitor port. Then enable port mirroring function. Monitor port should be connected to the watch program installed PC. You can designate only one monitor port but many mirrored ports for one switch.

Step 1 Activate the port mirroring, using the following command.

Command	Mode	Description
mirror enable	Global	Activates port mirroring.

Step 2 Designate the monitor interface, use the following command.

Command	Mode	Description
mirror monitor cpu	Global	Specifies the packet mirroring to CPU. The TX packets from the local CPU is not available.
no mirror monitor cpu		Deletes the packet mirroring to CPU.

To specify the monitor interface, use the following command.

Command	Mode	Description
mirror monitor	Interface [GE/XE/GPON]	Designates the monitor interface.
no mirror monitor		Deletes a designated monitor port.

Step 3 Designate the mirrored port, use the following command.

Command	Mode	Description
mirror direction {**both** | **receive** | **transmit**}	Interface [GE/XE/GPON]	Designates the mirrored ports. receive: traffic in the ingress (RX) direction transmit: traffic in the egress (TX) direction
no mirror direction {**both** | **receive** | **transmit**}		Deletes the mirrored port configuration.

Step 4 To disable monitoring function, use the following command.

Command	Mode	Description
mirror disable	Global	Deactivates monitoring.

To display a configured port mirroring, use the following command.

Command	Mode	Description
show mirror	Enable Global Interface [GE/XE/GPON]	Shows a configured port mirroring.
show mirror interface {**gpon** | **gigabitethernet** | **tengigabitethernet** } *IFPORT*		

7.11 Max Host

You can limit the number of users by configuring the maximum number of users also named as max hosts for each Ethernet/PON port. In this case, you need to consider not only the number of PCs in the network but also devices such as switches in the network.

For the LD3032, you have to block the port like MAC filtering before configuring max hosts. In case of ISPs, it is possible to arrange a billing plan for each user by using this configuration.

To specify the maximum number of hosts that can be attached to an Ethernet/PON interface, use the following command.

Command	Mode	Description
max-hosts *VALUE*	Interface [GE/XE/GPON]	Specifies the maximum number of hosts that be attached to an Ethernet/PON port on this interface. VALUE: the maximum number of hosts for a particular interface. Valid range is from 1 to 2147483646 hosts.
no max-hosts		Resets the allowable number of hosts attached to a particular interface to the default value of unlimited hosts.

To display the configured maximum number of hosts for interfaces, use the following command.

Command	Mode	Description
show max-hosts	Enable Global Interface [GE/XE/GPON]	Shows the configured maximum number of hosts for the interfaces.

7.11.1 Max New Hosts

Max-new-hosts is to limit the number of users by configuring the number of MAC addresses that can be learned on the system and on the port for a second. The number of MAC addresses that can be learned on the system has the priority.

To configure max new hosts, use the following command.

Command	Mode	Description
max-new-hosts *VALUE*	Interface [GE/XE/GPON]	The number of MAC addresses that can be learned on the interface for a second. VALUE: maximum MAC number <1-2147483646>
max-new-hosts system *VALUE*	Global	The number of MAC addresses that can be learned on the system for a second. VALUE: maximum MAC number <1-2147483646>

To delete configured max new hosts, use the following command.

Command	Mode	Description
no max-new-hosts	Interface [GE/XE/GPON]	Deletes the number of MAC addresses that can be learned on the interface.
no max-new-hosts system	Global	Deletes the number of MAC addresses that can be learned on the system.

To display configured max new hosts, use the following command.

Command	Mode	Description
show max-new-hosts	Enable Global Interface [GE/XE/GPON]	Shows the configured Max-new-hosts.

If MAC that already counted disappears before passing 1 second and starts learning again, it is not counted. In case the same MAC is detected on the other port also, it is not counted again. For example, if MAC that was learned on port 1 is detected on port 2, it is supposed that MAC moved to the port 2. So, it is deleted from the port 1 and learned on the port 2 but it is not counted.

7.12 MAC Table

A dynamic MAC address is automatically registered in the MAC table, and it is removed if there is no access to/from the network element corresponding to the MAC address during the specified MAC aging time. On the other hand, a static MAC address is manually registered by user. This will not be removed regardless of the MAC aging time before removing it manually.

To manage a MAC table in the system, use the following command.

Command	Mode	Description
mac-address-table *NAME MAC-ADDR*	Interface [GE/XE/GPON]	Specifies a static MAC address in the MAC table. NAME: bridge name MAC-ADDR: MAC address
mac aging-time <10-21474830>	Global	Specifies MAC aging time: 10-21474830: aging time (default: 300)

To display the configured mac aging-time, use the following command.

Command	Mode	Description
show mac aging-time	Global	Shows mac aging-time

To remove the registered dynamic MAC addresses from the MAC table, use the following command.

Command	Mode	Description
clear mac *NAME MAC-ADDR*	Global	Clears dynamic MAC addresses. MAC-ADDR: MAC address

To remove the static MAC addresses manually registered by user from the MAC table, use the following command.

Command	Mode	Description
no mac-address-table *NAME MAC-ADDR*	Interface [GE/XE/GPON]	Deletes a specified static MAC address. NAME: bridge name MAC-ADDR: MAC address

To clear all MAC address entries in the forwarding database, use the following command.

Command	Mode	Description
clear mac address-table {**dynamic** | **static** | **multicast**} [**bridge** <1-32>]	Enable	Clears all dynamic/static/multicast MAC address entries. 1-32: bridge group
clear mac address-table dynamic {**address** *MAC-ADDR* | **interface** { **gigabitethernet** *IFPORT* | **tengigabitethernet** *IFPORT* | **gpon** *IFPORT* | **channelgroup**		Clears all dynamic MAC address entries of the specified address or interface or bridge.

IFPORT | **vlan** *VLAN*}} [{**instance** *INST* **bridge** <1-32> | **bridge** <1-32>}]		
clear mac address-table { **static** | **multicast**} {**address** *MAC-ADDR* | **interface** { **gigabitethernet** *IFPORT* | **tengigabitethernet** *IFPORT* | **gpon** *IFPORT* | **channelgroup** *IFPORT* | **vlan** *VLAN*}} [**bridge** <1-32>]		Clears all static/multicast MAC address entries of the specified address or interface or bridge.

To display the MAC table in the switch, use the following command.

Command	Mode	Description
show mac *NAME MAC-ADDR*	Enable Global Interface [GE/XE/GPON]	Shows switch MAC address, selection by port number (subscriber port only): NAME: bridge name MAC-ADDR: MAC address
show mac interface {**channelgroup** | **gigabitethernet** | **tengigabitethernet** | **gpon**} *IFPORTS*		
show mac interface vlan *VLANS* {**channelgroup** | **gigabitethernet** | **tengigabitethernet** | **gpon**} *IFPORTS*		

There are more than a thousand of MAC addresses in MAC table, so it is difficult to find information you need at one sight. For that reason, the system shows a certain amount of addresses displaying –**more**– on standby status. Press any key to search more. After you find the information, you can go back to the system prompt without displaying the other table by pressing <**q**>.

7.12.1 Admimistered MAC Address

To configure an administered MAC address and change H/W address of LD3032 in the active SFU, use the following command.

Command	Mode	Description
administered-mac *MAC-ADDR*	Global	Configures an administered MAC address. MAC-ADDR: administered MAC address
clear administered-mac		Clears the configured administered MAC address.

To apply the user-defined MAC address to the system, the system must restart using the **reload** command! For more information, see Section 4.1.4.1. To display the administered MAC address, use **show system** command.

7.13 MAC Filtering

It is possible to forward frame to MAC address of destination. Without specific performance degradation, maximum 4096 MAC addresses can be registered.

7.13.1 Default MAC Filter Policy

The basic policy of filtering based on system is set to allow all packets for each port. However, the basic policy can be changed for user’s requests.

After configuring basic policy of filtering for all packets, use the following command.

Command	Mode	Description
mac-filter default-policy {**deny** | **permit**}	Interface [GE/XE/GPON]	Configures basic policy of MAC Filtering in specified port.

By default, basic filtering policy provided by system is configured to permit all packets in each port.

Sample Configuration

This is an example of blocking all packets in port 6 to 7 and port 8.

```
SWTICH(config-if)#  mac-filter default-policy deny 6-8
SWTICH(config-if)# show mac-filter default-policy
-------------------------
  PORT POLICY | PORT POLICY
  ------------+------------
    1 PERMIT |    2 PERMIT
    3 PERMIT |    4 PERMIT
    5 PERMIT |    6 DENY
    7 DENY    |    8 DENY
    9 PERMIT |   10 PERMIT
   11 PERMIT |   12 PERMIT
   13 PERMIT |   14 PERMIT
   15 PERMIT |   16 PERMIT
   17 PERMIT |   18 PERMIT
SWTICH(config-if)#
```

7.13.2 Configuring MAC Filter Policy

You can add the policy to block or to allow some packets of specific address after configuring the basic policy of MAC Filtering. To add this policy, use the following commands.

Command	Mode	Description
mac-filter add *MAC-ADDR* {**deny** | **permit**} <1-4094>	Interface [GE/XE/GPON]	Allows or blocks packet which brings a specified MAC address to specified port. MAC-ADDR: MAC address

		1-4094: VLAN ID

To delete MAC filtering policy, use the following command.

Command	Mode	Description
mac-filter del *MAC-ADDR*	Global Interface [GE/XE/GPON]	Deletes filtering policy for specified MAC address. MAC-ADDR: MAC address

To delete MAC filtering function, use the following command.

Command	Mode	Description
no mac-filter	Global	Deletes all MAC filtering functions.

7.13.3 Displaying MAC Filter Policy

To show a configuration about MAC filter policy, use the following command.

Command	Mode	Description
show mac-filter	Enable Global Interface [GE/XE/GPON]	Shows a configured MAC filter policy.
show mac-filter default-policy		Shows the default MAC filter policy.

7.14 ICMP Message Control

ICMP stands for Internet Control Message Protocol. When it is impossible to transmit data or configure route for data, ICMP sends error message about it to host. The first 4 bytes of all ICMP messages are same, but the other parts are different according to type field value and code field value. There are fifteen values of field to distinguish each different ICMP message, and code field value helps to distinguish each type in detail.

The following table shows explanation for fifteen values of ICMP message type.

Type	Value	Type	Value
ICMP_ECHOREPLY	0	ICMP_DEST_UNREACH	3
ICMP_SOURCE_QUENCH	4	ICMP_REDIRECT	5
ICMP_ECHO	8	ICMP_TIME_EXCEEDED	11
ICMP_PARAMETERPROB	12	ICMP_TIMESTAMP	13
ICMP_TIMESTAMPREPLY	14	ICMP_INFO_REQUEST	15
ICMP_INFO_REPLY	16	ICMP_ADDRESS	17
ICMP_ADDRESSREPLY	18	-	-

Tab. 7.2 ICMP Message Type

The following figure shows simple ICMP message structure.

0	7	15 16	31
8-bit Type	8-bit Code	16-bit Checksum	
(Contents Depend on Type and Code)			

Fig. 7.9 ICMP Message Structure

It is possible to control ICMP message through user’s configuration. You can configure to block the echo reply message to the partner who is doing ping test to device and interval to transmit ICMP message.

7.14.1 Blocking Echo/Bogus Reply Message

It is possible to configure block echo reply message to the partner who is doing ping test to switch. To block echo reply message, use the following command.

Command	Mode	Description
ip icmp ignore echo all	Global	Blocks echo reply message to all partners who are taking ping test to device.
ip icmp ignore echo broadcast		Blocks echo reply message to partner who is taking broadcast ping test to device.

To release the blocked echo reply message, use the following command.

Command	Mode	Description
no ip icmp ignore echo all	Global	Releases blocked echo reply message to all partners who are taking ping test to device.
no ip icmp ignore echo broadcast		Releases blocked echo reply message to partner who is taking broadcast ping test to device.

To block the ICMP bogus packets, use the following command.

Command	Mode	Description
ip icmp ignore bogus error responses	Global	Blocks the ICMP bogus packets.
no ip icmp ignore bogus error responses		Releases blocked ICMP bogus packets.

7.14.2 Interval for Transmit ICMP Message

User can configure the interval for transmit ICMP message. After you configure the interval, ICMP message will be blocked until the configured time based on the last message is up. For example, if you configure the interval as 1 second, ICMP will not be sent within 1 second after the last message has been sent.

To configure interval to transmit ICMP message, the administrator should configure the type of message and the interval time.

Use the following command, to configure the interval for transmit ICMP message.

Command	Mode	Description
ip icmp interval rate-mask *MASK*	Global	Configures the interval for transmit ICMP message. MASK: user should input hexadecimal value until 0xFFFFFFFF. The default is 0x1818.

If mask that is input as hexadecimal number is calculated as binary number "1" means "Status ON", "0" means "Status OFF". In binary number, if the digit showed as "1" matches with the value of ICMP message. It means ICMP Message is selected as "Status ON". Digit value starts from 0.

For example, if hexadecimal number "8" is changed as binary number, it is "1000". In 1000, 0 digit is "0" and 1 digit is "0", 2 digit is "0" and 3 digit is "1". The digit showed as "1" is "3" and ICMP_DEST_UNREACH means ICMP value is "3". Therefore, ICMP_DEST_UNREACH is chosen the message of limiting the transmission time.

Default is 0x1818. If 1818 as hexadecimal number is changed as binary number, it is 1100000011000. By calculating from 0 digit, 3 digit, 4 digit, 11 digit, 12 digit is "1" and it is "STATUS ON". Therefore, the message that corresponds to 3, 4, 11, and 12 is chosen as the message limiting the transmission rate.

The table shows the result of mask calculation of default value.

Type	Status
ICMP_ECHOREPLY (0)	OFF
ICMP_DEST_UNREACH (3)	ON
ICMP_SOURCE_QUENCH (4)	ON
ICMP_REDIRECT (5)	OFF
ICMP_ECHO (8)	OFF
ICMP_TIME_EXCEEDED (11)	ON
ICMP_PARAMETERPROB (12)	ON
ICMP_TIMESTAMP (13)	OFF
ICMP_TIMESTAMPREPLY (14)	OFF
ICMP_INFO_REQUEST (15)	OFF
ICMP_INFO_REPLY (16)	OFF
ICMP_ADDRESS (17)	OFF
ICMP_ADDRESSREPLY (18)	OFF

Tab. 7.3 Mask Calculation of Default Value

To configure the limited ICMP transmission time, use the following command.

Command	Mode	Description
ip icmp interval rate-limit *INTERVAL*	Global	Configures a limited ICMP transmission time. INTERVAL: 0-2000000000 (unit: 10 ms)

i The default ICMP interval is 1 second (100 ms).

To return to default ICMP configuration, use the following command.

Command	Mode	Description
ip icmp interval default	Global	Returns to default configuration.

To display ICMP interval configuration, use the following command.

Command	Mode	Description
show ip icmp interval	Enable Global	Shows ICMP interval configuration.

7.14.3 ICMP Destination Unreachable Message

If the switch receives a packet that has an unknown protocol or no route to the destination address, the switch sends an ICMP unreachable message to its source address. To enable/disable generation of ICMP unreachable messages, use the following command.

Command	Mode	Description
ip unreachables	Interface [VLAN]	Enables sending ICMP unreachable messages on the interface. (default)
no ip unreachables		Disables sending ICMP unreachable messages on the interface.

7.15 TCP Flag Control

Transmission Control Protocol (TCP) header includes six kinds of flags that are URG, ACK, PSH, RST, SYN, and FIN. For the LD3032, you can configure RST and SYN as the below.

7.15.1 RST Configuration

RST sends a message when TCP connection cannot be done to a person who tries to make it. However, it is also possible to configure to block the message. This function will help prevent that hackers can find impossible connections.

To configure not to send the message that informs TCP connection cannot be done, use the following command.

Command	Mode	Description
ip tcp ignore rst-unknown	Global	Configures to block the message that informs TCP connection cannot be done.
no ip tcp ignore rst-unknown		Disables the unknown RST ignoring.

7.15.2 SYN Configuration

SYN sets up TCP connection. The LD3032 transmits cookies with SYN to a person who tries to make TCP connection. And only when transmitted cookies are returned, it is possible to permit TCP connection. This function prevents connection overcrowding because of accessed users who are not using and helps the other users use service.

To permit connection only when transmitted cookies are returned after sending cookies with SYN, use the following command.

Command	Mode	Description
ip tcp syncookies	Global	Permits only when transmitted cookies are returned after sending cookies with SYN.
no ip tcp syncookies		Disables configuration to permit only when transmitted cookies are returned after sending cookies with SYN.

To restrict the amount of SYN packet flooding into CPU within a specific bandwidth, use the following command.

Command	Mode	Description
ip tcp syn-guard *BANDWIDTH*	Global	Blocks SYN packet toward local CPU.
no ip tcp syn-guard		Configures the system to receive SYN packet toward local CPU.

To restrict the amount of IPv6 TCP SYN packet flooding into CPU within a specific bandwidth, use the following command.

Command	Mode	Description

ipv6 tcp syn-guard *BANDWIDTH*	Global	Blocks SYN packet toward local CPU.
no ipv6 tcp syn-guard		Configures the system to receive SYN packet toward local CPU.

7.16 Packet Dump

Failures in network can occurr by certain symptom. Each symptom can be traced to one or more problems by using specific troubleshooting tools. The LD3032 switch provides the debug command to dump packet. Use debug commands only for problem isolation. Do not use it to monitor normal network operation. The debug commands produce a large amount of processor overhead.

The LD3032 also provides debug command for Layer 3 routing protocols (BGP, OSPF, RIP). If you want to debug about them, refer to the each configuration chapter.

7.16.1 Packet Dump by Protocol

You can see packets about BOOTPS, DHCP, ARP and ICMP using the following command.

Command	Mode	Description
debug packet {**interface** *INTERFACE* | **port** *PORTS*} **protocol** {**bootps** | **dhcp** | **arp** | **icmp**} {**src-ip** *A.B.C.D* | **dest-ip** *A.B.C.D*}	Enable	Shows packet dump by protocol.
debug packet {**interface** *INTERFACE* | **port** *PORTS*} **host** {**src-ip** *A.B.C.D* | **dest-ip** *A.B.C.D*} {**src-port** <1-65535> | **dest-port** <1-65535>}		Shows host packet dump.
debug packet {**interface** *INTERFACE* | **port** *PORTS*} **multicast** {**src-ip** *A.B.C.D* | **dest-ip** *A.B.C.D*}		Shows multicast packet dump.

7.16.2 Packet Dump with Option

You can verify packets with TCP dump options using the following command.

Command	Mode	Description
debug packet *OPTION*	Enable	Shows packet dump using options.

Tab.7.4 shows the options for packet dump.

Option	Description
-a	Change Network & Broadcast address to name.
-d	Change the complied packet-matching code to readable letters and close it
-e	Output link-level header of each line
-f	Output outer internet address as symbol
-l	Buffer output data in line. This is useful when other application tries to receive data from tcpdump.
-n	Do not translate all address (e.g. port, host address)
-N	When output host name, do not print domain.
-O	Do not run packet-matching code optimizer. This option is used to find bug in optimizer

-p	Interface is not remained in promiscuous mode
-q	Reduce output quantity of protocol information. Therefore, output line is shorter.
-S	Output TCP sequence number not relative but absolute
-t	Time is not displayed on each output line
-v	Display more information
-w	Save the captured packets in a file instead of output
-x	Display each packet as hex code
-c *NUMBER*	Close the debug after receive packets as many as the number
-F *FILE*	Receive file as filter expression. All additional expressions on command line are ignored.
-i *INTERFACE*	Designate the interface where the intended packets are transmitted. If not designated, it automatically select a interface which has the lowest number within the system interfaces (Loopback is excepted)
-r FILE	Read packets from the file which created by '-w' option.
-s *SNAPLEN*	This is used to configure sample packet except the 68 byte default value. The 68 byte is appropriate value for IP, ICMP, TCP and UDP, but it can truncate protocol information of Name server or NFS packets. If sample size is long, the system should take more time to inspect and packets can be dropped for small buffer size. On the contrary, if the sample size is small, information can be leaked as the amount. Therefore, user should adjust the size as header size of protocol.
-T TYPE	Display the selected packets by conditional expression as the intended type. rpc (Remote Procedure Call) rtp (Real-time Transport Protocol) rtcp (Real-time Transport Control Protocol) vat (Visual Audio Tool) wb (distributed White Board)
EXPRESSION	Conditional expression

Tab. 7.4 Options for Packet Dump

7.16.3 Debug Packet Dump

The LD3032 provides network debugging function to prevent system overhead for unknown packet inflow. Monitoring process checks CPU load per 5 seconds. If there is more traffic than threshold, user can capture packets using TCP dump and save it to file. You can download the dump file with the name of file-number.dump after FP connection to the system. See the dumped packet contents with a packet analyze program.

To debug packet dump, use the following command.

Command	Mode	Description
debug packet log *COUNT VALUE TIME* [<1-10>]	Enable	Debugs packet dump logs according to a condition. COUNT: packet counting VALUE: CPU threshold 1-10: file number
no debug packet log		Deletes the information of packet dump log.

7.16.4 Displaying Dump Packets

To display the dump packets, use the following command.

Command	Mode	Description
show dump packets	Enable Global	Shows the dump packets.

7.16.5 Dump File

To back up a dump file using FTP or TFTP, use the following command.

Command	Mode	Description
copy {**ftp** | **tftp**} **dumpfile upload** [*FILE-NAME*]	Enable	Uploads a dump file to FTP or TFTP server with the name configured by user.

i

To access FTP to back up the configuration or use the backup file, you should know FTP user ID and the password. To back up the dump file through FTP, you can recognize the file transmission because hash function is automatically turned on.

To delete a dump file, use the following command.

Command	Mode	Description
delete dumpfile [*FILENAME*]	Enable	Deletes a specified dump file. FILENAME: dump file name

To display a list of dump files, use the following command.

Command	Mode	Description
show dumpfile-list	Enable	Shows a current startup configuration.

7.17 Access List

An IP access list (ACL) is a filter that enables you to restrict specific IP traffic. If you create an ACL entry to filter multicast packets based on their destination IP address, the LD3032 can deny the packets matching to the destination IP address, a multicast address.

There are three types of IP ACLs you can configure:

- Standard Access List
- Extended Access List
- Named Access List

Standard ACLs uses IP addresses (whether they are source address or not) for matching conditions. On the other hand, Extended ACLs define detailed filters with source IP, source mask, destination IP, and destination mask. More concrete filtering could be done with the extended ACL. IP ACLs also can be named with any characters and the numbers not defined in both standard and extended ACLs.

In most cases, you can simply define ACLs in *Global Configuration* mode. If you want to apply them to any of L3 functions, you can perform it where the actual access control should be made. For example, ACL could be applied to another command such as **ip igmp access-group** or **ip pim rp-address**. However, ARP has an exception. ARP has an access list itself, and you cannot define an access list in the *Global Configuration* mode.

Processing ACLs

An ACL entry has several statements. That is, an ACL entry 1 can have multiple filtering statements (conditions) as the following:

```
SWITCH(config)# access-list 1 deny 10.55.193.109
SWITCH(config)# access-list 1 permit 10.55.193.109 0.0.0.255
SWITCH(config)# access-list 1 deny any
```

Traffic that comes into the switch is compared to ACL entries based on the order that the entries have been created in the switch. New entries are added to the end of the list. The switch continues to look until it has a match. If no matches are found when the switch reaches the end of the list, the traffic is permitted. Likewise, if a couple of statements exist within one ACL entry and traffic comes in, the switch looks through the statements in the order that they are created. If the traffic hits the first condition, the switch processes as described in the first condition and next conditions are ignored.

```
SWITCH(config)# access-list 1 deny 10.55.193.109
SWITCH(config)# access-list 1 permit 10.55.193.109 0.0.0.255
SWITCH(config)# access-list 1 deny any
```

Scan through conditions in the order of creation

Wildcard Bits

Masks are used with IP addresses in IP ACLs to specify a range of IP addresses. Compared to subnet mask, masks for IP ACLs are the reverse. The mask bits 0.0.0.255 in IP ACL are same as 255.255.255.0 in subnet mask, for instance. This is called a wildcard mask or an inverse mask, because 1 and 0 in the binary format means the opposite of what they mean in a subnet mask; 0 meaning “check” and 1 meaning “ignore.”

IP Address	Wildcard Bits	Addresses that ACL controls

10.55.10.2	0.0.0.255	10.55.10.1 – 10.55.10.255
10.55.10.2	0.0.0.0	10.55.10.2

Tab. 7.5 Examples of Wildcard Masking

If you put 10.55.10.2 and 0.0.0.255 for an IP address and wildcard mask to permit, all traffic that begins with 10.55.10.1 to 10.55.10.255 (10.55.10.0/24) are accepted. If you set any IP address with wildcard bits 0.0.0.0, it indicates the IP address itself that should be processed.

7.17.1 Standard Access List

To create a standard IP address-based access list entry, use the following command.

Command	Mode	Description
access-list {<1-99> | <1300-1999>} {**deny** | **permit**} *A.B.C.D* [*WILDCARD-BITS*]	Global	Specifies a deny or permit statement of the standard ACL with IP addresses and wildcard bits 1-99: IP standard access list 1300-1999: IP standard access list (extended range) deny: denies packets if conditions are matched. permit: permits packets if conditions are matched. A.B.C.D: IP address to match WILDCARD-BITS: bits for use of wildcard masking
access-list {<1-99> | <1300-1999>} {**deny** | **permit**} **any**		Specifies a deny or permit statement of the standard ACL with any source host. any: any source host
access-list {<1-99> | <1300-1999>} {**deny** | **permit**} **host** *A.B.C.D*		Specifies a deny or permit statement of the standard ACL with a specific host. A.B.C.D: host address to match
access-list {<1-99> | <1300-1999>} **remark** *LINE*		Adds comments for the standard ACL. LINE: access list entry comments up to 100 characters

Add entries to the list by repeating the command for different IP addresses.

To delete an existing standard IP address-based access list entry, use the following command.

Command	Mode	Description
no access-list {<1-99> | <1300-1999>} {**deny** | **permit**} *A.B.C.D* [*WILDCARD-BITS*]	Global	Deletes an entry of the standard ACL.
no access-list {<1-99> | <1300-1999>} {**deny** | **permit**} **any**		
no access-list {<1-99> | <1300-1999>} {**deny** | **permit**} **host** *A.B.C.D*		
no access-list {<1-99> | <1300-1999>} **remark** *LINE*		

7.17.2 Extended Access List

To create an extended IP address-based access list entry, use the following command.

Command	Mode	Description
access-list {<100-199> | <2000-2699>} {**deny** | **permit**} **ip** *A.B.C.D WILDCARD-BITS A.B.C.D WILD-CARD-BITS*	Global	Specifies a deny or permit statement of the extended ACL with source/destination addresses and their wild masks. 100-199: IP extended access list 2000-2699: IP extended access list (extended range) deny: denies packet if conditions are matched. permit: permits packet if conditions are matched. ip: any Internet Protocol A.B.C.D: source/destination IP address to match WILDCARD-BITS: bits for use of source/destination IP address wildcard masking
access-list {<100-199> | <2000-2699>} {**deny** | **permit**} **ip host** *A.B.C.D A.B.C.D WILDCARD-BITS*		Specifies a deny or permit statement of the extended ACL with a single source host and other variables. host: single source host A.B.C.D: source/destination IP address of a host to match WILDCARD-BITS: bits for use of host destination IP address wildcard masking
access-list {<100-199> | <2000-2699>} {**deny** | **permit**} **ip host** *A.B.C.D* **any**		Specifies a deny or permit statement of the extended ACL with a single source host and other variables. host: single source host A.B.C.D: source IP address of a host to match any: destination host
access-list {<100-199> | <2000-2699>} {**deny** | **permit**} **ip host** *A.B.C.D* **host** *A.B.C.D*		Specifies a deny or permit statement of the extended ACL with a single source host and other variables. host: single source/destination host A.B.C.D: source/destination IP address of a host to match
access-list {<100-199> | <2000-2699>} {**deny** | **permit**} **ip any** *A.B.C.D WILDCARD-BITS*		Specifies a deny or permit statement of the extended ACL with any source host and other variables. any: any source host A.B.C.D: destination IP address to match WILDCARD-BITS: bits for use of destination IP address wildcard masking
access-list {<100-199> | <2000-2699>} {**deny** | **permit**} **ip any any**		Specifies a deny or permit statement of the extended ACL with any source host and other variables. any: any source/destination host
access-list {<100-199> | <2000-2699>} {**deny** | **permit**} **ip any host** *A.B.C.D*		Specifies a deny or permit statement of the extended ACL with any source host and other variables. any: any source host host: single destination host A.B.C.D: destination IP address to match
access-list {<100-199> | <2000-2699>} **remark** *LINE*		Adds comments for the extended ACL. LINE: access list entry comments up to 100 characters

i Add entries to the list by repeating the command for different IP addresses.

To delete an existing extended IP address-based access list entry, use the following command.

Command	Mode	Description
no access-list {<100-199> | <2000-2699>} {**deny** | **permit**} **ip** *A.B.C.D WILDCARD-BITS A.B.C.D WILDCARD-BITS*	Global	Deletes an entry of the extended ACL.
no access-list {<100-199> | <2000-2699>} {**deny** | **permit**} **ip host** *A.B.C.D A.B.C.D WILDCARD-BITS*		
no access-list {<100-199> | <2000-2699>} {**deny** | **permit**} **ip host** *A.B.C.D* **any**		
no access-list {<100-199> | <2000-2699>} {**deny** | **permit**} **ip host** *A.B.C.D* **host** *A.B.C.D*		
no access-list {<100-199> | <2000-2699>} {**deny** | **permit**} **ip any** *A.B.C.D A.B.C.D WILDCARD-BITS*		
no access-list {<100-199> | <2000-2699>} {**deny** | **permit**} **ip any any**		
no access-list {<100-199> | <2000-2699>} {**deny** | **permit**} **ip any host** *A.B.C.D*		
no access-list {<100-199> | <2000-2699>} **remark** *LINE*		

Sample Configuration

This is an example of creating the extended ACL entries.

```
SWITCH(config)# access-list 100 permit ip 10.55.10.2 0.0.0.255 10.55.193.5
0.0.0.255
SWITCH(config)# access-list 100 deny ip 10.12.154.1 0.0.0.255 10.12.202.1
0.0.0.255
SWITCH(config)#
```

7.17.3 Named Access List

It defines an IP access list by name and any numeric characters that have not been defined from both standard ACL and extended ACL. To create a named IP access list entry, use the following command.

Command	Mode	Description
access-list *WORD* {**deny** | **permit**} *A.B.C.D/M* [**exact-match**]	Global	Specifies the named ACL entry with a prefix. WORD: access list name deny: denies packet if conditions are matched. permit: permits packet if conditions are matched. A.B.C.D/M: prefix to match exact-match: exact match against the prefixes
access-list *WORD* {**deny** | **permit**} **any**		Specifies the named ACL with any destination IP address. WORD: access list name deny: denies packet if conditions are matched. permit: permits packet if conditions are matched. any: any destination IP address
access-list *WORD* **remark** *LINE*		Adds comments for the named ACL. LINE: access list comments up to 100 characters

i

Add entries to the list by repeating the command for different IP addresses.

To delete an entry of the named ACL, use the following command.

Command	Mode	Description
no access-list *WORD* {**deny** | **permit**} *A.B.C.D/M* [**exact-match**]	Global	Deletes an entry of the named ACL.
no access-list *WORD* {**deny** | **permit**} **any**		
no access-list *WORD* **remark** *LINE*		

Sample Configuration

This is an example of creating a named ACL entry.

```
SWITCH(config)# access-list sample_ACL permit 10.55.193.109/24
SWITCH(config)#
```

7.17.4 Named Access List for IPv6 address

To create a named IPv6 access list entry, use the following command.

Command	Mode	Description
ipv6 access-list *WORD* {**deny | permit**} *X:X::X:X/M* [**exact-match**]	Global	Specifies the named ACL entry with a prefix. WORD: access list name deny: denies access of packet if conditions are matched. permit: permits access of packet if conditions are matched. X:X::X:X/M : prefix to match exact-match: exact match against the prefixes
ipv6 access-list *WORD* {**deny | permit**} **any**		Specifies the named ACL with any destination IP address. WORD: access list name any: any destination IP address
ipv6 access-list *WORD* **remark** *LINE*		Writes comments for the named ACL. LINE: access list entry comments up to 100 characters

i

Add entries to the list by repeating the command for different IPv6 addresses.

Use the no access-list command to delete an entry in the named ACL.

Command	Mode	Description
no ipv6 access-list *WORD* {**deny | permit**} *X:X::X:X/M* [**exact-match**]	Global	Deletes an entry of the named ACL.
no ipv6 access-list *WORD* {**deny | permit**} **any**		
no ipv6 access-list *WORD* **remark** [*LINE*]		

To displays the existing Access List entries, use the following command.

Command	Mode	Description
show ipv6 access-list	Enable Global	Shows the existing ACL entries. WORD: IPv6 access list name
show ipv6 access-list *WORD*		

7.17.5 Access List Range

To add a user-defined range of the access lists for convenience, use the following command.

Command	Mode	Description
access-list-range {<1-1024> | *WORD*} {**deny** | **permit**} *A.B.C.D A.B.C.D*	Global	Applies the user-defined access list range and specifies those packets to reject/forward. 1-1024: IP standard access list range WORD: IP access-list-range name deny: denies access of packet if conditions are matched. permit: permits access of packet if conditions are matched. A.B.C.D: start/end IP address to specify the range any: any source address
access-list-range {<1-1024> | *WORD*} {**deny** | **permit**} **any**		

To delete a configured range of access list entries, use the following command.

Command	Mode	Description
no access-list-range {<1-1024> | *WORD*} [{**deny |** **permit**} *A.B.C.D A.B.C.D*]	Global	Deletes a configured range of access lists for rejecting/forwarding those packets. 1-1024: IP standard access list range WORD: IP access-list-range name A.B.C.D: start/end IP address to specify the range any: any source address
no access-list-range {<1-1024> | *WORD*} [{**deny | permit**} **any**]		

To write comments for the specified access list range, use the following command.

Command	Mode	Description
access-list-range {<1-1024> | *WORD*} **remark** *LINE*	Global	Writes comments for the specified ACL range. 1-1024: IP standard access list range WORD: IP access-list-range name LINE: access list entry comments up to 100 characters
no access-list-range {<1-1024> | *WORD*} **remark** [*LINE*]		Deletes the comments for the specific ACL range.

7.17.6 Access List Filter Configuration

IP address and MAC address based Access Control List (ACL) filters allow or disallow the forwarding of unicast and multicast packets that are sent to or from specific IP or MAC addresses.

There are three types of ACL-based filters you can configure:

- Standard IP Access Control Lists
- Extended IP Access Control Lists
- Extended MAC address Access Control Lists

7.17.6.1 Filters Using Standard IP ACLs

To create a standard named ACL to filter traffic based on specific source IP address, use the following command.

Command	Mode	Description
ip access-list standard {<1-99> | <1300-1999> | *WORD*}	Global	Creates a standard ACL entry. 1-99: standard IP access list number 1300-1999: standard IP access list number (expanded range) WORD: access-list name
no ip access-list standard {<1-99> | <1300-1999> | *WORD*}		Deletes the configured standard ACL entry.

After creating a standard IP address-based ACL entry, the prompt changes from SWITCH(config)# to SWITCH(config-std-nacl])#.

To configure a standard ACL entry, use the following command.

Command	Mode	Description
[<1-2147483647>] { **deny** | **permit** } {*A.B.C.D WILDCARD-BITS* | **host** *A.B.C.D* | **any**}	Standard IP ACL Mode	Specifies a deny or permit statement of the standard ACL with source IP addresses and wildcard bits 1-2147483647: sequence number deny: denies access of packet if conditions are matched. permit: permits access of packet if conditions are matched. A.B.C.D: source IP address to match WILDCARD-BITS: Bits for use of wildcard masking
remark *LINE*		Writes comments for this access-list. LINE: access list entry comments up to 100 characters
no <1-2147483647>		Deletes an entry of the standard ACL.
no { **deny** | **permit** } {*A.B.C.D A.B.C.D* | **host** *A.B.C.D* | **any**}		
no remark *LINE*		

Sequence number of ACLs enables you to insert or delete a specific ACL entry in your statement grouping without having to delete the entire ACL and rebuild it.

If you enter an ACL statement without specifying a sequence number, the V6744XG uses the default increment of 10 when adding the statement to the end of the list.

7.17.6.2 Filters Using Extended IP ACLs

To create an extended named ACL to filter traffic based on specific protocols, use the following command.

Command	Mode	Description
ip access-list extended {<100-199> | <2000-2699> | *WORD*}	Global	Creates an extended ACL entry. 100-199: extended access list number 2000-2699: extended access list number (expanded range) WORD: access-list name
no ip access-list extended {<100-199> | <2000-2699> | *WORD*}		Deletes the configured extended ACL entry.

After creating an extended IP address-based ACL entry, the prompt changes from SWITCH(config)# to SWITCH(config-ext-nacl])#.

To configure an extended ACL entry, use the following command.

Command	Mode	Description
[<1-2147483647>] { **deny** | **permit** } {<0-255> | **ahp** | **eigrp** | **esp** | **gre** | **ip** | **ipinip** | **nos** | **ospf** | **pcp** | **pim** } {**any** | **host** *A.B.C.D* | *A.B.C.D WILDCARD-BITS*} {**any** | **host** *A.B.C.D* | *A.B.C.D WILDCARD-BITS*} [{ **precedence** <0-7> | **tos** <0-255> | **dscp** <0-63>}] [{ **log** | **log-input**} **tag** *WORD*]	Extended ACL Mode	Specifies a deny or permit statement of the extended ACL with each protocol. 1-2147483647: sequence number any: any source/destination IP address host: A single source/destination IP address A.B.C.D: source/destination IP address to match WILDCARD-BITS: Bits for use of wildcard masking
[<1-2147483647>] { **deny** | **permit** } **icmp** {**any** | **host** *A.B.C.D* | *A.B.C.D WILDCARD-BITS*} {**any** | **host** *A.B.C.D* | *A.B.C.D WILDCARD-BITS*} [{*TYPE CODE* | **administratively-prohibited** | **alternate-address** | **conversion-error** | **dod-host-prohibited** | **dod-net-prohibited** | **echo** | **echo-reply** | **general-parameter-problem** | **host-isolated | host-precedence-unreachable | host-redirect | host-tos-redirect | host-tos-unreachable | host-unknown | host-unreachable | information-reply | information-request | mask-reply | mask-request | mobile-redirect | net-redirect | net-tos-redirect | net-tos-unreachable | net-unreachable | network-unknown | no-room-for-option | option-missing | packet-too-big | parameter-problem | port-unreachable | precedence-unreachable | protocol-unreachable | reassembly-timeout | redirect | router-advertisement | router-**		Specifies a deny or permit statement of the extended ACL based on ICMP.

solicitation | **source-quench** | **source-route-failed** | **time-exceeded** | **timestamp-reply** | **timestamp-request** | **traceroute** | **ttl-exceeded** | **unreachable** }] [{**precedence** <0-7> | **tos** <0-255> | **dscp** <0-63>}] [{ **log** | **log-input**} **tag** *WORD*]		
[<1-2147483647>] { **deny** | **permit** } **tcp** {**any** | **host** *A.B.C.D* | *A.B.C.D WILDCARD-BITS*} {**any** | **eq** *PORT* | **gt** *PORT* | **lt** *PORT* | **neq** *PORT* | **range** *RANGE* } {**any** | **host** *A.B.C.D* | *A.B.C.D WILDCARD-BITS*} {**any** | **eq** *PORT* | **gt** *PORT* | **lt** *PORT* | **neq** *PORT* | **range** *RANGE* } [{*TCP_FLAG* | **precedence** <0-7> | **tos** <0-255> | **dscp** <0-63>}] [{ **log** | **log-input**} **tag** *WORD*]		Specifies a deny or permit statement of the extended ACL based on TCP. eq: match only packets on a given port number gt: match only packets with a greater port number lt: match only packets with a lower port number neq: match only packets not on a given port number range: match only packets in the range of port numbers
[<1-2147483647>] { **deny** | **permit** } **udp** {**any** | **host** *A.B.C.D* | *A.B.C.D WILDCARD-BITS*} {**any** | **eq** *PORT* | **gt** *PORT* | **lt** *PORT* | **neq** *PORT* | **range** *RANGE* } {**any** | **host** *A.B.C.D* | *A.B.C.D WILDCARD-BITS*} {**any** | **eq** *PORT* | **gt** *PORT* | **lt** *PORT* | **neq** *PORT* | **range** *RANGE* } [{**precedence** <0-7> | **tos** <0-255> | **dscp** <0-63>}] [{ **log** | **log-input**} **tag** *WORD*]		Specifies a deny or permit statement of the extended ACL based on UDP. eq: match only packets on a given port number gt: match only packets with a greater port number lt: match only packets with a lower port number neq: match only packets not on a given port number range: match only packets in the range of port numbers
[<1-2147483647>] { **deny** | **permit** } **igmp** {**any** | **host** *A.B.C.D* | *A.B.C.D WILDCARD-BITS*} {**any** | **host** *A.B.C.D* | *A.B.C.D WILDCARD-BITS*} [{**dvmrp** | **host-query** | **host-report** | **pim** | **trace**}] [{**precedence** <0-7> | **tos** <0-255> | **dscp** <0-63>}] [{ **log** | **log-input**} **tag** *WORD*]		Specifies a deny or permit statement of the extended ACL based on IGMP.
remark *LINE*		Writes comments for this access-list. LINE: access list entry comments up to 100 characters

To delete the configured extended ACL entry, use the following command.

Command	Mode	Description
no <1-2147483647>	Extended ACL Mode	Deletes an entry of the extended ACL.
no { **deny** | **permit** } {<0-255> | **ahp** | **eigrp** | **esp** | **gre** | **ip** | **ipinip** | **nos** | **ospf** | **pcp** | **pim** } {**any** | **host** *A.B.C.D* | *A.B.C.D WILDCARD-BITS*} {**any** | **host** *A.B.C.D* | *A.B.C.D WILDCARD-BITS*} [{ **precedence** <0-7> | **tos** <0-255> | **dscp** <0-63>}]		

[{ **log** | **log-input**} **tag** *WORD*]		
no { **deny** | **permit** } {**tcp** | **udp**} {**any** | **host** *A.B.C.D* | *A.B.C.D WILDCARD-BITS*} {**any** | **eq** *PORT* | **gt** *PORT* | **lt** *PORT* | **neq** *PORT* | **range** *RANGE* } {**any** | **host** *A.B.C.D* | *A.B.C.D WILDCARD-BITS*} {**any** | **host** *A.B.C.D* | *A.B.C.D WILDCARD-BITS*} [{*TCP_FLAG* | **precedence** <0-7> | **tos** <0-255> | **dscp** <0-63>}] [{ **log** | **log-input**} **tag** *WORD*]		
no { **deny** | **permit** } **igmp** {**any** | **host** *A.B.C.D* | *A.B.C.D WILDCARD-BITS*} {**any** | **host** *A.B.C.D* | *A.B.C.D WILDCARD-BITS*} [{**dvmrp** | **host-query** | **host-report** | **pim** | **trace**}] [{**precedence** <0-7> | **tos** <0-255> | **dscp** <0-63>}] [{ **log** | **log-input**} **tag** *WORD*]		
no { **deny** | **permit** } **icmp** {**any** | **host** *A.B.C.D* | *A.B.C.D WILDCARD-BITS*} {**any** | **host** *A.B.C.D* | *A.B.C.D WILDCARD-BITS*} [{*TYPE CODE* | **administratively-prohibited** | **alternate-address** | **conversion-error** | **dod-host-prohibited** | **dod-net-prohibited** | **echo** | **echo-reply** | **general-parameter-problem** | **host-isolated** | **host-precedence-unreachable** | **host-redirect** | **host-tos-redirect** | **host-tos-unreachable** | **host-unknown** | **host-unreachable** | **information-reply** | **information-request** | **mask-reply** | **mask-request** | **mobile-redirect** | **net-redirect** | **net-tos-redirect** | **net-tos-unreachable** | **net-unreachable** | **network-unknown** | **no-room-for-option** | **option-missing** | **packet-too-big** | **parameter-problem** | **port-unreachable** | **precedence-unreachable** | **protocol-unreachable** | **reassembly-timeout** | **redirect** | **router-advertisement** | **router-solicitation** | **source-quench** | **source-route-failed** | **time-exceeded** | **timestamp-reply** | **timestamp-request** | **traceroute** | **ttl-exceeded** | **unreachable** }] [{*TCP_FLAG* | **precedence** <0-7> | **tos** <0-255> | **dscp** <0-63>}] [{ **log** | **log-input**} **tag** *WORD*]		
no remark *LINE*		

7.17.6.3 Filters Using Extended MAC ACLs

To create an extended MAC address-based ACL to filter client devices of the hard coded MAC address, use the following command.

Command	Mode	Description
mac access-list extended {<700-799> | <1100-1199> | *WORD*}	Global	Creates an extended MAC address-based ACL. 700-799: extended MAC access-list number 1100-1199: extended MAC access-list number (expanded range) WORD: access list name
no mac access-list extended {<700-799> | <1100-1199> | *WORD*}		Deletes the configured MAC address-based ACL.

After creating a standard MAC address-based ACL entry, the prompt changes from SWITCH(config)# to SWITCH(config-ext-macl])#.

To configure an extended MAC address-based ACL entry, use the following command.

Command	Mode	Description
[<1-2147483647>] { **deny** | **permit** } {**any** | **host** *HOST-MACADDR* | *MACADDR MACADDR-MASK* } {**any** | **host** *HOST-MACADDR* | *MACADDR MACADDR-MASK*} {*TYPE-NUM* | **aarp** | **amber** | **any** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp** } **cos** {<0-7> | **any**}	MAC ACL Mode	Specifies a deny or permit statement of the MAC address-based ACL. 1-2147483647: sequence number any: any source/destination MAC address host: A single source/destination MAC HOST-MACADDR: host MAC address MACADDR: source/destination MAC address MACADDR-MASK: source/destination MAC address mask TYPE-NUM: Ethernet type (ex: 0x0800 for IPv4)
remark *LINE*		Writes comments for this MAC address-based ACL. LINE: access list entry comments up to 100 characters
no <1-2147483647>		Deletes an entry of the MAC address-based ACL.
no {**deny** | **permit**} {**any** | **host** *HOST-MACADDR* | *MACADDR MACADDR-MASK* } {**any** | **host** *HOST-MACADDR* | *MACADDR MACADDR-MASK*} {*TYPE-NUM* | **aarp** | **amber** | **any** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp** } **cos** {<0-7> | **any**}		
no remark *LINE*		

To display the configured extended MAC address-based ACL, use the following command.

Command	Mode	Description
show mac access-list {<700-799> | <1100-1199> | *WORD*}	Global	Shows the configured extended MAC address-based ACL. 700-799: extended MAC access-list number 1100-1199: extended MAC access-list number (expanded range) WORD: access list name

7.17.6.4 Applying ACL Filters to Interface

After the IP based access list is defined, it must be applied to the interface (inbound). To apply the user-defined access list to the interface and specify its priority, use the following command.

Command	Mode	Description
ip access-group {<1-99> | <100-199> | <1300-1999> | <2000-2699> | *WORD*} **in priority** {**low | medium** | **high** | **highest**}	Interface	Applies the user-defined access list to the interface. 1-99: standard IP access list number 1300-1999: standard IP access list number (expanded range) 100-199: extended access list number 2000-2699: extended access list number (expanded range) WORD: IP access list name in: inbound packets out: outbound packets
ip access-group {<1-99> | <100-199> | <1300-1999> | <2000-2699> | *WORD*} **out**		
no ip access-group [{<1-99> | <100-199> | <1300-1999> | <2000-2699> | *WORD*} {**in** | **out**}]		Removes the user-defined access list from the interface.

After the MAC address-based ACL is defined, it must be applied to the interface (inbound). To apply the user-defined access list to the interface and specify its priority, use the following command.

Command	Mode	Description
mac access-group {<700-799> | <1100-1199> | *WORD*} **in priority** {**low | medium** | **high** | **highest**}	Interface	Applies the user-defined MAC access list to the interface. 700-799: extended MAC access-list number 1100-1199: extended MAC access-list number (expanded range) WORD: MAC access list name in: inbound packets.
no mac access-group [{<700-799> | <1100-1199> | *WORD*} **in**]		Removes the user-defined MAC access list from the interface.

One interface can be applied by one IP based ACL and one MAC based ACL. Up to 64 interfaces can be used for the ACL bindings.

To display the configured IP/MAC address-based ACL bindings with an interface, use the following command.

Command	Mode	Description
show access-group interface [*INTERFACE*]	Enable Global	Shows the IP/MAC access group configuration.

7.17.6.5 ACL Logging

The commands of ACL logging can be used to configure how often syslog messages are generated and sent after the initial packet match. To enable/disable logging of ACL entries, use the following command.

Command	Mode	Description
ip rule access-list log-buffer <1-1000>	Global	Specifies the number of ACL entries in log-buffer. 1-1000: access-list log count (default: 1000)
ip rule access-list log-update count <0-2147483647>		Specifies the number of packets that are matched by the ACL 0-2147483647: access-list log count value (default: 2147483647)
ip rule access-list log-update time <1-10>		Specifies the interval between ACL log updates. 1-10: periodic update time value (default: 5 mins)
no ip rule access-list {**log-buffer** | **log-update count** | **log-update time**}		Removes the user-defined ACL logging configurations.

To display the information of IP rule access-list logging, use the following command.

Command	Mode	Description
show ip rule access-list log	Enable Global	Shows the information of IP rule ACL logging.

To clear the existing ACL entries, use the following command.

Command	Mode	Description
clear ip access-list counters {<1-99> | <100-199> | <1300-1999> | <2000-2699> | *WORD*}	Enable Global	Clears the counters of packets that are matched to ACL.

7.17.6.6 Resequencing IP/MAC ACLs

With sequenced ACLs, each ACL entry is associated with a sequence number. Sequence numbers can be used to insert an ACL into the middle of an existing list or to delete an existing statement in the list. You can resequence the numbers with your own numbering scheme.

To resequence the numbers in the IP address-based ACL, use the following command.

Command	Mode	Description
ip access-list resequence *WORD* <1-2147483647> <1-2147483647>	Global	Resequences the numbers in the IP address-based ACL. 1-2147483647: starting sequence number (default:10) 1-2147483647: step to increment the sequence number (default: 10)

To resequence the numbers in the MAC address-base ACL, use the following command.

Command	Mode	Description
mac access-list resequence *WORD* <1-2147483647> <1-2147483647>	Global	Resequences the numbers in the MAC address-based ACL. WORD: access-list name 1-2147483647: sequence number (default: 10) 1-2147483647: step to increment the sequence number (default: 10)

7.17.7 Access List Entries Limit

To configure the maximum number of available access list, use the following command.

Command	Mode	Description
maximum-access-list <1-4294967294>	Global	Configures the maximum number of ACL
no maximum-access-list		Deletes the configured ACL limit.

7.17.8 Displaying Access List Entries

To displays the existing Access List entries, use the following command.

Command	Mode	Description
show access-list	Enable Global	Shows the existing ACL entries.
show ip access-list		
show ip access-list {<1-99> | <100-199> | <1300-1999> | <2000-2699> | WORD}		Shows the existing ACL entries for a given ACL type. 1-99: IP standard access list 1300-1999: IP standard access list (extended range) 100-199: IP extended access list 2000-2699: IP extended access list (extended range) WORD: access list name
show access-list-range		Shows the existing IP access range lists. 1-99: IP standard access list 1300-1999: IP standard access list (extended range) 100-199: IP extended access list 2000-2699: IP extended access list (extended range) WORD: access list name
show ip access-list-range		
show ip access-list-range {<1-99> | <100-199> | <1300-1999> | <2000-2699> | WORD}		

Sample Configuration

This is an example of displaying the configured ACL entries.

```
SWITCH(config)# show ip access-list
Standard IP access list 5
   permit 10.55.10.0, wildcard bits 0.0.0.255
   deny 10.55.1.0, wildcard bits 0.0.0.255
Extended IP access list 100
   permit ip 10.55.10.0 0.0.0.255 10.55.193.0 0.0.0.255
   deny ip 10.12.154.0 0.0.0.255 10.12.202.0 0.0.0.255
ZebOS IP access list sample_ACL
   permit 10.55.193.109/24
SWITCH(config)#
```

8 System Security

8.1 Address Resolution Protocol (ARP)

Devices connected to IP network have two addresses, LAN address and network address. LAN address is sometimes called as a data link address because it is used in Layer 2 level, but more commonly the address is known as a MAC address. A switch on Ethernet needs a 48-bit-MAC address to transmit packets. In this case, the process of finding a proper MAC address from the IP address is called an address resolution.

On the other hand, the progress of finding the proper IP address from the MAC address is called reverse address resolution. Our switches and DSLAMs find their MAC addresses from the IP addresses through Address Resolution Protocol (ARP). ARP saves these addresses in ARP table for quick search. Referring to the IP addresses in ARP table, the packets containing the IP address are transmitted to network. When configuring the ARP table, it is possible to do it only in some specific interfaces.

8.1.1 ARP Table

Hosts typically have an ARP table, which is a cache of IP/MAC address mappings. The ARP Table automatically maps the IP address to the MAC address of a switch. In addition to address information, the table shows the age of the entry in the table, the encapsulation method, and the switch interface (VLAN ID) where packets are forwarded.

The LD3032 ARP saves IP/MAC addresses mappings in ARP table for quick search. Referring to the information in ARP table, packets attached IP address is transmitted to network. When configuring ARP table, it is possible to do it only in some specific interfaces.

8.1.1.1 Registering ARP Table

The contents of ARP table are automatically registered when MAC address corresponds to IP address. The network administrator could use MAC address of specific IP address in network by registering on ARP table.

To specify a static ARP entry, use the following command.

Command	Mode	Description
arp *A.B.C.D MACADDR*	Global	Specifies a static ARP entry. MAC-ADDR: MAC address.
arp *A.B.C.D MACADDR INTERFACE*		Specifies a static ARP entry with an interface name. INTERFACE: interface name MAC-ADDR: MAC address
no arp [*A.B.C.D*]		Deletes static ARP entries.
no arp *A.B.C.D INTERFACE*		

To delete ARP entries, use the following command.

Command	Mode	Description
clear arp	Global	Deletes all ARP entries. A.B.C.D: IP address (e.g. 10.1.1.20) A.B.C.D/M: IP prefix (e.g. 10.1.1.20/24)
clear arp *A.B.C.D*		
clear arp *A.B.C.D/M*		
clear arp interface {channelgroup | gpon | tengigabitethernet } *IFPORT*		Deletes the ARP entries on a specified interface. IFPORT: interface port number VLANID: VLAN ID
clear arp interface vlan *VLANID*		

8.1.1.2 Displaying ARP Table

To display ARP table registered in switch, use the following command.

Command	Mode	Description
show arp	Enable Global	Shows ARP table.
show arp {*INTERFACE* | *A.B.C.D*}		Shows ARP table for specified interface or IP address, enter the interface name (br1, br2, ...) or IP address.

The following is an example of displaying a current ARP table for all interfaces.

```
SWITCH# show arp
Flags : (C)completed entry (M)permanent entry (H)writed entry to chip
IP Address     Mac Address       Flags Mask  HW Type   Interface   Port
---------------------------------------------------------------------------
10.45.192.254  b8:26:d4:2a:50:d7  C          ether     mgmt        --
SWITCH#
```

8.1.2 ARP Request Message Interval

To set the interval for sending ARP request packets from the switch to prevent the connected network devices to get overloaded, use the following command.

Command	Mode	Description
ip arp-request interval mc_probe <2-10>	Interface [VLAN]	Sets the maximum number of attempts to send multicast probes before asking the ARP daemon. 2-10: retry attempt interval of multicast solicitation (default: 3 seconds)
ip arp-request interval retrans <1-300>		Sets the number of seconds to delay before retransmitting the ARP request. 1-300: retry attempt interval of retransmission (default: 1 second)
ip arp-request interval uc_probe <2-10>		Sets the maximum number of attempts to send unicast probes before asking the ARP daemon. 2-10: retry attempt interval of unicast solicitation (default: 3 seconds)

To the configured interval of ARP request messages, use the following command.

Command	Mode	Description
no ip arp-request interval mc_probe	Interface [VLAN]	Deletes the configured interval of ARP request message.
no ip arp-request interval retrans		
no ip arp-request interval uc_probe		

8.1.3 ARP Alias

Although clients are joined in the same client switch, it may be impossible to communicate between them for security reasons. When you need to make them communicate each other, the LD3032 supports ARP alias, which responses the ARP request from client net through the concentrating switch.

To register the address of client net range in ARP alias, use the following command.

Command	Mode	Description
arp alias *A.B.C.D A.B.C.D* [*XX:XX:XX:XX:XX:XX*]	Global	Registers the IP address range and MAC address in ARP alias to make the system response to an ARP request.
arp alias *A.B.C.D A.B.C.D* **vlan** *VLAN* **gateway** *GATEWAY*		Registers gateway IP address within IP address range to make the system response automatically MAC address of gateway. VLAN: 1-4094 GATEWAY: gateway IP address
no arp alias *A.B.C.D A.B.C.D*		Deletes the registered IP address range of ARP alias.

To register the MAC address of client in ARP alias per VLAN interface, use the following command.

Command	Mode	Description
ip arp alias [*XX:XX:XX:XX:XX:XX*]	Interface [VLAN]	Registers a MAC address in ARP alias to make the VLAN response to an ARP request.
no ip arp alias		Deletes the registered MAC address of ARP alias.

i Unless you input a MAC address, the MAC address of user’s device will be used for ARP response.

To set aging time of gateway IP address in ARP alias, use the following command.

Command	Mode	Description
arp alias aging-time <5-2147483647>	Global	Sets the aging time of gateway IP address. 5-2147483647: aging time (default: 300 seconds)
no arp alias aging-time		Deletes the aging time of gateway IP address.

To display a registered ARP alias, use the following command.

Command	Mode	Description
show arp alias	Enable Global	Shows a registered ARP alias.

8.1.4 ARP Inspection

ARP provides IP communication by mapping an IP address to a MAC address. But a malicious user can attack ARP caches of systems by intercepting traffic intended for other hosts on the subnet. For example, Host B generates a broadcast message for all hosts within the broadcast domain to obtain the MAC address associated with the IP address of Host A. If Host C responses with an IP address of Host A (or B) and a MAC address of Host C, Host A and Host B can use Host C's MAC address as the destination MAC address for traffic intended for Host A and Host B.

ARP inspection is a security feature that validates ARP packets in a network. It intercepts and discards ARP packets with invalid IP-MAC address binding.

To enable/disable the ARP inspection, use the following command.

Command	Mode	Description
ip arp inspection vlan *VLANS*	Global	Enables ARP inspection on a specified VLAN. VLANS: VLAN name
no ip arp inspection vlan *VLANS*		Disables ARP inspection on a specified VLAN.

8.1.4.1 ARP Access List

You can exclude a given range of IP addresses from the ARP inspection using ARP access lists. ARP access lists are created by the **arp access-list** command on the *Global Configuration* mode. ARP access list permits or denies the ARP packets of a given range of IP addresses.

To create/delete ARP access list (ACL), use the following command.

Command	Mode	Description
arp access-list *NAME*	Global	Opens ARP ACL configuration mode and creates an ARP access list. NAME: ARP access list name
no arp access-list *NAME*		Deletes an ARP access list.

After opening *ARP Access List Configuration* mode, the prompt changes from SWITCH(config)# to SWITCH(config-arp-acl[*NAME*])#. After opening *ARP ACL Configuration* mode, a range of IP addresses can be configured to apply ARP inspection.

i

By default, ARP Access List discards the ARP packets of all IP addresses and MAC addresses.

To configure the range of IP address to deny ARP packets, use the following command.

Command	Mode	Description
deny ip any mac {**any** | **host** *MACADDR*}	ARP-ACL	Discards all ARP packets of all IP addresses with all MAC addresses which have not learned before on ARP inspection table or a specific MAC address any: ignores sender IP/MAC address host: sender host MACADDR: sender MAC address
deny ip host *A.B.C.D* **mac** {**any** | **host** *MACADDR*}		Discards ARP packets from a specific host. MACADDR: MAC address
deny ip range *A.B.C.D A.B.C.D* **mac any**		Discards ARP packets of a given range of IP addresses. A.B.C.D: start/end IP address of sender
deny ip *A.B.C.D/A* **mac** {**any** | **host** *MACADDR*}		Discards ARP packets of a sender IP network addresses. A.B.C.D/A: sender IP network address
deny ip {**any** | **host** *A.B.C.D* | *A.B.C.D/A*} **mac pattern** *PATTERN* **offset** <0-5>		Discards ARP packets according to IP address and MAC address pattern. any: ignores sender IP address A.B.C.D: sender IP address of host A.B.C.D/A: sender IP network address PATTERN: MAC address pattern (e.g. 10, 10:11, ~ 10:10:11:20:20) offset: character location within sender MAC address pattern

To delete the configured range of IP address for discarding ARP packets, use the following command.

Command	Mode	Description
no deny ip any mac {**any** | **host** *MACADDR*}	ARP-ACL	Deletes a configured range of IP address to discard ARP packets. any: ignores sender MAC address host: sender host MACADDR: sender MAC address A.B.C.D: start/end IP address of sender A.B.C.D/A: sender IP network address PATTERN: MAC address pattern (e.g. 10, 10:11, ~ 10:10:11:20:20) offset: character location within sender MAC address pattern
no deny ip host *A.B.C.D* **mac** {**any** | **host** *MACADDR*}		
no deny ip range *A.B.C.D A.B.C.D* **mac any**		
no deny ip *A.B.C.D/A* **mac** {**any** | **host** *MACADDR*}		
no deny ip {**any** | **host** *A.B.C.D* | *A.B.C.D/A*} **mac pattern** *PATTERN* **offset** <0-5>		

To specify the range of IP address to forward ARP packets, use the following command.

Command	Mode	Description
permit ip any mac {**any** | **host** *MACADDR*}	ARP-ACL	Permits ARP packets of all IP addresses with all MAC addresses which have not learned before on ARP inspection table or a specific MAC address. any: ignores sender MAC address host: sender host MACADDR: sender MAC address
permit ip host *A.B.C.D* **mac** {**any** | **host** *MACADDR*}		Permits ARP packets from a specific host. MACADDR: MAC address
permit ip range *A.B.C.D A.B.C.D* **mac any**		Permits ARP packets of a given range of IP addresses. A.B.C.D: start/end IP address of sender
permit ip *A.B.C.D/A* **mac** {**any** | **host** *MACADDR*}		Permits ARP packets of a sender IP network addresses. A.B.C.D/A: sender IP network address
permit ip {**any** | **host** *A.B.C.D* | *A.B.C.D/A*} **mac pattern** *WORD* **offset** <0-5>		Permits ARP packets according to IP address and MAC address pattern. any: ignores sender IP address A.B.C.D: sender IP address of host A.B.C.D/A: sender IP network address PATTERN: MAC address pattern (e.g. 10, 10:11, ~ 10:10:11:20:20) offset: character location within sender MAC address pattern

To delete the configured ranged of IP address to permit ARP packets, use the following command.

Command	Mode	Description
no permit ip any mac {**any** | **host** *MACADDR*}	ARP-ACL	Deletes a configured range of IP address to permit ARP packets. any: ignores sender MAC address host: sender host MACADDR: sender MAC address A.B.C.D: start/end IP address of sender A.B.C.D/A: sender IP network address PATTERN: MAC address pattern (e.g. 10, 10:11, ~ 10:10:11:20:20) offset: character location within sender MAC address pattern
no permit ip host *A.B.C.D* **mac** {**any** | **host** *MACADDR*}		
no permit ip range *A.B.C.D A.B.C.D* **mac any**		
no permit ip *A.B.C.D/A* **mac** {**any** | **host** *MACADDR*}		
no permit ip {**any** | **host** *A.B.C.D* | *A.B.C.D/A*} **mac pattern** *PATTERN* **offset** <0-5>		

By the following command, the ARP access list also refers to a DHCP snooping binding table to permit the ARP packets for DHCP users. This reference enables the system to permit ARP packets only for the IP addresses on the DHCP snooping binding table. The ARP access list with the DHCP snooping allows IP communications to users authorized by the DHCP snooping.

To permit/discard ARP packets for the users authorized by the DHCP snooping, use the following command.

Command	Mode	Description
permit dhcp-snoop-inspection	ARP-ACL	Permits ARP packets of users authorized by the DHCP snooping.
no permit dhcp-snoop-inspection		Discards a configured ARP packets of users authorized by the DHCP snooping.

To display the configured APR access lists, use the following command.

Command	Mode	Description
show arp access-list [*NAME*]	Global	Displays existing ARP access list names.

8.1.4.2 Enabling ARP Inspection Filtering

To enable/disable the ARP inspection filtering of a certain range of IP addresses from the ARP access list, use the following command.

Command	Mode	Description
ip arp inspection filter *NAME* **vlan** *VLANS*	Global	Enables ARP inspection filtering with a configured ARP access list on specified VLAN. NAME: ARP access list name
no ip arp inspection filter *NAME* **vlan** *VLANS*		Disables ARP inspection filtering with a configured ARP access list on specified VLAN.

i

ARP inspection actually runs in the system after the configured ARP access list applies to specific VLAN using the **ip arp inspection filter** command.

8.1.4.3 ARP Address Validation

The LD3032 also provides the ARP validation feature. Regardless of a static ARP table, the ARP validation will discard ARP packets in the following cases:

- In case a sender MAC address of ARP packet does not match a source MAC address of Ethernet header
- In case a target MAC address of ARP reply packet does not match a destination MAC address of Ethernet header
- In case of a sender IP address of ARP packet or target IP address is 0.0.0.0, 255.255.255.255 or one of multicast IP addresses

To enable/disable the ARP validation, use the following command.

Command	Mode	Description
ip arp inspection validate {**src-**	Global	Enables the ARP validation with the following options.

mac | **dst-mac** | **ip**}		src-mac: source MAC address. dst-mac: destination MAC address. ip: source/destination IP address.
no ip arp inspection validate {**src-mac** | **dst-mac** | **ip**}		Disables the ARP validation.

i

The **src-mac**, **dst-mac**, and **ip** options can be configured together.

8.1.4.4 ARP Inspection on Trust Port

The ARP inspection defines 2 trust states, trusted and untrusted. Incoming packets via trusted ports bypass the ARP inspection process, while those via untrusted ports go through the ARP inspection process. Normally, the ports connected to subscribers are configured as untrusted, while the ports connected to an upper network are configured as trusted.

To set a trust state on a port for the ARP inspection, use the following command.

Command	Mode	Description
ip arp inspection trust port	Interface [GE/XE/GPON]	Sets a trust state on a port as trusted
no ip arp inspection trust port		Sets a trust state on a port as untrusted

To display a configured trust port of the ARP inspection, use the following command.

Command	Mode	Description
show ip arp inspection trust	Enable Global	Shows a configured trust port of the ARP inspection.
show ip arp inspection trust interface {**channelgroup**|**gpon**|**gigabitethernet** |**tengigabitethernet** } *PORTS*		

8.1.4.5 ARP Inspection Log-buffer

Log-buffer function shows the list of subscribers who have been used invalid fixed IP addresses. This function saves the information of users who are discarded by ARP inspection and generates periodic syslog messages.

Log-buffer function is automatically enabled with ARP inspection. If LD3032 receives invalid or denied ARP packets by ARP inspection, it creates the table of entries that include the information of port number, VLAN ID, source IP address, source MAC address and time. In addition, you can specify the maximum number of entries.

After one of entries is displayed as a syslog message, it is removed in the order in which the entries appear in the list.

To configure the options of log-buffer function, use the following command.

Command	Mode	Description
ip arp inspection log-buffer entries <0-1024>	Global	Specifies the number of entries in log-buffer. 0-1024: the max. number of entries (default: 32)
ip arp inspection log-buffer logs <0-1024> **interval** <0-86400>		Sets the interval for displaying syslog messages of entries. 0-1024: the number of syslog messages per specified interval (default: 5) 0-86400: interval value in second (default: 1 sec)

To delete the configured options of log-buffer function, use the following command.

Command	Mode	Description
no ip arp inspection log-buffer {**entries** | **logs**}	Global	Deletes the configured options of log-buffer function.

To display the configured log-buffer function and entries' information, use the following command.

Command	Mode	Description
show ip arp inspection log	Enable Global	Displays the configured log-buffer function.

To clear all of collected entries in the list, use the following command.

Command	Mode	Description
clear ip arp inspection log	Enable Global	Clears all of collected entires in the log-buffer list.

8.1.4.6 Displaying ARP Inspection

To display a status of the ARP inspection, use the following command.

Command	Mode	Description
show ip arp inspection [**vlan** *VLANS*]	Enable Global	Shows a status of the ARP inspection.
show ip arp inspection statistics [**vlan** *VLANS*]		Shows collected statistics of the ARP inspection.

To clear collected statistics of the ARP inspection, use the following command.

Command	Mode	Description
clear ip arp inspection statistics [**vlan** *VLANS*]	Global	Clears collected statistics of the ARP inspection.

8.1.5 Gratuitous ARP

Gratuitous ARP is a broadcast packet like an ARP request. It containing IP address and MAC address of gateway, and the network is accessible even though IP addresses of specific host's gateway are repeatedly assigned to the other.

Configure Gratuitous ARP interval and transmission count using following commands. And configure transmission delivery-start in order to transmit Gratuitous ARP after ARP reply. Gratuitous ARP is transmitted after some time from transmitting ARP reply.

Command	Mode	Description
arp patrol *TIME COUNT* [*TIME*]	Global	Configures a gratuitous ARP. TIME: transmit interval COUNT: transmit count
no arp patrol		Disables a gratuitous ARP.

8.1.6 Proxy ARP

The LD3032 supports the proxy ARP. Proxy ARP is the technique in which one host, usually a router, answers ARP requests intended for another machine. By “faking” its identity, the router accepts responsibility for routing packets to the “real” destination. Proxy ARP can help the switches on a subnet reach remote subnets without configuring routing or a default gateway.

The host A has a /16 subnet mask. What this means is that the host A believes that it is directly connected to all of network 172.16.0.0. When the host A needs to communicate with any switches if believes are directly connected, it will send an ARP request to the destination. Therefore, when the host A needs to send a packet to the host D, the host A believes that the host D is directly connected, so it sends an ARP request to the host D.

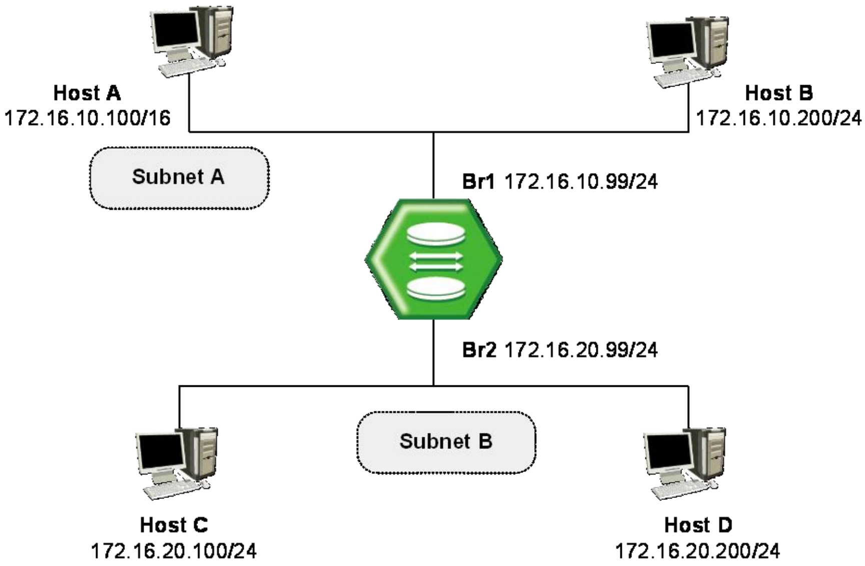


Fig. 8.1 Proxy ARP

The host A needs the MAC address of the host D to reach the host D. Therefore, the host A broadcasts an ARP request on the subnet A, including the LD3032's br1 interface, but does not reach the host D. By default, the LD3032 does not forward broadcasts. Since the LD3032 knows that the target address (the host D's IP address) is on another subnet and can reach the host D, it will reply with its own MAC address to the host A.

The proxy ARP replies that the LD3032 sends to the host A. The proxy ARP reply packet is encapsulated in an Ethernet frame with its MAC address as the source address and the host A's MAC address as the destination address. The ARP replies are always unicast to the original requester. On receiving this ARP reply, the host A updates its ARP table.

From now on, the host A will forward all the packets that it wants to reach the host D to the MAC address of the LD3032. Since the LD3032 knows how to reach the host D, the router forwards the packet to the host D. The ARP cache on the hosts in the subnet A is populated with the MAC address of the LD3032 for all the hosts on the subnet B. Hence, all packets destined to the subnet B are sent to the router. The LD3032 forwards those packets to the hosts in the subnet B.

To configure the interface to accept and respond to proxy ARP, use the following command on *Interface Configuration* mode.

Command	Mode	Description
ip proxy-arp	Interface [VLAN]	Enables the proxy ARP function on specific interface.
no ip proxy-arp		Disables the proxy ARP function.

8.2 IPv6 Neighbor Discovery

Neighbor discovery (ND) is specified in RFC 2464. ND combines Address Resolution Protocol (ARP) and ICMP router discovery and Redirect. With IPv4, we have no means to detect whether or not a neighbor is reachable. With ND protocol, a neighbor unreachability detection mechanism has been defined.

IPv6 nodes use neighbor discovery for the following purposes:
- To determine Layer 2 addresses of nodes on the same link
- To find neighboring routers that can forward their packets
- To keep track of which neighbor are reachable and which are not, and detect changed link-layer addresses

The neighbor discovery protocol consists of five ICMP messages:

- **Router Solicitation / Router Advertisement (RS & RA)**
  The routers send out Router Advertisement (RA) message in regular intervals. The hosts can request RA message by issuing a Router Solicitation message.
  RA message contains the information of link prefixes, link MTU, specific routers, and duration.

- **Neighbor Solicitation / Neighbor Advertisement (NS & NA)**
  These messages fulfill the functions that the link-layer address resolution in IPv4 and the neighbor unreachability detection mechanism. The IPv6 host sends Neighbor Solicitation message to discover the link-layer address of an on-link IPv6 node. IPv6 node sends the Neighbor Advertisement message in response to a NS and sends unsolicited NA to inform neighboring nodes of link-layer addresses.

- **ICMP redirect message**
  IPv6 router sends ICMP redirect message to inform an originating host of a better first-hop address for specific destination.

8.2.1 Stateful Auto Configuration

Router Advertisements sent from this interface have the Managed Address Configuration Flag or not. It decides that the hosts are thus permitted to use IPv6 stateless autoconfiguration to create global unicast addresses for themselves. This means that the attached hosts should use stateful autoconfiguration to obtain addresses if the flag is set.

To set the managed address configuration flag in IPv6 RA messages, use the following command.

Command	Mode	Description
ipv6 nd managed-config-flag	Interface [VLAN/MGMT /LO]	Sets the managed address configuration flag in RA.
no ipv6 nd managed-config-flag		Clears the managed address configuration flag from RA. (default)

To set the other stateful configuration flag in RA message, use the following command.

Command	Mode	Description
ipv6 nd other-config-flag	Interface [VLAN/MGMT /LO]	Sets the other stateful configuration flag in RA.
no ipv6 nd other-config-flag		Clears the other stateful configuration flag from RA. (default)

8.2.2 Configuring IPv6 Prefix

To configure how IPv6 prefixes are advertised in the IPv6 RA message, use the following command.

Command	Mode	Description
ipv6 nd prefix *X:X::X:X/M*	Interface [VLAN/MGMT /LO]	Configures how IPv6 prefixes are advertised in the RA message. X:X::X:X/M: IPv6 prefix 0-4294967295: valid lifetime 0-4294967295: preferred lifetime no-autoconfig: specifies prefix cannot be used for IPv6 autoconfiguration. off-link: specifies prefix to assigned to the link
ipv6 nd prefix *X:X::X:X/M* <0-4294967295> <0-4294967295> [**no-autoconfig** | **off-link**]		
no ipv6 nd prefix *X:X::X:X/M*		Deletes a configured how IPv6 prefixes are advertised in the RA message.

To configure existing IPv6 address on interface as ND prefix in the IPv6 RA message, use the following command.

Command	Mode	Description
ipv6 nd prefix default	Interface [VLAN/MGMT /LO]	Configures the existing IPv6 address assigned on an interface as ND prefix.
ipv6 nd prefix default <0-4294967295> <0-4294967295> [**no-autoconfig** | **off-link**]		Configures the existing IPv6 address assigned on an interface as ND prefix and sets its parameters.
no ipv6 nd prefix default		Clears a configured ND prefix using the existing IPv6 address of interface

8.2.3 Interval of RA Messages

To prevent synchronization with other IPv6 nodes, the actual value used should be randomly adjusted to within plus or minus 20 percent of the specified value. To configure the interval between IPv6 Router Advertisement transmissions from this interface, use the following command.

Command	Mode	Description
ipv6 nd ra-interval <3-1800> [<3-1350>]	Interface [VLAN/MGMT /LO]	Specifies the interval between IPv6 RA messages. (default: 600 seconds)
no ipv6 nd ra-interval		Deletes a configured interval between IPv6 RA mes-

		sages

The interval value should be less than or equal to the IPv6 Router Lifetime if this is a default router.

8.2.4 Router's Lifetime

This value is included in all IPv6 Router Advertisements sent out this interface. If the router is not a default router, this will have a value of zero. The default value is 1,800 seconds.

To configure the lifetime of a RA messages, use the following command.

Command	Mode	Description
ipv6 nd ra-lifetime <0-9000>	Interface [VLAN/MGMT /LO]	Specifies the lifetime of IPv6 RA message. (default: 1800 seconds)
no ipv6 nd ra-lifetime		Deletes a configured lifetime of IPv6 RA message

If the router is a default router, this value will be non-zero and should not be less than the minimum Router Advertisement interval.

8.2.5 Reachable Time

RA reachable time is the amount of time that a remote IPv6 node is reachable for a specified time after a reachable confirmation event. The reachable time enables detecting unavailable neighbors. The configured reachable time is included in all router advertisements sent out of an interface so that nodes on the same link use the same time value.

To specify the reachable time that the switch can reach a remote IPv6 node after the reachability confirmation event has occurred, use the following command.

Command	Mode	Description
ipv6 nd reachable-time <0-3600000>	Interface [VLAN/MGMT /LO]	Specifies the reachable time. 0-3600000: IPv6 reachable time in milliseconds (A value of 0 indicates that the configured time is unspecified by this switch.)
no ipv6 nd reachable-time		Deletes a configured reachable time and restores the default time.

If the switch is configured with shorter reachable times, it enables detecting unavailable neighbors more quickly, however, shorter times consume more IPv6 network bandwidth and processing resources in all IPv6 network devices. We do not recommend configuring a short reachable time value.

For example, to configure the reachable time of 1000 milliseconds for Ethernet interface br2, enter the following commands:

```
SWITCH(config)# interface br2
SWITCH(config-if)# ipv6 nd reachable-time 1000
SWITCH(config-if)#
```

8.2.6 RA Suppression

If IPv6 unicast routing is enabled on an Ethernet interface, by default, this interface sends IPv6 router advertisement messages. However, by default, non-LAN interface types, for example, tunnel interfaces, do not send router advertisement messages.

To control transmission of IPv6 RA messages on the interface, use the following command.

Command	Mode	Description
ipv6 nd suppress-ra	Interface [VLAN/MGMT /LO]	Disables the sending of RA messages on an Ethernet interface.
no ipv6 nd suppress-ra		Sends RA messages on an interface.

8.2.7 Hop Limit

To configure the maximum number of hops used in RA messages and all IPv6 packets, use the following command.

Command	Mode	Description
ipv6 nd ra-hoplimit <0-255>	Interface [VLAN/MGMT /LO]	Configures the maximum number of hops in RA messages. 0-255: RA hop limit
no ipv6 nd ra-hoplimit		Returns the hop limit to its default value.

8.2.8 Retrans-time

To configure the interval between IPv6 neighbor solicitation retransmissions on an interface, use the following command.

Command	Mode	Description
ipv6 nd retrans-time <0-4294967295>	Interface [VLAN/MGMT /LO]	Specifies the interval between IPv6 neighbor solicitation retransmissions. 0-4294967295: IPv6 NS retransmission time in milliseconds
no ipv6 nd retrans-time		Deletes a configured interval between IPv6 neighbor solicitation retransmissions.

8.2.9 Static IPv6 Neighbor Entry

The Neighbor Discovery (ND) protocol is a new messaging protocol that was created as part of IPv6 to perform a number of the tasks that ICMP and ARP accomplish in IPv4. Just like ARP, ND builds a cache of dynamic entries, and the administrator can configure the mapping between IPv6 address and MAC address to add static entries in the ND cache table.

To add a static entry in the ND cache table by specifying the mapping between an IPv6 address and a MAC address, use the following command.

Command	Mode	Description
ipv6 neighbor *X:X::X:X MAC-ADDR*	Global	Sets a static neighbor entry, enter the IPv6 address and the MAC address. X:X::X:X: IPv6 address MACADDR: enter the MAC address.
ipv6 neighbor *X:X::X:X MAC-ADDR* { **gigabitethernet** | **tengigabitethernet** | **gpon** | **channelgroup**} *IFPORT*		Sets a static neighbor entry, enter the IPv6 address, MAC address and interface name. MACADDR: enter the MAC address.

To remove the configured static entry from the ND cache table, use the following command.

Command	Mode	Description
no ipv6 neighbor [*X:X::X:X*]	Global	Remove the configured static entry from the ND cache table
no ipv6 neighbor *X:X::X:X* {**gigabitethernet** | **tengigabitethernet** | **gpon** | **channelgroup**} *IFPORT*		

8.2.10 IPv6 Neighbor Discovery (ND) Inspection

IPv6 Neighbor Discovery (ND) inspection feature can protect switches against IPv6 address spoofing. It provides IPv6 communication by mapping an IPv6 address to a MAC address. However, a malicious user can attack ND caches of system by intercepting the traffic intended for other hosts on the subnet. ND inspection is a security feature that validates ND packets in a network. It discards ND packets with invalid IP-MAC address binding.

To activate/deactivate the ND inspection function on a VLAN, use the following command.

Command	Mode	Description
ipv6 nd inspection vlan *VLANS*	Global	Activates ND inspection on a VLAN. VLANS: VLAN ID (1-4094)
no ipv6 nd inspection vlan *VLANS*		Deactivates ND inspection on a VLAN.

8.2.10.1 ND Access List

You can exclude a given range of IP addresses from the ND inspection using ND access lists. ND access lists are created by the **ipv6 nd access-list** command on the *Global Configuration* mode. ND access list permits or denies the ND packets of a given range of IPv6 addresses.

To create/delete ND access control list (ACL), use the following command.

Command	Mode	Description
ipv6 nd access-list *NAME*	Global	Opens ND ACL configuration mode and creates a ND access list. NAME: ND access list name
no ipv6 nd access-list *NAME*		Deletes a ND access list.
ipv6 nd access-list delete all		Deletes all ND access lists.

After opening *ND Access List Configuration* mode, the prompt changes from SWITCH(config)# to SWITCH(config-nd-acl[*NAME*])#. After opening *ND ACL Configuration* mode, a range of IPv6 addresses can be configured to apply ND inspection.

By default, ND Access List discards the Neighbor Discovery protocol packets, of all IPv6 addresses and MAC addresses.

To specify the IPv6 address and MAC address to forward the ND messages, use the following command.

Command	Mode	Description
permit ipv6 {**host** *X:X::X:X* | *X:X::X:X/M* | **any**} **mac** {**any** | **host** *MACADDR*}	ND-ACL	Permits ND packets based on their IPv6 address and MAC address, which have not learned before on ND inspection table. mac any: ignores sender MAC address ipv6 any: ignores sender IPv6 address host: sender host X:X::X:X: sender IPv6 address X:X::X:X/M: sender IPv6 network address MACADDR: sender MAC address
permit ipv6 range *X:X::X:X X:X::X:X* **mac any**		Permits ND packets of a given range of IPv6 addresses. X:X::X:X: start/end IPv6 address of sender

To delete the configured range of IPv6 address or MAC address to permit ND packets, use the following command.

Command	Mode	Description
no permit ipv6 {**host** *X:X::X:X* | *X:X::X:X/M* | **any**} **mac** {**any** | **host** *MACADDR*}	ND-ACL	Deletes the configured range of IPv6 address to permit ND packets. any: ignores sender MAC address host: sender host MACADDR: sender MAC address X:X::X:X: start/end IPv6 address of sender X:X::X:X/M: sender IPv6 network address
no permit ipv6 range *X:X::X:X X:X::X:X* **mac any**		

To specify the IPv6 address and MAC address to deny ND packets, use the following command.

Command	Mode	Description
deny ipv6 {**host** *X:X::X:X* | *X:X::X:X/M* | **any**} **mac** {**any** | **host** *MACADDR*}	ND-ACL	Discards ND packets based on their IPv6 address and MAC address, which have not learned before on ND inspection table. mac any: ignores sender MAC address ipv6 any: ignores sender IPv6 address host: sender host X:X::X:X: sender IPv6 address X:X::X:X/M: sender IPv6 network address MACADDR: sender MAC address
deny ipv6 {**host** *X:X::X:X* | *X:X::X:X/M* | **any**} **mac pattern** *WORD* **offset** <0-5>		Discards ND packets based on their IPv6 address and MAC pattern, which have not learned before on ND inspection table. ipv6 any: ignores sender IPv6 address host: sender host X:X::X:X: sender IPv6 address X:X::X:X/M: sender IPv6 network address WORD: sender MAC pattern value 0-5: offset value
deny ipv6 range *X:X::X:X X:X::X:X* **mac any**		Discards ND packets of a given range of IPv6 addresses. X:X::X:X: start/end IPv6 address of sender

To delete the configured IPv6 address and MAC address for discarding ND packets, use the following command.

Command	Mode	Description
no deny ipv6 {**host** *X:X::X:X* | *X:X::X:X/M* | **any**} **mac** {**any** | **host** *MACADDR*}	ND-ACL	Deletes a configured range of IP address to discard ND packets. any: ignores sender MAC address host: sender host MACADDR: sender MAC address X:X::X:X: start/end IPv6 address of sender X:X::X:X/M: sender IPv6 network address
no deny ipv6 {**host** *X:X::X:X* | *X:X::X:X/M* | **any**} **mac pattern** *WORD* **offset** <0-5>		
no deny ipv6 range *X:X::X:X X:X::X:X* **mac any**		

By the following command, the ND access list also refers to a DHCP snooping binding table to permit the ND packets for DHCP users. This feature enables the system to permit ND packets only for the IPv6 addresses on the DHCP snooping binding table. The ND access list with the DHCP snooping allows IP communications to users authorized by the DHCP snooping. The source IP address and MAC address of each packet are checked against the table, and if a valid match is not found, the packet is dropped.

To permit/discard ND packets for the users authorized by the DHCPv6 snooping, use the following command.

Command	Mode	Description
permit dhcpv6-snoop-inspection	ND-ACL	Permits ND packets of users authorized by the DHCPv6 snooping.
no permit dhcpv6-snoop-inspection		Discards the configured ND packets of users authorized by the DHCPv6 snooping.

To display the configured ND access lists, use the following command.

Command	Mode	Description
show ipv6 nd access-list [*NAME*]	Global	Displays the existing ND access lists.

8.2.10.2 Enabling ND Inspection Filtering

To enable/disable the ND inspection filtering of a certain range of IPv6 addresses from the ND access list, use the following command.

Command	Mode	Description
ipv6 nd inspection filter *NAME* **vlan** *VLANS*	Global	Enables ND inspection filtering with the configured ND access list on the VLAN. NAME: ND access list name
no ipv6 nd inspection filter *NAME* **vlan** *VLANS*		Disables ND inspection filtering with a configured ND access list on specified VLAN.

i

ND inspection actually runs in the system after the configured ND access list applies to specific VLAN ID using the **ip nd inspection filter** command.

8.2.10.3 ND Inspection on Trust Port

The ND inspection defines 2 trust states, trusted and untrusted. Incoming packets via trusted ports bypass the ND inspection process, while those via untrusted ports go through the ND inspection process. Normally, the ports connected to subscribers are configured as untrusted, while the ports connected to an upper network are configured as trusted.

To set a trust state on a port for the ND inspection, use the following command.

Command	Mode	Description
ipv6 nd inspection trust port *PORTS*	Global	Sets a trust state on a port as trusted PORTS: port number
no ipv6 nd inspection trust port *PORTS*		Sets a trust state on a port as untrusted PORTS: port number

To display the configured trust port of the ND inspection, use the following command.

Command	Mode	Description
show ipv6 nd inspection trust [**port** *PORTS*]	Enable Global	Shows the configured trust port of the ND inspection.

8.2.10.4 ND Inspection Log-buffer

Log-buffer function shows the list of subscribers who have been used invalid fixed IP addresses. This function saves the information of users who are discarded by ND inspection and generates periodic syslog messages.

Log-buffer function is automatically enabled with ND inspection. If LD3032 receives invalid or denied ND packets by ND inspection, it creates the table of entries that include the information of port number, VLAN ID, source IP address, source MAC address and time. In addition, you can specify the maximum number of entries.

After one of entries is displayed as a syslog message, it is removed in the order in which the entries appear in the list.

To configure the options of log-buffer function, use the following command.

Command	Mode	Description
ipv6 nd inspection log-buffer entries <0-1024>	Global	Specifies the number of entries in log-buffer. 0-1024: the max. number of entries (default: 32)
ipv6 nd inspection log-buffer logs <0-1024> **interval** <0-86400>		Sets the interval for displaying syslog messages of entries. 0-1024: the number of syslog messages per specified interval (default: 5) 0-86400: interval value in second (default: 1 second)

To delete the configured options of log-buffer function, use the following command.

Command	Mode	Description
no ipv6 nd inspection log-buffer {**entries** | **logs**}	Global	Deletes the configured options of log-buffer function.

To display the configured log-buffer function and entries' information, use the following command.

Command	Mode	Description
show ipv6 nd inspection log	Enable Global	Displays the configured log-buffer function.

To clear all of collected entries in the list, use the following command.

Command	Mode	Description
clear ipv6 nd inspection log	Enable Global	Clears all of collected entries in the log-buffer list.

8.2.10.5 ND Inspection Delay Time

This function sets the time before ND inspection starts to run. Before setting this feature, ND inspection should be enabled. ND inspection checks validity of incoming ND packets by using DHCP snooping binding table and denies the ND packets if they are not identified in the table.

However, the LD3032 may be rebooted with any reason, then DHCP snooping binding table entries, which are dynamically learned from DHCP packets back and forth the LD3032, would be lost. Thus, ND inspection should be delayed to start during some time so that DHCP snooping table can build entries. If no time is given, ND inspection sees empty snooping table and drop every ND packet.

To specify the ND inspection delay time, use the following command.

Command	Mode	Description
ipv6 dhcp snooping nd-inspection start <1-2147483637>	Global	Configures the ND inspection delay time. If reboot, ND inspection resumes after the time you configure. 1-2147483637: delay time (unit: second, default:1800 seconds)
no ipv6 dhcp snooping nd-inspection start		Delete the configured ND inspection delay time.

8.2.10.6 ND RA Guard

The IPv6 RA Guard feature provides support for allowing the network administrator to block or reject unwanted or rogue router advertisement (RA) guard messages that arrive at the network device.

To set a trust state on a port for the ND inspection, use the following command.

Command	Mode	Description
ipv6 nd raguard policy *NAME*	Global	Enables RA guard policy configuration mode. NAME: policy name
ipv6 nd raguard policy delete all		Deletes all RA policy configured with the RA guard.

To display the RA guard policy on all interfaces configured with RA guard, use the following command.

Command	Mode	Description
show ipv6 nd raguard policy	Enable Global	Shows the configured RA guard policy. .

8.2.10.7 Displaying ND Inspection

To display a status of the ND inspection, use the following command.

Command	Mode	Description
show ipv6 nd inspection [**vlan** *VLANS*]	Enable Global	Shows a status of the ND inspection.
show ipv6 nd inspection statistics [**vlan** *VLANS*]		Shows collected statistics of the ND inspection.

To clear the collected statistics of the ND inspection, use the following command.

Command	Mode	Description
clear ipv6 nd inspection statistics [**vlan** *VLANS*]	Enable Global	Clears collected statistics of the ND inspection.

8.2.11 Gratuitous ND

Gratuitous ND is a broadcast packet like an ND request. It containing IPv6 address and MAC address of gateway, and the network is accessible even though IPv6 addresses of a specific host's gateway are repeatedly assigned to the other.

To configure the interval and transmission count for Gratuitous ND messages, use the following command. And set the transmission start-delivery time in order to transmit Gratuitous ND after ND reply. Gratuitous ND is transmitted after some time from transmitting ND reply.

Command	Mode	Description
ipv6 nd patrol *TIME COUNT* [*TIME*]	Global	Configures a gratuitous ND. TIME: transmit interval COUNT: the number of attempts to send Gratuitous ND
no ipv6 nd patrol		Disables the configured parameters of Gratuitous ND.

8.2.12 Displaying Neighbor Discovery

To display IPv6 neighbor discovery cache information table, use the following command.

Command	Mode	Description
show ipv6 neighbors [{*X:X::X:X* | *X:X::X:X/M*}]	Enable Global	Shows IPv6 neighbors discovery cache information.
show ipv6 neighbors { **gigabitethernet** | **tengigabitethernet** | **gpon** | **channelgroup**} *IFPORT*		

To clear IPv6 neighbor discovery cache information table, use the following command.

Command	Mode	Description
clear ipv6 neighbors [{*X:X::X:X* | *X:X::X:X/M*}]	Enable Global	Clears IPv6 neighbor discovery cache information.
clear ipv6 neighbors { **gigabitethernet | tengigabitethernet | gpon | channelgroup**} *IFPORT*		

8.2.13 Debugging Neighbor Discovery

To enable/disable a ND packet debugging, use the following command.

Command	Mode	Description
debug ipv6 nd	Enable	Enables IPv6 ND debugging.
debug ipv6 nd {recv | send}		
no debug ipv6 nd		Disables IPv6 ND debugging.
no debug ipv6 nd {recv | send }		

To display the debugging information, use the following command.

Command	Mode	Description
show debugging ipv6 nd	Enable Global	Shows the debugging information of ND.

8.3 System Authentication

For the enhanced system security, the LD3032 provides two authentication methods to access the switch such as Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+).

8.3.1 Authentication Method

To set the system authentication method, use the following command.

Command	Mode	Description
login {**local** | **remote**} {**radius** | **tacacs** | **host** | **all**} {**enable** | **disable**}	Global	Sets a system authentication method. local: console access remote: telnet/SSH access radius: RADIUS authentication tacacs: TACACS+ authentication host: nominal system authentication (default) all: all types of the authentication
no login {**local** | **remote**} {**radius** | **tacacs** | **host** | **all**}		Deletes a configured system authentication method.
no login		

8.3.2 Authentication Interface

If more than 2 interfaces exist in the LD3032, you can set one interface to access RADIUS or TACACS server.

To set an authentication interface, use the following command.

Command	Mode	Description
login radius interface {**management** | **vlan** *VLANS* | **loopback** | **gigabitethernet** *IFPORT* | **tengigabitethernet** *IFPORT* | **gpon** *IFPORT* | **channelgroup** *GROUP*} [*A.B.C.D*]	Global	Sets an authentication interface. radius: RADIUS authentication tacacs: TACACS+ authentication INTERFACE: interface name A.B.C.D: source IP address (optional)
login tacacs interface {**management** | **vlan** *VLANS* | **loopback** | **gigabitethernet** *IFPORT* | **tengigabitethernet** *IFPORT* | **gpon** *IFPORT* | **channelgroup** *GROUP*} [*A.B.C.D*]		
no login {**radius** | **tacacs**} **interface**		Deletes a specified authentication interface.

8.3.3 Primary Authentication Method

You can set the order of the authentication method by giving the priority to each authentication method.

To set the primary authentication method, use the following command

Command	Mode	Description
login {**local** | **remote**} {**radius** | **tacacs** | **host**} **primary**	Global	Sets a system authentication method. local: console access remote: telnet/SSH access radius: RADIUS authentication tacacs: TACACS+ authentication host: nominal system authentication (default)

8.3.4 RADIUS Server

8.3.4.1 RADIUS Server for System Authentication

To add/delete a RADIUS server for system authentication, use the following command.

Command	Mode	Description
login radius server *A.B.C.D* *KEY* [**auth_port** *PORT* **acct_port** *PORT*]	Global	Adds a RADIUS server with its information. A.B.C.D: IP address KEY: authentication key value auth_port: authentication port (optional) acct_port: accounting port (optional)
no login radius server [*A.B.C.D*]		Deletes an added RADIUS server.

i

You can add up to 5 RADIUS servers.

8.3.4.2 RADIUS Server Priority

To specify the priority of a registered RADIUS server, use the following command.

Command	Mode	Description
login radius server move *A.B.C.D* <1-5>	Global	Specifies a priority of RADIUS server. A.B.C.D: IP address 1-5: priority of RADIUS server

8.3.4.3 Timeout of Authentication Request

After an authentication request, the LD3032 waits for a response from a RADIUS server for specified time.

To specify a timeout value, use the following command.

Command	Mode	Description
login radius timeout <1-100>	Global	Specifies a timeout value. 1-100: timeout value for a response (default: 5)
no login radius timeout		Deletes a specified timeout value.

8.3.4.4 Frequency of Retransmit

In case of no response from a RADIUS server, the LD3032 is supposed to retransmit an authentication request. To set the frequency of retransmitting an authentication request, use the following command.

Command	Mode	Description
login radius retransmit <1-10>	Global	Sets the frequency of retransmit. 1-10: frequency count (default: 3)
no login radius retransmit		Deletes a specified frequency count.

8.3.5 TACACS+ Server

8.3.5.1 TACACS+ Server for System Authentication

To add/delete the TACACS+ server for system authentication, use the following command.

Command	Mode	Description
login tacacs server *A.B.C.D KEY*	Global	Adds a TACACS+ server with its information. A.B.C.D: IP address KEY: authentication key value
no login tacacs server [*A.B.C.D*]		Deletes an added TACACS+ server. A.B.C.D: IP address

i You can add up to 5 TACACS+ servers.

8.3.5.2 TACACS+ Server Priority

To specify the priority of a registered TACACS+ server, use the following command.

Command	Mode	Description
login tacacs server move *A.B.C.D* <1-5>	Global	Specifies the priority of TACACS+ server. A.B.C.D: IP address 1-5: priority of TACACS server

8.3.5.3 Timeout of Authentication Request

After the authentication request, the LD3032 waits for the response from the TACACS+ server for specified time. To specify a timeout value, use the following command.

Command	Mode	Description
login tacacs timeout <1-100>	Global	Specifies a timeout value. 1-100: timeout value for the response (default: 5)
no login tacacs timeout		Deletes a specified timeout value.

8.3.5.4 Additional TACACS+ Configuration

The LD3032 provides several additional options to configure the system authentication via TACACS+ server.

TCP Port for the Authentication

To specify TCP port for the system authentication, use the following command.

Command	Mode	Description
login tacacs socket-port <1-65535>	Global	Specifies TCP port for the authentication. 1-65535: TCP port
no login tacacs socket-port		Deletes a specified TCP port for the authentication.

Authentication Type

To select the authentication type for TACACS+, use the following command.

Command	Mode	Description
login tacacs auth-type {**ascii** | **pap** | **chap**}	Global	Selects an authentication type for TACACS+. ascii: plain text pap: password authentication protocol chap: challenge handshake authentication protocol
no login tacacs auth-type		Deletes a specified authentication type.

Priority Level

According to a defined priority level, the user has different authority to access the system. This priority should be defined in the TACACS+ server in the same way. To define the priority level of user, use the following command.

Command	Mode	Description
login tacacs priority-level {**min** | **user** | **max** | **root**}	Global	Defines the priority level of user, see the below information for the order of priority.
no login tacacs priority-level		Deletes a defined priority level.

i The order of priority is **root** = **max** > **user** > **min**.

8.3.6 Accounting Mode

The LD3032 provides the accounting function of AAA (Authentication, Authorization, and Accounting). Accounting is the process of measuring the resources a user has consumed. Typically, accounting measures the amount of system time a user has used or the amount of data a user has sent and received.

To set an accounting mode, use the following command.

Command	Mode	Description
login accounting-mode {**none** | **start** | **stop** | **both**}	Global	Sets an accounting mode. start: measures start point only. stop: measures stop point only. both: measures start and stop point both.
no login accounting-mode		Deletes a configured accounting mode.

8.3.7 Displaying System Authentication

To display a configured system authentication, use the following command.

Command	Mode	Description
show login	Enable Global	Shows a configured system authentication.

8.4 Secure Shell (SSH)

Network security is getting more important because the access network has been generalized among numerous users. However, typical FTP and telnet service have big weakness for their security. Secure shell (SSH) is a network protocol that allows establishing a secure channel between a local and a remote computer. It uses public-key cryptography to authenticate the remote computer and to allow the remote computer to authenticate the user.

8.4.1 SSH Server

The LD3032 can be operated as SSH server. You can configure the switch as SSH server with the following procedure.

- Enabling SSH Server
- Displaying On-line SSH Client
- Disconnecting SSH Client
- Assigning Specific Authentication Key
- Displaying Connection History of SSH Client

8.4.1.1 Enabling SSH Server

To enable/disable SSH server, use the following command.

Command	Mode	Description
ssh server enable	Global	Enables SSH server.
ssh server disable		Disables SSH server.

8.4.1.2 Displaying On-line SSH Client

To display SSH clients connected to SSH server, use the following command.

Command	Mode	Description
show ssh	Enable Global	Shows SSH clients connected to SSH server.

8.4.1.3 Disconnecting SSH Client

To disconnect an SSH client connected to SSH server, use the following command.

Command	Mode	Description
ssh disconnect *PID*	Global	Disconnects SSH clients connected to SSH server. PID: SSH client number
ssh disconnect all		

8.4.1.4 Assigning Specific Authentication Key

After enabling SSH server, each client will upload its own generated authentication key. The SSH server can assign the specific key among the uploaded keys from several clients.

To verify an authentication key, use the following command.

Command	Mode	Description
ssh key verify *PUBLIC-KEY*	Global	Verifies a generated authentication key.

i If the SSH server verify the key for specific client, other clients must download the key file from SSH server to login.

8.4.1.5 Displaying Connection History of SSH Client

To display the connection history of SSH client, use the following command.

Command	Mode	Description
show ssh history	Enable Global	Shows the connection history of SSH clients who are connected to SSH server up to now.

8.4.2 SSH Client

The LD3032 can be used as SSH client with the following procedure.

- Login to SSH Server
- Secured File Copy
- Authentication Key

8.4.2.1 Login to SSH Server

To login to SSH server after configuring the LD3032 as SSH client, use the following command.

Command	Mode	Description
ssh login *DESTINATION* [*PUBLIC-KEY*]	Enable	Logins to SSH server. DESTINATION: IP address of SSH server PUBLIC-KEY: public key

8.4.2.2 Secured File Copy

To copy a system configuration file from/to SSH server, use the following command.

Command	Mode	Description
copy {**scp** | **sftp**} **config upload** *FILENAME*	Enable	Downloads and uploads a file to through SSH server. FILE: destination file name

8.4.2.3 Authentication Key

SSH client can access to server through authentication key after configuring authentication key and informing it to server. It is safer to use authentication key than inputting password every time for login, and it is possible to connect to several SSH servers with using one authentication key.

To configure an authentication key in the LD3032, use the following command.

Command	Mode	Description
ssh keygen {**rsa1** | **rsa** | **dsa**}	Global	Configures an authentication key. rsa1: SSH ver. 1 authentication rsa: SSH ver. 2 authentication dsa: SSH ver. 2 authentication FILENAME: key file name
copy {**scp** | **sftp**} **key upload** *FILENAME*	Enable	

To configure authentication key and connect to SSH server with the authentication key, perform the following procedure:

Step 1 Configure the authentication key in the switch.

```
SWITCH_A(config)# ssh keygen dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/etc/.ssh/id_dsa):
Enter passphrase (empty for no passphrase):networks
Enter same passphrase again:networks
Your identification has been saved in /etc/.ssh/id_dsa.
Your public key has been saved in /etc/.ssh/id_dsa.pub.
The key fingerprint is:
d9:26:8e:3d:fa:06:31:95:f8:fe:f6:59:24:42:47:7e root@LD3032
SWITCH_A(config)#
```

Step 2 Copy the generated authentication key to SSH server.

Step 3 Connect to SSH server with the authentication key.

```
SWITCH_A(config)# ssh login 172.16.209.10
Enter passphrase for key '/etc/.ssh/id_dsa': networks
SWITCH_B#
```

To display the configured authentication keys in the LD3032, use the following command.

Command	Mode	Description
show key-list	Enable Global	Shows an authentication key of SSH server.

8.5 802.1x Authentication

To enhance security and portability of network management, there are two ways of authentication based on MAC address and port-based authentication which restrict clients attempting to access to port.

In a word, port-based authentication (802.1x) decides to give access to a RADIUS server having the information about user who tries to access.

802.1x authentication adopts EAP (Extensible Authentication Protocol) structure. In EAP system, there are EAP-MD5 (Message Digest 5), EAP-TLS (Transport Level Security), EAP-SRP (Secure Remote Password), EAP-TTLS (Tunneled TLS) and the LD3032 supports EAP-MD5 and EAP-TLS. Accessing with user's ID and password, EAP-MD5 is 1-way Authentication based on the password. EAP-TLS accesses through the mutual authentication system of server authentication and personal authentication and it is possible to guarantee high security because of mutual authentication system.

At a request of user Authentication, from user's PC EAPOL-Start type of packets are transmitted to authenticator and authenticator again requests identification. After getting respond about identification, request to approve access to RADIUS server and be authenticated by checking access through user's information.

The following figure explains the process of 802.1x authentication.

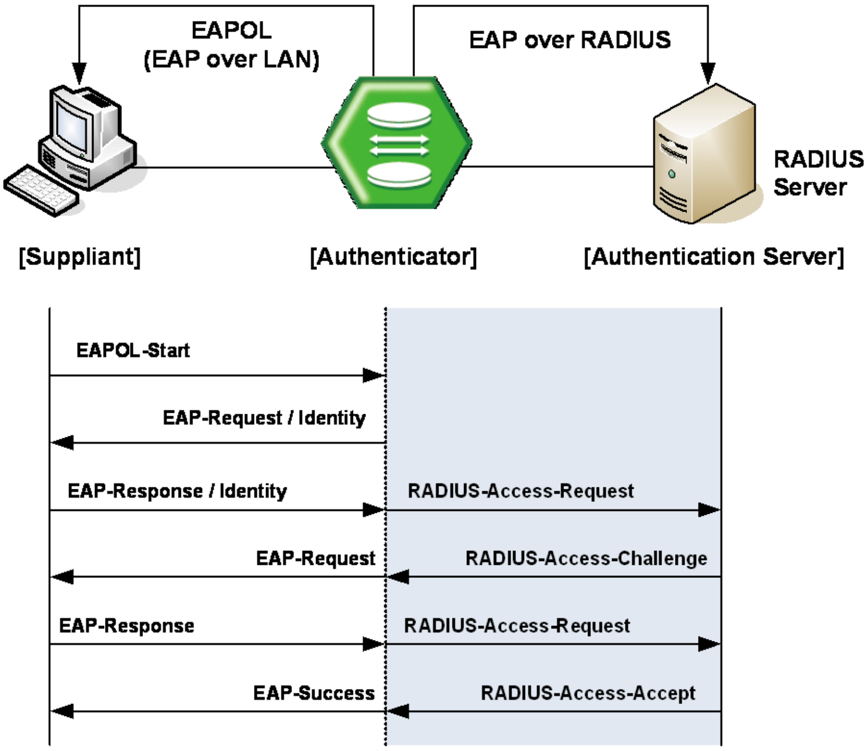


Fig. 8.2 Process of 802.1x Authentication

8.5.1 802.1x Authentication

8.5.1.1 Enabling 802.1x

To configure 802.1x, the user should enable 802.1x daemon first. To enable 802.1x daemon, use the following command.

Command	Mode	Description
dot1x system-auth-control	Global	Enables 802.1x daemon.
no dot1x system-auth-control		Disables 802.1x daemon.

8.5.1.2 RADIUS Server

As RADIUS server is registered in authenticator, authenticator also can be registered in RADIUS server.

Here, authenticator and RADIUS server need extra data authenticating each other besides they register each other's IP address. The data is key and should be the same value for each other. For the key value, every kinds of character can be used except the space or special character.

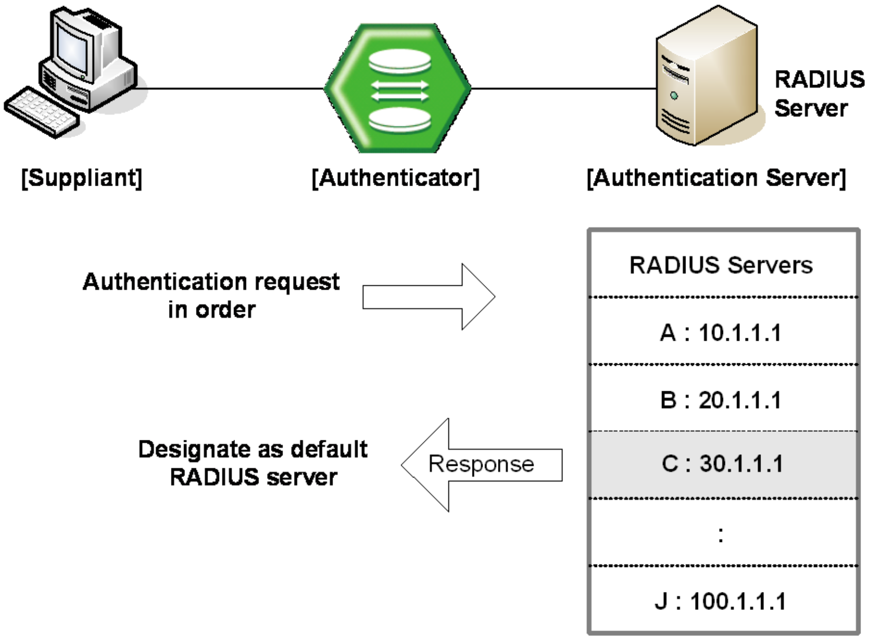


Fig. 8.3 Multiple Authentication Servers

If you register in several servers, the authentication server starts form RADIUS server registered as first one, then requests the second RADIUS server in case there's no response. According to the order of registering the authentication request, the authentication request is tried and the server which responds to it becomes the default server from the point of response time.

After default server is designated, all requests start from the RADIUS server. If there's no response from default server again, the authentication request is tried for RADIUS server designated as next one.

To configure IP address of RADIUS server and key value, use the following command.

Command	Mode	Description
dot1x radius-server host {*A.B.C.D* | *NAME*} **auth-port** <0-65535> **key** *KEY*	Global	Registers RADIUS server with key value and UDP port of radius server. 0-65535: UDP port (default: 1812)
dot1x radius-server host {*A.B.C.D* | *NAME*} **key** *KEY*		Configures IP address of RADIUS server and key value.
no dot1x radius-server host {*A.B.C.D* | *NAME*}		Deletes a registered RADIUS server.

You can designate up to 5 RADIUS servers as authenticator.

The **key** option is authentication information between the authenticator and RADIUS server. The authenticator and RADIUS server must have a same key value, and you can use alphabetic characters and numbers for the key value. The space or special character is not allowed.

To set priority to a registered RADIUS server, use the following command..

Command	Mode	Description
dot1x radius-server move {*A.B.C.D* | *NAME*} **priority** *PRIORITY*	Global	Sets priority to a registered RADIUS server.

8.5.1.3 Authentication Mode

You can set the authentication mode from the port-based to the MAC-based. To set the authentication mode, use the following command.

Command	Mode	Description
dot1x auth-mode mac-base *PORTS*	Global	Sets the authentication mode to the MAC-based.
no dot1x auth-mode mac-base *PORTS*		Restores the authentication mode to the port-based.

Before setting the authentication mode to the MAC-based, you need to set a MAC filtering policy to **deny** for all the Ethernet ports. To configure a MAC filtering policy, see Section 7.13 MAC Filtering.

8.5.1.4 Authentication Port

After configuring 802.1x authentication mode, you should select the authentication port.

Command	Mode	Description
dot1x nas-port *PORTS*	Global	Designates 802.1x authentication port.
no dot1x nas-port *PORTS*		Disables 802.1x authentication port.

8.5.1.5 Force Authorization

The LD3032 can permit the users requesting the access regardless of the authentication from RADIUS server. For example, even though a client is authenticated from the server, it is possible to configure not to be authenticated from the server.

To manage the approval for the designated port, use the following command.

Command	Mode	Description
dot1x port-control {**auto** | **force-authorized** | **force-unauthorized**} *PORTS*	Global	Configures a state of the authentication port. auto: authorization up to RADIUS server (default) force-authorized: force authorization force-unauthorized: force unauthorization
no dot1x port-control *PORTS*		Deletes a configured authentication port state.

8.5.1.6 Interval for Retransmitting Request/Identity Packet

In the LD3032, it is possible to specify how long the device waits for a client to send back a response/identity packet after the device has sent a request/identity packet. If the client does not send back a response/identity packet during this time, the device retransmits the request/identity packet.

To configure the number of seconds that the switch waits for a response to a request/identity packet, use the following command.

Command	Mode	Description
dot1x timeout tx-period <1-65535> *PORTS*	Global	Sets reattempt interval for requesting request/identity packet. 1-65535: retransmit interval (default: 30)
no dot1x timeout tx-period *PORTS*		Disables the interval for requesting identity.

8.5.1.7 Number of Requests to RADIUS Server

After 802.1x authentication configured as explained above and the user tries to connect with the port, the process of authentication is progressed among user’s PC and the equipment as authenticator and RADIUS server. It is possible to configure how many times the device which will be authenticator requests for authentication to RADIUS server.

To configure times of authentication request in the LD3032, use the following command.

Command	Mode	Description
dot1x radius-server retries <1-10>	Global	Configure times of authentication request to RADIUS server. 1-10: retry number (default: 3)

8.5.1.8 Interval of Request to RADIUS Server

For the LD3032, it is possible to set the time for the retransmission of packets to check RADIUS server. If there is a response from other packets, the switch waits for a response from RADIUS server during the configured time before resending the request.

Command	Mode	Description
dot1x radius-server timeout <1-120>	Global	Configures the interval of request to RADIUS server. 1-120: interval (default: 1)

You should consider the distance from the server for configuring the interval of requesting the authentication to RADIUS server. If you configure the interval too short, the authentication could not be realized. If it happens, you had better to reconfigure the interval longer.

8.5.2 802.1x Re-Authentication

In the LD3032, it is possible to update the authentication status on the port periodically. To enable re-authentication on the port, you should perform the below procedure:

Step 1 Enable 802.1x re-authentication.

Step 2 Configure the interval of re-authentication.

Step 3 Configure the interval of requesting re-authentication in case of re-authentication fails.

Step 4 Execute 802.1x re-authenticating regardless of the interval.

8.5.2.1 Enabling 802.1x Re-Authentication

To enable 802.1x re-authentication using the following command.

Command	Mode	Description
dot1x reauth-enable *PORTS*	Global	Enables 802.1x re-authentication.
no dot1x reauth-enable *PORTS*		Disables 802.1x re-authentication.

8.5.2.2 Interval of Re-Authentication

RAIDIUS server contains the database about the user who has access right. The database is real-time upgraded so it is possible for user to lose the access right by updated database even though he is once authenticated. In this case, even though the user is accessible to network, he should be authenticated once again so that the changed database is applied to. Besides, because of various reasons for managing RADIUS server and 802.1x authentication port, the user is supposed to be re-authenticated every regular time. The administrator of the LD3032 can configure a term of re-authentication.

To configure a term of re-authentication, use the following command.

Command	Mode	Description
dot1x timeout reauth-period <1-4294967295> *PORTS*	Global	Sets the period between re-authentication attempts.
no dot1x timeout reauth-period *PORTS*		Deletes the period between re-authentication attempts.

8.5.2.3 Interval of Requesting Re-Authentication

When the authenticator sends request/identity packet for re-authentication and no response is received from the suppliant for the number of seconds, the authenticator retransmits the request to the suppliant. In the LD3032, you can set the number of seconds that the authenticator should wait for a response to request/identity packet from the suppliant before retransmitting the request.

To set reattempt interval for requesting request/identity packet, use the following command.

Command	Mode	Description
dot1x timeout quiet-period <1-65535> *PORTS*	Global	Sets reattempt interval for requesting request/identity packet. 1-65535: reattempt interval (default: 30)
no dot1x timeout quiet-period *PORTS*		Disables the interval for requesting identity.

8.5.2.4 802.1x Re-Authentication

In Section 8.5.2.2, it is described even though the user is accessible to network, he should be authenticated so that the changed database is applied to.

Besides, because of various reasons managing RADIUS server and 802.1x authentication port, the user is supposed to be re-authenticated every regular time.

However, there are some cases of implementing re-authentication immediately. In the LD3032, it is possible to implement re-authentication immediately regardless of configured time interval.

Command	Mode	Description
dot1x reauthenticate *PORTS*	Global	Performs re-authentication regardless of the configured time interval.

8.5.3 Initializing Authentication Status

The user can initialize the entire configuration on the port. Once the port is initialized, the supplicants accessing to the port should be re-authenticated.

Command	Mode	Description
dot1x initialize *PORTS*	Global	Initializes the authentication status on the port.

8.5.4 Restoring Default Value

To restore the default value of the 802.1x configuration, use the following command.

Command	Mode	Description
dot1x default *PORTS*	Global	Restores the default value of the 802.1x configuration.

8.5.5 Displaying 802.1x Configuration

To display 802.1x configuration, use the following command.

Command	Mode	Description
show dot1x	Enable Global	Shows 802.1x configuration on the system.
show dot1x *PORTS*		Shows 802.1x configuration on the port.

8.5.6 802.1x User Authentication Statistics

It is possible for user to make reset state by showing and deleting the statistics of 802.1x user authentication.

To display the statistics about the process of 802.1x user authentication, use the following command.

Command	Mode	Description
show dot1x statistics *PORTS*	Enable Global	Shows the statistics of 802.1x user authentication on the port.

To make reset state by deleting the statistics of 802.1x user authentication, use the following command.

Command	Mode	Description
dot1x clear statistics *PORTS*	Global	Makes reset state by deleting the statistics of 802.1x on the port.

9 System Main Functions

9.1 Virtual Local Area Network (VLAN)

The first step in setting up your bridging network is to define VLAN on your switch. VLAN is a bridged network that is logically segmented by customer or function. Each VLAN contains a group of ports called VLAN members. On the VLAN network, packets received on a port are forwarded only to the ports that belong to the same VLAN as the receiving port. Network devices in different VLANs cannot communicate with one another without a Layer 3 switching device to route traffic between the VLANs. VLAN reduces the amount of broadcast traffic so that flow control could be realized. It also has security benefits by completely separating traffics between different VLANs.

Enlarged Network Bandwidth

Users belonged in each different VLAN can use more enlarged bandwidth than no VLAN composition because they do not receive unnecessary Broadcast information. A properly implemented VLAN will restrict multicast and unknown unicast traffic to only those links necessary to only those links necessary to reach members of the VLAN associated with that multicast (or unknown unicast) traffic.

Cost-Effective Way

When you use VLAN to prevent unnecessary traffic loading because of broadcast, you can get cost-effective network composition since switch is not needed.

Enhanced Security

When using a shared-bandwidth LAN, there is no inherent protection provided against unwanted eavesdropping. In addition to eavesdropping, a malicious user on a shared LAN can also induce problems by sending lots of traffic to specific targeted users or network as a whole. The only cure is to physically isolate the offending user. By creating logical partitions with VLAN technology, we further enhance the protections against both unwanted eavesdropping and spurious transmissions. As depicted in Figure, a properly implemented port-based VLAN allows free communication among the members of a given VLAN, but does not forward traffic among switch ports associated with members of different VLANs. That is, a VLAN configuration restricts traffic flow to a proper subnet comprising exactly those links connecting members of the VLAN. Users can eavesdrop only on the multicast and unknown unicast traffic within their own VLAN: presumably the configured VLAN comprises a set of logically related users.

User Mobility

By defining a VLAN based on the addresses of the member stations, we can define a workgroup independent of the physical location of its members. Unicast and multicast traffic (including server advertisements) will propagate to all members of the VLAN so that they can communicate freely among themselves.

9.1.1 Port-based VLAN

The simplest implicit mapping rule is known as port-based VLAN. A frame is assigned to a VLAN based solely on the switch port on which the frame arrives. In the example depicted in Fig. 9.1, frames arriving on ports 1 through 4 are assigned to VLAN 1, frame from ports 5 through 8 are assigned to VLAN 2, and frames from ports 9 through 12 are assigned to VLAN 3.

Stations within a given VLAN can freely communicate among themselves using either unicast or multicast addressing. No communication is possible at the Data Link layer between stations connected to ports that are members of different VLANs. Communication among devices in separate VLANs can be accomplished at higher layers of the architecture, for example, by using a Network layer router with connections to two or more VLANs.

Multicast traffic, or traffic destined for an unknown unicast address arriving on any port, will be flooded only to those ports that are part of the same VLAN. This provides the desired traffic isolation and bandwidth preservation. The use of port-based VLANs effectively partitions a single switch into multiple sub-switches, one for each VLAN.

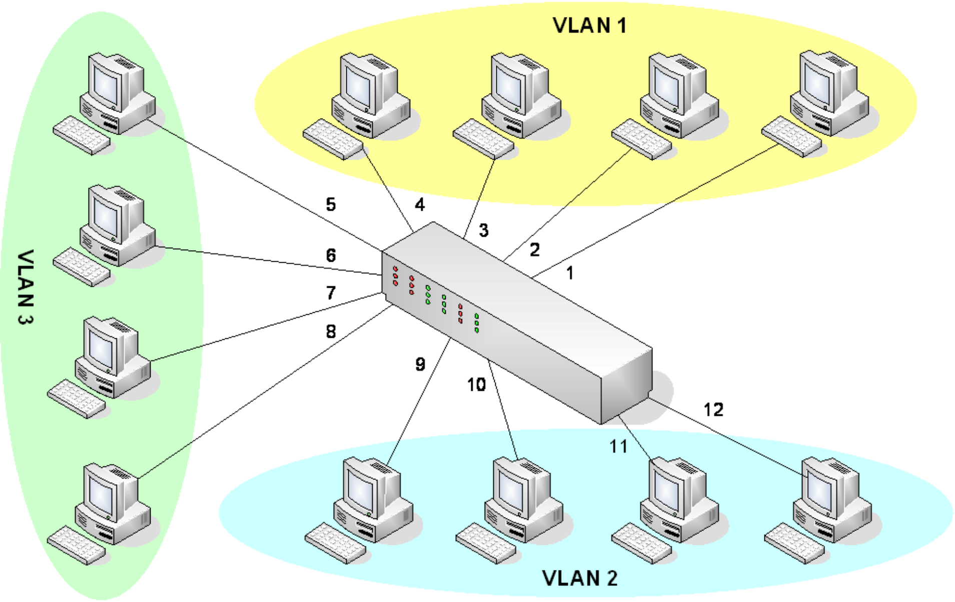


Fig. 9.1 Port-based VLAN

The IEEE 802.1Q based ports on the switches support simultaneous tagged and untagged traffic. An 802.1Q port is assigned a default port VLAN ID (PVID), and all untagged traffic is assumed to belong to the port default PVID. Thus, the ports participating in the VLANs accept packets bearing VLAN tags and transmit them to the port VLAN ID.

In a VLAN environment, a frame’s association with a given VLAN is soft; the fact that a given frame exists on some physical cable does not imply its membership in any particular VLAN. VLAN association is determined by a set of rules applied to the frames by VLAN-aware stations and/or switches.

There are two methods for identifying the VLAN membership of a given frame:
- Parse the frame and apply the membership rules (implicit tagging).
- Provide an explicit VLAN identifier within the frame itself.

VLAN Tag

A VLAN tag is a predefined field in a frame that carries the VLAN identifier for that frame. VLAN tags are always applied by a VLAN-aware device. VLAN-tagging provides a number of benefits, but also carries some disadvantages.

Advantages	Disadvantages
VLAN association rules only need to be applied once.	Tags can only be interpreted by VLAN aware devices.
Only edge switches need to know the VLAN association rules.	Edge switches must strip tags before forwarding frames to legacy devices or VLAN-unaware domains.
Core switches can get higher performance by operating on an explicit VLAN identifier.	Insertion or removal of a tag requires recalculation of the FCS, possibly compromising frame integrity.
VLAN-aware end stations can further reduce the performance load of edge switches.	Tag insertion may increase the length of a frame beyond the maximum allowed by legacy equipment.

Tab. 9.1 Advantages and Disadvantages of Tagged VLAN

9.1.1.1 Creating VLAN

To open the VLAN Database mode, use the following command.

Command	Mode	Description
vlan database	Global	Opens the VLAN Database mode.

To create a VLAN ID on user’s network, use the following command.

Command	Mode	Description
vlan *VLANS*	VLAN Database	Creates a VLAN by assigning VLAN ID: VLANS: VLAN ID (2-4094, multiple entries possible)

i

After a VLAN ID creation on the *VLAN Database* mode, you can enter the *VLAN interface* mode to configure the addtional settings.

To enable/disable a VLAN and set its name, use the following command.

Command	Mode	Description
vlan *VLANS* **state** {**enable** | **disable**}	VLAN Database	Enables/disables the VLAN operational state. (default: enable) VLANS: VLAN ID (2-4094, multiple entries possible)
vlan *VLANS* **name** *NAME*		Sets the name of VLAN. NAME: The ascii name of the VLAN
vlan *VLANS* **name** *NAME* [**state** {**enable** | **disable**}]		Enables/disables the VLAN operational state and sets the name.

To specify a VLAN description, use the following command.

Command	Mode	Description
vlan description *VLANS DESC*	VLAN Database	Specifies a VLAN description. VLANS: VLAN ID (1-4094) DESC: description
no vlan description *VLANS*		Deletes a specified description.

i The variable *VLANS* is a particular set of interfaces. Frames are bridged only among interfaces in the same VLAN.

9.1.1.2 Adding a Member Port to VLAN Group

All planning ports are in access mode, and belong to the default VLAN (whose VID=1). If the port is added to a VLAN without specifying tagged or untagged, the default setting is untagged (switchport mode access).

To add the member port to a new VLAN ID, use the following command.

Command	Mode	Description
switchport mode access	Interface [XE/GE/ /GPON/CG]	Configures the VLAN membership access mode of a port. access: indicates an untagged L2 VLAN port (default)
switchport access vlan *VLANS*		Changes the default VLAN for the interface and configures the VLAN ID to the untagged interface. This command is available when the interface is in access mode. VLANS: VLAN ID for the interface (2-4094)
no switchport access vlan		Removes the associated interface from the specified VLAN ID and returns to the default VLAN ID 1.

i When you assign several interfaces to VLAN, you have to enter each port separated by a comma without space or use dash mark “-” to arrange port range.

i When you add a port in another VLAN, this port in default VLAN is automatically deleted.

To add the member port to a VLAN ID and specify a VLAN ID to the tagged L2 VLAN interface, use the following command.

Command	Mode	Description

switchport mode trunk	Interface [XE/GE /GPON/CG]	Configures the VLAN membership trunk mode of a port. trunk: indicates a tagged L2 VLAN port
switchport trunk allowed vlan all		Sets allowed all VLANs for the trunk interface.
switchport trunk allowed vlan except *VLAN_ID*		Sets allowed all VLANs for the trunk interface except the VLAN_ID.
switchport trunk allowed vlan none		Sets no VLANs for the trunk.
switchport trunk allowed vlan remove *VLAN_ID*		Sets a VLAN that will be removed from trunk port.
switchport trunk allowed vlan add *VLAN_ID*		Adds a member port to a VLAN and configures a VLAN ID to the tagged interface. VLAN_ID: VLAN ID (2-4094) to be added
no switchport trunk		Deletes associated interface from the specified VLAN:

To set the native VLAN for classifying untagged traffic through the L2 interface, use the following command.

Command	Mode	Description
switchport trunk native vlan *VLANS*	Interface [XE/GE/ GPON/CG]	Configures a VLAN ID as the native VLAN. VLANS: native VLAN ID (2-4094)
no switchport trunk native vlan		Deletes the configured native VLAN ID

9.1.1.3 Deleting VLAN

To delete a VLAN ID from the interface, use the following command.

Command	Mode	Description
no vlan *VLANS*	VLAN Database	Deletes VLAN, enter the VLAN ID to be deleted. VLANS: VLAN ID (2-4094)

9.1.1.4 Specifying PVID

By default, PVID 1 is specified to all ports. You can also configure a PVID.

To configure a PVID in a port, use the following command.

Command	Mode	Description
pvid *PVIDS*	Interface [XE/GE/ GPON]	Configures a PVID. PVIDS: PVID (1-4094, multiple entries possible)
no pvid		Deletes the configured PVID.
show pvid	Enable Global	Shows configured PVIDs.

	Interface [XE/GE/GPON]	

9.1.2 Protocol-based VLAN

User can use a VLAN mapping that associates a set of processes within stations to a VLAN rather than the stations themselves. Consider a network comprising devices supporting multiple protocol suites. Each device may have an IP protocol stack, an AppleTalk protocol stack, an IPX protocol stack and so on.

If we configure VLAN-aware switches such that they can associate a frame with a VLAN based on a combination of the station's MAC source address and the protocol stack in use, we can create separate VLANs for each set of protocol-specific applications.

To configure a protocol-based VLAN, follow these steps.

1. Configure VLAN groups for the protocols you want to use.
2. Create a protocol group for each of the protocols you want to assign to a VLAN.
3. Then map the protocol for each interface to the appropriate VLAN.

Command	Mode	Description
vlan pvid ethertype *ETHERTYPE VLANS*	Interface [XE/GE/GPON]	Adds a port with a protocol-based VLAN. ETHERTYPE: Ethernet type (e.g. 0x800) VLANS: VLAN ID (2-4094)
no vlan pvid ethertype [*ETHERTYPE*]		Removes a port from a protocol-based VLAN.

Because Protocol Based VLAN and normal VLAN run at the same time, Protocol Based VLAN operates only matched situation comparing below two cases.

1. When Untagged Frame comes in and matches with Protocol VLAN Table, tags PVID which configured on Protocol VLAN. But in no matched situation, tags PVID which configured on and operates VLAN.
2. When Tagged Frame comes in and VID is 0, it switches by Protocol VLAN Table. But if VID is not 0, it switches by normal VLAN Table.

9.1.3 Reserved VLAN

Before creating/enabling a port interface or subinterface, you can specify a range of reserved VLANs for internal purpose. To add/delete the internal reserved VLAN ID for the port interface, use the following command.

Command	Mode	Description
vlan reserved add *VLANS*	Global	Assigns the reserved VLAN IDs which are internally usable for the port interface. If the VLAN ID is already created and assigned by user, you can not assign same VLAN ID for the port interface or subinterface. VLANS: VLAN IDs (2-4094)

vlan reserved delete *VLANS*		Deletes the assigned VLAN ID.
no vlan reserved		Clears all of the reserved VLAN IDs for the port/sub-interfaces.

9.1.4 VLAN Description

To specify a VLAN description, use the following command.

Command	Mode	Description
vlan description *VLANS DESC*	VLAN Database	Specifies a VLAN description. VLANS: VLAN ID (1-4094) DESC: description
no vlan description *VLANS*		Deletes a specified description.

To display a specified VLAN description, use the following command.

Command	Mode	Description
show vlan description	Enable Global	Shows a specified VLAN description.

9.1.5 Displaying VLAN Information

To display the VLAN information, use the following command.

Command	Mode	Description
show vlan	Enable Global	Shows all VLAN configurations.
show vlan <1-4094>		Shows information of selected VLAN
show vlan brief		Shows VLAN information for all bridges
show vlan description		Shows a description for specific VLAN.
show vlan {**static** | **dynamic**} [**bridge** <1-32>]		Shows the static / dynamic VLANs.
show vlan dot1q-tunnel		Shows QinQ configuration.
show vlan protocol		Shows VLAN based on protocol.
show vlan range-tagging in-bound [*PORTS*]		Shows VLAN range based tagging configuration. PORTS: port number
show vlan reserved		Shows the assigned VLAN IDs for the port/sub-interfaces.
show vlan subnet		Shows VLAN based on subnet.

9.1.6 QinQ

QinQ or Double Tagging is one way for tunneling between several networks.

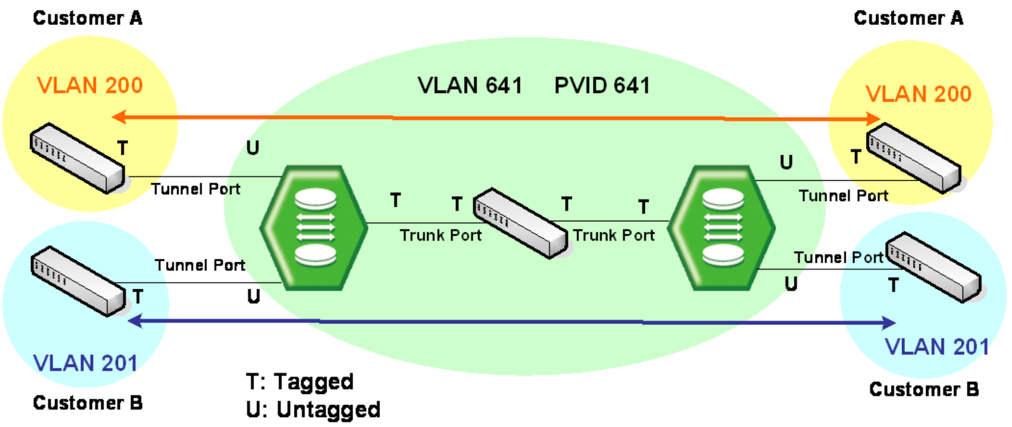
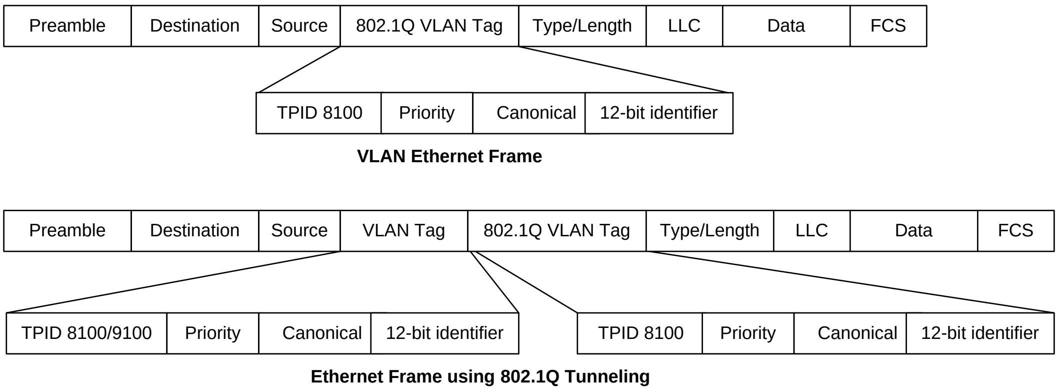


Fig. 9.2 Example of QinQ Configuration

If QinQ is configured on the LD3032, it transmits packets adding another Tag to original Tag. Customer A group and customer B group can guarantee security because telecommunication is done between each VLANs at Double Tagging part.

Double tagging is implemented with another VLAN tag in Ethernet frame header.



Preamble	Destination	Source	802.1Q VLAN Tag	Type/Length	LLC	Data	FCS

TPID 8100	Priority	Canonical	12-bit identifier

VLAN Ethernet Frame

Preamble	Destination	Source	VLAN Tag	802.1Q VLAN Tag	Type/Length	LLC	Data	FCS

TPID 8100/9100	Priority	Canonical	12-bit identifier

TPID 8100	Priority	Canonical	12-bit identifier

Ethernet Frame using 802.1Q Tunneling

Fig. 9.3 QinQ Frame

Port which connected with Service Provider is Uplink port (internal), and which connected with customer is Access port (external).

Tunnel Port

By tunnel port we mean a LAN port that is configured to offer 802.1Q-tunneling support. A tunnel port is always connected to the end customer, and the input traffic to a tunnel port is always 802.1Q tagged traffic.

The different customer VLANs existing in the traffic to a tunnel port shall be preserved when the traffic is carried across the network

Trunk Port

By trunk port we mean a LAN port that is configured to operate as an inter-switch link/port, able of carrying double-tagged traffic. A trunk port is always connected to another trunk port on a different switch. Switching shall be performed between trunk ports and tunnels ports and between different trunk ports.

9.1.6.1 Double Tagging Operation

Step 1
If there is no S-VLAN Tag on the received packet, S-VLAN Tag is added.
S-VLAN Tag = TPID : Configured TPID
VID : PVID of input port

Step 2
If a received packet is tagged with C-VLAN, the switch transmits it to uplink port changing to S-VLAN + C-VLAN. When the TPID value of received packet is same with the port TPID, it is recognized as S-VLAN, and if not, it is recognized as C-VLAN.

Step 3
If Egress port is Access port (configured as Untagged), remove S-VLAN. If egress port is uplink port, transmit as it is.

Step 4
The LD3032 switch has the 0x8100 TPID value as default and other values are used as hexadecimal number.

9.1.6.2 Double Tagging Configuration

Step 1
Open *Ethernet/GPON Interface Configuration* mode to enable the QinQ (UNI) port.

Command	Mode	Description
vlan dot1q-tunnel enable	Interface [XE/GE/ GPON]	Enables a QinQ port.

Step 2
Configure the same PVID with the VLAN of peer network on the designated QinQ port.

Command	Mode	Description
pvid <1-4094>	Interface [XE/GE/GPON]	Configures the same PVID with the VLAN. 1-4094: PVID

To disable double tagging, use the following command.

Command	Mode	Description
vlan dot1q-tunnel disable	Interface [XE/GE/GPON]	Disables the QinQ port.

i

When you configure double tagging on the LD3032, note the following attention list.

- DT and HTLS cannot be configured at the same time. (If the switch should operate as DT, HTSL has to be disabled.)
- The TPID value of all ports on the switch is the same.
- Access port should be configured as Untagged, and uplink port as Tagged.
- Ignore all tag information which comes from untagged port (Access port).
- The port with DT function can configure Jumbo function also.

9.1.6.3 TPID Configuration

TPID (Tag Protocol Identifier) is a type of Tag protocol, and it indicates the currently used tag information. Users can change the TPID. By default the port configured as 802.1q (0x8100) cannot work as VLAN member.

To set TPID on QinQ port, use the following command.

Command	Mode	Description
vlan dot1q-tunnel {**inner** | **outer**} **tpid** *TPID*	Global	Configures TPID of S-VLAN/C-VLAN. inner : TPID for C-VLAN outer : TPID for S-VLAN TPID : Tag Protocol Identifier (hex digit default : 0x8100)
vlan dot1q-tunnel outer tpid *TPID*	Interface [XE/GE/ GPON]	Configures TPID of S-VLAN on the interface.

9.1.6.4 C-VLAN Configuration

To configure a C-VLAN ID that is used for the inner tag of incoming untagged packet, use the following command.

Command	Mode	Description
vlan dot1q-tunnel inner-tag vlan-id *VLANS*	Interface [XE/GE/ GPON]	Specifies a C-VLAN ID that is used for incoming un-tagged packets to UNI port. VLANS: 0 to 4094, VLAN ID
no vlan dot1q-tunnel inner-tag		Deletes the configured C-VLAN ID.

To attach the configured C-VLAN in the inner tag field of incoming untagged packet on a port, use the following command.

Command	Mode	Description
vlan dot1q-tunnel ingress push inner-tag	Interface [XE/GE/ GPON]	Adds the configured C-VLAN tag in the inner tag field of incoming packet on an ingress port
no vlan dot1q-tunnel ingress push inner-tag		Disables the C-VLAN inner tagging on an ingress port.

To remove the C-VLAN inner tag from the outgoing packet on a port, use the following command.

Command	Mode	Description
vlan dot1q-tunnel egress pop inner-tag	Interface [XE/GE/ GPON]	Removes C-VLAN tag from the outgoing packet on an egress port
no vlan dot1q-tunnel egress pop inner-tag		Disables the C-VLAN inner tag removal on an egress port.

9.1.6.5 Attaching a S-VLAN tag

To attach an S-VLAN tag to inbound packet with a given VLAN on a port basis, use the following command.

Command	Mode	Description
vlan tagging inbound vlan *VLAN_ID1* **vlan** *VLAN_ID2*	Interface [XE/GE/ GPON]	Attaches an S-VLAN tag to packet with the specified C-VLAN. It is available on the UNI port. VLAN_ID1: VLAN ID that incoming packet belongs to VLAN_ID2: service VLAN in the outer-tag to attach
vlan range-tagging inbound vlan *VLAN_RANGE* **vlan** *VLAN_ID*		Attaches an S-VLAN tag to packet with the specified C-VLAN ID range. VLAN_RANGE: multiple VLAN IDs that incoming packet belongs to VLAN_ID: service VLAN to attach
no vlan tagging inbound vlan *VLAN_ID1*		Deletes the S-VLAN tagging.
no vlan range-tagging inbound vlan *VLAN_RANGE*		

To see the vlan tagging configuration, use the following command.

Command	Mode	Description
show vlan tagging inbound [*PORTS*]	Enable Global	Displays the S-VLAN tagging configuration.

9.1.6.6 Detaching a S-VLAN tag

To remove an S-VLAN tag of the outbound packet on a port basis, use the following command.

Command	Mode	Description
vlan tagging outbound vlan *VLAN_ID*	Interface [XE/GE/GPON]	Detaches a S-VLAN tag of the packets with the specified S-VLAN ID. VLAN_ID: service VLAN
no vlan tagging outbound vlan *VLAN_ID*		Deletes the S-VLAN untagging.

To see the vlan untagging configuration, use the following command.

Command	Mode	Description
show vlan tagging outbound [*PORTS*]	Enable Global	Displays the S-VLAN untagging configuration.

9.1.7 VLAN Translation

VLAN Translation is simply an action of Rule. This function is to translate the value of specific VLAN ID which classified by Rule. The switch makes Tag adding PVID on Untagged packets, and use Tagged Packet as it is. That is, all packets are tagged in the Switch, and VLAN Translation is to change the VLAN ID value of Tagged Packet in the Switch. This function is to adjust traffic flow by changing the VLAN ID of packet.

Step 1
Open *Rule Configuration* mode using the **flow** *NAME* **create** command.

Step 2
Classify the packet that VLAN Translation will be applied by Rule.

Step 3
Designate the VLAN ID that will be changed in the first step by the **action match vlan** <1-4094> command.

Step 4
Open *Interface Configuration* mode using the **interface** command.

Step 5
Add the classified packet to VLAN members of the VLAN ID that will be changed.

To translate a VLAN tag from old VLAN ID to new VLAN ID for inbound/outbound packets on a interface basis, use the following command.

Command	Mode	Description
vlan translation inbound vlan *VLAN_ID1* **vlan** *VLAN_ID2*	Interface [XE/GE/ GPON]	Enables the inbound VLAN translation. VLAN_ID1: old VLAN id to be translated VLAN_ID2: new VLAN id
vlan translation outbound vlan *VLAN_ID1* **vlan** *VLAN_ID2*		Enables the outbound VLAN translation.
no vlan translation inbound vlan *VLAN_ID1*		Disables the inbound VLAN translation.
no vlan translation outbound vlan *VLAN_ID1*		Disables the outbound VLAN translation.

i

In case “ADD_VID = 0” in matching entry, this entry translates C-VID to new VLAN ID. In case of “ADD_VID = 1”, new vlan id of this entry attaches S-VID.

To see the inbound/outbound VLAN translation, use the following command.

Command	Mode	Description

show vlan translation inbound [*PORTS*]	Enable Global	Shows the inbound VLAN translation information.
show vlan translation outbound [*PORTS*]		Shows the outbound VLAN translation information

9.2 Link Aggregation (LAG)

Link aggregation complying with IEEE 802.3ad bundles several physical ports together to one logical port so that you can get enlarged bandwidth.

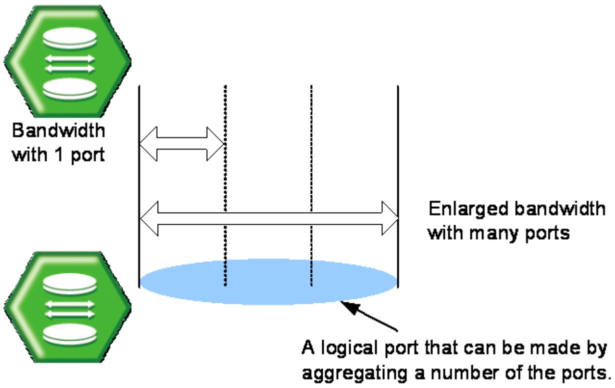

Bandwidth with 1 port
Enlarged bandwidth with many ports
A logical port that can be made by aggregating a number of the ports.

Fig. 9.4 Link Aggregation

The LD3032 supports two kinds of link aggregation as port trunk and LACP. There is a little difference in these two ways. In case of port trunking, it is quite troublesome to set the configuration manually and the rate to adjust to the network environment changes when connecting to the switch using logical port. On the other hand, in case of LACP, once you specify LACP member ports between the switches, the ports will be automatically aggregated by LACP without manually configuring the aggregated ports.

9.2.1 Port Trunk

Port trunking enables you to dynamically group the similarly configured interfaces into a single logical link (aggregate port) to increase bandwidth, while reducing the traffic congestion.

9.2.1.1 Configuring Port Trunk

To create a logical port by aggregating the ports, use the following command.

Command	Mode	Description
channel-group static <1-12>	Interface [XE/GE]	Creates a channel-group and adds the member ports within a Trunk group.
channel-group active-link <1-8>	Interface [CG]	Specifies the number of minimum active member ports within a Trunk (channel) group. A Trunk group is automatically disabled if the operational member ports fall at the same value or below the configured number. 1-8: the number of minimum active member ports (default:1)
channel-group distmode {**srcmac** | **dstmac** | **srcdstmac** | **srcip** | **dstip** | **srcdstip**}		Selects the distribution mode for a specified aggregation group. (default: srcdstmac)

It is possible to input 1 to 12 to the trunk group ID because the LD3032 supports 12 logical aggregated ports, and the group ID of port trunk and the aggregator number of LACP cannot coexist.

If packets enter to logical port aggregating several ports and there is no way to decide packet route, the packets could be gathered on particular member port so that it is not possible to use logical port effectively. Therefore, the LD3032 is configured to decide the way of packet route in order to divide on member port effectively when packets enter. It is decided with source IP address, destination IP address, source MAC address, destination MAC address and the user could get information of packets to decided packet route.

The followings are the simple descriptions for the distribution modes:

- **dstip**: destination IP address
- **dstmac**: destination MAC address
- **srcdstip**: source and destination IP address
- **srcdstmac**: source and destination MAC address
- **srcip**: source IP address
- **srcmac**: source MAC address

The port designated as a member port of port trunk is automatically deleted from existing VLAN. Therefore, if the member port and aggregated port exist in different VLAN each other, VLAN configuration should be changed for their aggregation.

9.2.1.2 Disabling Port Trunk

To disable the configured port trunk, use the following command.

Command	Mode	Description
no channel-group	Interface [XE/GE]	Releases a configured trunk port.
no channel-group active-link	Interface [CG]	

If a port is deleted from a logical port or the port trunk is disabled, the port will be added to the default VLAN.

9.2.1.3 Displaying Port Trunk

To display a configuration of port trunk, use the following command.

Command	Mode	Description
show channel-group	Enable Global	Shows a configuration for trunk.

9.2.2 Link Aggregation Control Protocol (LACP)

Link aggregation control protocol (LACP) is the function of using wider bandwidth by aggregating more than two ports as a logical port as previously stated port trunk function.

If the aggregated port by port trunk is in different VLAN from the VLAN where the existing member port originally belongs to, it should be moved to VLAN where the existing member port belongs to. However, the integrated port configured by LACP is automatically added to appropriate VLAN.

i

LACP can generate up to 12 aggregators whose number value could be 1 to 12. The group ID of port trunk and the aggregator number of LACP cannot be configured with the same value.

9.2.2.1 LACP Operation Mode

After configuring the member port, configure the LACP operation mode of the member port. This defines the operation way for starting LACP operation. You can select the operation mode between the active and passive mode.

The active mode allows the system to start LACP operation regardless of other connected devices. On the other hand, the passive mode allows the system to start LACP operation only when receiving LACP messages from other connected devices.

⚠

In case of an LACP connection between 2 switches, if the member ports of both switches are configured as the passive mode, the link between the switches cannot be established.

You can activate LACP function and configure the physical port that is a member of aggregated port. To add the port interface to LACP aggregator ID and configure the operation mode of the member port, use the following command.

Command	Mode	Description
channel-group lacp *AGGREGETIONS* **mode** {**active** | **passive**}	Interface [XE/GE]	Enables LACP and specifies physical port that is member port of LACP aggregator ID. Configures the operation mode of the member port. (default: active) AGGREGATIONS: aggregator ID(1-12)

To delete the configured operation mode of the member port, use the following command.

Command	Mode	Description
no channel-group *AGGREGETIONS* **mode**	Interface [XE/GE]	Deletes the configured operation mode of the member port.

9.2.2.2 Distribution Mode

If packets enter to logical port aggregating several ports and there’s no way to decide packet route, the packets could be gathered on particular member port so that it is not possible to use logical port effectively.

Therefore, the LD3032 is configured to decide the way of packet route in order to distribute (or forward) packets to the member port effectively when packets enter. It is decided with Source IP address, destination IP address, source MAC address, destination MAC address and the user could get information of packets to decided packet route. **dstip** is destination IP address and **dstmac** means destination MAC address.

i For the LD3032, a source destination MAC address is basically used to decide packet route.

After configuring an LACP aggregator, you should configure the distribution mode. The following is the command for configuring the distribution mode of the LACP aggregator.

Command	Mode	Description
channel-group distmode {**srcmac** | **dstmac** | **srcdstmac** | **srcip** | **dstip** | **srcdstip**}	Interface [CG]	Configures the distribution mode of the LACP aggregator: srcmac: source MAC address dstmac: destination MAC address srcdstmac: source/destination MAC address (default) srcip: source IP address dstip: destination IP address srcdstip: source/destination IP address

To delete a configured distribution mode, use the following command.

Command	Mode	Description
no channel-group distmode *AGGREGETIONS*	Interface [CG]	Deletes a configured distribution mode.

9.2.2.3 Priority of Switch

In case the member ports of connected switches are configured as Active mode (LACP system enabled), it is required to configure which switch would be a standard for it. For this case, the user could configure the priority on switch. The following is the command of configuring the priority of the switch in LACP function.

Command	Mode	Description
channel-group system priority <1-65535>	Global	Sets the priority of the switch in LACP function, enter the switch system priority. (default: 32768)

To delete the priority of configured switch, use the following command.

Command	Mode	Description
no channel-group system priority	Global	Clears the priority of the configured switch.

9.2.2.4 Manual Aggregation

The port configured as member port is basically configured to aggregate to LACP. However, even though the configuration as member port is not released, they could operate as independent port without being aggregated to LACP. These independent ports cannot be configured as trunk port because they are independent from being aggregated to LACP under the condition of being configured as member port.

To configure member port to aggregate to LACP, use the following command.

Command	Mode	Description
channel-group aggregation {**aggregatable** | **individual**}	Interface [XE/GE]	Configures the property of a specified member port for LACP. (default: aggregatable)

To clear aggregated to LACP of configured member port, use the following command.

Command	Mode	Description
no channel-group aggregation	Interface [XE/GE]	Deletes the configured property of a specified member port for LACP.

9.2.2.5 BPDU Transmission Rate

Member port transmits BPDU with its information. For the LD3032, it is possible to configure the BPDU transmission rate, use the following command.

Command	Mode	Description
channel-group timeout {**short** | **long**}	Interface [XE/GE]	Configures BPDU transmission rate: short: short timeout (1 sec) long: long timeout (30 sec: default)

To clear BPDU transmission rate, use the following command (clear means long timeout).

Command	Mode	Description
no channel-group timeout	Interface [XE/GE]	Clears BPDU transmission rate of configured member port, select the port number.

9.2.2.6 Administrational Key

Member port of LACP has key value. All member ports in one aggregator have same key values. To make the aggregator consisted of specified member ports, configure the different key value with the key value of another port.

Command	Mode	Description
channel-group admin-key <1-15>	Interface [XE/GE]	Configures the key value of a member port: PORTS: select the port number. 1-15: key value (default: 1)

To delete the key value of a specified member port, use the following command.

Command	Mode	Description
no channel-group admin-key *PORTS*	Interface [XE/GE]	Deletes the key value of a specified member port, select the member port number.

9.2.2.7 Port Priority

To configure priority of an LACP member port, use the following command.

Command	Mode	Description
channel-group priority <1-65535>	Interface [XE/GE]	Sets the LACP priority of a member port. (default: 32768)

To delete the configured priority of the member port, use the following command.

Command	Mode	Description
no channel-group priority	Interface [XE/GE]	Removes the configured interface priority from this channel-group.

9.2.2.8 Displaying LACP Configuration

To display the configured LACP, use the following command.

Command	Mode	Description
show channel-group lacp	Enable Global Interface [XE/GE]	Shows the information of aggregated port.
show channel-group lacp aggregator *AGGREGATIONS*		Shows the information of selected aggregated port.
show channel-group lacp interface all		Shows the information of member port.
show channel-group lacp interface {**gigabitethernet** | **tengigabitethernet**} *IFPORT*		Shows the information of appropriated member port.
show channel-group lacp statistics		Shows the aggregator statistics.

To clear LACP statistics information, use the following command.

Command	Mode	Description
clear channel-group lacp statistic	Enable Global	Clears the collected statistics.

9.3 Rule and QoS

The LD3032 provides a rule and QoS feature for traffic management. The rule classifies incoming traffic, and then processes the traffic according to user-defined policies. You can use the physical port, 802.1p priority (CoS), VLAN ID, DSCP, and so on to classify incoming packets.

You can configure the policy in order to change some data fields within a packet or to relay packets to a mirror monitor by a rule. QoS (Quality of Service) is one of useful functions to provide more reliable service for traffic flow control. It is very serviceable to prevent overloading and delaying or failing of sending traffic by giving priority to traffic.

QoS can give priority to specific traffic by basically offering higher priority to the traffic or lower priority to the others.

When processing traffic, the traffic is usually supposed to be processed in time-order like first in, first out. This way, not processing specific traffic first, might cause undesired traffic loss in case of traffic overloading. However, in case of overloading traffic, QoS can apply processing order to traffic by reorganizing priorities according to its importance. By favor of QoS, you can predict network performance in advance and manage bandwidth more efficiently.

The QoS provides the following benefits:

Control over network resources

Bandwidth, delay and packet loss can be effectively controlled by QoS feature. The network administrator can limit the bandwidth for non-critical applications (such as FTP file transfers), so that other applications have a greater amount of bandwidth available to them.

Effective use of resources

An effective use of network resorces can support guaranteed bandwidth to a few critical applications to ensure reliable application performance. QoS ensures that the most important and critical traffic is transmitted immediately without starvation.

Customized service

QoS helps the internet service providers provide differentiated services for their customers of the network. It allocates guaranteed bandwidth to more important applications that produce real-time traffic, such as voice, video and audio.

Traffic Prioritization

As you deploly QoS, it guarantees bandwidth and reduces delay time to ensure the applications can transmit the packets properly by handling the traffic with higher priority than regular traffic.

9.3.1 How to Operate QoS

QoS operation is briefly described as below.

Incoming packets are classified by configured conditions, and then processed by packet counter and rate-limiting on specific policer. After marking and remarking action, the switch transmits those classified and processed packets via a given scheduling algorithm.

Fig. 9.5 shows the simple procedure of QoS operation.

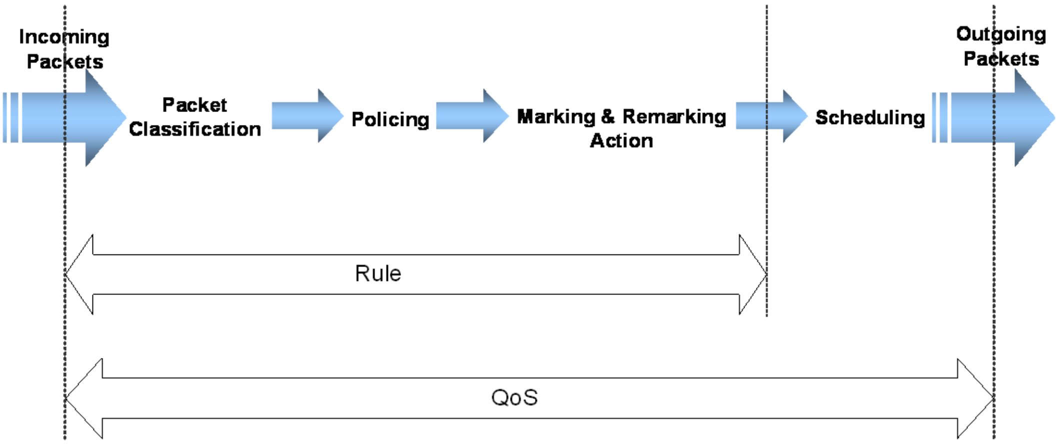


Fig. 9.5 Procedure of QoS operation

The structure of Rule has 4 types of categories with different roles for QoS.

- **Flow**
  Defines traffic classification criterias such as L3 source and destination IP address, L2 source and destination MAC address, Ethernet type, length, Class of Service (CoS), Differentiated Services Code Point (DSCP) and so on. A unique name needs to be assigned to each flow.

- **Class**
  Includes more than 2 flows for the efficient traffic management in the application of rule to this set of flows. Additionally, a unique name needs to be assigned to each class.

- **Policer**
  Defines the packet counter and rate-limit. The policer adjusts how and what is to be classified within transmitted packets.
  − **packet counter** calculates the classified packets for identifying a flow.
  − **rate-limit** defines which packets conform to or exceed the given rate.

- **Policy**
  Configures the policy classifying the action(s) to be performed if the configured rule classification fits transmitted packet(s). It cannot only include a specified Flow, Class or Policer but also set marking/remarking according to the various parameters such as CoS and DSCP which determine the rule action or priority of packets.
  − **mirror** transmits the classified traffic to the monitor port.
  − **redirect** transmits the classified traffic to the specified port.
  − **permit** allows traffic matching given characteristics.

- **deny** blocks traffic matching given characteristics.
- **copy-to-cpu** duplicates the profile of classified packets and sends a copy to CPU packets filtering.

- **Scheduling Algorithm**
  To handle traffic, you need to configure differently processing orders of traffic by using scheduling algorithms. The LD3032 provides:
  - Strict Priority Queuing (SP)
  - Deficit Round Robin (DRR)
  - Weighted Round Robin (WRR)

An already applied rule cannot be modified. It needs to be deleted and then created again with changed values.

Weight can be used to additionally adjust the scheduling mode per queue in WRR mode. Weight controls the scheduling precedence of the internal packet queues.

Fig. 9.6 shows the relationship of Flow, Class, Policer and Policy on basic structure of Rule.

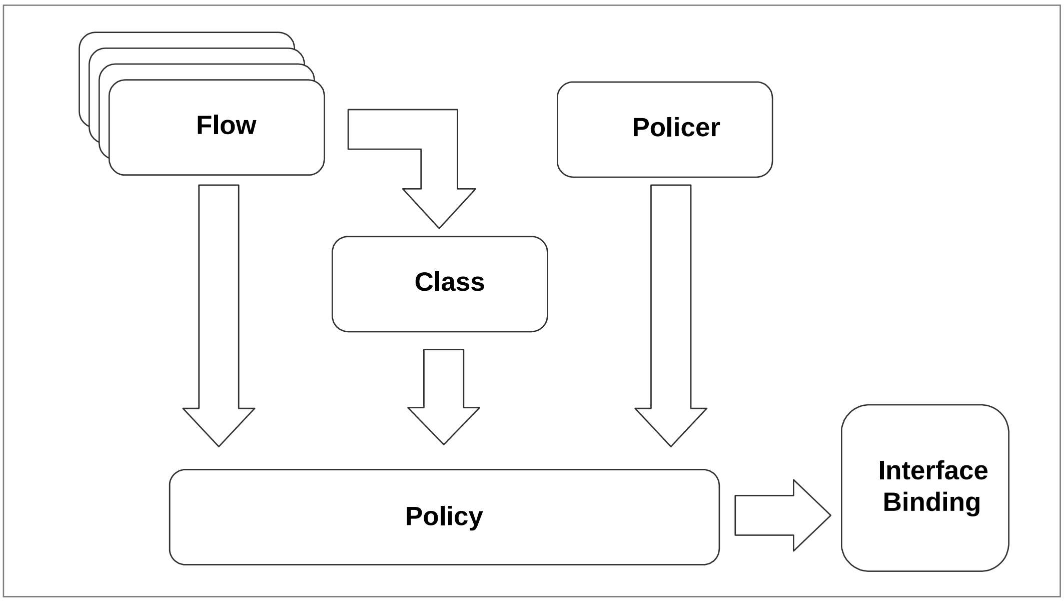


Fig. 9.6 Structure of Rule

You can simply manage more than 2 Flows through one Class. Flow or Class and Policer can be implemented by one policy.

Both Flow and Class cannot belong to one policy together. It means that one policy can include only one either Flow or Class. However, a single flow or class can belong to multiple policies. Otherwise, only one policer can belong to one policy.

9.3.2 Packet Classification

Packet classification features allow traffic to be partitioned into multiple priority levels, or classes of service. In *Flow Configuration* mode, you can set packet classification criterias via flow, which is with unique name. If you specify the value of parameters, the LD3032 classifies the packets corresponding to the parameters.

9.3.2.1 Flow Creation

The packet classification involves a traffic descriptor to categorize a packet within a specific flow for QoS handling in the network. You need to open *Flow Configuration* mode first to classify the packets. To open *Flow Configuration* mode, use the following command.

Command	Mode	Description
flow *NAME* **create**	Global	Creates a flow and opens *Flow Configuration* mode. NAME: flow name.

After opening *Flow Configuration* mode, the prompt changes from SWITCH(config)# to SWITCH(config-flow[NAME])#.

To delete the configured Flow or all Flows, use the following command.

Command	Mode	Description
no flow *NAME*	Global	Deletes a specified flow.
no flow all		Deletes all flows.

After opening *Flow Configuration* mode, a flow can be configured by user. The packet classification can be configured for each flow.

- The flow name must be unique. Its size is limited to 32 significant characters.
- The flow name cannot start with the alphabet “a” or “A”.
- The order in which the following configuration commands are entered is arbitrary.
- The configuration of a flow being configured can be changed as often as wanted until the **apply** command is entered.
- Use the **show flow-profile** command to display the configuration entered up to now.

You cannot create the flow name which started with alphabet ‘a’ If you try to make a flow name started with alphabet ‘a’, the error message will display.

9.3.2.2 Configuring Flow

The packet classification condition needs to be defined. You can classify the packets via MAC address, IP address, Ethernet type, CoS, DSCP etc. To specify a packet-classifying pattern with source/destination IP address or MAC address, use the following command.

Command	Mode	Description
ip {*A.B.C.D* | *A.B.C.D/M* | **any**} {*A.B.C.D* | *A.B.C.D/M* | **any**} [<0-255>]	Flow	Classifies an IP address. A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address 0-255: IP protocol number
ip {*A.B.C.D* | *A.B.C.D/M* | **any**} {*A.B.C.D* | *A.B.C.D/M* | **any**} **icmp**		Classifies an IP protocol (ICMP). A.B.C.D: source/destination IP address

Command	Mode	Description
		A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address
ip {*A.B.C.D* | *A.B.C.D/M* | **any**} {*A.B.C.D* | *A.B.C.D/M* | **any**} **icmp** {<0-255> | **any**} {<0-255> | **any**}		Classifies an IP protocol (ICMP). A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address 0-255: ICMP message type number 0-255: ICMP message code number
ip {*A.B.C.D* | *A.B.C.D/M* | **any**} {*A.B.C.D* | *A.B.C.D/M* | **any**} {**tcp** | **udp**}		Classifies an IP protocol (TCP/UDP). A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address
ip {*A.B.C.D* | *A.B.C.D/M* | **any**} {*A.B.C.D* | *A.B.C.D/M* | **any**} {**tcp** | **udp**} {<1-65535> | **any**} {<1-65535> | **any**}		Classifies an IP protocol (TCP/UDP). A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address 0-65535: TCP/UDP source/destination port range any: any TCP/UDP source/destination port
ip {*A.B.C.D* | *A.B.C.D/M* | **any**} {*A.B.C.D* | *A.B.C.D/M* | **any**} **tcp** {<1-65535> | **any**} {<1-65535> | **any**} {*TCP-FLAG* | **any**}		Classifies an IP protocol (TCP). A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address 0-65535: TCP source/destination port range any: any TCP source/destination port TCP-FLAG: TCP flag (e.g. S(SYN), F(FIN)) any: any TCP flag
mac {*SRC-MAC-ADDR* | *SRC-MAC-ADDR/M* | **any**} {*DST-MAC-ADDR* | *DST-MAC-ADDR*/M | **any**}		Classifies MAC address. SRC-MAC-ADDR: source MAC address DST-MAC-ADDR: destination MAC address SRC/DST-MAC-ADDR/M: source/destination MAC address with mask bit any: any source/destination MAC address (ignore)

When specifying a source and destination IP address as a packet-classifying pattern, the destination IP address must be after the source IP address.

To specify a packet-classifying pattern with IPv6 address, use the following command.

Command	Mode	Description
ipv6 { *X:X::X:X* | *X:X::X:X/M* | **any**} {*X:X::X:X* |*X:X::X:X/M* | **any**} [<0-255>]	Flow	Classifies an IPv6 address. X:X::X:X : source/destination IPv6 address X:X::X:X/M: source/destination IPv6 address with mask any: any source/destination IPv6 address 0-255: IP protocol number
ipv6 { *X:X::X:X* | *X:X::X:X/M* | **any**}		Classifies an IP protocol (ICMP).

Command	Mode	Description
{*X:X::X:X* |*X:X::X:X/M* | **any**} **icmp**		X:X::X:X : source/destination IPv6 address X:X::X:X/M: source/destination IPv6 address with mask any: any source/destination IPv6 address
ipv6 { *X:X::X:X* | *X:X::X:X/M* | **any**} {*X:X::X:X* |*X:X::X:X/M* | **any**} **icmp** {<0-255> | **any**} {<0-255> | **any**}		
ipv6 { *X:X::X:X* | *X:X::X:X/M* | **any**} {*X:X::X:X* |*X:X::X:X/M* | **any**} {**tcp** | **udp**}		Classifies an IP protocol (TCP/UDP). X:X::X:X : source/destination IPv6 address X:X::X:X/M: source/destination IPv6 address with mask any: any source/destination IPv6 address
ipv6 { *X:X::X:X* | *X:X::X:X/M* | **any**} {*X:X::X:X* |*X:X::X:X/M* | **any**} **tcp** {<1-65535> | **any**} {<1-65535> | **any**} [*TCP_FLAG* | **any**]		Classifies an IP protocol (TCP/UDP). X:X::X:X : source/destination IPv6 address X:X::X:X/M: source/destination IPv6 address with mask any: any source/destination IPv6 address 0-65535: TCP/UDP port range any: any TCP/UDP port TCP_FLAG: TCP flag vlaue
ipv6 { *X:X::X:X* | *X:X::X:X/M* | **any**} {*X:X::X:X* |*X:X::X:X/M* | **any**} **udp** {<1-65535> | **any**} {<1-65535> | **any**}		

To specify a packet-classifying pattern with various parameters (DSCP, CoS, ToS, IP precedence, packet length, Ethernet type, IP header), use the following command.

Command	Mode	Description
dscp {<0-63> | **any**}	Flow	Classifies a DSCP value. 0-63: DSCP value any: any DSCP (ignore)
cos {<0-7> | **any**}		Classifies an 802.1p priority. 0-7: 802.1p priority value any: any 802.1p priority value (ignore)
tos {<0-255> | **any**}		Classifies all ToS field. 0-255: ToS value any: any ToS value (ignore)
ip-precedence {<0-7> | **any**}		Classifies IP precedence. 0-7: IP precedence value any: any IP precedence value (ignore)
length {<21-65535> | **any**}		Classifies a packet length. (This can be used only in the extension mode!) 21-65535: IP packet length any: any IP packet length (ignore)
ethtype {*TYPE-NUM* | **arp** | **any**}		Classifies the Ethernet type. TYPE-NUM: Ethernet type field (hex, e.g. 0800 for IPv4) arp: address resolution protocol any: any Ethertype (ignore)
inner-vid {<1-4094 | **any**}		Classifies a VLAN ID of the inner/outer tag. 1-4094: VLAN ID
outer-vid {<1-4094 | **any**}		
inner-cos {<0-7> | **any**}		Classifies a CoS value of the inner/outer tag.

Command	Mode	Description
outer-cos {<0-7> | **any**}		0-7: 802.1p priority value any: any 802.1p priority value (ignore)
onu circuit-id <1-50000>		Classifies the ONU’s circuit-ID value. 1-50000: downstream unicast packet per VLAN ID of ONU default: downstream DLF and broadcast packets ds-dlf: downstream DLF packets ds-broadcast: downstream broadcast packets
onu circuit-id {**default** | **ds-dlf** | **ds-broadcast**}		

To delete a specified packet-classifying pattern, use the following command.

Command	Mode	Description
no cos	Flow	Deletes a specified packet-classifying pattern for each option.
no dscp		
no tos		
no length		
no ip-precedence		
no ethtype		
no mac		
no inner-vid		
no outer-vid		
no inner-cos		
no outer-cos		
no ip		
no ipv6		
no onu circuit-id		

9.3.2.3 Applying and modifying Flow

After configuring a flow using the above commands, apply it to the system with the following command. If you do not apply the flow to the system, all specified configurations on *Flow Configuration* mode will be lost. To save and apply a flow, use the following command.

Command	Mode	Description
apply	Flow	Applies a flow to the system.

To modify a flow, use the following command.

Command	Mode	Description
flow *NAME* **modify**	Global	Modifies a flow, enter a flow name.

You should save and apply the flow to system whenever you modify or configure the flow.

9.3.2.4 Class Creation

A class is a set of flows. More than 2 flows can belong to one class. You can simply handle and configure the packets on several flows at once.

To create a class including more than 2 flows, use the following command.

Command	Mode	Description
class *NAME* **flow** *FLOW1* [*FLOW2*] [*FLOW3*]⋯	Global	Creates a class including more than 2 flows. NAME: class name FLOW: flow name

To display created class, use the following command.

Command	Mode	Description
show class [*NAMES*]	Global	Shows specified class
show class admin [*NAMES* | **detail**]		Shows the information relating ro class name NAMES: class name
show class detail [*NAMES*]		

To delete configured class or all classes, use the following command.

Command	Mode	Description
no class all	Global	Deletes all classes.
no class *NAME*		Deletes specified class, enter the class name.
no class *NAME* **flow** *FLOW1* [*FLOW2*] [*FLOW3*]⋯		Removes specified flows from class.

9.3.3 Packet Conditioning

After defining traffic classification criteria in *Flow Configuration* mode, then configure how to process the packets. The classified traffic from flow or class is being treated according to the policer configuration. On *Policer Configuration* mode, a policer enforces a rate-limiting and the packet counter for traffic. The traffic is identified via policers, which are used to define traffic conditions including rate-limit and counter. And the policy actions for the identified traffic are created with policy. One policer can belong to one policy.

9.3.3.1 Policer Creation

To configure how to handle the classified packets according to the policer settings, you need to create a policer and open *Policer Configuration* mode.

To open *Policer Configuration* mode, use the following command.

Command	Mode	Description
policer *NAME* **create**	Global	Creates a policer and opens *Policer Configuration*

		mode. NAME: policer name.

After opening *Policer Configuration* mode, the prompt changes from SWITCH(config)# to SWITCH(config-policer[NAME])#.

After opening *Policer Configuration* mode, a policer can be configured by user. The rate-limit, meter and packet count can be configured for each policer.

- The policer name must be unique. Its size is limited to 32 significant characters.
- The policer name cannot start with the alphabet “a” or “A”.
- The order in which the following configuration commands are entered is arbitrary.
- The configuration of a polcer being configured can be changed as often as wanted until the **apply** command is entered.
- Use the **show policer-profile** command to display the configuration entered up to now.

To delete configured policer or all policers, use the following command.

Command	Mode	Description
no policer *NAME*	Global	Deletes a policer, enter a policer name.
no policer all		Deletes all policers.

9.3.3.2 Packet Counter

The packet counter function provides information on the total number of packets that the rule received and analyzed. This feature allows you to know the type of packets transmitted in the system according to rule configuration. To count the number of packets matching to corresponding policer, use the following command.

Command	Mode	Description
counter	Policer	Enables a packet counter function.
no counter		Disables a packet counter function.

To reset a collected policy counter, use the following command.

Command	Mode	Description
clear policy counter { *NAME* | **all**}	Enable Global	Resets a collected policy counter.

To display the number of packets on each rule, use the following command.

Command	Mode	Description
show flow statistics	Enable Global	Shows a collected flow counter.
show class statistics		Shows a collected class counter.
show policer statistics		Shows a collected policer counter.

show policy statistics		Shows a collected policy counter.

9.3.3.3 Rate-limit

You can configure the rate limit in kbps unit for the classified packets and control the bandwidth. To set the bandwidth of classified packets in specified policer, use the following command.

Command	Mode	Description
rate-limit *BANDWIDTH*	Policer	Sets the bandwidth for classified packets belonging to specified policer (unit: kbps)
no rate-limit		Deletes the configured bandwidth for classified packets of specified policer.

9.3.3.4 Applying and modifying Policer

After configuring a policer using the above commands, apply it to the system with the following command. If you do not apply the policer to the system, all specified configurations on *Policer Configuration* mode will be lost.

To save and apply a policer, use the following command.

Command	Mode	Description
apply	Policer	Applies a policer to the system.

To modify a policer, use the following command.

Command	Mode	Description
policer *NAME* **modify**	Global	Modifies a policer, enter a policer name.

9.3.4 Rule Action

9.3.4.1 Policy Creation

To configure a policy, you need to open *Policy Configuration* mode first. To open *Policy Configuration* mode, use the following command.

Command	Mode	Description
policy *NAME* **create**	Global	Creates a policy and opens *Policy Configuration* mode. NAME: policy name.

After opening *Policy Configuration* mode, the prompt changes from SWITCH(config)# to SWITCH(config-policy[NAME])#.

To delete configured policy or all policies, use the following command.

Command	Mode	Description
no policy *NAME*	Global	Deletes a policy, enter a policy name.

no policy all		Deletes all policies.

After opening *Policy Configuration* mode, a policy can be configured by user. The rule priority and rule action(s) can be configured for each policy.

- The policy name must be unique. Its size is limited to 32 significant characters.
- The policy name cannot start with the alphabet “a” or “A”.
- The order in which the following configuration commands are entered is arbitrary.
- The configuration of a policy being configured can be changed as often as wanted until the **apply** command is entered.
- Use the **show policy-profile** command to display the configuration entered up to now.

If you already create the policy, you need to include specified flow or class and policer to specify the rule action for the packets matching configured classifying patterns on flow or class and policer.

To include specific flow or class and policer in policy, use the following command.

Command	Mode	Description
include-flow *NAME*	Policy	Includes specified flow in policy. NAME:flow name
include-class *NAME*		Includes specified class in policy. NAME:class name
include-policer *NAME*		Includes specified policer in policy. NAME:policer name

One policy is not able to include both flow and class at the same time. Either flow or class can belong to one policy.

Only one policer can belong to one policy.

To remove flow or class, policer from the policy, use the following command.

Command	Mode	Description
no include-flow	Policy	Removes the flow from policy.
no include-class		Removes the class from policy.
no include-policer		Removes the policer from policy.

9.3.4.2 Metering

Meters measure the temporal state of a flow or a set of flows against a traffic profile. In this event, a meter might be used to trigger real-time traffic conditioning actions (e.g. marking, policing, or shaping).

Typical parameters of a traffic profile are:

- Committed Information Rate (CIR)

- Peak Information Rate (PIR)
- Committed Burst Size (CBS)
- Excess Burst Size (EBS)
- Peak Burst Size (PBS)

A typical meter measures the rate at which traffic stream passes it. Its rate estimation depends upon the flow state kept by the meter. There is a time constraint during which if the flow state is transferred from the old switch to the new switch, then it is effective in estimating the rate at the new switch as if though no transfer of flow has happened.

The LD3032 provides Token Bucket (srTCM and trTCM) meters.

Token Bucket

The token bucket is a control mechanism that transmits traffic by tokens in the bucket. The tokens are consumed by transmitting traffic and regenerated at the given rate. If all tokens in the bucket are consumed out, traffic cannot be transmitted any more; a flow can transmit traffic up to its peak burst rate. The transmitting cost and regenerating rate of tokens are configurable.

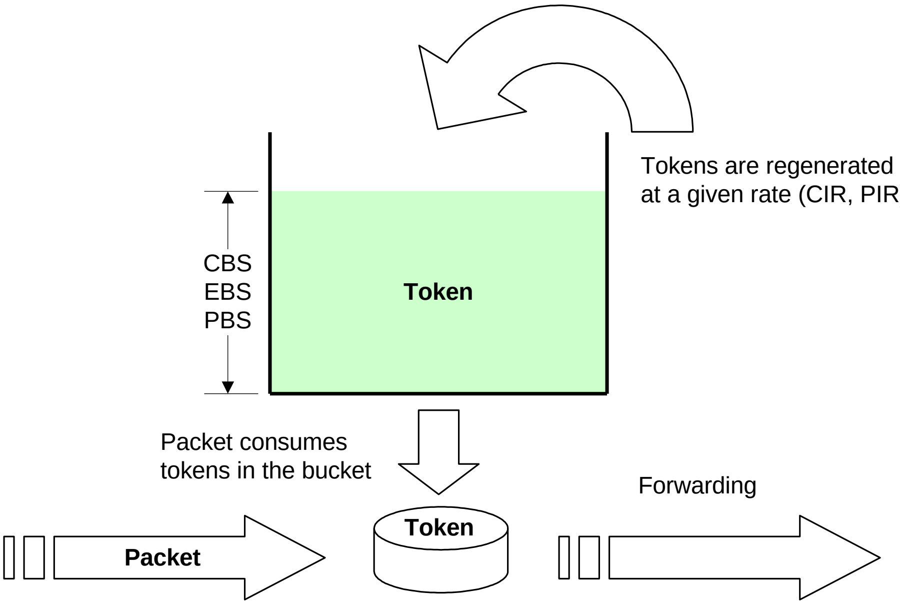


Fig. 9.7 Token Bucket Meter

Single Rate Three Color Marker (srTCM)

The srTCM meters an IP packet stream and marks its packet the one among green, yellow, and red using Committed Information Rate (CIR) and two associated burst sizes, Committed Burst Size (CBS) and Excess Burst Size (EBS). A packet is marked green if it does not exceed the CBS, yellow if it exceeds the CBS, but not the EBS, and red otherwise. The srTCM is useful for ingress policing of a service, where only the length, not the peak rate, of the burst determines service eligibility.

CIR is the regenerating rate of tokens measured in bytes of IP packets per second. CBS and EBS are the maximum size for each token bucket, C and E, measured in bytes. Both token buckets share the common rate CIR. At least one of them (CBS and EBS) must be configured, and it is recommended that the value is larger than or equal to the size of the largest possible IP packet in the stream.

The token buckets C and E are initially full. When a packet arrives, the tokens in the bucket C are decremented by the size of that packet with the green color-marking. If no more tokens to transmit a packet remain in the bucket C, then the tokens in the bucket E are decremented by the size of that packet with the yellow color-marking. If both buckets are empty, a packet is marked red.

The following figures show the behavior of the srTCM.

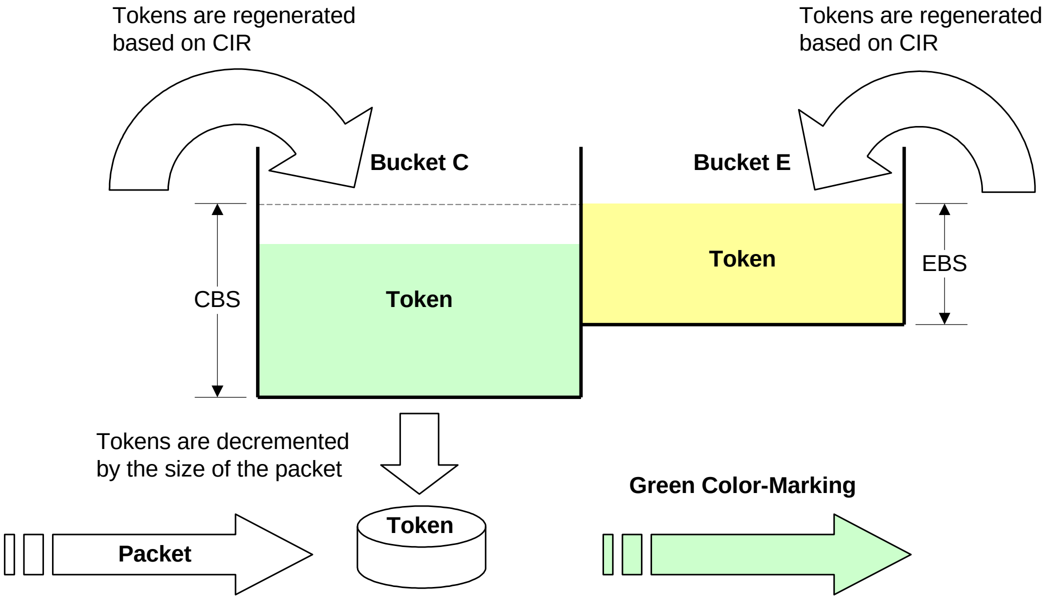

Tokens are regenerated based on CIR
Tokens are regenerated based on CIR
Bucket C
Bucket E
CBS
Token
Token
EBS
Tokens are decremented by the size of the packet
Green Color-Marking
Packet
Token

Fig. 9.8 Behavior of srTCM (1)

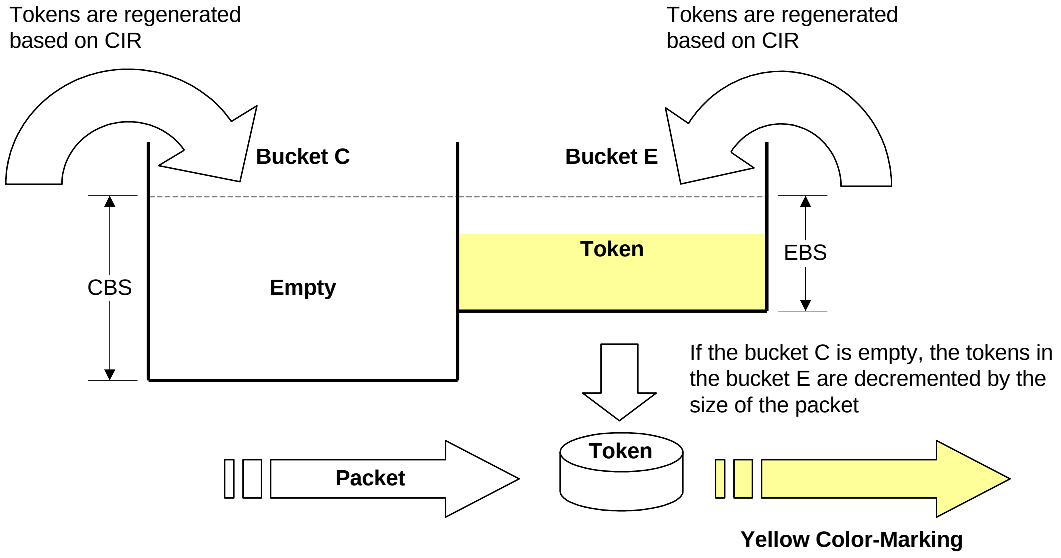

Tokens are regenerated based on CIR
Tokens are regenerated based on CIR
Bucket C
Bucket E
CBS
Empty
Token
EBS
If the bucket C is empty, the tokens in the bucket E are decrementd by the size of the packet
Packet
Token
Yellow Color-Marking

Fig. 9.9 Behavior of srTCM (2)

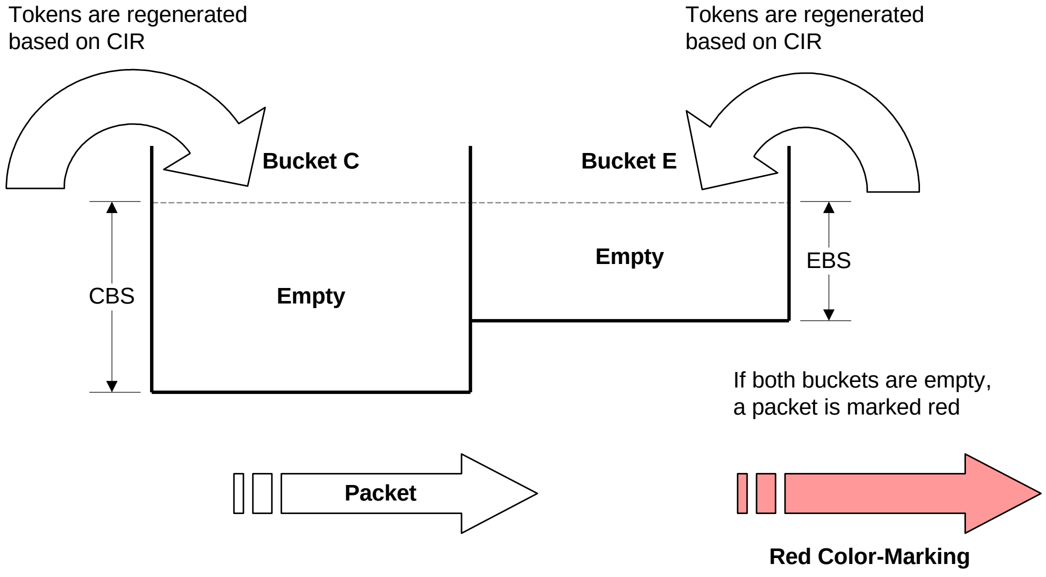

Tokens are regenerated based on CIR
Tokens are regenerated based on CIR
Bucket C
Bucket E
CBS
Empty
Empty
EBS
If both buckets are empty, a packet is marked red
Packet
Red Color-Marking

Fig. 9.10 Bahavior of srTCM (3)

Two Rate Three Color Marker (trTCM)

The trTCM meters an IP packet stream and marks its packet the one among green, yellow, and red using Peak Information Rate (PIR) and its associated Peak Burst Size (PBS) and Committed Information Rate (CIR) and its associated Committed Burst Size (CBS). A packet is marked red if it exceeds the PIR. Otherwise, it is marked either yellow or green depending on whether it exceeds or does not exceed CIR. The trTCM is useful for ingress policing of a service, where a peak rate needs to be enforced separately from a committed rate.

PIR and CIR are the regenerating rate of tokens for PBS and CBS respectively, which is measured in bytes of IP packets per second. PIR must be equal to or greater than CIR. PBS and CBS are the maximum size for each token bucket, P and C, measured in bytes. Both of them must be configured with the values equal to or greater than the size of the largest possible IP packet in the stream.

The token buckets P and C are initially full. When a packet arrives, if the tokens in the bucket P are smaller than the size of that packet, the packet is marked red. Else, if the tokens in the bucket C are smaller than the size of that packet, those are decremented by the size of that packet with the yellow color-marking. Else, if the tokens in the bucket C are larger than the size of that packet, those of both bucket P and C are decremented by the size of that packet with the green color-marking.

Note that in the trTCM algorithm, when a packet arrives, the availability of tokens in the token bucket P is checked first contrary to the srTCM; the order of color-marking is red-yellow-green.

The following figures show the behavior of the trTCM.

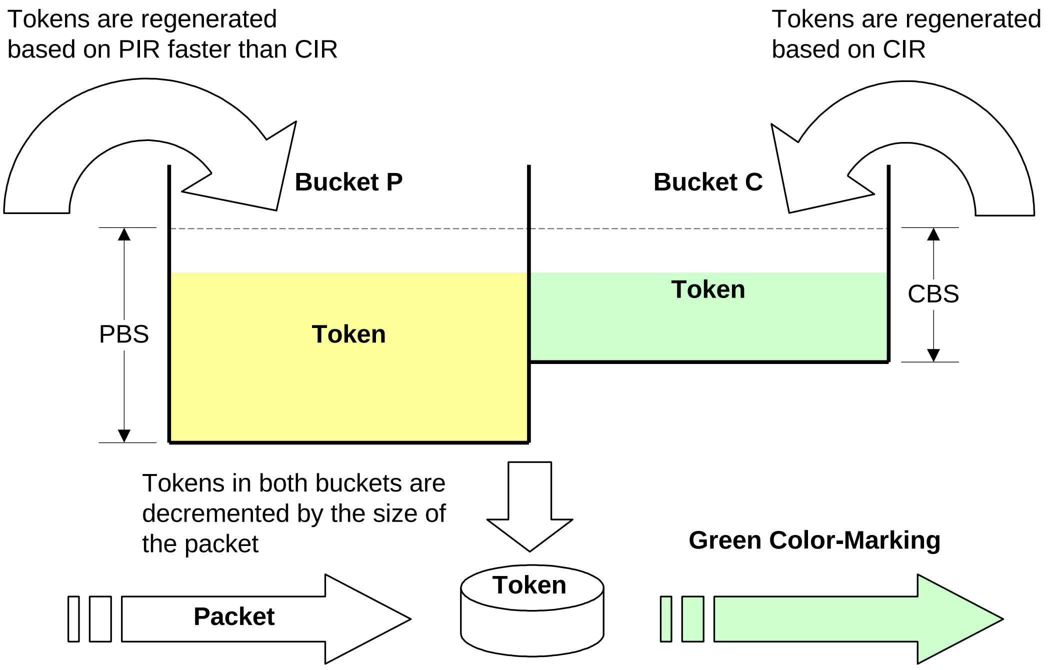

Tokens are regenerated based on PIR faster than CIR
Tokens are regenerated based on CIR
Bucket P
Bucket C
PBS
Token
Token
CBS
Tokens in both buckets are decremented by the size of the packet
Green Color-Marking
Packet
Token

Fig. 9.11 Behavior of trTCM (1)

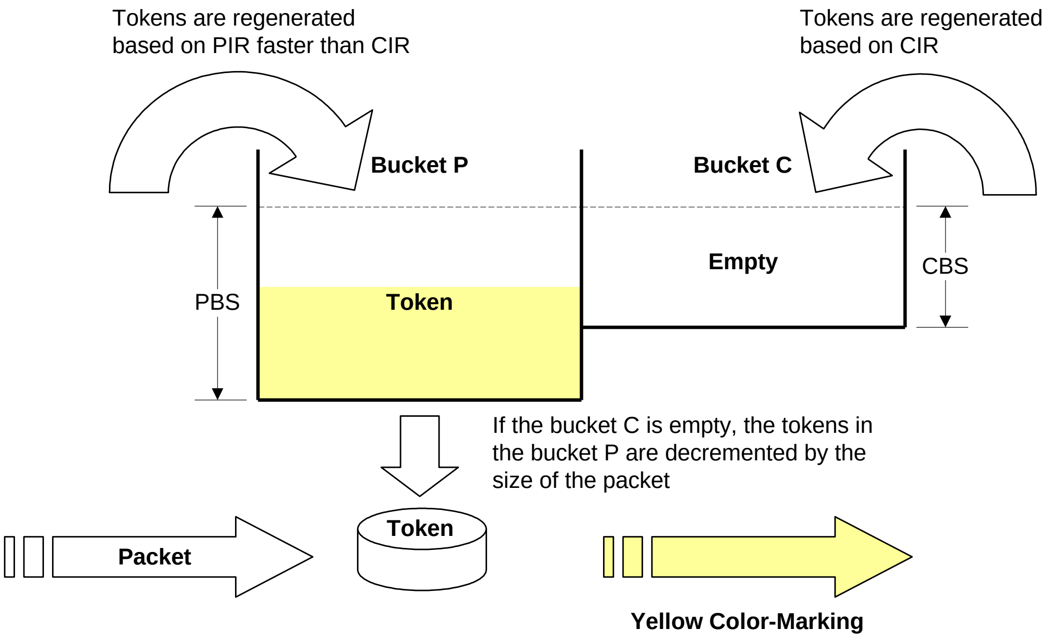

Tokens are regenerated based on PIR faster than CIR
Tokens are regenerated based on CIR
Bucket P
Bucket C
Empty
CBS
PBS
Token
If the bucket C is empty, the tokens in the bucket P are decremented by the size of the packet
Packet
Token
Yellow Color-Marking

Fig. 9.12 Behavior of trTCM (2)

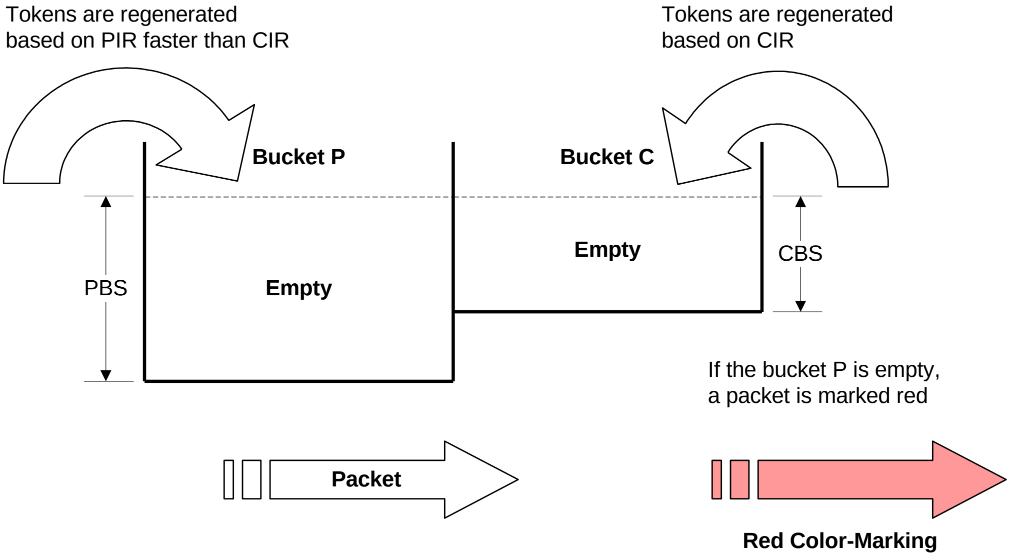

Tokens are regenerated based on PIR faster than CIR
Tokens are regenerated based on CIR
Bucket P
Bucket C
Empty
CBS
PBS
Empty
If the bucket P is empty, a packet is marked red
Packet
Red Color-Marking

Fig. 9.13 Behavior of trTCM (3)

To set the metering mode, use the following command.

Command	Mode	Description
color mode {**srtcm** | **trtcm**} **blind**	Policer	Sets the metering mode. blind: color-blind mode
no color mode		Sets to the default setting.

In the color-blind mode, the meter assumes that the packet stream is uncolored. In the color-aware mode the meter assumes that some preceding entity has pre-colored the incoming packet stream so that each packet is the one among green, yellow, and red.

To specify the value for metering parameters, use the following command.

Command	Mode	Description
color cir *BANDWIDTH* **cbs** *BURST*	Policer	Specifies CIR and CBS. BANDWIDTH: regenerating rate of token (unit: Kbps) BURST: maximum size of token bucket (unit: byte)
color pir *BANDWIDTH* **pbs** *BURST*		Specifies PIR and PBS. (trTCM only)
color ebs *BURST*		Specifies EBS. (srTCM only)

To configure DSCP values for the colored-packets, use the following command.

Command	Mode	Description
color dscp <0-63> {**green** | **yellow** | **red** }	Policer	Sets DSCP values for each colored packets.

In the color-blind mode, you can configure all red-colored or yellow-colored packets to discard. To configure the meter to discard all red-colored or yellow-colored packets, use the following command.

Command	Mode	Description
color { **yellow** | **red** } **action drop**	Policer	Configures the meter to discard colored packets.
no color { **yellow** | **red** } **action**		Configures the meter to permit colored packets.

In the color-aware mode, you can configure the DSCP remarking for red-colored packets or yellow-colored packets only. To configure DSCP remarking, use the following command.

Command	Mode	Description
color { **yellow** | **red** } **action marking**	Policer	Configures DSCP remarking for colored packets.
color { **yellow** | **red** } **action marking drop-precedence** {**green** | **yellow** | **red** }		Configures DSCP remarking and drop precedence for colored packets.

9.3.4.3 Policy Priority

If rules that are more than two match the same packet then the rule having a higher priority will be processed first. To set a priority for a policy, use the following command.

Command	Mode	Description

priority {**low** | **medium** | **high-middle** | **high** | **highest**}	Policy	Sets a priority for a policy. (default: medium)

9.3.4.4 Policy Action

To specify the rule action for the packets matching configured classifying patterns, use the following command.

Command	Mode	Description
action match deny	Policy	Denies the classified packets.
action match permit		Permits the classified packets.
action match mirror		Sends a copy of classified packets to mirror monitoring port.
action match vlan *VLANS*		Specifies a VLAN ID of classified packets. VLANS: VLAN ID (1-4094)
action match copy-to-cpu		Sends a copy of classified packets to CPU.
action match donot-copy-to-cpu		Do not send a coppy of classified packets to CPU.
action match dmac *MAC-ADDR*		Specifies the destination MAC address of classified packets.
action match route next-hop *A.B.C.D* [*A.B.C.D*] **verify-reachability**		Specifies next-hop address of classified packets. A.B.C.D: IP address of next hop

To delete a specified rule action, use the following command.

Command	Mode	Description
no action match deny	Policy	Deletes a specified rule action.
no action match permit		
no action match mirror		
no action match vlan		
no action match copy-to-cpu		
no action match donot-copy-to-cpu		
no action match dmac		
no action match route next-hop		

9.3.4.5 Setting CoS and ToS values

To specify a CoS or ToS value for a matching condition, use the following command.

Command	Mode	Description
action match cos <0-7> [**over-write**]	Policy	Configures the 802.1p class of service value. 0-7: CoS value overwrite: changes 802.1p class of service value with

		the one you set
action match cos same-as-ip-precedence overwrite		Changes the 802.1p CoS field in the packet with an IP ToS precedence value
action match tos <0-255>		Changes ToS bits in the packets. 0-255: ToS value
action match dscp <0-63>		Marks the packets with DSCP field. 0-63: DSCP value
action match ip-precedence <0-7>		Configures the IP ToS precedence value in the packet. 0-7: ToS precedence value
action match ip-precedence same-as-cos		Changes the IP ToS precedence value in the packet with an 802.1p CoS value.

To delete the CoS or ToS matching condition, use the following command.

Command	Mode	Description
no action match cos [**overwrite**]	Policy	Deletes the CoS /ToS/ DSCP matching condition.
no action match cos same-as-ip-precedence overwrite		
no action match tos		
no action match dscp		
no action match ip-precedence		
no action match ip-precedence same-as-cos		

9.3.4.6 Applying and Modifying Policy

After configuring a policy using the above commands, apply it to the system with the following command. If you do not apply the policy to the system, all specified configurations from *Policy Configuration* mode will be lost.

To save and apply a policy, use the following command.

Command	Mode	Description
apply	Policy	Applies a policy to the system.

To modify a policy, use the following command.

Command	Mode	Description
policy *NAME* **modify**	Global	Modifies a policy, enter a policy name.

9.3.4.7 Attaching a Policy to an Interface

After you configure a rule including the packet classification, policing and rule action, you should attach a policy to an interface and to specify port or VLAN in which the policy should be applied. If you do not specify an interface for rule, rule does not work properly.

To attach the policy to this interface for the inbound/outbound packet management, use the following command.

Command	Mode	Description
service-policy {**input** | **output**} *NAME*	Interface [XE/GE/GPON /VLAN/CG]	Attaches the policy to a specified interface for the inbound/outbound packets. NAME: name of a previously configured policy
no service-policy {**input** | **output**} *NAME*		Removes the attached policy from interface.
no service-policy all		

9.3.5 Displaying Rule

To show a rule profile configured by user, use the follwing command.

Command	Mode	Description
show flow-profile	Flow	Shows a profile of flow.
show policer-profile	Policer	Shows a profile of policer.
show policy-profile	Policy	Shows a profile of policy.

To dispaly a certain rule by its name or a specific rule of a certain type, use the following command.

Command	Mode	Description
show { **flow** | **class** | **policer** | **policy** } [*NAME*]	Enable Global	Shows the information relating to each rule, enter a rule name.
show { **flow** | **class** | **policer** | **policy** } **detail** [*NAME*]		
show running-config { **flow** | **policer** | **policy** }	All	Shows all configurations of each rule

9.3.6 Admin Rule

For the LD3032, it is possible to block a specific service connection like telnet, FTP, ICMP, etc with an admin rule function.

9.3.6.1 Creating Admin Flow for packet classification

To classify packets by a specific admin flow for the LD3032, you need to open *Admin-Flow Configuration* mode first. To open *Admin-Flow Configuration* mode, use the following command.

Command	Mode	Description
flow admin *NAME* **create**	Global	Creates an admin flow and opens *Admin-Flow Configuration* mode. NAME: admin-flow name.

To display created admin flow, use the following command.

Command	Mode	Description
show flow admin	Global	Shows created admin flow.
show flow admin {*NAME* | **detail**}		Shows specified admin flow.

After opening *Admin-Flow Configuration* mode, the prompt changes from SWITCH(config)# to SWITCH(config-admin-flow[NAME])#.

To delete configured admin flow or all admin flows, use the following command.

Command	Mode	Description
no flow admin *NAME*	Global	Deletes specified admin flow.
no flow admin all		Deletes all admin flows.

After opening *Admin-Flow Configuration* mode, an admin flow can be configured by user. The packet classification can be configured for each admin-flow.

i

- The admin-flow name must be unique. Its size is limited to 32 significant characters.
- The admin-flow name cannot start with the alphabet “a” or “A”.
- The order in which the following configuration commands are entered is arbitrary.
- The configuration of a flow being configured can be changed as often as wanted until the **apply** command is entered.
- Use the **show flow-profile admin** command to display the configuration entered up to now.

9.3.6.2 Configuring Admin Flow

You can classify the packets according to IP address, ICMP, TCP, UDP and IP header length. To specify a packet-classifying pattern, use the following command.

Command	Mode	Description
ip {*A.B.C.D* | *A.B.C.D/M* | **any**} {*A.B.C.D* | *A.B.C.D/M* | **any**} [0-255]	Admin-Flow	Classifies an IP address: A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address 0-255: IP protocol number
ip {*A.B.C.D* | *A.B.C.D/M* | **any**} {*A.B.C.D* | *A.B.C.D/M* | **any**} **icmp**		Classifies an IP protocol (ICMP): A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address
ip {*A.B.C.D* | *A.B.C.D/M* | **any**} {*A.B.C.D* | *A.B.C.D/M* | **any**} **icmp** {<0-255> | **any**} {<0-255> | **any**}		Classifies an IP protocol (ICMP): A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address 0-255: ICMP message type number 0-255: ICMP message code number
ip {*A.B.C.D* | *A.B.C.D/M* | **any**} {*A.B.C.D* | *A.B.C.D/M* | **any**} {**tcp** |		Classifies an IP protocol (TCP/UDP): A.B.C.D: source/destination IP address

Command	Mode	Description
udp}		A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address
ip {*A.B.C.D* | *A.B.C.D/M* | **any**} {*A.B.C.D* | *A.B.C.D/M* | **any**} {**tcp** | **udp**} {<0-65535> | **any**} {<0-65535> | **any**}		Classifies an IP protocol (TCP/UDP): A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address 0-65535: TCP/UDP source/destination port number any: any TCP/UDP source/destination port
ip {*A.B.C.D* | *A.B.C.D/M* | **any**} {*A.B.C.D* | *A.B.C.D/M* | **any**} **tcp** {<0-65535> | **any**} {<0-65535> | **any**} {*TCP-FLAG* | **any**}		Classifies an IP protocol (TCP): A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address 0-65535: TCP source/destination port number any: any TCP source/destination port TCP-FLAG: TCP flag (e.g. S(SYN), F(FIN)) any: any TCP flag
ip header-length <1-15>		Classifies an IP header length: 1-15: IP header length value

When specifying a source and destination IP address as a packet-classifying pattern, the destination IP address must be after the source IP address.

To specify a packet-classifying pattern with IPv6 address, use the following command.

Command	Mode	Description
ipv6 { *X:X::X:X* | *X:X::X:X/M* | **any**} {*X:X::X:X* |*X:X::X:X/M* | **any**} [<0-255>]	Admin-Flow	Classifies an IPv6 address. X:X::X:X : source/destination IPv6 address X:X::X:X/M: source/destination IPv6 address with mask any: any source/destination IPv6 address 0-255: IP protocol number
ipv6 { *X:X::X:X* | *X:X::X:X/M* | **any**} {*X:X::X:X* |*X:X::X:X/M* | **any**} **icmp**		Classifies an IP protocol (ICMP). X:X::X:X : source/destination IPv6 address X:X::X:X/M: source/destination IPv6 address with mask any: any source/destination IPv6 address
ipv6 { *X:X::X:X* | *X:X::X:X/M* | **any**} {*X:X::X:X* |*X:X::X:X/M* | **any**} **icmp** {<0-255> | **any**} {<0-255> | **any**}		
ipv6 { *X:X::X:X* | *X:X::X:X/M* | **any**} {*X:X::X:X* |*X:X::X:X/M* | **any**} {**tcp** | **udp**}		Classifies an IP protocol (TCP/UDP). X:X::X:X : source/destination IPv6 address X:X::X:X/M: source/destination IPv6 address with mask any: any source/destination IPv6 address
ipv6 { *X:X::X:X* | *X:X::X:X/M* | **any**} {*X:X::X:X* |*X:X::X:X/M* | **any**} **tcp** {<1-65535> | **any**} {<1-65535> | **any**} [*TCP_FLAG* | **any**]		Classifies an IP protocol (TCP/UDP). X:X::X:X : source/destination IPv6 address X:X::X:X/M: source/destination IPv6 address with mask

Command	Mode	Description
ipv6 { *X:X::X:X* | *X:X::X:X/M* | **any**} {*X:X::X:X* |*X:X::X:X/M* | **any**} **udp** {<1-65535> | **any**} {<1-65535> | **any**}		any: any source/destination IPv6 address 0-65535: TCP/UDP port range any: any TCP/UDP port TCP_FLAG: TCP flag vlaue

To delete a specified packet-classifying pattern, use the following command.

Command	Mode	Description
no ip	Admin-Flow	Deletes a specified packet-classifying pattern for each option.
no ipv6		
no ip header-length		

9.3.6.3 Applying and modifying Admin Flow

After configuring an admin flow using the above commands, apply it to the system with the following command. If you do not apply it to the system, all specified configurations from *Admin-Flow Configuration* mode will be lost.

To save and apply an admin flow, use the following command.

Command	Mode	Description
apply	Admin-Flow	Applies an admin flow to the system.

To modify an admin flow, use the following command.

Command	Mode	Description
flow admin *NAME* **modify**	Global	Modifies a flow, enter an admin flow name.

You should save and apply the admin flow to system using **apply** command whenever you modify any configuration of the admin flow.

9.3.6.4 Class Creation

One class can include several flows. You can simply handle and configure the packets on several flows at once.

To create a class including more than 2 flows, use the following command.

Command	Mode	Description
class admin *NAME* **flow** *FLOW1* [*FLOW2*] [*FLOW3*]	Global	Creates an admin class including at least 2 admin flows. NAME: admin class name FLOW: admin flow name

To delete configured admin class or all admin classes, use the following command.

Command	Mode	Description
no class admin all	Global	Deletes all admin classes.
no class admin *NAME*		Deletes specified admin class. NAME: admin class name
no class admin *NAME* **flow** *FLOW1* [*FLOW2*] [*FLOW3*]		Removes specified admin flows from class. NAME: admin class name FLOW: admin flow name

9.3.7 Admin Rule Action

9.3.7.1 Admin Policy Creation

For the LD3032, you need to open *Admin-Policy Configuration* mode first. To open *Policy Configuration* mode, use the following command.

Command	Mode	Description
policy admin *NAME* **create**	Global	Creates an admin policy and opens *Admin-Policy Configuration* mode. NAME: admin-policy name.

After opening *Admin Policy Configuration* mode, the prompt changes from SWITCH(config)# to SWITCH(config-admin-policy[NAME])#.

To display elete configured admin policy or all admin policies, use the following command.

Command	Mode	Description
show policy admin [*NAMES]*	Global	Shows specified admin policy.

To delete configured admin policy or all admin policies, use the following command.

Command	Mode	Description
no policy admin *NAME*	Global	Deletes specified admin policy.
no policy admin all		Deletes all admin policies.

After opening *Admin-Policy Configuration* mode, an admin policy can be configured by user. You can specify the rule action for the classified packets in each admin-policy.

i

- The admin-policy name must be unique. Its size is limited to 32 significant characters.
- The admin- policy name cannot start with the alphabet “a” or “A”.
- The order in which the following configuration commands are entered is arbitrary.
- The configuration of an admin policy being configured can be changed as often as wanted until the **apply** command is entered.
- Use the **show policy-profile admin** command to display the configuration entered up to now.

If you create the admin policy already, you need to include specified flow or class to specify the rule action for the packets matching configured classifying patterns on flow or class.

To include specific flow or class in an admin policy, use the following command.

Command	Mode	Description
include-flow *NAME*	Admin-Policy	Includes an admin flow in a specified policy. NAME:admin-flow name
include-class *NAME*		Includes an admin class in a specified policy. NAME:admin-class name

One admin policy cannot include both flow and class at the same time. Either admin flow or admin class can belong to one policy.

To remove flow or class from the policy, use the following command.

Command	Mode	Description
no include-flow	Admin-Policy	Removes the admin flow from this policy.
no include-class		Removes the admin class from this policy.

9.3.7.2 Admin Policy Priority

If rules that are more than two match the same packet then the rule having a higher priority will be processed first. To set a priority for an admin access rule, use the following command.

Command	Mode	Description
priority {**highest** | **high** | **medium**| **low**}	Admin-Policy	Sets a priority for an admin policy. (default: low)

9.3.7.3 Admin Policy Action

To specify the rule action (**action match**) for the packets matching configured classifying patterns, use the following command.

Command	Mode	Description
action match deny	Admin-Policy	Denies a packet.
action match permit		Permits a packet.

To delete a specified rule action(**action match**), use the following command.

Command	Mode	Description
no action match deny	Admin-Policy	Deletes a specified rule action.
no action match permit		

To specify a rule action (**action no-match**) for the packets **not** matching configured classifying patterns, use the following command.

Command	Mode	Description
action no-match deny	Admin-Policy	Denies a packet.
action no-match permit		Permits a packet.

To delete a specified rule action(**action no-match**), use the following command.

Command	Mode	Description
no action no-match deny	Admin-Policy	Deletes a specified rule action.
no action no-match permit		

9.3.7.4 Applying and Modifying Admin Policy

After configuring an admin policy using the above commands, apply it to the system with the following command. If you do not apply this policy to the system, all specified configurations from *Admin-Policy Configuration* mode will be lost.

To save and apply an admin policy, use the following command.

Command	Mode	Description
apply	Admin-Policy	Applies an admin policy to the system.

To modify an admin policy, use the following command.

Command	Mode	Description
policy admin *NAME* **modify**	Global	Modifies an admin policy. NAME: admin-policy name.

9.3.8 Displaying Admin Rule

To show an admin rule profile configured by user, use the follwing command.

Command	Mode	Description
show flow-profile admin	Admin-Flow	Shows a profile of admin flow.
show policy-profile admin	Admin-Policy	Shows a profile of admin policy.

The following command can be used to show a certain rule by its name, all rules of a certain type, or all rules at once sorted by a rule type.

Command	Mode	Description
show { **flow** | **class** | **policy** } **admin** [*NAME*]	Enable Global	Shows the information relating to each rule, enter an admin rule name.
show { **flow** | **class** | **policy** } **admin detail** [*NAME*]		

show running-config { **admin-flow** | **admin-policy** }	All	Shows all configurations of admin rules.

9.3.9 Displaying Policy Interface Configuration

To show a configuration about poclicy interface, use the following command.

Command	Mode	Description
show policy interface {channelgroup | gpon | tengigabitethernet} *IFPORT*	Enable Global	Shows a configured policy on specified interface.
show policy interface vlan *VLANID*		

9.3.10 Scheduling

To process incoming packets by the queue scheduler, the LD3032 provides the scheduling algorithm as Strict Priority Queuing (SP), Weighted Round Robin (WRR) and Deficit Round Robin (DRR).

Strict Priority Queuing (SP)

SPQ processes first more important data than the others. Since all data are processed by their priority, data with high priority can be processed fast but data without low priority might be delayed and piled up. This method has a strong point of providing the distinguished service with a simple way. However, if the packets having higher priority enter, the packets having lower priority are not processed.

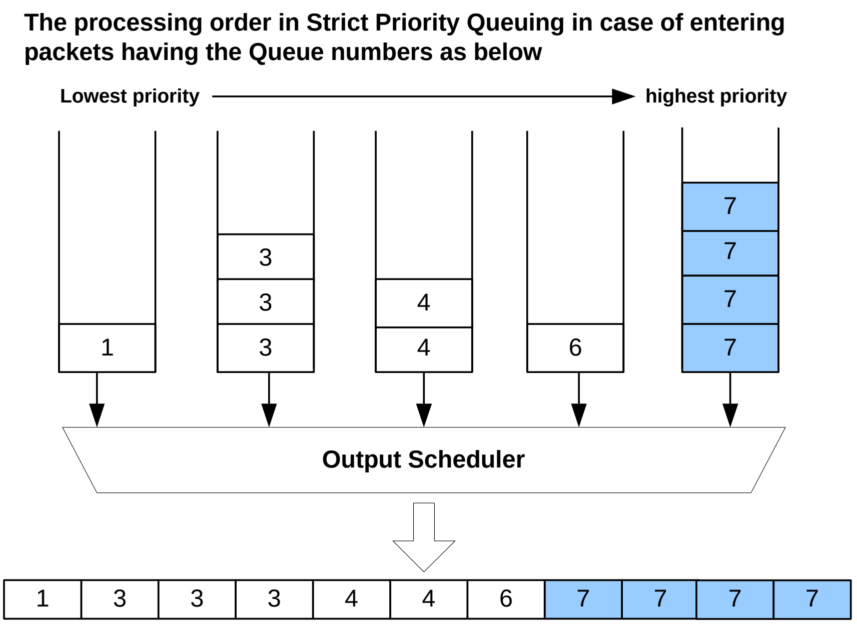

The processing order in Strict Priority Queuing in case of entering packets having the Queue numbers as below
Lowest priority
highest priority
1
3
3
3
4
4
6
7
7
7
7
Output Scheduler
1 3 3 3 4 4 6 7 7 7 7

Fig. 9.14 Strict Priority Queuing

Deficit Round Robin (DRR)

DRR is a modified WRR. This can handle packets of variable size without knowing their mean size. A maximum packet size number is subtracted from the packet length, and packets that exceed that number are held back until the next visit of the scheduler.

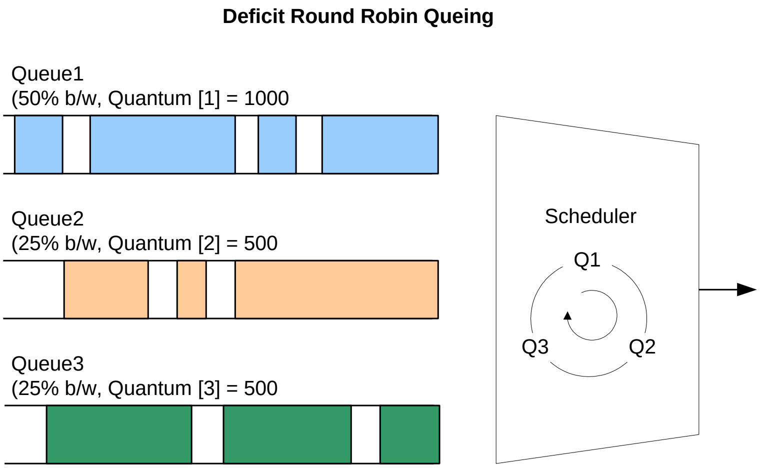

Deficit Round Robin Queing
Queue1
(50% b/w, Quantum [1] = 1000
Queue2
(25% b/w, Quantum [2] = 500
Queue3
(25% b/w, Quantum [3] = 500
Scheduler
Q1
Q3
Q2

Fig. 9.15 Deficit Round Robin

Weighted Round Robin (WRR)

WRR processes packets as much as weight. Processing the packets that have higher priority is the same way as strict priority queuing. However, it passes to next stage after processing as configured weight so that it is possible to configure for packet process to the packets having higher priority. However, there’s a limitation of providing differentiated service from those existing service.

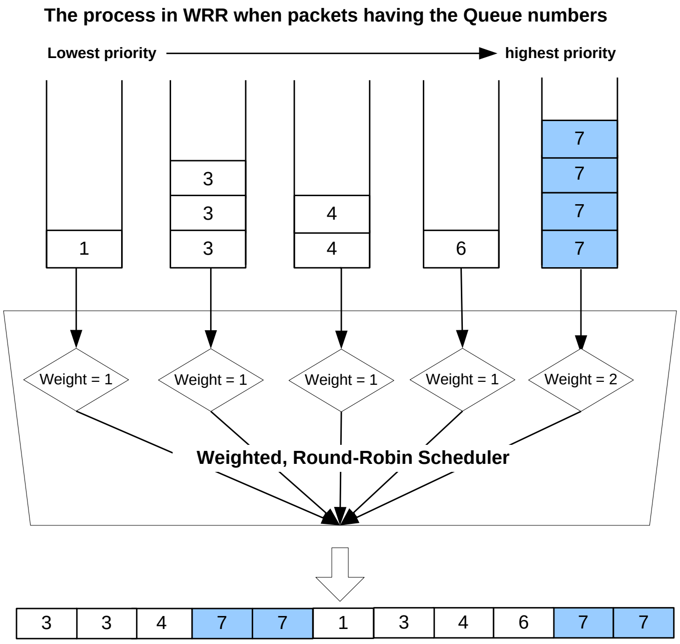


Fig. 9.16 Weighted Round Robin

9.3.10.1 Scheduling mode

To select a packet scheduling mode, use the following command.

Command	Mode	Description
qos scheduling-mode {**sp** | **wrr** | **dwrr**}	Interface [XE/GE/GPON]	Selects a packet scheduling mode for an interface: sp: strict priority queuing wrr: weighted round robin drr: deficit round robin
qos cpu scheduling-mode {**sp** | **wrr**}	Global	Sets CPU packet scheduling mode. sp: strict priority queuing

i The default scheduling mode is **WRR**. And it is possible to assign a different scheduling mode to each port.

9.3.10.2 Weight and Quantum

To set a weight for WRR scheduling mode, use the following command.

Command	Mode	Description
qos weight {<0-7> | **all**} {<1-127> | **unlimited**}	Interface [XE/GE/GPON]	Sets a weight for each port and queue: PORTS: port numbers 0-7: queue number 1-127: weight value (default: 1) unlimited: strict priority queuing
qos cpu weight <0-7> {<1-15> | **unlimited**}	Global	Sets a weight of queue for CPU packets: 0-7: queue number 1-15: weight value unlimited: strict priority based queuing

To set a quantum for DRR scheduling mode, use the following command.

Command	Mode	Description
qos quantum {<0-7> | **all**} {<1-127> | **unlimited**}	Interface [XE/GE/ GPON]	Sets a quantum for each port and queue: PORTS: port numbers 0-7: queue number 1-127: quantum value (default: 1) unlimited: strict priority queuing

9.3.10.3 Maximum and Minimum Bandwidth

To set a maximum bandwidth, use the following command.

Command	Mode	Description
qos max-bandwidth {<0-7> | **all**} {*BANDWIDTH* | **unlimited**}	Interface [XE/GE/ GPON]	Sets a maximum bandwidth for each port and queue: PORTS: port numbers 0-7: queue number BANDWIDTH: bandwidth in the unit of MB unlimited: unlimited bandwidth

To set a minimum bandwidth, use the following command.

Command	Mode	Description
qos min-bandwidth {<0-7> | **all**} {*BANDWIDTH* | **unlimited**}	Interface [XE/GE/GPON]	Sets a minimum bandwidth for each port and queue: PORTS: port numbers 0-7: queue number BANDWIDTH: bandwidth in the unit of MB (default: 0) unlimited: unlimited bandwidth

⚠ A maximum/minimum bandwidth can be set only in **WRR** scheduling mode.

9.3.10.4 Egress Admission Control

The egress admission control feature is to support fair access to the buffering resources among congested egress queues. To set guaranteed/shared buffer size on the interface and queue number for egress traffic control, use the following command.

Command	Mode	Description
qos buffer egress {<0-7> | **all**} **max-limit dynamic** <0-10> {**unicast** | **non-unicast**}	Interface [XE/GE/GPON]	Sets the egress admission control. 9360-71424: buffer size (default: 6144bytes) 0-7: queue number all: all queues max-limit: maximum limitation (shared buffer limit) min-limit: minimum limitation (guaranteed buffer cell limit) dynamic: apply dynamic policy to limit shared buffer size static: apply static policy to limit shared buffer size 0-10: set buffer limitation (alpha factor) 16-20000: set buffer limitation (unit : cell, cell size : 208bytes) 8-1000: set buffer limitation (unit : cell, cell size : 208bytes)
qos buffer egress {<0-7> | **all**} **max-limit static** <16-20000> {**unicast** | **non-unicast**}		
qos buffer egress {<0-7> | **all**} **min-limit** <8-1000> {**unicast** | **non-unicast**}		

		unicast: unicast queue non-unicast: non-unicast queue
no qos buffer egress {<0-7> | **all**} **max-limit** {**unicast** | **non-unicast**}		Removes the buffer cell limit values.
no qos buffer egress {<0-7> | **all**} **min-limit** {**unicast** | **non-unicast**}		

To display the configured guaranteed buffer size of the port and queue number, use the following command.

Command	Mode	Description
show qos buffer-config {**gigabitethernet** | **tengigabitethernet** | **gpon** } *IFPORT* {**unicast** | **non-unicast**}	Enable Global	Shows the configured guaranteed buffer size of the port.
show interface queue-status all {**unicast** | **non-unicast**}		Shows the unicast/multicast packet buffer usage status per queue. IFPORTS: interface port number unicast: unicast traffic non-unicast: multicast traffic
show interface queue-status cpu		
show interface queue-status {**gigabitethernet** | **tengigabitethernet** | **gpon** *IFPORT* {**unicast** | **non-unicast**}		
show interface statistics {**avg-perq** | **buffer** } **all** {**unicast** | **non-unicast**}		Shows the traffic statistics of buffer or the average packet per queue for all Ethernet/PON ports. unicast: unicast traffic non-unicast: multicast traffic
show interface statistics {**avg-perq** | **buffer** } **cpu**		Shows the incoming traffic statistics of buffer or the average packet per queue into CPU.
show interface statistics {**avg-perq** | **buffer** } {**gigabitethernet** | **tengigabitethernet** | **gpon** } *IFPORT* {**unicast** | **non-unicast**}		Shows the traffic statistics of buffer or the average packet per queue for a specified Ethernet/PON port. IFPORTS: interface port number unicast: unicast traffic non-unicast: multicast traffic

9.3.10.5 Displaying QoS

To display the configuration of QoS, enter following command.

Command	Mode	Description
show qos	Enable Global Interface [XE/GE/GPON]	Shows the configuration of QoS for all ports.
show qos interface {**gigabitethernet** | **tengigabitethernet** | **gpon** } *IFPORT*		Shows the configuration of QoS per each port.
show qos cpu	Enable Global	Shows the configuration of QoS for CPU packets.

9.3.10.6 Displaying Queue Status

To display the traffic statistic information on each queue, use the following command.

Command	Mode	Description
show queue-status {**gigabitethernet** | **tengigabitethernet** | **gpon** } *IFPORT* {**unicast** | **non-unicast**}	Enable Global Interface [XE/GE/GPON]	Shows the information of queue status on the interface.
show queue-status cpu		Shows the CPU queue cell information and packet usage.

9.3.10.7 Random Early Detection (WRED)

The LD3032 supports Weighted Random Early Detection (WRED) which can selectively discard lower priority traffic when an interface gets congested. WRED provides differentiated performance characteristics for different classes of service. It minimizes the impact of dropping high priority traffic. WRED is based on the RED algorithm.

RED, which utilizes end-to-end flow-control of TCP, is a random packet dropping function when traffic reaches the user-given threshold even before it reaches maximum buffer size. If traffic amount reaches maximum buffer size, all packets can be dropped, which makes packet loss. Therefore, in order to prevent packet loss or unstable traffic transmission, user can restrict excessive traffic over buffer size by setting up a threshold. With RED function, packet loss is reduced and stable packet transmission can be acquired.

One of the drawbacks to implement RED function is that it randomly drops a large number of packets, and is easy to drop high priority of packets. Unlike RED, WRED is not as random when dropping packets. WRED combines the capabilities of the RED algorithm with the IP precedence feature to provide for preferential traffic handling of high-priority packets.

To utilize WRED function, a start queue length value, end queue length value and drop probability are necessary.

- **WRED min-threshold (start queue length value)** is the starting point of random packet dropping.
- **WRED max-threshold (end queue length value)** is the point of complete dropping.
- **drop probability** indicates the percentage of packet dropping from the starting point of random packet dropping to the point of complete dropping. .

If probability is a large value, the amount of packets would be dropped. Therefore complete dropping point is slowly reached. On the other hand, if probability is small, a small amount of packets would be dropped. Therefore complete dropping point is quickly reached. If the probability value is 1, dropping packet would be none and the value is 100, all packets would be discarded from the point of start queue length value is reached.

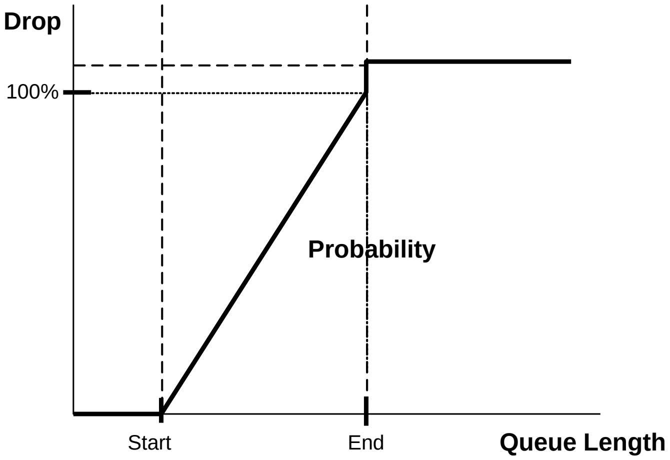


Fig. 9.17 WRED Packet Drop Probability

To configure WRED parameters, use the following command.

Command	Mode	Description
qos random-detect {**green** | **yellow** | **red** } <0-7> **min** <0-1000> **max** <0-20000> **probability** <0-100>	Global	Configures a WRED parameter values. 0-7: queue number min: WRED min-threshold max: WRED max-threshold 0-1000: minimum threshold to begin dropping (default: 32 cells) 0-20000: maximum threshold to drop all packets (default: 192 cells) 1-100: drop probability (default: 5%)
qos random-detect <0-7> **weight** <0-15>		Configures a WRED queue number and weight. 0-7: queue number 1-15: queue weight (default:1)

To enable/disable WRED function, use the following command.

Command	Mode	Description
qos random-detect enable	Global	Enables WRED function.
qos random-detect disable		Disables WRED function.

To display the WRED parameter values per queue number, use the following command.

Command	Mode	Description
show qos random-detect	Enable Global	Shows WRED function.

9.4 Spanning Tree Protocol (STP)

The local area network (LAN), which is composed of double paths like token ring, has the advantage that it is possible to access in case of disconnection with one path. However there is another problem called a loop when you always use the double paths.

The loop may occur when double paths are used for the link redundancy between switches and one sends unknown unicast or multicast packet that causes endless packet floating on the LAN like loop topology. That superfluous traffic eventually can result in network fault. It causes superfluous data transmission and network fault.

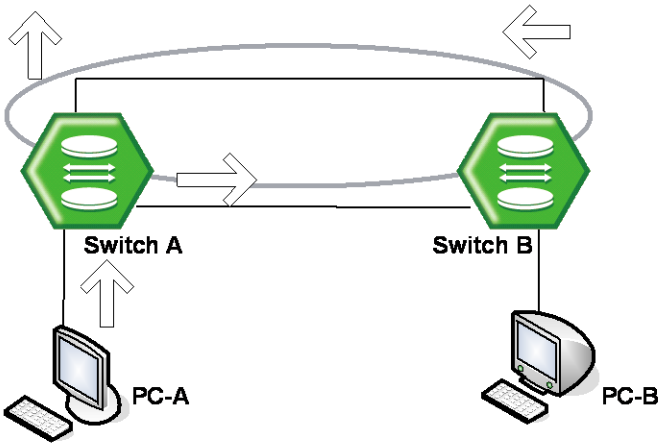


Fig. 9.18 Example of Loop

The spanning tree protocol (STP) is the function to prevent the loop in LAN with more than two paths and to utilize the double paths efficiently. It is defined in IEEE 802.1d. If the STP is configured in the system, there is no loop since it chooses more efficient path of them and blocks the other path. In other words, when SWITCH C in the below figure sends packet to SWITCH B, path 1 is chosen and path 2 is blocked.

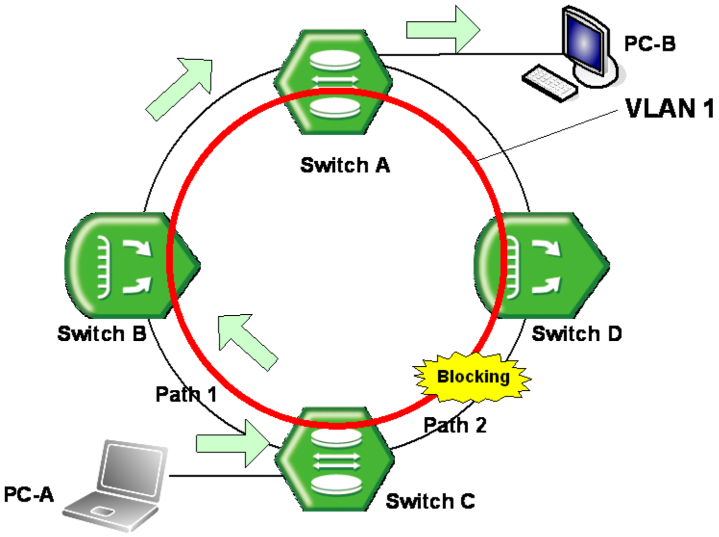


Fig. 9.19 Principle of Spanning Tree Protocol

Meanwhile, the rapid spanning tree protocol (RSTP) defined in IEEE 802.1w dramatically reduces the time of network convergence on the spanning tree protocol (STP). It is easy and fast to configure new protocol. The IEEE 802.1w also supports backward compatibility with IEEE 802.1d.

9.4.1 STP Operation

The 802.1d STP defines port state as blocking, listening, learning, and forwarding. When STP is configured in LAN with double paths, switches exchange their information including the bridge ID.

It is named as BPDU (Bridge Protocol Data Unit). Switches decide port state based on the exchanged BPDU and automatically decide an optimized path to communicate with the root switch.

9.4.1.1 Root Switch

The most important information to decide the root switch is bridge ID. A bridge ID is composed of 2 bytes-priority and 6 bytes-MAC address. The root switch has the lowest bridge ID.

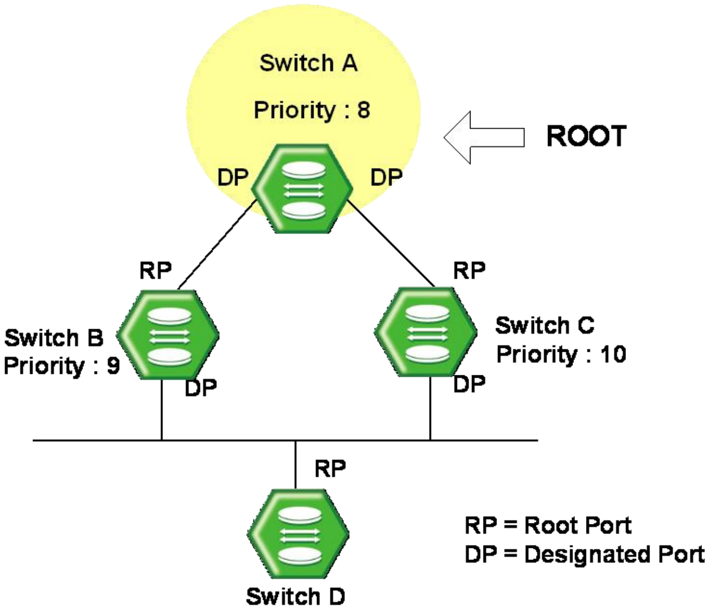


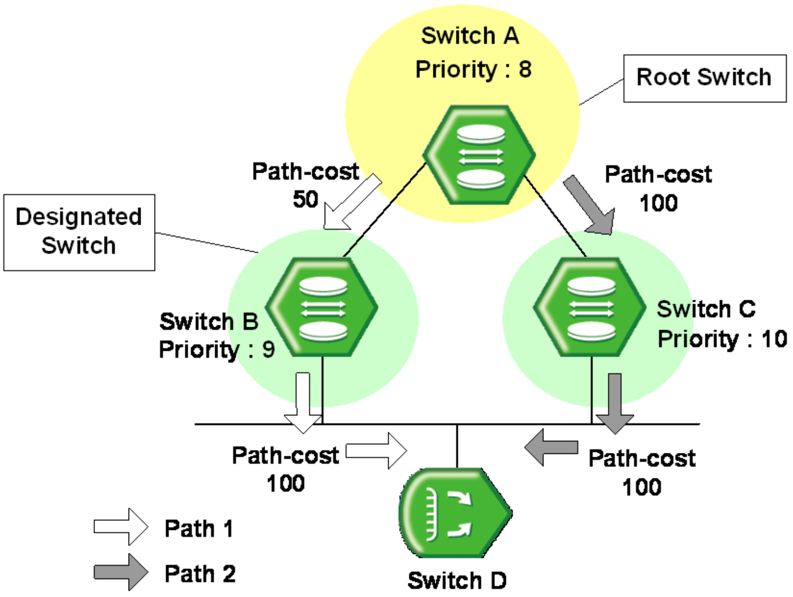
Fig. 9.20 Root Switch

After configuring STP, these switches exchange their information. The priority of SWITCH A is 8, the priority of SWITCH B is 9, and the priority of SWITCH C is 10. In this case, SWITCH A is automatically configured as the root switch.

9.4.1.2 Designated Switch

After deciding the root switch, while SWITCH A transmits packets to SWITCH C, SWITCH A compares the exchanged BPDU to decide the path to link. The critical information to decide path is the path-cost. The path-cost depends on the transmit rate of the LAN interface, and the path with the lower path-cost is selected.

The standard to decide designated switch is total root path-cost which is added with path-cost to the root. The path-cost depends on the transmit rate of the switch LAN interface, and the switch with lower path-cost is selected as designated switch.



(PATH 1 = 50 + 100 = 150, PATH 2 = 100 + 100 = 200, PATH 1 < PATH 2, ∴ **PATH 1 selected**

Fig. 9.21 Designated Switch

In case of the above figure with SWITCH A sending packet, the path-cost of PATH 1 is 150 and the path-cost of PATH 2 is total 200(100 + 100 ; path-cost of SWITCH A to C + path-cost of SWITCH C to D). Therefore the PATH 1 with lower path-cost is chosen. In this case, the port connected to the Root switch is named the Root port. In the above figure, the port of SWITCH C connected to SWITCH A as Root switch is the Root port. There can be only one Root port on the equipment.

The switch with lower path-cost is selected to be designated switch. If the root path-costs are same, bridge IDs are compared.

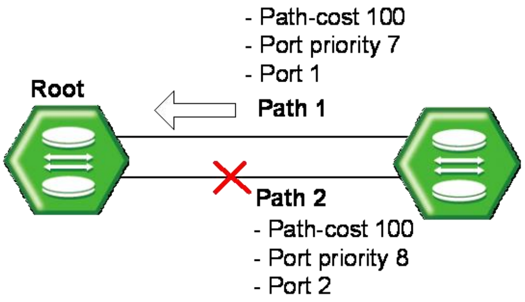
9.4.1.3 Designated Port and Root Port

Root Port is the port in the active topology that provides connectivity from the Desig-nated Switch toward the root. Designated Port is the port in the active topology used to forward traffic away from the root onto the link. That is, except the root port in each switch, the selected port to communicate is desig-nated port. The other ports, except root port and designated port, are named blocked port.

9.4.1.4 Port Priority

If the path-costs of two paths are same, decisions are based on port-priorities. In the figure below, suppose that two switches are connected. Since the path-costs of two paths are both 100, their port priorities are compared and the port with smaller port priority is selected to transmit the packet.

i All these functions are automatically performed by BPDU, which is the bridge information exchange between switches to activate or disable a specific port. It is also possible to configure BPDU to modify the root switch or the path manually.



(path-cost of PATH 1 = path-cost of PATH 2 = 100 ∴ unable to compare
PATH 1 port priority = 7, PATH 2 port priority = 8, PATH 1< PATH 2, ∴ **PATH 1 is chosen**)

Fig. 9.22 Port Priority

Port States

Each port on a switch can be in one of five states.

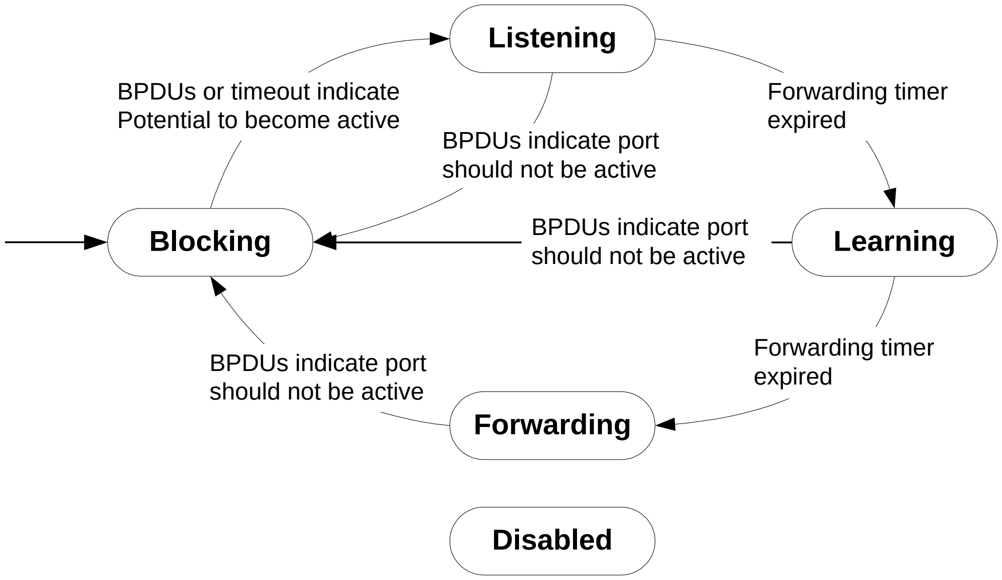


Fig. 9.23 Port States

- **Blocking**
  A port that is enabled, however neither a Designated port nor a Root port, will be in the blocking state. A blocking port will not receive or forward data frames, nor will it transmit BPDUs, but instead it will listen to other's BPDUs to determine if and when the port should consider becoming active in the spanning tree.
- **Listening**
  The port is still not forwarding data traffic, but is listening to BPDUs in order to compute the spanning tree. The port is comparing its own information (path cost, Bridge Identifier, Port Identifier) with the information received from other candidates and deciding which is best suited for inclusion in the spanning tree.
- **Learning**
  The port is preparing to forward data traffic. The port waits for a period of time to build its MAC address table before actually forwarding data traffic. This time is the forwarding delay.
- **Forwarding**
  After learning address, it is allowed to forward data frame. This is the steady state for a switch port in the active spanning tree.
- **Disabled**
  When disabled, a port will neither receive nor transmit data or BPDUs. A port is in this state because it is broken or disabled by administrator.

9.4.2 RSTP Operation

STP or RSTP is configured on network where Loop can be created. However, RSTP is more rapidly progressed than STP at the stage of reaching to the last topology. This section describes how the RSTP more improved than STP works. It contains the below sections.

- Port States
- BPDU Policy
- Rapid Network Convergence
- Compatibility with 802.1d

9.4.2.1 Port States

RSTP defines port states as discarding, learning, and forwarding. Blocking of 802.1d and listening is combined into discarding. Same as STP, root port and designated port are decided by port state. But a port in blocking state is divided into alternate port and backup port. An alternate port means a port blocking BPDUs of priority of high numerical value from other switches, and a backup port means a port blocking BPDUs of priority of high numerical value from another port of same equipment.

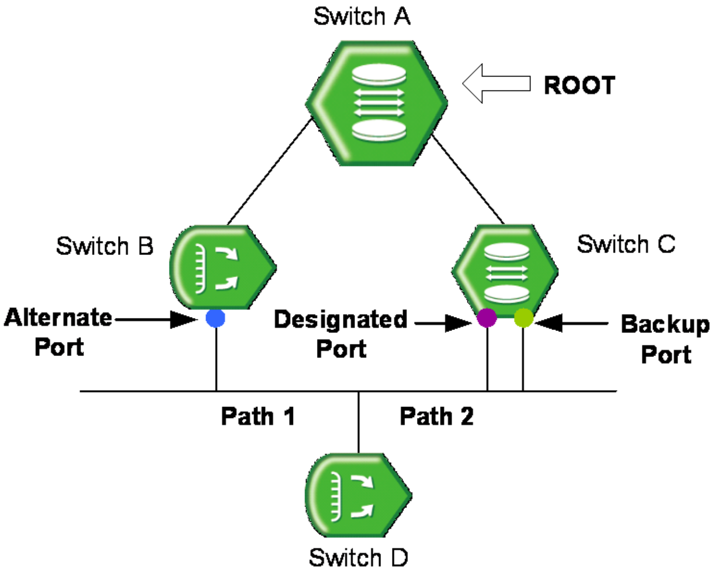


Fig. 9.24 Alternate Port and Backup port

The difference of between alternate port and backup port is that an alternate port can alternate the path of packet when there is a problem between Root switch and SWITCH C but Backup port cannot provide stable connection in that case.

9.4.2.2 BPDU Policy

In 802.1d, only the root switch forwards BPDU following Hello-time. However in 802.1w, not only root switch but also all the other switches forward BPDU following Hello-time. In 802w, BPDU is forwarded more frequently than the interval of transmitting BPDU by the root switch in 802.1d.

If low BPDU is received from the root switch or the designated switch, it is immediately accepted. For example, suppose that the root switch is disconnected from the switch B in the figure below. Then, the switch B is considered to be the root due to the disconnection, and it forwards BPDU.

In this case, the switch C transmits BPDU including the root information to the switch B. Thus, SWITCH B configures a port connected to SWITCH C as the new root port.

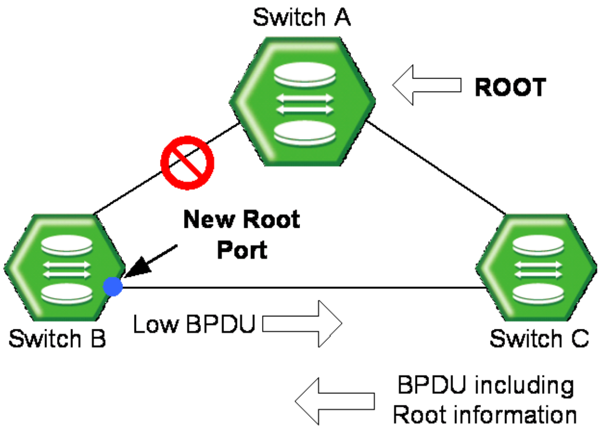


Fig. 9.25 Example of Receiving Low BPDU

9.4.2.3 Rapid Network Convergence

In the figure below, a new link is connected between SWITCH A and the root. Root and SWITCH A are not directly connected, but indirectly connected through SWITCH D. After SWITCH A is newly connected to the root, packets cannot be transmitted between the ports because the state of two switches becomes listening, and no loop is created.

In this state, if the root transmits BPDU to SWITCH A, SWITCH A transmits new BPDU to SWITCH B and SWITCH C, then SWITCH C transmits new BPDU to SWITCH D. SWITCH D, which received BPDU from SWITCH C, turns the port connected to SWITCH C into blocking state to prevent the loop after the new link.

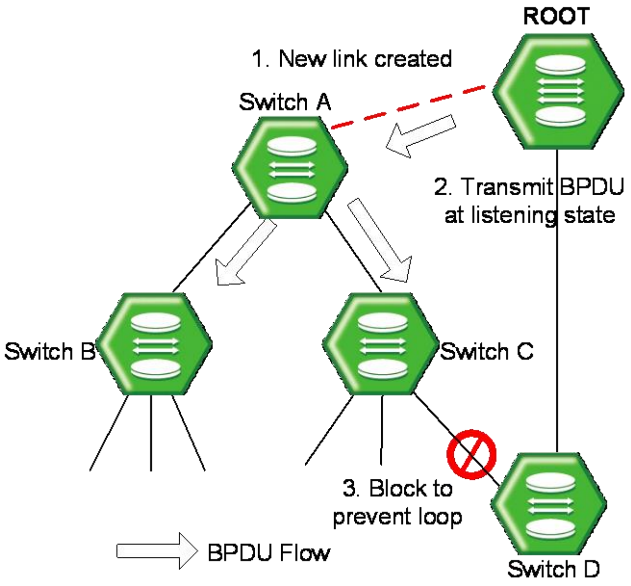


Fig. 9.26 Convergence of 802.1d Network

This is a very epochal way of preventing a loop. The matter is that communication is SWITCH D and SWITCH C is blocked. Then, right after the connection, it is possible to transmit BPDU although packets can not be transmitted and received between SWITCH A and the root.

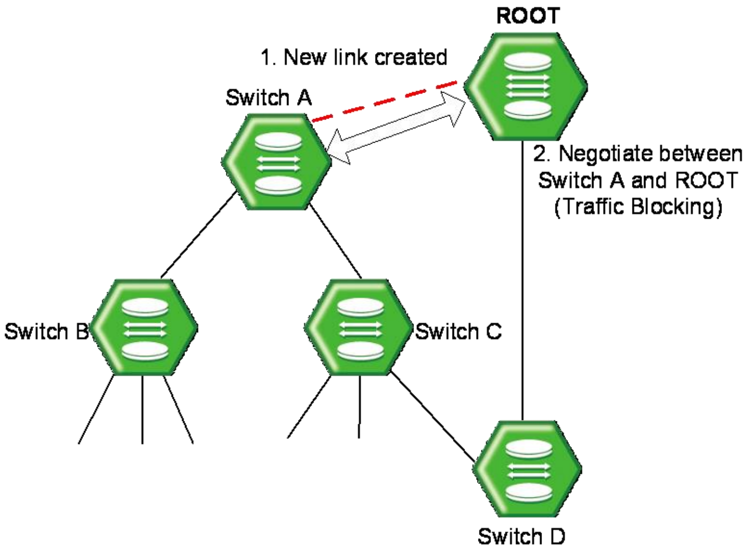


Fig. 9.27 Network Convergence of 802.1w (1)

SWITCH A negotiates with the root through BPDU. To make link between SWITCH A and the root, the state of non-edge designated port of SWITCH C is changed to blocking. Although SWITCH A is connected to the root, loop will not be generated because SWITCH A is blocked to SWITCH B and SWITCH C. In this state, BPDU from the root is transmitted to SWITCH B and SWITCH C through SWITCH A. To configure the forwarding state of SWITCH A, SWITCH A negotiates with SWITCH B and SWITCH C.

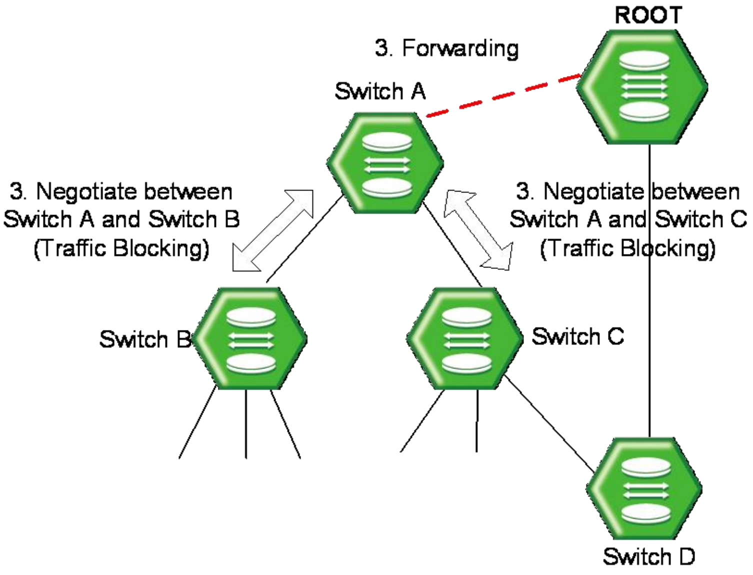


Fig. 9.28 Network Convergence of 802.1w (2)

SWITCH B has only edge-designated port. Edge-designated does not cause loop, so it is defined in 802.1w to be changed to forwarding state. Therefore, SWITCH B does not need to block specific port to the forwarding state of SWITCH A. However since SWITCH C has a port connected to SWITCH D, the port should be in the blocking state.

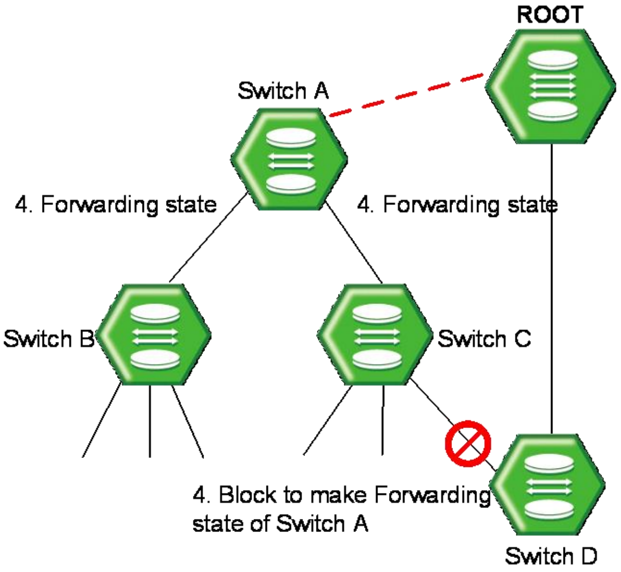


Fig. 9.29 Network Convergece of 802.1w (3)

It is same with 802.1d to block the connection of SWITCH D and SWITCH C. However, 802.1w does not need any configured time to negotiate between switches to make the forwarding state of specific port. So it is progressed very fast. During the progress to the port forwarding state, listening and learning are not needed. The negotiations use BPDU.

9.4.2.4 Compatibility with 802.1d

RSTP internally includes STP, so it has compatibility with 802.1d. Therefore, RSTP can recognize the BPDU of STP. However, STP cannot recognize the BPDU of RSTP. For example, assume that SWITCH A and SWITCH B are operated as RSTP and that SWITCH A is connected to SWITCH C as the designated switch. If SWITCH C is with 802.1d ignoring the BPDU of RSTP, it is interpreted as not connected to any switch or segment.

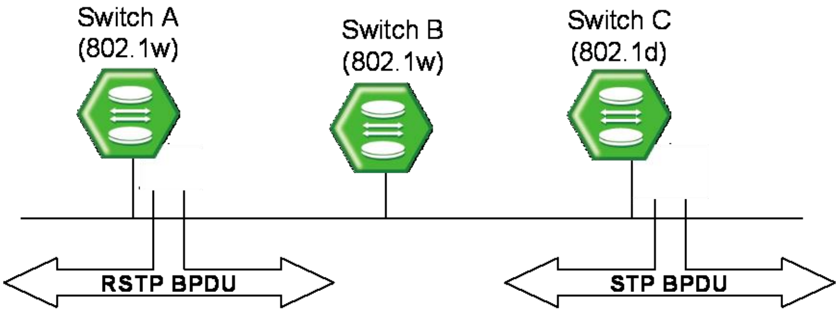


Fig. 9.30 Compatibility with 802.1d (1)

However, SWITCH A converts the port receiving BPDU into RSTP of 802.1d because it can read the BPDU of SWITCH C. Then SWITCH C can read BPDU of SWITCH A and accepts SWITCH A as the designated switch.

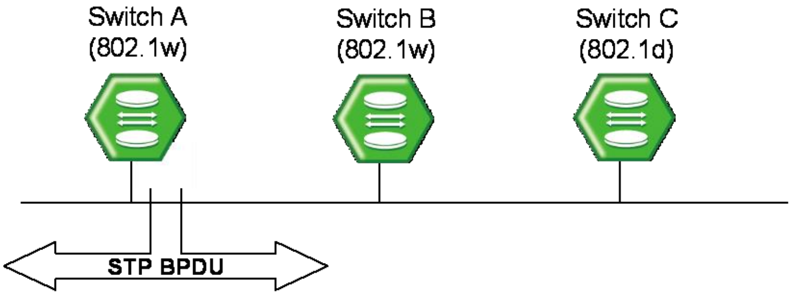


Fig. 9.31 Compatibility with 802.1d (2)

9.4.3 MSTP Operation

To operate the network more effectively, the LD3032 uses MSTP (Multiple Spanning-Tree Protocol). It constitutes the network with VLAN subdividing logically the existing LAN domain and configures the route by VLAN or VLAN group instead of existing routing protocol.

Operation

This section explains how STP/MSTP operate differently on the LAN. Suppose to configure 100 VLANs in the switch A, B, and C. In case of STP, there’s only an STP on all of VLANs and it does not provide multiple Instances.

While existing STP is a protocol to prevent Loop in a LAN, domain establishes STP per VLAN in order to realize the routing suitable to the VLAN environment.

It does not need to calculate all STPs for several VLANs so that traffic overload could be reduced. By reducing unnecessary overload and providing multiple transmission routes for data forwarding, load balancing is realized and multiple VLANs are provided through Instances.

9.4.3.1 MSTP

In MSTP, VLAN is classified to the groups with the same Configuration ID. Configuration ID is composed of Revision name, Region name and VLAN/Instance mapping. Therefore, to have the same Configuration ID, all of the tree conditions should be the same. VLAN classified with the same Configuration ID is called MST region. In a region, there's only an STP so that it is possible to reduce the number of STP compared with PVSTP. There's no limitation for the region in a network environment, however it is possible to generate Instances up to 64 (1 to 64). Spanning-tree operating in each region is IST (Internal Spanning-Tree). CST is applied by connecting each spanning-tree of region. Instance 0 means that there is not any Instance generated from grouping VLAN, that is, it does not operate as MSTP. Therefore Instance 0 exists on all the ports of the equipment. After starting MSTP, all the switches in CST exchanges BPDU and CST root is decided by comparing their BPDU. The switches that don't operate with MSTP have Instance 0 so that they can also join BPDU exchanges. The operation of deciding CST Root is called CIST (Common & Internal Spanning-Tree).

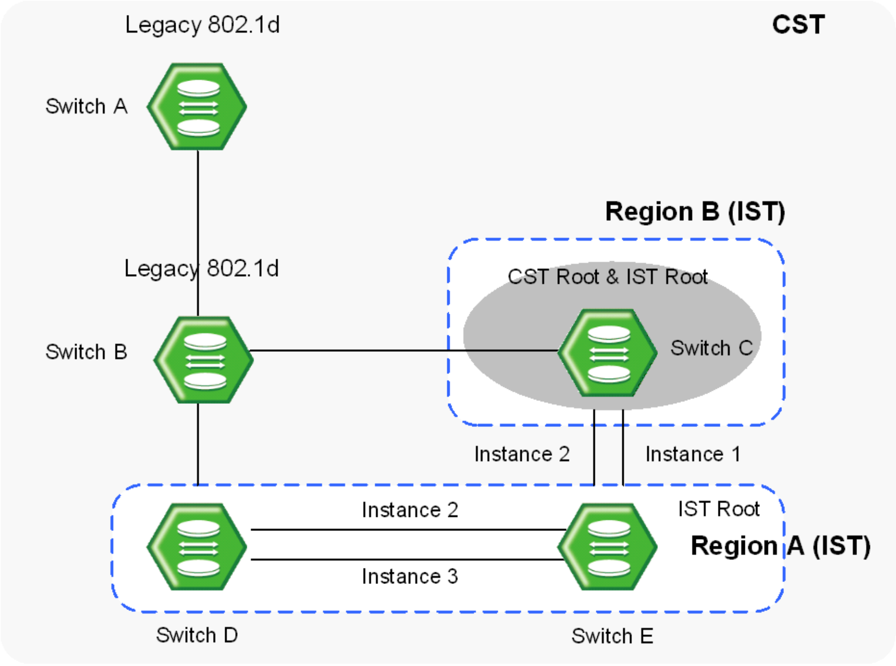


Fig. 9.32 CST and IST of MSTP (1)

In CST, A and B are the switches operating with STP, and C, D and E are those operating with MSTP. First, in CST, CIST is established to decide CST Root. After CST root is decided, the closest switch to CST root is decided as the IST root of the region. Here, the CST root in IST is IST root.

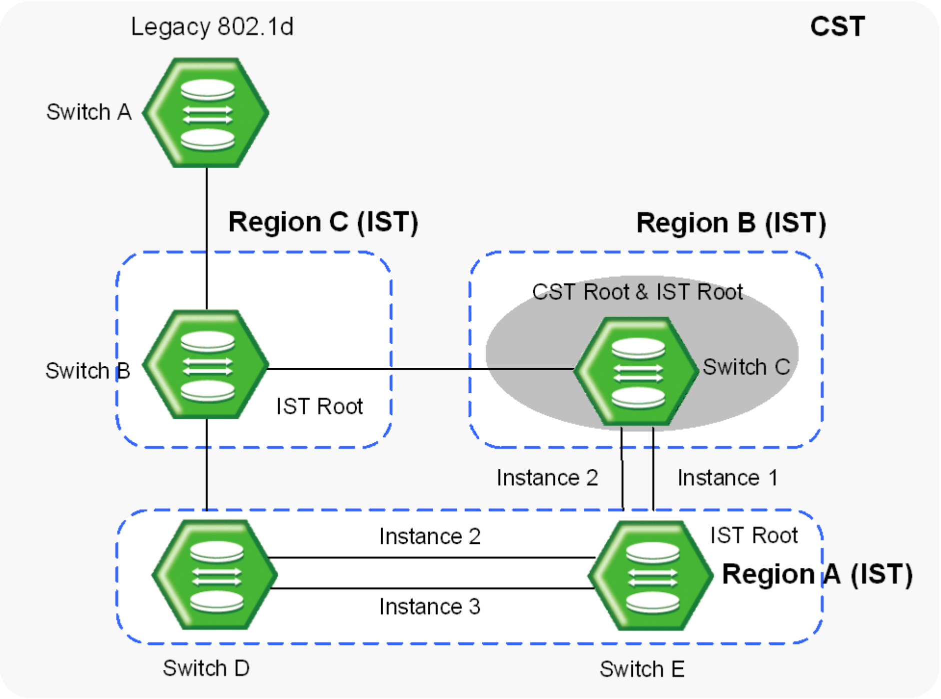


Fig. 9.33 CST and IST of MSTP (2)

In the above situation, if B operates with MSTP, B will send its BPDU to CST root and IST root in order to request itself to be CST root. However, if any BPDU with higher priority than that of B is sent, B cannot be CST root.

9.4.4 Enabling STP Function

First of all, you need to enable STP function. You cannot configure any parameters related to Spanning Tree Protocol without this command.

To enable STP function on the LD3032, use the following command.

Command	Mode	Description
spanning-tree	Global	Enables STP function.

To disable STP function from the system, use the following command.

Command	Mode	Description
no spanning-tree	Global	Disables STP function.

To enable STP function on a interface, use the following commane.

Command	Mode	Description
spanning-tree enable	Interface [XE/VLAN/CG]	Enables STP function per the interface.

To disable STP function from the interface, use the following command.

Command	Mode	Description
spanning-tree disable	Interface [XE/VLAN/CG]	Disables STP function per interface.

9.4.5 STP Mode

To select the spanning tree mode, use the following command.

Command	Mode	Description
spanning-tree mode { **mst** | **rstp** | **stp** | **rapid-pvst** | **rapid-pvst+**}	Global	Configures a spanning-tree mode: mst: Multiple Spanning Tree Protocol (default) rapid-pvst: Per-vlan Rapid STP

To delete the configured spanning tree mode, use the following command.

Command	Mode	Description
no spanning-tree mode	Global	Deleted a configured spanning tree mode. (default: MSTP)

9.4.6 STP Basic Configuration

To configure STP, use the following steps.

Step 1
Enable STP function using the **spanning-tree** command.

Step 2
Configure detail options if specific commands are required.

9.4.6.1 Path-cost Method

After deciding a root switch, you need to decide to which route you will forward the packet. To do this, the standard is a path-cost.

Generally, a path cost depends on the transmission speed of LAN interface in the switch. The following table shows the path cost according to the transmit rate of LAN interface.

You can use same commands to configure STP and RSTP, but their path-costs are totally different. Please be careful not to make mistake.

Transmit Rate (bps)	Path-cost
4M	250
10M	100
100M	19
1G	4
10G	2

Tab. 9.2 STP Path-cost (short)

Transmit Rate (bps)	Path-cost
4M	20000000
10M	2000000
100M	200000
1G	20000
10G	2000

Tab. 9.3 RSTP Path-cost (long)

To decide the path-cost calculation method, use the following command.

Command	Mode	Description
spanning-tree pathcost method long	Global	Selects the method for calculating a RSTP path-cost: long: 32 bits of RSTP path-cost (IEEE 802.1D-2004).
spanning-tree pathcost method short		Selects the method for calculating a STP path-cost: short: 16bits of STP path-cost (IEEE 802.1D-1998).

To delete a configured method for caculating the path-cost and return the configuration to the default, use the following command.

Command	Mode	Description
no spanning-tree pathcost method	Global	Deletes the configured method of path-cost. (default: long)

When the route decided by path-cost gets overloading, you would better take another route. Considering these situations, it is possible to configure the path-cost of root port so that user can configure a route manually. To specify the path-cost value, use the following command.

Command	Mode	Description
spanning-tree cost <1-200000000>	Interface [XE/GE]	Configures path-cost to configure route: PORTS: port number. 1-200000000: the path cost value.
no spanning-tree cost		Deletes the configured path-cost, enter the port number.

9.4.6.2 Edge Ports

Edge ports are defined that the ports are connected to a nonbridging device. There are no switches or spanning-tree bridges directly connected to the edge port. To configure all ports as edge ports globally, use the following command.

Command	Mode	Description
spanning-tree edgeport default	Global	Configures all ports as edge ports.
no spanning-tree edgeport default		Deleted a configured edge ports for all ports. (default)

To configure a specified port as edge port, use the following command.

Command	Mode	Description
spanning-tree edgeport enable	Interface [XE/GE]	Configures specified port as edge port.
spanning-tree edgeport disable		Disables edge port for specified port. PORTS: port number
no spanning-tree edgeport		

9.4.6.3 Port Priority

When all conditions of two switches are same, the last standard to decide route is port-priority. It is also possible to configure port priority so that user can configure route manually. To configure the port-priority, use the following command.

Command	Mode	Description
spanning-tree interface-priority <0-240>	Interface [XE/GE]	Configures port priority. 0-240: port priority in increments of 16 (default:128)
no spanning-tree interface-priority		Deleted a configured port priority.

9.4.6.4 Link Type

A port that operates in full-duplex is assumed to be point-to-point link type, while a half-duplex is considered as a shared port. .

To configure the link type of port, use the following command.

Command	Mode	Description
spanning-tree link-type {**point-to-point** | **shared**}	Interface [XE/GE]	Specifies a link-type for a designated port point-to-point: full-duplex shared: half-duplex

To delete a configured link type of port, use the following command.

Command	Mode	Description
no spanning-tree link-type	Interface [XE/GE]	Deletes a configured link type.

9.4.6.5 Displaying Configuration

To display the configurations of STP, use the following command.

Command	Mode	Description
show spanning-tree	Enable Global	Shows all configurations of STP
show spanning-tree active [**detail**]	Global	Shows STP information on active interface: detail: detailed STP information (as option).
show spanning-tree blockedif		Shows information of the blocked ports

show spanning-tree detail [**active**]		Shows detailed information of STP.
show spanning-tree inconsistentports		Shows information of root-inconsistency state.
show spanning-tree bridge { **address** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **protocol** | **priority** [**system-id**] }		Shows information of the bridge status and configuration
show spanning-tree root { **address** | **cost** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **port** | **priority** [**system-id**] }		Shows the status and configuration for the root bridge.
show spanning-tree interface *IFPORTS* [**active** [**detail**] | **cost** | **detail** [**active**] | **edgeport** | **inconsistency** | **rootcost** | **state** | **priority**]		Shows STP information of specified port.
show spanning-tree summary [**totals**]		Shows a summary of STP: totals: the total lines of STP

9.4.7 Configuring MSTP

To configure MSTP, use the following steps.

Step 1
Enable STP function using the **spanning-tree** command.

Step 2
Select a MSTP mode using the **spanning-tree mode mst** command.

Step 3
Configure detail options if specific commands are required.

Step 4

Enable a MSTP daemon using the **spanning-tree mst** command.

9.4.7.1 MST Region

To set the configuration ID of MST region in detail, you need to open *MSTP Configuration* mode first. To open *MSTP Configuration* mode, use the following command.

Command	Mode	Description
spanning-tree mst configuration	Global	Opens *MSTP Configuration* mode.

After opening *MSTP Configuration* mode, the prompt changes from SWITCH(config)# to SWITCH(config-mst)#.

To delete all configations from *MSTP Configuration* mode, use the following command.

Command	Mode	Description
no spanning-tree mst	Global	Deletes all configurations on *MSTP Configuration*

configuration		mode, returns to the default values.

If MSTP is established in the LD3032, decide a MSTP region the switch is going to belong to by configuring the MST configuration ID. Configuration ID contains a region name, revision, and a VLAN map.

To set the configuration ID, use the following command on *MSTP Configuration* mode.

Command	Mode	Description
name *NAME*	MST-config	Sets the MSTP region name: NAME: the name of MSTP region.
instance <1-64> **vlan** *VLANS*		Maps the specified vlans to an MSTP instance: 1-64: select an instance ID number. VLANS: VLAN ID (1-4094)
revision <0-65535>		Specifies a revision number: 0-65535: the MSTP configuration revision number.

In case of configuring STP and RSTP, you do not need to set the configuration ID. If you try to set configuration ID on STP or RSTP, an error message will be displayed.

You can create the MSTP regions without limit on the network. But the instance id numbers of each region should not be over 64.

To delete the configuration ID setting, use the following command.

Command	Mode	Description
no name	MST-config	Deletes the name of MSTP region
no instance <1-64> **vlan** *VLANS*		Deletes part of vlan-mapping, select the instance ID number and vlan id to remove from the specified instance 1-64: instance ID number VLANS: VLAN ID (1-4094)
no revision		Deletes the configured revision number.

After configuring the configuration ID in the LD3032, you should apply the configuration to the switch. After changing or deleting the configuration, you must apply it to the switch. If not, it does not being reflected into the switch.

To apply the configuration to the system, use the following command.

Command	Mode	Description
apply	MST-config	Apllies the configuration of the region to the system.

After deleting the configured configuration ID, apply it to the system using the above command.

To display the current and edited configuration on *MSTP Configuration* mode, use the following command.

Command	Mode	Description
show current	MSTP	Shows the current configuration as it is used to run MSTP
show pending		Shows the edited configuration of MSTP.
show		Shows all configurations of MSTP

For example, after setting the configuration ID, if you apply it to the switch with the **apply** command, you can check the configuration ID with the **show current** command.

However, if the user did not use the **apply** command to apply the configurations to the switch, the configuration could be checked with the **show pending** command.

9.4.7.2 Root Switch

To establish MSTP function, a root switch should be chosen first. In MSTP, a root switch is called as IST root switch. Each switch has its own bridge ID, and one of the switchs on same LAN is chosen as a root switch by comparing with their bridge IDs. However, you can configure the priority and make it more likely that the switch will be chosen as the root switch. The switch having the lowest priority becomes the root switch.

To configure the priority for an MSTP instance number, use the following command.

Command	Mode	Description
spanning-tree mst <0-64> **priority** <0-61440>	Global	Configures the priority of the switch: 0-64: MSTP instance ID number. 0-61440: priority value in increments of 4096 (default: 32768)
no spanning-tree mst <0-64> **priority**		Clears the Priority of the switch, enter the instance number.

i

If you configure a priority of STP or RSTP in the LD3032, you should configure MSTP instance ID number as 0.

9.4.7.3 Path-cost

After deciding a root swich, you need to decide to which route you will forward the packet. To do this, the standard is a path-cost. By the path-cost of root port, you can configure a route manually. To configure the path-cost value for specified instance number in MSTP, use the following command.

Command	Mode	Description
spanning-tree mst <0-64> **cost** <1-200000000>	Interface [XE/GE]	Configures path-cost for specified MSTP instance number: 0-64: MSTP instance ID number. 1-200000000: the path cost value.

no spanning-tree mst <0-64> **cost**		Deletes a configured path-cost.

9.4.7.4 Port Priority

When all conditions of two routes of switch are same, the last standard to decide a route is port-priority. You can configure port priority and select a route manually.

To configure a port priority for MSTP instance, use the following command.

Command	Mode	Description
spanning-tree mst <0-64> **interface-priority** <0-240>	Interface [XE/GE]	Configures the port priority of MSTP instance. 0-64: MSTP instance ID number. 0-240: port priority in increments of 16 (default:128)
no spanning-tree mst <0-64> **interface-priority**		Deletes a configured port priority of MSTP instance.

9.4.7.5 Displaying Configuration

To display the configuration of MSTP, use the following command.

Command	Mode	Description
show spanning-tree mst <1-64>	Enable Global	Shows all configurations of a specific MSTP instance: 1-64: MSTP instance ID number
show spanning-tree mst <1-64> **active** [**detail**]	Global	Shows information of a specific MSTP instance on active interface: 1-64: MSTP instance ID number. detail: detailed MSTP information (as option).
show spanning-tree mst <1-64> **blockedif**		Shows information of the blocked ports
show spanning-tree mst <1-64> **detail** [**active**]		Shows detailed information of the specific MSTP instance: 1-64: MSTP instance ID number.
show spanning-tree mst <1-64> **inconsistentports**		Shows information of root-inconsistency state. 1-64: MSTP instance ID number.
show spanning-tree mst <1-64> **bridge** [**address** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **protocol** | **priority** | **priority [system-id]**]		Shows information of the bridge status and configuration of a specific MSTP instance 1-64: MSTP instance ID number.
show spanning-tree mst <1-64> **root** [**address** | **cost** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **port** | **priority** | **priority [system-id]**]		Shows the status and configuration for the root bridge of a specifiec MSTP instance. 1-64: MSTP instance ID number.
show spanning-tree mst <1-64> **interface** *IFPORTS* [**active** [**detail**] | **cost** | **detail** [**active**] | **edge-**		Shows information of MSTP instance for specified port. 1-64: MSTP instance ID number.

Command	Mode	Description
port | **inconsistency** | **rootcost** | **state** | **priority**]		
show spanning-tree mst configuration [**digest**]		Shows information of the region configuration: digest: MD5 digest included in the current MSTCI
show spanning-tree mst <1-64> **summary** [**totals**]		Shows a summary of a specific MSTP instance: totals: the total lines of MSTP

9.4.8 Configuring PVSTP

STP and RSPT are designed with one VLAN in the network. If a port becomes blocking state, the physical port itself is blocked. But PVSTP (Per VLAN Spanning Tree Protocol) and PVRSTP (Per VLAN Rapid Spanning Tree Protocol) maintains spanning tree instance for each VLAN in the network. Because PVSTP treats each VLAN as a separate network, it has the ability to load balance traffic by forwarding some VLANs on one trunk and other VLANs. PVRSTP provides the same functionality as PVSTP with enhancement.

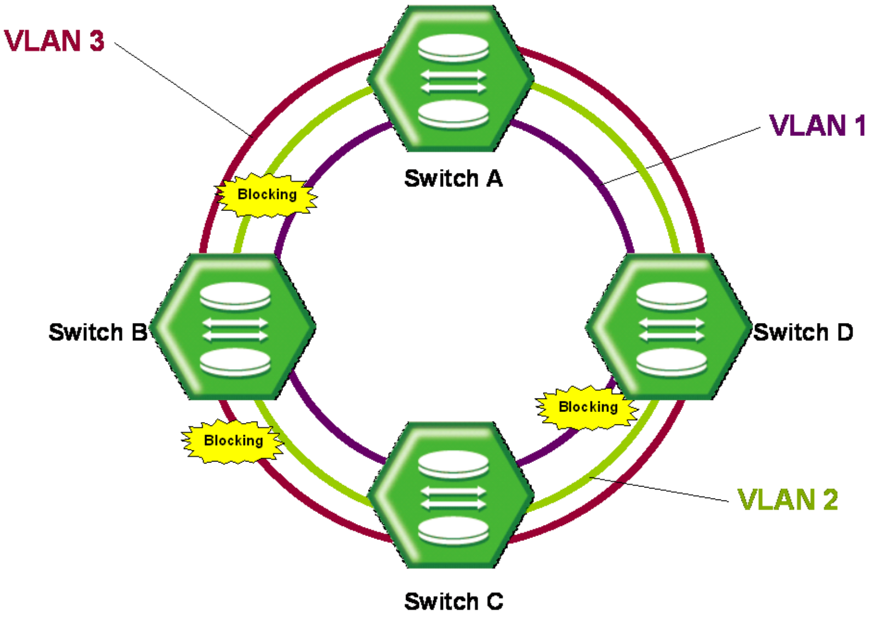


Fig. 9.34 Example of PVSTP

To configure PVSTP, use the following steps.

Step 1
Enable STP function using the **spanning-tree** command.

Step 2
Decide PVSTP mode using the **spanning-tree mode rapid-pvst** command.

Step 3
Enable PVSTP function using the **spanning-tree vlan** *VLANS* command.

Step 4
Configure detail options if specific commands are required.

9.4.8.1 Enabling PVSTP

To enable PVSTP function, use the following command.

Command	Mode	Description
spanning-tree vlan *VLANS*	Global	Activates PVSTP function. VLANS: VLAN ID (1-4094)

PVSTP is activated after selecting PVSTP mode using **spanning-tree mode rapid-pvst** command. In PVSTP, you can configure the current VLAN only. If you input VLAN that does not exist, error message is displayed.

For the switches in LAN where dual path does not exist, Loop does not generate even though STP function is not configured.

To disable a configured PVSTP, use the following command.

Command	Mode	Description
no spanning-tree vlan *VLANS*	Global	Disables PVSTP in VLAN. VLANS: VLAN ID (1-4094)

9.4.8.2 Root Switch

To establish PVSTP function, a root switch should be chosen first. Each switch has its own bridge ID, and one of the switchs on same LAN is chosen as a root switch by comparing with their bridge IDs. A bridge ID, consisting of the switch priority and the switch MAC address, is associated with each instance. However, you can configure the priority and make it more likely that the switch will be chosen as the root switch. The switch having the lowest priority becomes the root switch for that VLAN.

To configure the switch priority for a VLAN, use the following command.

Command	Mode	Description
spanning-tree vlan *VLANS* **priority** <0-61440>	Global	Configures a priority for specified VLAN. VLANS: VLAN ID (1-4094) 0-61440: priority value in increments of 4096 (default: 32768)
no spanning-tree vlan *VLANS* **priority**		Deletes a configured priority for specified VLAN.

9.4.8.3 Path-cost

After deciding Root switch, you need to decide to which route you will forward the packet. To do this, the standard is path-cost. Generally, path-cost depends on transmission speed of LAN interface in switch. In case the route is overload based on Path-cost, it is better to take another route.

By considering the situation, the user can configure Path-cost of Root port in order to designate the route on ones own.

To configure the path-cost value for specified vlan in PVSTP, use the following command.

Command	Mode	Description
spanning-tree vlan *VLANS* **cost** <1-200000000>	Interface [XE/GE]	Configures path-cost to configure route on user's own. VLANS: VLAN ID (1-4094)
no spanning-tree vlan *VLANS* **port** *PORTS* **cost**		Deleted a configured path-cost.

9.4.8.4 Port Priority

When all conditions of two routes of switch are same, the last standard to decide a route is port-priority. You can configure port priority and select a route manually.

To configure a port priority for specified VLAN, use the following command.

Command	Mode	Description
spanning-tree vlan *VLANS* **interface-priority** <0-240>	Interface [XE/GE]	Configures the port priority of specific VLAN. VLANS: VLAN ID (1-4094) 0-240: port priority in increments of 16 (default:128)
no spanning-tree vlan *VLANS* **interface-priority**		Deleted the configuration port priority of specifiec VLAN

9.4.8.5 Displaying Configuration

To display the configuration after configuring PVSTP, use the following command.

Command	Mode	Description
show spanning-tree vlan *VLANS*	Enable Global	Shows all configurations of a specific vlan id: VLANS: VLAN ID (1-4094)
show spanning-tree vlan *VLANS* **interface** *IFPORTS* [**active** [**detail**] | **cost** | **detail** [**active**] | **edgeport** | **cost** | **inconsistency** | **rootcost** | **state** | **priority**]		Shows information of vlan id for specified port. VLANS: VLAN ID (1-4094)
show spanning-tree vlan *VLANS* **active** [**detail**]	Global	Shows information of a specific vlan id on active interface: detail: detailed PVSTP information (as option).
show spanning-tree vlan *VLANS* **blockedif**		Shows information of the blocked ports
show spanning-tree vlan *VLANS* **detail** [**active**]		Shows detailed information of the specific vlan id: VLANS: VLAN ID (1-4094)
show spanning-tree vlan *VLANS* **inconsistentports**		Shows information of root-inconsistency state. VLANS: VLAN ID (1-4094)
show spanning-tree vlan *VLANS* **bridge** [**address** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **protocol** | **priority** [**system-id**]]		Shows information of the bridge status and configuration of a specific vlan id VLANS: VLAN ID (1-4094)
show spanning-tree vlan *VLANS* **root** [**address** | **cost** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **port** | **priority** [**system-id**]]		Shows the status and configuration for the root bridge of a specifiec vlan id. VLANS: VLAN ID (1-4094)
show spanning-tree vlan *VLANS* **summary** [**totals**]		Shows a summary of a specific vlan id: totals: the total lines of PVSTP

9.4.9 Root Guard

The standard STP does not allow the administrator to enforce the position of the root bridge, as any bridge in the network with lower bridge ID will take the role of the root bridge. Root guard feature is designed to provide a way to enforce the root bridge placement in the network. Even if the administrator sets the root bridge priority to zero in an effort to secure the root bridge position, there is still no guarantee against bridge with priority zero and a lower MAC address.

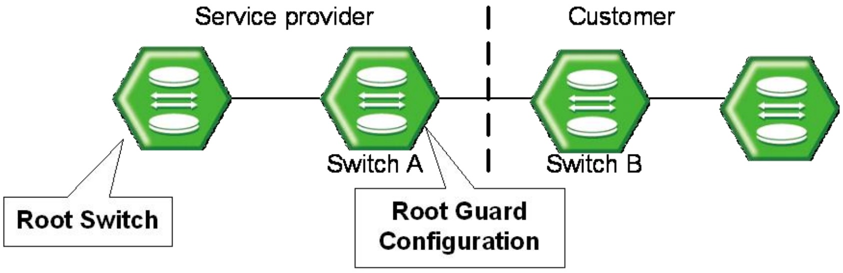


Fig. 9.35 Root Guard

Software-based bridge applications launched on PCs or other switches connected by a customer to a service-provider network can be elected as root switches. If the priority of bridge B is zero or any value lower than that of the root bridge, device B will be elected as a root bridge for this VLAN. As a result, network topology could be changed. This may lead to sub-optimal switching. But, by configuring root guard on switch A, no switches behind the port connecting to switch A can be elected as a root for the service provider’s switch network. In which case, switch A will block the port connecting switch B.

To configure Root-Guard, use the following command.

Command	Mode	Description
spanning-tree guard root	Interface [XE/GE]	Configures Root Guard on the network.

To delete a configured Root-Guard of specified port, use the following command.

Command	Mode	Description
spanning-tree guard none	Interface [XE/GE]	Disables Root Guard function.
no spanning-tree guard		Deletes a configured Root Guard, returns to default configurations.

9.4.10 Restarting Protocol Migration

MSTP protocol has a backward compatibility. MSTP is compatible with STP and RSTP. If some other bridge runs on STP mode and sends the BPDU version of STP or RSTP, MSTP automatically changes to STP mode. But STP mode cannot be changed to MSTP mode automatically. If administrator wants to change network topology to MSTP mode, administrator has to clear the previously detected detected protocol manually.

To prevent this, the LD3032 provides the **clear spanning-tree detected-protocols** command. If you enable this command, the switch checks STP protocol packet once again. To clear configured Restarting Protocol Migration, use the following command.

Command	Mode	Description
clear spanning-tree detected-protocols	Global Interface [XE/GE]	Restarts protocol migration function.

9.4.11 Loop Back Detection

The problem occurs because the keepalive packet is looped back to the port that sent the keepalive. Keepalives are sent on the switches in order to prevent loops in the network. You see this problem on the device that detects and breaks the loop, but not on the device that causes the loop.

To enable error-disable detection for loop back cause, use the following command.

Command	Mode	Description
errdisable detect cause loopback	Global	Enables error-disable detection for loop back cause
no errdisable detect cause loopback		Disables error-disable detection for loop back cause

To display the status of error-disable cause, use the following command.

Command	Mode	Description
show errdisable detect cause	Global	Shows status of error-disable causes

To enable/disable the error-disable recovery function for loop back cause, use the following command.

Command	Mode	Description
errdisable recovery cause all	Global	Enables the recovery function for all cause
errdisable recovery cause loopback		Enables the recovery function for loop back error-disable cause
errdisable recovery cause bpduguard		Enables the recovery function for bpduguard error-disable cause

no errdisable recovery cause { all | loopback | bpduguard }		Disables the recovery function.

To specify the time to recover from a specified error-disable cause, use the following command.

Command	Mode	Description
errdisable recovery interval <30-86400>	Global	Sets the interval of error-disable recovery: 30-86400: the recovery interval (default: 300 sec)
no errdisable recovery interval		Deleted the con figured time for error-disable recovery and returns to the default setting.

To display information of error-disable recovery function, use the following command.

Command	Mode	Description
show errdisable recovery	Global	Shows information of error-disable recovery function.

To enable/disable the debugging function of error-disable status caused by loop back, use the following command.

Command	Mode	Description
debug errdisable loopback enable	Enable	Enables the debugging for loop back error-disable cause.
debug errdisable loopback disable		Disables the debugging for loop back error-disable cause.

9.4.12 BPDU Configuration

BPDU is a transmission message in LAN in order to configure, and maintain the configuration for STP/RSTP/MSTP. Switches that STP is configured exchange their information BPDU to find the best path. MSTP BPDU is a general STP BPDU having additional MST data on its end. MSTP part of BPDU does not rest when it is out of region.

- **Hello Time**
  Hello time is an interval of which a switch transmits BPDU. It can be configured from 1 to 10 seconds. The default is 2 seconds.

- **Max Age**
  Root switch transmits new information every time based on information from other switches. However, if there are many switches on network, it takes lots of time to transmit BPDU. And if network status is changed while transmitting BPDU, this information is useless. To get rid of useless information, max age should be identified each information.

- **Forward Delay**

Switches find the location of other switches connected to LAN though received BPDU and transmit packets. Since it takes certain time to receive BPDU and find the location before transmitting packet, switches send packet at regular interval. This interval time is named forward delay.

i The configuration for BPDU is applied as selected in force-version. The same commands are used for STP, RSTP, MSTP and PVSTP.

9.4.12.1 Hello Time

Hello time decides an interval time when a switch transmits BPDU. To configure hello time, use the following command.

Command	Mode	Description
spanning-tree mst hello-time <1-10>	Global	Configures hello time to transmit the message in MSTP. 1-10: the hello time. (default: 2 sec)
spanning-tree vlan *VLANS* **hello-time** <1-10>		Configures hello time to transmit the message in PVSTP per VLAN. 1-10: the hello time. (default: 2 sec) VLANS: VLAN ID (1-4094)

To delete a configured hello-time, use the following command.

Command	Mode	Description
no spanning-tree mst hello-time	Global	Returns to the default hello time value of STP, RSTP and MSTP.
no spanning-tree vlan *VLANS* **hello-time**		Returns to the default hello time value of PVSTP.

9.4.12.2 Forward Delay Time

It is possible to configure forward delay, which means time to take port status from listening to forwarding. To configure forward delay, use the following command.

Command	Mode	Description
spanning-tree mst forward-time <4-30>	Global	Sets the forward-delay time for all MST instances: 4-30: forward delay time value (default:15)
spanning-tree vlan *VLANS* **forward-time** <4-30>		Sets the forward-delay time of PVSTP per VLAN: VLANS: VLAN ID (1-4094) 4-30: forward delay time value (default:15)

To delete a configured forward delay time, use the following command.

Command	Mode	Description
no spanning-tree mst forward-	Global	Returns to the default value of MSTP.

time		
no spanning-tree vlan *VLANS* **forward-time**		Returns to the default value of PVSTP per VLAN.

9.4.12.3 Max Age

Maximum aging time is the number of seconds a switch waits without receiving spanning-tree configuration messages before attempting a reconfiguration. To configure the maximum aging time for deleting useless messages, use the following command.

Command	Mode	Description
spanning-tree mst max-age <6-40>	Global	Changes the maximum aging time of route message of MSTP. 6-40: maximum aging time value (default: 20 sec)
spanning-tree vlan *VLANS* **max-age** <6-40>		Changes the maximum aging time of route message of PVSTP per specified VLAN. VLANS: VLAN ID (1-4094) 6-40: maximum aging time value (default: 20 sec)

We recommend that the maximum aging time is set less than twice of forward delay time and more than twice of hello time.

To delete a configured maximum aging time, use the following command.

Command	Mode	Description
no spanning-tree mst max-age	Global	Returns to the default maximum aging time value of MSTP.
no spanning-tree vlan *VLANS* **max-age**		Returns to the default maximum aging time value of PVSTP. VLANS: VLAN ID (1-4094)

9.4.12.4 BPDU Hop Count

In MSTP, it is possible to configure the number of hops in order to prevent BPDU from wandering. BPDU passes the switches as the number of hops by this function.

To configure the number of hops of BPDU in MSTP, use the following command.

Command	Mode	Description
spanning-tree mst max-hops <1-40>	Global	Configures the number of hops for BPDU, set the number of possible hops in MSTP region: 1-40: the number of hops for BPDU (default:20)
no spanning-tree mst max-hops		Deletes the number of hops for BPDU in MSTP.

9.4.12.5 BPDU Transmit hold count

You can configure the BPDU burst size by changing the transmit hold count value. To configure the transmit hold-count, use the following command.

Command	Mode	Description
spanning-tree transmit hold-count <1-20>	Global	Sets the number of BPDUs that can be sent before pausing for 1 second: 1-20: BPDU transmit hold-count value (default:6)
no spanning-tree transmit hold-count		Deletes a configured transmit hold-count value and returns to the default setting.

⚠ If you change this parameter to a higher value can have a significant impact on CPU utilization, especially in Rapid-PVST mode. We recommend that you maintain the default setting.

9.4.12.6 BPDU Filtering

BPDU filtering allows you to avoid transmitting on the ports that are connected to an end system. If the BPDU Filter feature is enabled on the port, then incoming BPDUs will be filtered and BPDUs will not be sent out of the port.

To enable or disable the BPDU filtering function on the port, use the following command.

Command	Mode	Description
spanning-tree bpdufilter enable	Interface [XE/GE]	Enables a BPDU filtering fuction on specific port.
spanning-tree bpdufilter disable		Disables a BPDU filtering fuction on specific port.
no spanning-tree bpdufilter		

By default, it is disabled. The BPDU filter-enabled port acts as if STP is disabled on the port. This feature can be used for the ports that are usually connected to an end system or the port that you don't want to receive and send unwanted BPDU packets. Be cautious about using this feature on STP enabled uplink or trunk port. If the port is removed from VLAN membership, correspond BPDU filter will be automatically deleted.

To enable or disable the BPDU filtering function on the edge port, use the following command.

Command	Mode	Description
spanning-tree edgeport bpdufilter default	Global	Enables a BPDU filtering function by default on all edge ports.
no spanning-tree edgeport bpdufilter default		Disables a BPDU filtering function by default on all edge ports.

9.4.12.7 BPDU Guard

BPDU guard has been designed to allow network designers to enforce the STP domain borders and keep the active topology predictable. The devices behind the ports with STP enabled are not allowed to influence the STP topology. This is achieved by disabling the port upon receipt of BPDU. This feature prevents Denial of Service (DoS) attack on the network by permanent STP recalculation. That is caused by the temporary introduction and subsequent removal of STP devices with low (zero) bridge priority.

To configure BPDU guard in the switch, perform the following procedure.

Step 1
Configure the specific port as edge-port.

Command	Mode	Description
spanning-tree edgeport enable	Interface [10GE/GE]	Configures the port as Edge port.

Step 2
Enable BPDU guard function on edge port or specific port, use the following command.

Command	Mode	Description
spanning-tree edgeport bpduguard default	Global	Enables BPDU Guard function on edge ports
spanning-tree bpduguard enable	Interface [XE/GE]	Enables BPDU Guard function on specified port

To disable BPDU guard function on edge port or specific port, use the following command.

Command	Mode	Description
no spanning-tree edgeport bpduguard default	Global	Disables BPDU Guard function of edge ports (default)
spanning-tree bpduguard disable	Interface [XE/GE]	Disables BPDU Guard function of specified port. (default)
no spanning-tree bpduguard		

However, BPDU Guard can be corrupted by unexpected cause. In this case, the edge port is blocked immediately and remains at this state until user recovers it. To prevent this problem, the LD3032 provides error-disable recovery function for BPDU guard cause. When an edge port is down for BPDU packet which came from other switch, the port is recovered automatically after configured time.

To enable the recovery function for BPDU guard error-disable cause, use the following command.

Command	Mode	Description
errdisable recovery cause bpduguard	Global	Enables the recovery function for BPDU guard error-disable cause
no errdisable recovery cause bpduguard		Disables the recovery function for BPDU guard error-disable cause

To display information of error-disable recovery function, use the following command.

Command	Mode	Description
show errdisable recovery	Global	Shows information of error-disable recovery function.

9.5 Loop Detection

The loop may occur when double paths are used for the link redundancy between switches and one sends unknown unicast or multicast packet that causes endless packet floating on the LAN like loop topology. That superfluous traffic eventually can result in network fault. It causes superfluous data transmission and network fault.

To prevent this, the LD3032 provides the loop detecting function. The loop detecting mechanism is as follows:

The switch periodically sends the loop-detecting packet to all the ports with a certain interval, and then if receiving the loop-detecting packet sent before, the switch performs a pre-defined behavior.

To enable/disable the loop detection globally, use the following command.

Command	Mode	Description
loop-detect {**enable** | **disable**}	Global	Enables/disables the loop detection globally.

For the detailed configuration of the loop detection, you need to issuing the **loop-detect enable** command first. If you do not, all the commands concerning the loop detection will show an error message.

You can also configure the source MAC address of the loop-detecting packet. Normally the system's MAC address will be the source MAC address of the loop-detecting packet, but if needed, Locally Administered Address (LAA) can be the address as well.

If the switch is configured to use LAA as the source MAC address of the loop-detecting packet, the second bit of first byte of the packet will be set to 1. For example, if the switch's MAC address is b8:26:d4:00:00:01, the source MAC address will be changed to b8:26:d4:00:00:01. To select the source MAC address type of the loop-detecting packet, use the following command.

Command	Mode	Description
loop-detect srcmac laa	Global	Uses LAA as the source MAC address of the loop-detecting packet.
loop-detect srcmac system		Uses the system's MAC address as the source MAC address of the loop-detecting packet. (default)

If you would like to change the source MAC address of the loop-detecting packet, you should disable the loop detection first using the **loop-detect disable** command.

To enable/disable the loop detection on a specified port, use the following command.

Command	Mode	Description
loop-detect	Interface [XE/GE/GPON/CG]	Enables the loop detection on a specified port.
no loop-detect		Disables the loop detection on a specified port.

To define the behavior on a specified port when a loop is occurred, use the following command.

Command	Mode	Description
loop-detect block	Interface [XE/GE/GPON/CG]	Enables the blocking option. This configures a specified port to automatically change its state to BLOCKED when a loop is detected on it. (default: disable)
loop-detect unblock		Forces the state of a blocked port to change to NORMAL.
loop-detect timer <0-86400>		Sets the interval of changing the state of a blocked port to NORMAL.. If you set the interval as 0, the state of the blocked port will not be changed automatically. (default: 600 seconds)
no loop-detect block		Disables the blocking option.

To set the interval of sending the loop-detecting packet, use the following command.

Command	Mode	Description
loop-detect period <1-60>	Interface [XE/GE/GPON/CG]	Sets the interval of sending the loop-detecting packet. (default: 30 seconds)

To display a current configuration of the loop detection, use the following command.

Command	Mode	Description
show loop-detect {**all** | **summary**}	Enable Global Interface [XE/GE/GPON/CG]	Shows the brief information of the loop detection.

⚠ The loop detection cannot operate with LACP.

9.6 Dynamic Host Configuration Protocol (DHCP)

Dynamic Host Configuration Protocol (DHCP) is a TCP/IP standard for simplifying the administrative management of IP address configuration by automating address configuration for network clients. The DHCP standard provides for the use of DHCP servers as a way to manage dynamic allocation of IP addresses and other relevant configuration details to DHCP-enabled clients on the network.

Every device on a TCP/IP network must have a unique IP address in order to access the network and its resources. The IP address (together with its relevant subnet mask) identifies both the host computer and the subnet to which it is attached. When you move a computer to a different subnet, the IP address must be changed. DHCP allows you to dynamically assign an IP address to a client from a DHCP server IP address database on the local network.

The DHCP provides the following benefits:

Saving Cost

Numerous users can access the IP network with a small amount of IP resources in the environment that most users do not have to access the IP network at the same time all day long. This allows the network administrators to save the cost and IP resources.

Efficient IP Management

By deploying DHCP in a network, this entire process is automated and centrally managed. The DHCP server maintains a pool of IP addresses and leases an address to any DHCP-enabled client when it logs on to the network. Because the IP addresses are dynamic (leased) rather than static (permanently assigned), addresses no longer in use are automatically returned to the pool for reallocation.

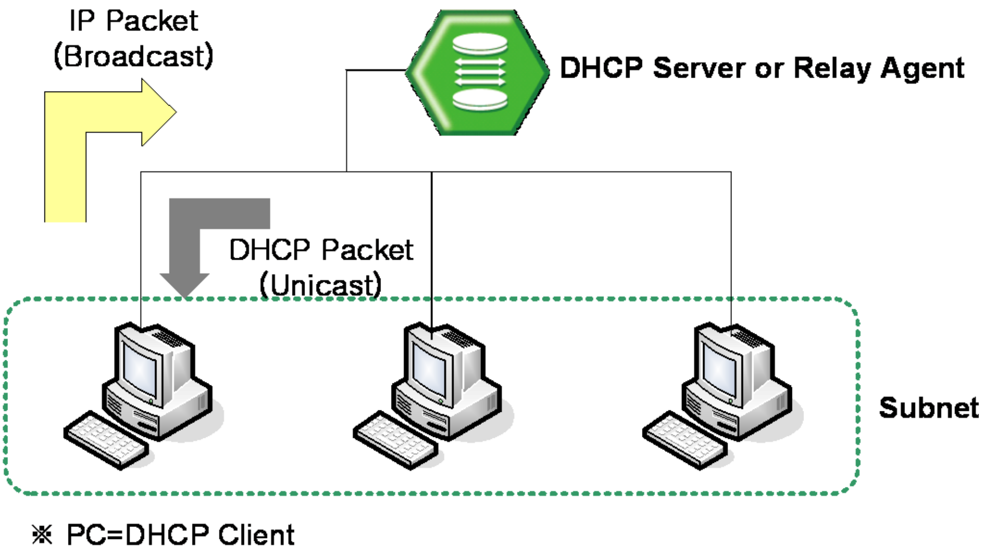


Fig. 9.36 DHCP Service Structure

The LD3032 flexibly provides the functions as the DHCP server or DHCP relay agent according to your DHCP configuration.

This chapter contains the following sections:

- DHCP Server
- DHCP Address Allocation with Option 82
- DHCP Lease Database
- DHCP Relay Agent
- DHCP Option
- DHCP Option 82
- DHCP Snooping
- IP Source Guard
- DHCP Client
- DHCP Filtering
- Debugging DHCP

9.6.1 DHCP Server

This section describes the following DHCP server-related features and configurations:

- DHCP Pool Creation
- DHCP Subnet
- Range of IP Address
- Default Gateway
- IP Lease Time
- DNS Server
- Manual Binding
- Domain Name
- DHCP Server Option
- Static Mapping
- Recognition of DHCP Client
- IP Address Validation
- Authorized ARP
- Prohibition of 1:N IP Address Assignment
- Ignoring BOOTP Request
- DHCP Packet Statistics
- Setting DHCP Pool Size
- Displaying DHCP Pool Configuration

To activate/deactivate the DHCP function in the system, use the following command.

Command	Mode	Description
service dhcp	Global	Activates the DHCP function in the system.
no service dhcp		Deactivates the DHCP function in the system.

i

Before configuring DHCP server or relay, you need to use the **service dhcp** command first to activate the DHCP function in the system.

9.6.1.1 DHCP Pool Creation

The DHCP pool is a group of IP addresses that will be assigned to DHCP clients by DHCP server. You can create various DHCP pools that can be configured with a different network, default gateway and range of IP addresses. This allows the network administrators to effectively handle multiple DHCP environments.

To create a DHCP pool, use the following command.

Command	Mode	Description
ip dhcp pool *POOL*	Global	Creates a DHCP pool and opens *DHCP Pool Configuration* mode.
no ip dhcp pool *POOL*		Deletes a created DHCP pool.

The following is an example of creating the DHCP pool as *sample*.

```
SWITCH(config)# service dhcp
SWITCH(config)# ip dhcp pool sample
SWITCH(config-dhcp[sample])#
```

9.6.1.2 DHCP Subnet

To specify a subnet of the DHCP pool, use the following command.

Command	Mode	Description
network *A.B.C.D/M*	DHCP Pool	Specifies a subnet of the DHCP pool. A.B.C.D/M: network address
no network *A.B.C.D/M*		Deletes a specified subnet.

The following is an example of specifying the subnet as 100.1.1.0/24.

```
SWITCH(config)# service dhcp
SWITCH(config)# ip dhcp pool sample
SWITCH(config-dhcp[sample])# network 100.1.1.0/24
SWITCH(config-dhcp[sample])#
```

You can also specify several subnets in a single DHCP pool.

9.6.1.3 Range of IP Address

To specify a range of IP addresses that will be assigned to DHCP clients, use the following command.

Command	Mode	Description
range *A.B.C.D A.B.C.D*	DHCP Pool	Specifies a range of IP addresses. A.B.C.D: start/end IP address
no range *A.B.C.D A.B.C.D*		Deletes a specified range of IP addresses.

The following is an example for specifying the range of IP addresses.

```
SWITCH(config)# service dhcp
SWITCH(config)# ip dhcp pool sample
SWITCH(config-dhcp[sample])# network 100.1.1.0/24
SWITCH(config-dhcp[sample])# default-router 100.1.1.254
SWITCH(config-dhcp[sample])# range 100.1.1.1 100.1.1.100
SWITCH(config-dhcp[sample])#
```

You can also specify several inconsecutive ranges of IP addresses in a single DHCP pool, e.g. 100.1.1.1 to 100.1.1.62 and 100.1.1.129 to 100.1.1.190.

When specifying a range of IP address, the start IP address must be prior to the end IP address.

9.6.1.4 Default Gateway

To specify a default gateway of the DHCP pool, use the following command.

Command	Mode	Description
default-router *A.B.C.D1* [*A.B.C.D2*] … [*A.B.C.D8*]	DHCP Pool	Specifies a default gateway of the DHCP pool. A.B.C.D: default gateway IP address
no default-router *A.B.C.D1* [*A.B.C.D2*] … [*A.B.C.D8*]		Deletes a specified default gateway.
no default-router all		Deletes all the specified default gateways.

The following is an example of specifying the default gateway 100.1.1.254.

```
SWITCH(config)# service dhcp
SWITCH(config)# ip dhcp pool sample
SWITCH(config-dhcp[sample])# network 100.1.1.0/24
SWITCH(config-dhcp[sample])# default-router 100.1.1.254
SWITCH(config-dhcp[sample])#
```

9.6.1.5 IP Lease Time

Basically, the DHCP server leases an IP address in the DHCP pool to DHCP clients, which will be automatically returned to the DHCP pool when it is no longer in use or expired by IP lease time.

To specify IP lease time, use the following command.

Command	Mode	Description
lease-time default <120-2147483637>	DHCP Pool	Sets default IP lease time in the unit of second. (default: 3600)
lease-time max <120-2147483637>		Sets maximum IP lease time in the unit of second. (default: 3600)
no lease-time {**default** | **max**}		Deletes specified IP lease time.

The following is an example of setting default and maximum IP lease time.

```
SWITCH(config)# service dhcp
SWITCH(config)# ip dhcp pool sample
SWITCH(config-dhcp[sample])# network 100.1.1.0/24
SWITCH(config-dhcp[sample])# default-router 100.1.1.254
SWITCH(config-dhcp[sample])# range 100.1.1.1 100.1.1.100
SWITCH(config-dhcp[sample])# lease-time default 5000
SWITCH(config-dhcp[sample])# lease-time max 10000
SWITCH(config-dhcp[sample])#
```

9.6.1.6 DNS Server

To specify a DNS server to inform DHCP clients, use the following command.

Command	Mode	Description
dns-server *A.B.C.D1* [*A.B.C.D2*] … [*A.B.C.D8*]	DHCP Pool	Specifies a DNS server. Up to 8 DNS servers are possible. A.B.C.D: DNS server IP address
no dns-server *A.B.C.D1* [*A.B.C.D2*] … [*A.B.C.D8*]		Deletes a specified DNS server.
no dns-server all		Deletes all the specified DNS servers.

The following is an example of specifying a DNS server.

```
SWITCH(config)# service dhcp
SWITCH(config)# ip dhcp pool sample
SWITCH(config-dhcp[sample])# network 100.1.1.0/24
SWITCH(config-dhcp[sample])# default-router 100.1.1.254
SWITCH(config-dhcp[sample])# range 100.1.1.1 100.1.1.100
SWITCH(config-dhcp[sample])# lease-time default 5000
SWITCH(config-dhcp[sample])# lease-time max 10000
SWITCH(config-dhcp[sample])# dns-server 200.1.1.1 200.1.1.2 200.1.1.3
SWITCH(config-dhcp[sample])#
```

i If you want to specify a DNS server for all the DHCP pools, use the **dns server** command.

9.6.1.7 Manual Binding

To manually assign a static IP address to a DHCP client who has a specified MAC address, use the following command.

Command	Mode	Description
fixed-address *A.B.C.D MAC-ADDR*	DHCP Pool	Assigns a static IP address to a DHCP client. A.B.C.D: static IP address MAC-ADDR: MAC address
no fixed-address *A.B.C.D*		Deletes a specified static IP assignment.

9.6.1.8 Domain Name

To set a domain name, use the following command.

Command	Mode	Description
domain-name *DOMAIN*	DHCP Pool	Sets a domain name.
no domain-name		Deletes a specified domain name.

9.6.1.9 DHCP Server Option

The switch operating DHCP server can include DHCP option information in the DHCP communication. Before using this function, a global DHCP option format should be created. For details of setting the DHCP option format, refer to the 9.6.5 DHCP Option.

To specify a DHCP server option, use the following command.

Command	Mode	Description
option code <1-254> **format** *NAME*	DHCP Pool	Specifies a DHCP option format for a DHCP server. code: DHCP option code NAME: DHCP option format name
no option code <1-254> **format**		Removes a specified DHCP option for a DHCP server.

DHCP server may not have any DHCP option that is configured in the DHCP pool mode. Then DHCP server finds the DHCP default option. If it exists, DHCP server sends DHCP clients a DHCP reply packet (Offer/ACK) with the default option information.

To specify a DHCP server default option, use the following command.

Command	Mode	Description
ip dhcp default-option code <1-254> **format** *NAME*	Global	Specifies a DHCP default option format for a DHCP server. code: DHCP option code NAME: DHCP option format name
no ip dhcp default-option code <1-254>		Removes a specified DHCP default option for a DHCP server.

9.6.1.10 Static Mapping

The LD3032 provides a static mapping function that enables to assign a static IP address without manually specifying static IP assignment by using a DHCP lease database in the DHCP database agent.

To perform a static mapping, use the following command.

Command	Mode	Description
origin file *A.B.C.D FILE*	DHCP Pool	Performs a static mapping. A.B.C.D: DHCP database agent address FILE: file name of DHCP lease database
no origin file		Cancels a static mapping.

i For more information of the file naming of a DHCP lease database, see Section 9.6.3.1.

9.6.1.11 Recognition of DHCP Client

Normally, a DHCP server is supposed to prohibit assigning an IP address when DHCP packets have no client ID (CID). However, some Linux clients may send DHCP discover messages without CID. To solve such a problem, the switch provides the additional option to verify a hardware address (MAC address) instead of CID.

To select a recognition method of DHCP clients, use the following command.

Command	Mode	Description
ip dhcp database-key {**client-id** | **hardware-address**}	Global	Selects a recognition method of DHCP clients

9.6.1.12 IP Address Validation

Before assigning an IP address to a DHCP client, a DHCP server will validate if the IP address is used by another DHCP client with a ping or ARP. If the IP address does not respond to a requested ping or ARP, the DHCP server will realize that the IP address is not used then will assign the IP address to the DHCP client.

To select an IP address validation method, use the following command.

Command	Mode	Description
ip dhcp validate {**arp** | **ping**}	Global	Selects an IP address validation method.

You can also set a validation value of how many responses and how long waiting (timeout) for the responses from an IP address for a requested ping or ARP when a DHCP server validates an IP address.

To set a validation value of how many responses from an IP address for a requested ping or ARP, use the following command.

Command	Mode	Description
ip dhcp {**arp** | **ping**} **packet** <0-20>	Global	Sets a validation value of how many responses. 0-20: response value (default: 2)

To set a validation value of timeout for the responses from an IP address for a requested ping or ARP, use the following command.

Command	Mode	Description
ip dhcp {**arp** | **ping**} **timeout** <100-5000>	Global	Sets a validation value of timeout for the responses in the unit of millisecond. 100-5000: timeout value (default: 500)

9.6.1.13 Authorized ARP

The authorized ARP is to limit the lease of IP addresses to authorized users. This feature enables a DHCP server to add ARP entries only for the IP addresses currently in lease referring to a DHCP lease table, discarding ARP responses from unauthorized users (e.g. an illegal use of a static IP address).

When this feature is running, dynamic ARP learning on an interface will be disabled, since DHCP is the only authorized component currently allowed to add ARP entries.

⚠ The authorized ARP is enabled only in a DHCP server.

To limit the lease of IP addresses to authorized users, use the following command.

Command	Mode	Description
ip dhcp authorized-arp start <120-2147483637> **timeout** <120-2147483637>	Global	Discards an ARP response from unauthorized user. start: starting time (default: 3600 sec) timeout: expire time
ip dhcp authorized-arp <120-2147483637>		Discards an ARP response from unauthorized user. 120-2147483637: expire time
no ip dhcp authorized-arp		Disables the authorized ARP function.

You can verify the valid and invalid list for the authorized ARP. The valid list includes the IP addresses currently in lease, while the invalid list includes the IP addresses that send ARP requests, but not in lease. Both lists include IP addresses of a DHCP pool, but the authorized ARP only allows the ARP response of the IP addresses in the valid list.

To display entries of the valid and invalid lists, use the following command.

Command	Mode	Description
show ip dhcp authorized-arp valid	Enable Global	Shows entries of the valid list.
show ip dhcp authorized-arp invalid		Shows entries of the invalid list.

To delete entries of the invalid list, use the following command.

Command	Mode	Description
clear ip dhcp authorized-arp invalid	Enable Global	Deletes entries of the invalid IP addresses.

9.6.1.14 Prohibition of 1:N IP Address Assignment

The DHCP server may assign plural IP addresses to a single DHCP client in case of plural DHCP requests from the DHCP client, which has the same hardware address. Some network devices may need plural IP addresses, but most DHCP clients like personal computers need only a single IP address. In this case, you can configure the LD3032 to prohibit assigning plural IP addresses to a single DHCP client.

To prohibit assigning plural IP addresses to a DHCP client, use the following command.

Command	Mode	Description
ip dhcp check client-hardware-address	Global	Prohibits assigning plural IP addresses.
no ip dhcp check client-hardware-address		Permits assigning plural IP addresses.

9.6.1.15 Ignoring BOOTP Request

To allow a DHCP server to ignore received bootstrap protocol (BOOTP) request packets, use the following command.

Command	Mode	Description
ip dhcp bootp ignore	Global	Ignores BOOTP request packets.
no ip dhcp bootp ignore		Permits BOOTP request packets.

9.6.1.16 DHCP Packet Statistics

To display DHCP packet statistics of the DHCP server, use the following command.

Command	Mode	Description
show ip dhcp server statistics	Enable Global	Shows DHCP packet statistics.
clear ip dhcp statistics		Deletes collected DHCP packet statistics.

9.6.1.17 Setting DHCP Pool Size

To limit a size of DHCP pool, use the following command.

Command	Mode	Description
ip dhcp max-pool-size <1-8>	Global	Configures a maximum size of DHCP pool.

9.6.1.18 Displaying DHCP Pool Configuration

To display a DHCP pool configuration, use the following command.

Command	Mode	Description
show ip dhcp pool [*POOL*]	Enable Global	Shows a DHCP pool configuration.
show ip dhcp pool summary [*POOL*]		Shows a summary of a DHCP pool configuration. POOL: pool name

9.6.2 DHCP Address Allocation with Option 82

The DHCP server provided by the LD3032 can assign dynamic IP addresses based on DHCP option 82 information sent by the DHCP relay agent.

The information sent via DHCP option 82 will be used to identify which port the DHCP_REQUEST came in on. The feature introduces a new DHCP class capability, which is a method to group DHCP clients based on some shared characteristics other than the subnet in which the clients reside. The DHCP class can be configured with option 82 information and a range of IP addresses.

9.6.2.1 DHCP Class Capability

To enable the DHCP server to use a DHCP class to assign IP addresses, use the following command.

Command	Mode	Description
ip dhcp use class	Global	Enables the DHCP server to use a DHCP class to assign IP addresses.
no ip dhcp use class		Disables the DHCP server to use a DHCP class.

9.6.2.2 DHCP Class Creation

To create a DHCP class, use the following command.

Command	Mode	Description
ip dhcp class *CLASS*	Global	Creates a DHCP class and opens *DHCP Class Configuration* mode. CLASS: DHCP class name
no ip dhcp class [*CLASS*]		Deletes a created DHCP class.

9.6.2.3 Relay Agent Information Pattern

To specify option 82 information for IP assignment, use the following command.

Command	Mode	Description
relay-information remote-id ip *A.B.C.D* [**circuit-id** {**hex** *HEXSTRING* | **index** <0-65535> | **text** *STRING*}]	DHCP Class	Specifies option 82 information for IP assignment.
relay-information remote-id hex *HEXSTRING* [**circuit-id** {**hex** *HEXSTRING* | **index** <0-65535> | **text** *STRING*}]		
relay-information remote-id text *STRING* [**circuit-id** {**hex** *HEXSTRING* | **index** <0-65535> | **text** *STRING*}]		

To delete specified option 82 information for IP assignment, use the following command.

Command	Mode	Description
no relay-information remote-id ip *A.B.C.D* [**circuit-id** {**hex** *HEXSTRING* | **index** <0-65535> | **text** *STRING*}]	DHCP Class	Deletes specified option 82 information for IP assignment.
no relay-information remote-id hex *HEXSTRING* [**circuit-id** {**hex** *HEXSTRING* | **index** <0-65535> | **text** *STRING*}]		
no relay-information remote-id text *STRING* [**circuit-id** {**hex** *HEXSTRING* | **index** <0-65535> | **text** *STRING*}]		

To delete specified option 82 information for IP assignment, use the following command.

Command	Mode	Description
no relay-information remote-id all	DHCP Class	Deletes all specified option 82 information that contains only a remote ID.
no relay-information all		Deletes all specified option 82 information.

9.6.2.4 Associating DHCP Class

To associate a DHCP class with a current DHCP pool, use the following command.

Command	Mode	Description
class *CLASS*	DHCP Pool	Associates a DHCP class with a DHCP pool and opens *DHCP Pool Class Configuration* mode. CLASS: DHCP class name
no class [*CLASS*]		Releases an associated DHCP class from a current DHCP pool.

9.6.2.5 Range of IP Address for DHCP Class

To specify a range of IP addresses for a DHCP class, use the following command.

Command	Mode	Description
address range *A.B.C.D A.B.C.D*	DHCP Pool Class	Specifies a range of IP addresses. A.B.C.D: start/end IP address
no address range *A.B.C.D A.B.C.D*		Deletes a specified range of IP addresses.

A range of IP addresses specified with the **address range** command is valid only for a current DHCP pool. Even if you associate the DHCP class with another DHCP pool, the specified range of IP addresses will not be applicable.

9.6.3 DHCP Lease Database

9.6.3.1 DHCP Database Agent

The LD3032 provides a feature that allows to a DHCP server automatically saves a DHCP lease database on a DHCP database agent.

The DHCP database agent should be a TFTP server, which stores a DHCP lease database as numerous files in the form of **leasedb.***MAC-ADDRESS*, e.g. **leasedb.***0A:31:4B:1 A:77:6A*. The DHCP lease database contains a leased IP address, hardware address, etc.

To specify a DHCP database agent and enable an automatic DHCP lease database backup, use the following command.

Command	Mode	Description
ip dhcp database *A.B.C.D INTERVAL*	Global	Specifies a DHCP database agent and back-up interval. A.B.C.D: DHCP database agent address INTERVAL: 120-2147483637 (unit: second)
no ip dhcp database		Deletes a specified DHCP database agent.

i Upon entering the **ip dhcp database** command, the back-up interval will begin.

To display a configuration of the DHCP database agent, use the following command.

Command	Mode	Description
show ip dhcp database	Enable Global	Shows a configuration of the DHCP database agent.

9.6.3.2 Displaying DHCP Lease Status

To display current DHCP lease status, use the following command.

Command	Mode	Description
show ip dhcp lease {**all** | **bound** | **abandon** | **offer** | **fixed** | **free**} [*POOL*]	Enable Global	Shows current DHCP lease status. all: all IP addresses bound: assigned IP address abandon: illegally assigned IP address offer: IP address being ready to be assigned fixed: manually assigned IP address free: remaining IP address POOL: pool name
show ip dhcp lease detail [*A.B.C.D*]		

9.6.3.3 Deleting DHCP Lease Database

To delete a DHCP lease database, use the following command.

Command	Mode	Description
clear ip dhcp leasedb *A.B.C.D/M*	Enable Global	Deletes a DHCP lease database a specified subnet.
clear ip dhcp leasedb pool *POOL*		Deletes a DHCP lease database of a specified DHCP pool.
clear ip dhcp leasedb all		Deletes the entire DHCP lease database.

9.6.4 DHCP Relay Agent

A DHCP relay agent is any host that forwards DHCP packets between clients and servers. The DHCP relay agents are used to forward DHCP requests and replies between clients and servers when they are not on the same physical subnet. The DHCP relay agent forwarding is distinct from the normal forwarding of an IP router, where IP datagrams are switched between networks somewhat transparently.

By contrast, DHCP relay agents receive DHCP messages and then generate a new DHCP message to send out on another interface. The DHCP relay agent sets the gateway address and, if configured, adds the DHCP option 82 information in the packet and forwards it to the DHCP server. The reply from the server is forwarded back to the client after removing the DHCP option 82 information.

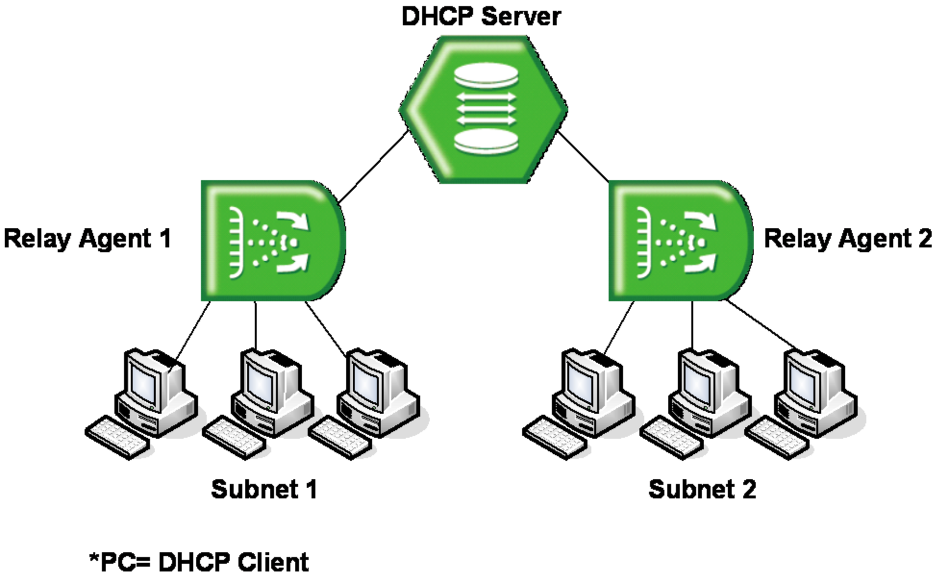


Fig. 9.37 Example of DHCP Relay Agent

To activate/deactivate the DHCP function in the system, use the following command.

Command	Mode	Description
service dhcp	Global	Activates the DHCP function in the system.
no service dhcp		Deactivates the DHCP function in the system.

Before configuring DHCP server or relay, you need to use the **service dhcp** command first to activate the DHCP function in the system.

9.6.4.1 DHCP Helper Address

A DHCP client sends DHCP_DISCOVER message to a DHCP server. DHCP_DISCOVER message is broadcasted within the network to which it is attached. If the client is on a network that does not have any DHCP server, the broadcast is not forwarded because the switch is configured to not forward broadcast traffic. To solve this problem, you can configure the interface that is receiving the broadcasts to forward certain classes of broadcast to a helper address.

To specify a DHCP helper address, use the following command.

Command	Mode	Description
ip dhcp helper-address *A.B.C.D*	Interface [VLAN]	Specifies a DHCP helper address. More than one address is possible. A.B.C.D: DHCP server address
no ip dhcp helper-address {*A.B.C.D* | **all**}		Deletes a specified packet forwarding address.

If a DHCP helper address is specified on an interface, the LD3032 will enable a DHCP relay agent.

You can also specify an organizationally unique identifier (OUI) when configuring a DHCP helper address. The OUI is a 24-bit number assigned to a company or organization for use in various network hardware products, which is a first 24 bits of a MAC address. If an OUI is specified, a DHCP relay agent will forward DHCP_DISCOVER message to a specific DHCP server according to a specified OUI.

To specify a DHCP helper address with an OUI, use the following command.

Command	Mode	Description
ip dhcp oui *XX:XX:XX* **helper-address** *A.B.C.D*	Interface [VLAN]	Specifies a DHCP helper address with an OUI. More than one address is possible. XX:XX:XX: OUI (first 24 bits of a MAC address in the form of hexadecimal) A.B.C.D: DHCP server address
no ip dhcp oui *XX:XX:XX* [**helper-address** *A.B.C.D*]		Deletes a specified DHCP helper address.

9.6.4.2 Smart Relay Agent Forwarding

Normally, a DHCP relay agent forwards DHCP_DISCOVER message to a DHCP server only with a primary IP address on an interface, even if there is more than one IP address on the interface.

If the smart relay agent forwarding is enabled, a DHCP relay agent will retry sending DHCP_DISCOVER message with a secondary IP address, in case of no response from the DHCP server.

To enable the smart relay agent forwarding, use the following command.

Command	Mode	Description
ip dhcp smart-relay	Global	Enables a smart relay.
no ip dhcp smart-relay		Disables a smart relay.

9.6.4.3 DHCP Relay Agent Configuration

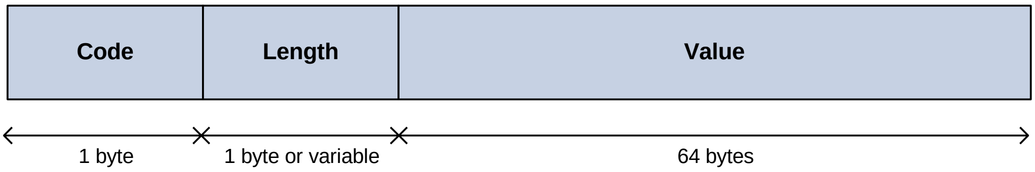
To display the information of DHCP relay related configuration, use the following command.

Command	Mode	Description
show ip dhcp relay	Enable Global	Shows DHCP relay configurations.

9.6.5 DHCP Option

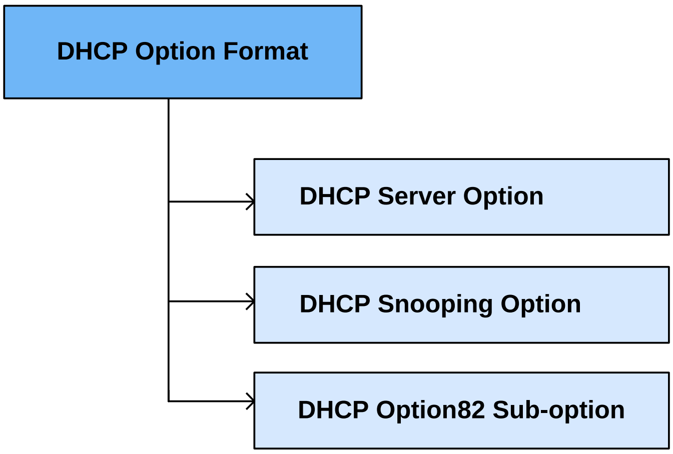
This function enables administrators to define DHCP options that are carried in the DHCP communication between DHCP server and client or relay agent. The following indicates the format of the DHCP options field.

DHCP Option Format



A code identifies each DHCP option. It can be expressed in value 0 to 255 by user configuration and some of them are predefined in the standards. (128 ~ 254 is site specific) A length can be variable according to value or can be fixed. A value contains actual information such an IP address, string, or index, which is inserted into the DHCP packet.

Administrators can configure a DHCP option format in *DHCP Option* mode, which is globally used over the DHCP functions. The DHCP option format can be applied in other DHCP software modules and the following figure indicates it.



9.6.5.1 Entering DHCP Option Mode

To enter the DHCP option mode, use the following command.

Command	Mode	Description
ip dhcp option format *NAME*	Global	Enters the DHCP option mode. NAME: DHCP option format name

9.6.5.2 Configuring DHCP Option Format

To configure a DHCP option format, use the following command.

Command	Mode	Description
attr <1-32> **type** <0-255> **length** {<1-64> | **variable**} **value** {**hex** | **index** | **if_ip** | **ip** | **string**} *VALUE*	DHCP Option	Sets the type, length, and value of an attribute for a DHCP option. attr: They can be made in a DHCP option and are applied in order of attribute value (1-32). type: The type of a value length: The length of a value. It could be a fixed length by user input or a variable length according to the actual value length. value: The actual value of an option
attr <1-32> **type** <0-255> **length-hidden** {<1-64> | **variable**} **value** {**hex** | **index** | **if_ip** | **ip** | **string**} *VALUE*		
attr <1-32> **length variable value** {**hex** | **index** | **if_ip** | **ip** | **string**} *VALUE*		Sets the length and value of an attribute for a DHCP option.
attr <1-32> **length** <1-64> **value** {**hex** | **index** | **if_ip** | **ip** | **string**} *VALUE*		
attr <1-32> **length-hidden variable value** {**hex** | **index** | **if_ip** | **ip** | **string**} *VALUE*		Sets the value of an attribute for a DHCP option.
attr <1-32> **length-hidden** <1-64> **value** {**hex** | **index** | **if_ip** |**ip** | **string**} *VALUE*		
no attr <1-32>		Deletes the given attribute.

i

The packets can be mapped to the option format string that defined by variable values with special character (%).

%FRAME: frame (chassis) number for receiving DHCP packets
%SLOT: slot number for receiving DHCP packets
%PORT: index port ID. If the switch is 4-slot chassis and associated 4-port modules, there are 16 index port IDs. In case the index port ID is 5, its slot number is 2 and physical port number is 1 (Port number = 2/1).
%IN_IF_IP: input interface IP address
%VID: VLAN ID tagged on packets
%CPU-MAC: system MAC address
%ONU-ID: ONU IP address
%ONU_DESC: ONU description written by administrator
%ONU_PORT_NUM: ONU port number
%REAL_PORT: real port
%ONU_PORT_DESCRIPTION: ONU port description written by administrator
%ONU_SERIAL_NUM: ONU serial number

⚠

The DHCP option format has the following restrictions;
- The value should be within 64 bytes.
- A hidden-length variable should be set once in a single attribute.
- The total length of an option format cannot exceed 254 bytes.

9.6.5.3 Deleting DHCP Option Format

To delete a specified DHCP option format, use the following command.

Command	Mode	Description
no ip dhcp option format *NAME*	Global	Deletes the given DHCP option format.

9.6.5.4 Displaying DHCP option

To print a specified DHCP option format, use the following command.

Command	Mode	Description
show ip dhcp option format *NAME* [**interface** {**gigabitethernet** | **tengigabitethernet** | **gpon** | **channelgroup**} *IFPORT* **vlan** *VLANS*]	Enable Global DHCP Option	Prints the given option format and actual raw data in the packet.

9.6.6 DHCP Option 82

In some networks, it is necessary to use additional information to further determine which IP addresses to allocate. By using the DHCP option 82, a DHCP relay agent can include additional information about itself when forwarding client-originated DHCP packets to a DHCP server. The DHCP relay agent will automatically add the circuit ID and the remote ID to the option 82 field in the DHCP packets and forward them to the DHCP server.

The DHCP option 82 resolves the following issues in an environment in which untrusted hosts access the internet via a circuit based public network:

Broadcast Forwarding

The DHCP option 82 allows a DHCP relay agent to reduce unnecessary broadcast flooding by forwarding the normally broadcasted DHCP response only on the circuit indicated in the circuit ID.

DHCP Address Exhaustion

In general, a DHCP server may be extended to maintain a DHCP lease database with an IP address, hardware address and remote ID. The DHCP server should implement policies that restrict the number of IP addresses to be assigned to a single remote ID.

Static Assignment

A DHCP server may use the remote ID to select the IP address to be assigned. It may permit static assignment of IP addresses to particular remote IDs, and disallow an address request from an unauthorized remote ID.

IP Spoofing

A DHCP client may associate the IP address assigned by a DHCP server in a forwarded DHCP_ACK message with the circuit to which it was forwarded. The circuit access device may prevent forwarding of IP packets with source IP addresses, other than, those it has associated with the receiving circuit. This prevents simple IP spoofing attacks on the central LAN, and IP spoofing of other hosts.

MAC Address Spoofing

By associating a MAC address with a remote ID, a DHCP server can prevent offering an IP address to an attacker spoofing the same MAC address on a different remote ID.

Client Identifier Spoofing

By using the agent-supplied remote ID option, the untrusted and as-yet unstandardized client identifier field need not be used by the DHCP server.

Fig. 9.38 shows how the DHCP relay agent with the DHCP option 82 operates.

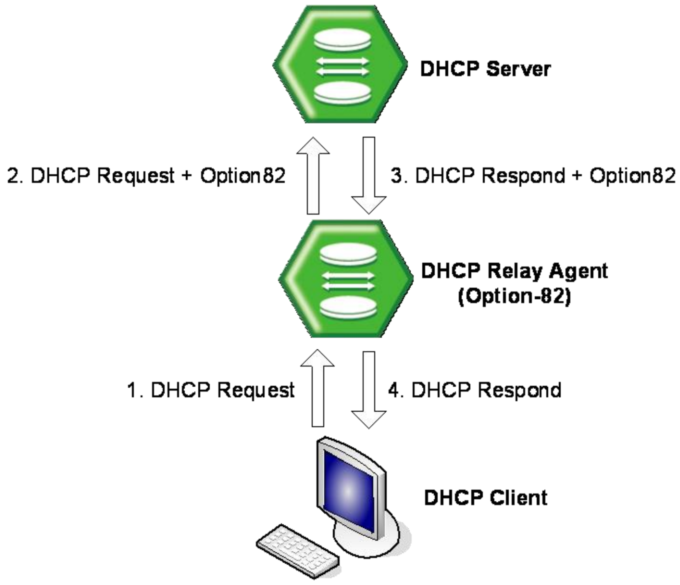


Fig. 9.38 DHCP Option 82 Operation

9.6.6.1 Enabling DHCP Option 82

To enable/disable the DHCP option 82, use the following command.

Command	Mode	Description
ip dhcp option82	Global	Enables the system to add the DHCP option 82 field.
no ip dhcp option82		Disables the system to add the DHCP option 82 field.

9.6.6.2 Option 82 Sub-Option

The DHCP option 82 enables a DHCP relay agent to include information about itself when forwarding client-originated DHCP packets to a DHCP server. The DHCP server can use this information to implement security and IP address assignment policies.

There are 2 sub-options for the DHCP option 82 information as follows:

- **Remote ID**
  This sub-option may be added by DHCP relay agents which terminate switched or permanent circuits and have mechanisms to identify the remote host of the circuit. Note that, the remote ID must be globally unique.

- **Circuit ID**
  This sub-option may be added by DHCP relay agents which terminate switched or permanent circuits. It encodes an agent-local identifier of the circuit from which a DHCP client-to-server packet was received. It is intended for use by DHCP relay agents in forwarding DHCP responses back to the proper circuit.

To specify a remote ID, use the following command.

Command	Mode	Description
system-remote-id hex *HEXSTRING*	Option 82	Specifies a remote ID. (default: system MAC address)
system-remote-id ip *A.B.C.D*		
system-remote-id text *STRING*		
system-remote-id option format *NAME*		

To specify a circuit ID, use the following command.

Command	Mode	Description
system-circuit-id hex *HEXSTRING*	Interface [XE/GE/ GPON]	Specifies a circuit ID. (default: port number)
system-circuit-id index <0-65535>		
system-circuit-id text *STRING*		
system-circuit-id option format *NAME*		
system-circuit-id port-type physical	Option 82	

To delete a specified remote and circuit ID, use the following command.

Command	Mode	Description
no system-remote-id	Option 82	Deletes a specified remote and circuit ID
no system-remote-id option format		
no system-circuit-id port-type physical		
no system-circuit-id [**option format**]	Interface [XE/GE/]	

9.6.6.3 Option 82 Reforwarding Policy

A DHCP relay agent may receive a DHCP packet from a DHCP server or another DHCP relay agent that already contains relay information. You can specify a DHCP option 82 reforwarding policy to be suitable for the network. To specify a DHCP option 82 reforwarding policy, use the following command.

Command	Mode	Description
policy {**replace** | **keep**}	Option 82	Specifies a DHCP option 82 reforwarding policy. replace: replaces an existing DHCP option 82 information with a new one. keep: keeps an existing DHCP option 82 information (default). normal: DHCP packet option82: DHCP option 82 packet none: no DHCP packet (default)
policy drop {**normal** | **option82** | **none**}		

9.6.6.4 Option 82 Trust Policy

Default Trust Policy

To specify the default trust policy for DHCP packets, use the following command.

Command	Mode	Description
trust default {**deny** | **permit**}	Option 82	Specifies the default trust policy for a DHCP packet.

ℹ If you specify the default trust policy as **deny**, the DHCP packet that carries the information you specifies below will be permitted, and vice versa.

Trusted Remote ID

To specify a trusted remote ID, use the following command.

Command	Mode	Description
trust remote-id hex *HEXSTRING*	Option 82	Specifies a trusted remote ID.
trust remote-id ip *A.B.C.D*		
trust remote-id text *STRING*		

To delete a specified trusted remote ID, use the following command.

Command	Mode	Description
no trust remote-id [**hex** *HEXSTRING*]	Option 82	Deletes a specified trusted remote ID.
no trust remote-id [**ip** *A.B.C.D*]		
no trust remote-id [**text** *STRING*]		

Trusted Physical Interface

To specify a trusted physical interface, use the following command.

Command	Mode	Description
trust interface {**normal** | **option82** | **all**}	Interface [XE/GE/GPON/CG]	Specifies a trusted physical interface. normal: DHCP packet option82: DHCP option 82 packet all: DHCP + option 82 packet
no trust interface {**normal** | **option82** | **all**}		Deletes a specified trusted interface.

9.6.6.5 Appending Enterprise Number

To add enterprise-number vlaue into dhcp option82, use the following command.

Command	Mode	Description
policy append enterprise-number <1-4294967295>	Option 82	Specifies the enterprise-number value.

9.6.7 DHCP Snooping

For enhanced security, the LD3032 provides the DHCP snooping feature. The DHCP snooping filters untrusted DHCP messages and builds/maintains a DHCP snooping binding table. The untrusted DHCP message is a message received from outside the network, and an untrusted interface is an interface configured to receive DHCP messages from outside the network.

The DHCP snooping basically permits all the trusted messages received from within the network and filters untrusted messages. In case of untrusted messages, all the binding entries are recorded in a DHCP snooping binding table. This table contains a hardware address, IP address, lease time, VLAN ID, interface, etc.

It also gives you a way to differentiate between untrusted interfaces connected to the end-user and trusted interfaces connected to the DHCP server or another switch.

The DHCP snooping only filters the DHCP server message such as a DHCP_OFFER or DHCP_ACK, which is received from untrusted interfaces.

9.6.7.1 Enabling DHCP Snooping

To enable the DHCP snooping globally, use the following command

Command	Mode	Description
ip dhcp snooping	Global	Enables the DHCP snooping globally.
no ip dhcp snooping		Disables the DHCP snooping globally. (default)

Upon enabling the DHCP snooping, the DHCP_OFFER and DHCP_ACK messages from all the ports will be discarded before specifying a trusted port.

To enable/disable the DHCP snooping on a VLAN/Interface, use the following command

Command	Mode	Description
ip dhcp snooping	Interface [VLAN/XE/GE/GPON/CG]	Enables the DHCP snooping on a specified VLAN/interface.
no ip dhcp snooping		Disables the DHCP snooping on a specified VLAN/interface.

You must enable DHCP snooping globally before enabling DHCP snooping on a VLAN.

9.6.7.2 DHCP Trust State

To define a state of a port as trusted or untrusted, use the following command.

Command	Mode	Description
ip dhcp snooping trust	Interface [XE/GE/	Defines a state of a specified port as trusted.
no ip dhcp snooping trust		Defines a state of a specified port as untrust-

	GPON/CG]	ed.(default)

9.6.7.3 DHCP Filter on Trust Port

To filter broadcast request packets outgoing from the specified trust port, use the following command.

Command	Mode	Description
ip dhcp snooping trust filter egress bcast-req	Interface [XE/GE/ GPON/CG]	Filters egress broadcast request packets on the trust port.
no ip dhcp snooping trust filter egress bcast-req		Disable filtering egress broadcast request packets on the trust port.

9.6.7.4 DHCP Rate Limit

To set the number of DHCP packets per second (pps) that an interface can receive, use the following command.

Command	Mode	Description
ip dhcp snooping limit-rate {**discover** | **request**} <1-32767>	Global	Sets a rate limit of DHCP dicover/request packets. (unit: pps)
no ip dhcp snooping limit-rate {**discover** | **request**}		Deletes a rate limit for DHCP packets.

i

Normally, the DHCP rate limit is specified to untrusted interfaces and 15 pps is recommended for a proper value. If, however, you want to set a rate limit for trusted interfaces, keep in mind that trusted interfaces aggregate all DHCP traffic in the switch, and you will need to adjust the rate limit to a higher value.

To set the number of DHCP packets per second (pps) that an interface can receive, use the following command.

Command	Mode	Description
ip dhcp snooping limit-rate <1-255>	Interface [XE/GE/ GPON/CG]	Sets a rate limit of DHCP packets. 1-255: the number of DHCP packets per second
no ip dhcp snooping limit-rate		Disable the discover message limit function.

9.6.7.5 DHCP Lease Limit

The number of entry registrations in DHCP snooping binding table can be limited. If there are too many DHCP clients on an interface and they request IP address at the same time, it may cause IP pool exhaustion.

To set the number of entry registrations in DHCP snooping binding table, use the following command.

Command	Mode	Description
ip dhcp snooping limit-lease <1-	Interface [XE/GE/	Enables a DHCP lease limit on a specified untrusted port.

2147483637>	GPON/CG]	1-2147483637: the number of entry registrations
no ip dhcp snooping limit-lease		Deletes a DHCP lease limit.

⚠ You can limit the number of entry registrations only for untrusted interfaces, because the DHCP snooping binding table only contains the information for DHCP messages from untrusted interfaces.

9.6.7.6 Source MAC Address Verification

The LD3032 can verify that the source MAC address in a DHCP packet that is received on untrusted ports matches the client hardware address in the packet.

To enable the source MAC address verification, use the following command.

Command	Mode	Description
ip dhcp snooping verify mac-address	Global	Enables the source MAC address verification.
no ip dhcp snooping verify mac-address		Disables the source MAC address verification.

9.6.7.7 Static DHCP Snooping Binding

The DHCP snooping binding table contains a hardware address, IP address, lease time, VLAN ID, and port information that correspond to the untrusted interfaces of the system.

To manually specify a DHCP snooping binding entry, use the following command.

Command	Mode	Description
ip dhcp snooping binding <1-4094> *A.B.C.D MAC-ADDR* <120-2147483637>	Interface [XE/GE/ GPON/CG]	Configures binding on DHCP snooping table. 1-4094: VLAN ID A.B.C.D: IP address MAC-ADDR: MAC address 120-2147483637: lease time (unit: second)
clear ip dhcp snooping binding {*A.B.C.D* | **all**}		Deletes a specified static DHCP snooping binding. all: all DHCP snooping bindings

9.6.7.8 DHCP Snooping Database Agent

When DHCP snooping is enabled, the system uses the DHCP snooping binding database to store information about untrusted interfaces. Each database entry (binding) has an IP address, associated MAC address, lease time, interface to which the binding applies and VLAN to which the interface belongs.

To maintain the binding when reload the system, you must use DHCP snooping database agent. If the agent is not used, the DHCP snooping binding will be lost when the switch is rebooted. The mechanism for the database agent saves the binding in a file at a remote location. Upon reloading, the switch reads the file to build the database for the binding. The system keeps the current file by writing to the file as the database changes.

To specify a DHCP database agent and enable an automatic DHCP snooping database back-up, use the following command.

Command	Mode	Description
ip dhcp snooping database *A.B.C.D INTERVAL*	Global	Specifies a DHCP snooping database agent and back-up interval. A.B.C.D: DHCP snooping database agent address INTERVAL: 120-2147483637 (unit: second)
no ip dhcp snooping database		Deletes a specified DHCP snooping database agent.

To request snooping binding entries from a DHCP snooping database agent, use the following command.

Command	Mode	Description
ip dhcp snooping database re-new *A.B.C.D*	Global	Requests snooping binding entries from a DHCP snooping database agent. A.B.C.D: DHCP snooping database agent address

i

The DHCP snooping database agent should be TFTP server.

9.6.7.9 ARP Inspection Start Time

This function sets the time before ARP inspection starts to run. Before setting this, ARP inspection should be turned on. ARP inspection checks validity of incoming ARP packets by using DHCP snooping binding table and denies the ARP packets if they are not identified in the table.

However, the LD3032 may be rebooted with any reason, then DHCP snooping binding table entries, which are dynamically learned from DHCP packets back and forth the LD3032, would be lost. Thus, ARP inspection should be delayed to start during some time so that DHCP snooping table can build entries. If no time given, ARP inspection sees empty snooping table and drop every ARP packet.

To specify the ARP inspection delay time, use the following command.

Command	Mode	Description
ip dhcp snooping arp-inspection start <1-2147483637>	Global	Configures the ARP inspection delay time. If reboot, ARP inspection resumes after the time you configure. 1-2147483637: delay time (unit: second)
no ip dhcp snooping arp-inspection start		Delete the configured ARP inspection delay time.

9.6.7.10 DHCP Snooping with Option82

In case of L2 environment, when forwarding DHCP messages to a DHCP server, a DHCP switch can insert or remove DHCP option82 data on the DHCP messages from the clients.

In case of a switch is enabled with DHCP snooping, it floods DHCP packets with DHCP option82 field when the DHCP option82 is enabled. This allows an enhanced security and efficient IP assignment in the Layer 2 environment with a DHCP option82 field.

i If DHCP snooping is enabled in the system of LD3032, DHCP packets includes DHCP option82 field by default.

To enable/disable the switch which is enabled by DHCP snooping to insert or remove DHCP option82 field, use the following command.

Command	Mode	Description
ip dhcp snooping information option	Global	Enables the switch to insert DHCP option 82 field in forwarded DHCP packets to the DHCP server.
no ip dhcp snooping information option		Disables the switch not to insert DHCP option 82 field in forwarded DHCP packets to the DHCP server

9.6.7.11 DHCP Snooping Option

DHCP snooping switch may receive DHCP messages (Discover/Request) with various different options from clients, which cause DHCP server hard to manage client's information in the perspective of data consistency. That's why this function is necessary.

The switch operating DHCP snooping can modify or attach an option field of the DHCP messages (Discover/Request) with a defined snooping option and can forward them to DHCP server. The snooping option can be applied on a port basis or on entire ports. Before using this function, a global DHCP option format should be created. For details of setting the DHCP option format, refer to the 9.6.5 DHCP Option.

To set a DHCP snooping option for a specific port, use the following command.

Command	Mode	Description
ip dhcp snooping opt-code <1-254> **format** *NAME*	Interface [XE/GE/GPON/CG]	Specifies a snooping option format on a port. opt-code: DHCP option code NAME: DHCP option format name
ip dhcp snooping opt-code <1-254> **policy** {**keep** | **replace**}		Configures a policy against DHCP option belonging to a DHCP message (default: replace) keep: forwards a DHCP message to DHCP server without any modification. replace: deletes the DHCP message's option and adds the snooping option if both of them are same. However, if they are different each other, **replace** option just adds the snooping option.
no ip dhcp snooping opt-code <1-254>		Removes the DHCP snooping option for a given port.

In case there is not a DHCP snooping option for a specific port, DHCP snooping switch finds the snooping default option. If it exists, DHCP snooping switch sends a DHCP server DHCP messages (Discover/Request) by replacing their options with the snooping default option.

To specify a DHCP server default option, use the following command.

Command	Mode	Description
ip dhcp snooping default-option code <1-254> **format** *NAME*	Global	Specifies a snooping default option format for a switch. NAME: DHCP option format name
ip dhcp snooping default-option code <1-254> **policy** <**keep** | **replace**>		Configures a policy against DHCP option belonging to a DHCP message (default: replace) keep: forwards a DHCP message to DHCP server without any modification. replace: deletes the DHCP message's option and adds the snooping default option if both of them are same. However, if they are different each other, **replace** option just adds the snooping default option.
no ip dhcp snooping default-option code <1-254>		Removes the DHCP snooping default option for a given port.

9.6.7.12 Displaying DHCP Snooping Configuration

To display DHCP snooping table, use the following command.

Command	Mode	Description
show ip dhcp snooping	Enable Global	Shows DHCP snooping configuration.
show ip dhcp snooping binding		Shows DHCP snooping binding entries.
show ip dhcp snooping binding total-cnt interface {**management** | **vlan** *VLANS* | **loopback** | **gigabitethernet** *IFPORT* | **tengigabitethernet** *IFPORT* | **gpon** *IFPORT* | **channelgroup** *GROUP*}		Shows the total count of DHCP snooping binding entries for the specified interface.

9.6.8 IP Source Guard

IP source guard is similar to DHCP snooping. This function is used on DHCP snooping untrusted Layer 2 port. Basically, except for DHCP packets that are allowed by DHCP snooping process, all IP traffic comes into a port is blocked. If an authorized IP address from the DHCP server is assigned to a DHCP client, or if a static IP source binding is configured, the IP source guard restricts the IP traffic of client to those source IP addresses configured in the binding; any IP traffic with a source IP address other than that in the IP source binding will be filtered out. This filtering limits a host's ability to attack the network by claiming a neighbor host's IP address.

IP source guard supports the Layer 2 port only, including both access and trunk. For each untrusted Layer 2 port, there are two levels of IP traffic security filtering:

- **Source IP Address Filter**
IP traffic is filtered based on its source IP address. Only IP traffic with a source IP address that matches the IP source binding entry is permitted. An IP source address filter is changed when a new IP source entry binding is created or deleted on the port, which will be recalculated and reapplied in the hardware to reflect the IP source binding change. By default, if the IP filter is enabled without any IP source binding on the port, a default policy that denies all IP traffic is applied to the port. Similarly, when the IP filter is disabled, any IP source filter policy will be removed from the interface.
- **Source IP and MAC Address Filter**
IP traffic is filtered based on its source IP address as well as its MAC address; only IP traffic with source IP and MAC addresses matching the IP source binding entry are permitted. When IP source guard is enabled in IP and MAC filtering mode, the DHCP snooping option 82 must be enabled to ensure that the DHCP protocol works properly. Without option 82 data, the switch cannot locate the client host port to forward the DHCP server reply. Instead, the DHCP server reply is dropped, and the client cannot obtain an IP address.

9.6.8.1 Enabling IP Source Guard

After configuring DHCP snooping, configure the IP source guard using the provided command. When IP source guard is enabled with this option, IP traffic is filtered based on the source IP address. The switch forwards IP traffic when the source IP address matches an entry in the DHCP snooping binding database or a binding in the IP source binding table.

To enable IP source guard, DHCP snooping needs to be enabled.

To enable IP source guard with a source IP address filtering on a port, use the following command.

Command	Mode	Description
ip dhcp verify source	Interface [XE/GE/GPON/CG]	Enables IP source guard with a source IP address filtering on a port.
no ip dhcp verify source		Disables IP source guard.

Note that the IP source guard is only enabled on DHCP snooping untrusted Layer 2 port! If you try to enable this function on a trusted port, the error message will be shown up.

9.6.8.2 Static IP Source Binding

The IP source binding table has bindings that are learned by DHCP snooping or manually specified with the **ip dhcp verify source binding** command. The switch uses the IP source binding table only when IP source guard is enabled.

To specify a static IP source binding entry, use the following command.

Command	Mode	Description
ip dhcp verify source binding <1-4094> *A.B.C.D MAC-ADDR*	Interface [XE/GE/GPON/CG]	Specifies a static IP source binding entry. 1-4094: VLAN ID A.B.C.D: IP address

		MAC-ADDR: MAC address
no ip dhcp verify source binding {*A.B.C.D* | **all**}		Deletes a specified static IP source binding.

9.6.8.3 Displaying IP Source Guard Configuration

To display IP source binding table, use the following command.

Command	Mode	Description
show ip dhcp verify source binding	Enable Global	Shows IP source binding entries.

9.6.9 DHCP Client

An interface of the LD3032 can be configured as a DHCP client, which can obtain an IP address from a DHCP server. The configurable DHCP client functionality allows a DHCP client to use a user-specified client ID, class ID or suggested lease time when requesting an IP address from a DHCP server. Once configured as a DHCP client, the LD3032 cannot be configured as a DHCP server or relay agent.

9.6.9.1 Enabling DHCP Client

To configure an interface as a DHCP client, use the following command.

Command	Mode	Description
ip address dhcp	Interface [MGMT/VLAN]	Enables a DHCP client on an interface.
no ip address dhcp		Disables a DHCP client.

9.6.9.2 DHCP Client ID

To specify a client ID, use the following command.

Command	Mode	Description
ip dhcp client client-id hex *HEXSTRING*	Interface [VLAN]	Specifies a client ID.
ip dhcp client client-id text *STRING*		
no ip dhcp client client-id		Deletes a specified client ID.

9.6.9.3 DHCP Class ID

To specify a class ID, use the following command.

Command	Mode	Description
ip dhcp client class-id hex *HEXSTRING*	Interface [VLAN]	Specifies a class ID. (default: system MAC address)
ip dhcp client class-id text *STRING*		
no ip dhcp client class-id		Deletes a specified class ID.

9.6.9.4 Host Name

To specify a host name, use the following command.

Command	Mode	Description
ip dhcp client host-name *NAME*	Interface [VLAN]	Specifies a host name.
no ip dhcp client host-name		Deletes a specified host name.

9.6.9.5 IP Lease Time

To specify IP lease time that is requested to a DHCP server, use the following command.

Command	Mode	Description
ip dhcp client lease-time <120-2147483637>	Interface [VLAN]	Specifies IP lease time in the unit of second (default: 3600).
no ip dhcp client lease-time		Deletes a specified IP lease time.

9.6.9.6 Requesting Option

To configure a DHCP client to request an option from a DHCP server, use the following command.

Command	Mode	Description
ip dhcp client request {**domain-name** | **dns**}	Interface [VLAN]	Configures a DHCP client to request a specified option.

To configure a DHCP client not to request an option, use the following command.

Command	Mode	Description
no ip dhcp client request {**domain-name** | **dns**}	Interface [VLAN]	Configures a DHCP client not to request a specified option.

9.6.9.7 Forcing Release or Renewal of DHCP Lease

The LD3032 supports two independent operation: immediate release a DHCP lease for a DHCP client and force DHCP renewal of a lease for a DHCP client. To force a release or renewal of a DHCP release for a DHCP client, use the following command.

Command	Mode	Description
release dhcp *INTERFACE*	Enable	Forces a release of a DHCP lease.
renew dhcp *INTERFACE*		Forces a renewal of a DHCP lease.

9.6.9.8 Displaying DHCP Client Configuration

To display a DHCP client configuration, use the following command.

Command	Mode	Description

show ip dhcp client [*INTERFACE*]	Enable Global Interface	Shows a configuration of DHCP client.

9.6.10 DHCP Filtering

9.6.10.1 DHCP Packet Filtering

For the LD3032, it is possible to block the specific client with MAC address. If the MAC address blocked by administrator requests an IP address, the server does not assign IP. This function is to strength the security of DHCP server. The following is the function of blocking to assign IP address on a port.

Command	Mode	Description
ip dhcp filter-interface	Interface [VLAN]	Configures a port in order not to assign IP.
no ip dhcp filter-interface		Disables DHCP packet filtering.

The following is to designate MAC address which IP address is not assigned.

Command	Mode	Description
ip dhcp filter-address *MAC-ADDR*	Global	Blocks a MAC address in case of requesting IP address. MAC-ADDR: MAC address
ip dhcp filter-address *MAC-ADDR* **type** {**ack** | **decline** | **discover** | **inform** | **nak** | **offer** | **release** | **request** }		Blocks a MAC address with DHCP message type options.
no ip dhcp filter-address *MAC-ADDR* [**type** {**ack** | **decline** | **discover** | **inform** | **nak** | **offer** | **release** | **request**}]		Disables DHCP MAC filtering.

9.6.10.2 DHCP Server Packet Filtering

Dynamic Host Configuration Protocol (DHCP) makes DHCP server assign IP address to DHCP clients automatically and manage the IP address. Most ISP operators provide the service as such a way. At this time, if a DHCP client connects with the equipment that can be the other DHCP server such as Internet access gateway router, communication failure might be occurred.

DHCP filtering helps to operate DHCP service by blocking DHCP request which enters through subscriber's port and goes out into uplink port or the other subscriber's port and DHCP reply which enters to the subscriber's port.

In the Fig. 9.39, server A has the IP area from 192.168.10.1 to 192.168.10.10. Suppose a user connects with client 3 that can be DHCP server to A in order to share IP address from 10.1.1.1 to 10.1.1.10.

Here, if client 1 and client 2 are not blocked from client 3 of DHCP server, client 1 and client 2 will request and receive IP from client 3 so that communication blockage will be occurred. Therefore, the filtering function should be configured between client 1 and client 3, client 2 and client 3 in order to make client 1 and client 2 receive IP without difficulty from DHCP server A.

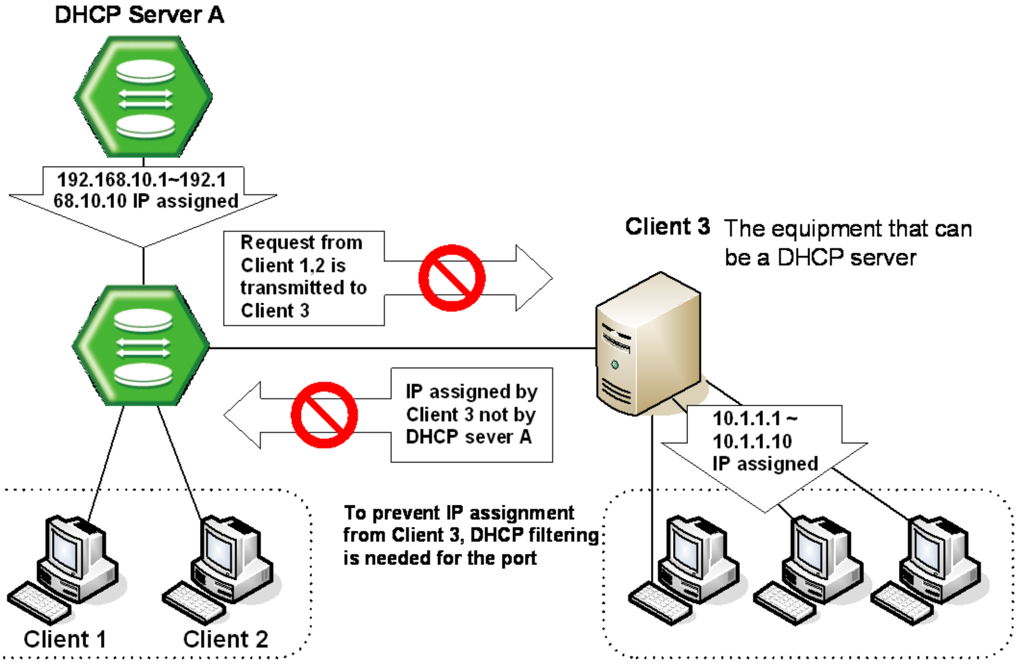

DHCP Server A
192.168.10.1~192.168.10.10 IP assigned
Request from Client 1,2 is transmitted to Client 3
Client 3
The equipment that can be a DHCP server
IP assigned by Client 3 not by DHCP sever A
10.1.1.1 ~ 10.1.1.10 IP assigned
To prevent IP assignment from Client 3, DHCP filtering is needed for the port
Client 1
Client 2

Fig. 9.39 DHCP Server Packet Filtering

To enable the DHCP server packet filtering, use the following command.

Command	Mode	Description
dhcp-server-filter on	Interface [XE/GE /GPON/CG]	Enables the DHCP server packet filtering.
dhcp-server-filter off		Disables the DHCP server packet filtering.

To display a status of the DHCP server packet filtering, use the following command.

Command	Mode	Description
show dhcp-server-filter	Enable Global	Show a status of the DHCP server packet filtering.

9.6.11 Debugging DHCP

To enable/disable a DHCP debugging, use the following command.

Command	Mode	Description
debug dhcp {**filter** | **lease** | **packet** | **service** | **all**}	Enable	Enables a DHCP debugging.
no debug dhcp {**filter** | **lease** |		Disables a DHCP debugging.

packet | **service** | **all**}		

To display the debugging information, use the following command.

Command	Mode	Description
show debugging dhcp	Enable Global	Shows the debugging information of DHCP.

9.7 Dynamic Host Configuration Protocol (DHCP) for IPv6

Dynamic Host Configuration Protocol (DHCP) for IPv6 provides a device with addresses assigned by a DHCP server and other configuration information, which are carried in options. DHCPv6 offers the capability of automatic allocation of reusable network addresses.

The basic DHCPv6 client, server and relay agent concept is similar to DHCP for IPv4. An advantage of DHCPv6 for dynamic address assignment is that it is capable of providing additional information to the nodes. DHCPv6 provides DNS information and uses a 16-bit option space.

DHCPv6 can record addresses assigned to hosts and assign addresses to specific hosts, thus facilitating network management. And it assigns prefixes to devices, thus facilitating automatic configuration and management of the entire network.

A node may autoconfigure addresses based on router advertisement (RA) under IPv6 environment.

DHCP Unique Identifier (DUID)

Using a DHCP unique identifier (DUID), each DHCP for IPv6 client and server is identified. A DUID is used to identify the device when exchanging DHCPv6 messages. The DUID is designed to be unique around all DHCPv6 clients and servers, and it is stable for any specific client or server. A DUID can be no longer than 128 octets. There are three types of DUIDs.

- **DUID-LLT (Link-layer address plus time)**
  Link-layer address of any one network interface that is connected to the DHCP device at the time that the DUID is generated.
- **DUID-EN (Enterprise number)**
  It consists of the vendor’s registered private enterprise number as maintained by IA_NA followed by a unique identifier assigned by the vendor.
- **DUID-LL (Link-layer address)**
  It consists of the link-layer address of any one network interface that is permanently connected to the client or server device.

An Identity Association (IA) is a construct through which a server and a client can identify, group, and manage a set of related IPv6 addresses. Each IA consists of an Identity Association Identifier (IAID) and associated configuration information. A client should associate at least one IA with each of its network interfaces for which it is to request the assignment of IPv6 addresses from a DHCP server. There are three main IPv6 prefix types: IA_PD, IA_NA, and IA_TA. Each Identity Association for Temporary Address (IA_TA) option contains at most one temporary address for each of the prefixes on the link to which the client is attached. The clients ask for temporary addresses and servers assign them. An Identity Association for Non-temporary Address (IA_NA) carries assigned addresses that are not temporary addresses. An Identity Association for Prefix Delegation (IA_PD) is a collection of prefixes assigned to the requesting router. Each IA_PD has an associated IAID.

DHCPv6 Address Assignment Mechanism

DHCP for IPv6 can provide stateful address configuration or stateless configuration settings to IPv6 hosts. IPv6 hosts use several methods to configure addresses:

- **Stateful Mechanism**
  It obtains interface address and configuration information from DHCP server. A site requires tighter control over exact address assignment.
- **Stateless Mechanism**
  It allows a host to generate its own address using a combination information advertisement by routers. A site is not concerned with the exact address hosts use.

DHCPv6 Message Types

There are 13 DHCP message types. The following table summarizes the DHCP message types.

DHCPv6 Message	Value	Description
Solicit	1	Sent by clients to locate DHCPv6 servers.
Advertise	2	Sent by server as a response to Solicit message received from a client to indicate that it is available for DHCP service.
Request	3	Sent by clients to request configuration parameters, including IP address or delegated prefixes, from a specific server.
Confirm	4	Sent by clients to verify that their address and configuration parameters are still valid.
Renew	5	Sent by clients to renew their configuration parameters with their original DHCP server when their lease is about to expire.
Rebind	6	Sent by client to extend the lifetime of their address and renew their configuration parameters with any DHCP server when their lease is about to expire
Reply	7	Sent by DHCP servers responding to Request, Confirm, Renew, Rebind, Release, and Decline messages.
Release	8	Sent by clients to release their IP address
Decline	9	Sent by clients to indicate that one or more addresses assigned to them are already in use on the link.
Reconfigure	10	Sent by DHCP servers to inform clients that the server has new or updated configuration information. The clients then must initiate a request in order to obtain the updated information.
Information-request	11	Sent by clients to request configuration parameters without the assignment of any IP addresses to the client.
Relay-forward	12	Sent by DHCP relays to forward client messages to servers. The relay encapsulates the client message in an option in the relay-forward message.
Relay-reply	13	Sent by DHCP servers to send messages to clients through a relay. The client message is encapsulated as an option in the relay-reply message. The relay decapsulates the message and forwards it to the client.

Tab. 9.4 DHCPv6 Message Types

- Message types from client to server
  - Solicit, Request, Confirm, Renew, Rebind, Release, Decline, Information-request
- Message types from server to client
  - Advertise, Replay, Reconfigure
- Message type from relay to relay/server
  - Relay-forward
- Message type from relay/server to relay
  - Relay-reply

- **DHCPv6 Client-Server Message**

DHCP servers communicate with DHCP clients by a series of DHCP messages. The Msg. Type field (1-byte) indicates the type of DHCPv6 message. The Transaction ID field (3-byte) is determined by a client and used to group the messages of a DHCPv6 message exchange together. Following the Transaction-ID field, DHCPv6 options are used to indicate client and server identification, addresses, and other configuration settings. For the list of defined DHCPv6 options, see RFC 3315. DHCPv6 options are formatted with the type-length-value (TLV) format.

The following figure shows the structure of DHCPv6 messages sent between client and server.

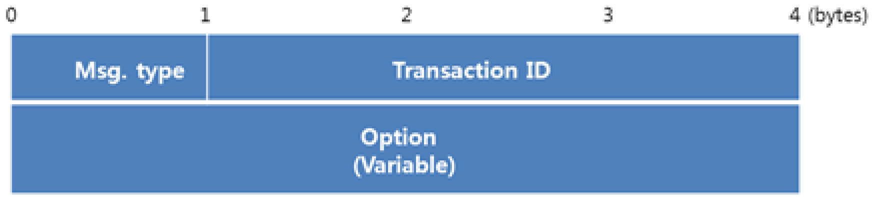


Fig. 9.40 Basic DHCPv6 Message Format

- **DHCPv6 Relay agent-Server Message**

DHCP relay agent is a node that acts as an intermediary to deliver DHCP messages between clients and servers, and is on the same link as the client. If there is a relay agent between the client and the server, the relay agent sends the server Relay-Forward messages containing the encapsulated Solicit and Request messages from the client. The server sends the relay agent Relay-Reply messages containing the encapsulated Advertise and Reply messages for the client.

There is a separate message structure for the messages exchanged between relay agents and servers to record additional information.

The following figure shows the structure of these kinds of messages.

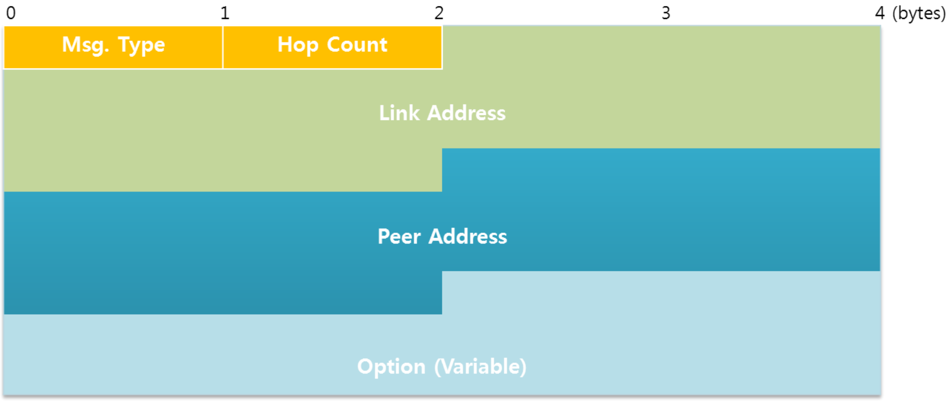


Fig. 9.41 General Shared Relay Message Format

The Hop Count field (1-byte) indicates the number of relay agents that have received the message. A receiving relay agent can discard the message if it exceeds a configured maximum hop count. The Link Address field (16-byte) contains a non-link-local address that is assigned to an interface connected to the subnet on which the client is located. From the Link Address field, the server can determine the correct address scope from which to assign an address. The Peer Address field (16-byte) contains the IPv6 address of the client that originally sent the message or the previous relay agent that relayed the message. The Relay Message option provides an encapsulation of the messages being exchanged between the client and the server.

Prefix Delegation for DHCPv6

This prefix delegation mechanism is appropriate for use by an ISP to delegate a prefix to a subscriber, where the delegated prefix would possibly be subnetted and assigned to the links within the subscriber's network. Prefix delegation with DHCP is independent of address assignment with DHCP. A requesting router can use DHCP for just prefix delegation or for prefix delegation along with address assignment and other configuration information.

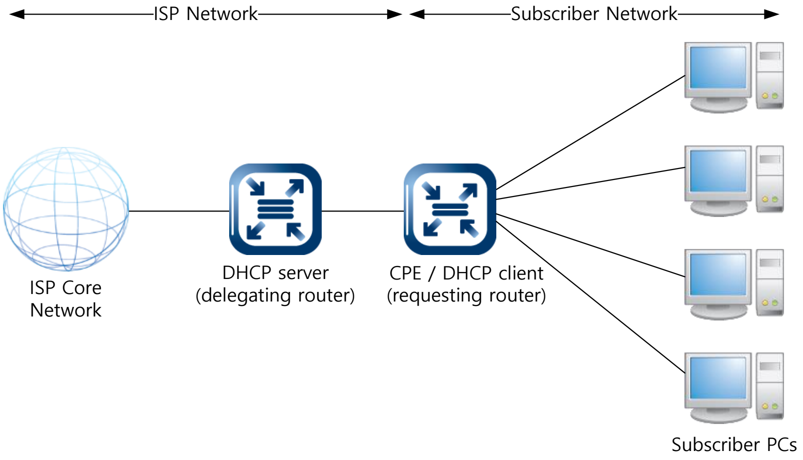

ISP Network
Subscriber Network
ISP Core Network
DHCP server (delegating router)
CPE / DHCP client (requesting router)
Subscriber PCs

Fig. 9.42 An Example of Prefix Delegation

The delegating router acts as a DHCP server, and is responding to the prefix request. It is configured with a set of prefixes to be used for assignment to customers at the time of each customer's first connection to the ISP service. The prefix delegation process begins when the requesting router requests configuration information through DHCPv6. The DHCP messages from the requesting router (DHCP client) are received by the delegating router in the aggregation device. When the delegating router receives the request, it selects an available prefix or prefixes for delegation to the requesting router. The delegating router then returns the prefix or prefixes to the requesting router. The requesting router subnets the delegated prefix and assigns the longer prefixes to links in the subscriber's network. The requesting router subnets a single delegated /48 prefix into /64 prefixes and assigns one /64 prefix to each of the links in the subscriber network.

The prefix delegation options can be used in conjunction with other DHCP options carrying other configuration information to the requesting router. The requesting router provides DHCP service to hosts attached to the internal network. For example, the requesting router may obtain the addresses of DNS and NTP servers from the ISP delegating router, and then pass that configuration information on to the subscriber hosts through a DHCP server in the requesting router.

DHCPv6 Basic Operation

DHCPv6 clients and servers exchange DHCP messages using UDP port. DHCPv6 clients listen for DHCP messages on UDP port 546. DHCPv6 servers and relay agents listen for DHCPv6 messages on UDP port 547. The client can obtain server or relay agent’s address using All-DHCP-Server and All-DHCP-Agent address.

	Port	Port #	Description
Client	UDP	546	Clients listen for DHCP messages on UDP port 546.
Server	UDP	547	Server and relay agents listen for DHCP messages on UDP port 547.

Tab. 9.5 DHCPv6 UDP port

There are no broadcast addresses defined for IPv6. Therefore, the use of the limited broadcast address for some DHCPv4 messages has been replaced with the use of the site-scoped multicast address (FF05::1:3) and link-scoped multicast address (FF02::1:2) for DHCPv6.

DHCPv6 Multicast Address		Description
All_DHCP_Servers **(Site-local scope)**	FF05::1:3	A site-scoped multicast address used by a relay agent or client to communicate with servers, either because the relay agent wants to send messages to all servers or because it does not know the unicast addresses of the servers. All DHCP servers within a site are members of this multicast group.
All_DHCP_Relay_Agents_and_Servers **(Link-local scope)**	FF02::1:2	A link-scoped multicast address used by a client to communicate with neighboring (i.e., on-link) relay agents and servers. All servers and relay agents are members of this multicast group.

Tab. 9.6 DHCPv6 Address

There is the four-message exchange handshake for a single interface with one IA_NA and one address for this IA_NA.

To obtain an IP address, the DHCP client daemon (dhcpcd6) sends a Solicit message to the link-scoped address (FF02::1:2), which is received by the server and processed. If a free address is available for that client, an Advertise message is created and sent back to the client. This message contains an IP address and other options that are appropriate for that client. The client receives the server DHCP Advertise message and stores it while waiting for other advertisements. When the client has chosen the best advertisement, it sends a DHCP Request to the link-scoped address (FF02::1:2) specifying which server advertisement it wants.

All configured DHCP servers receive the Request message. Each monitors to see if it is the requested server. The server does not process any packet with a server DUID that does not match its own. The requested server marks the address as assigned and returns a DHCP Reply, at which time, the transaction is complete. The client has an address for the period of time (valid-lifetime) designated by the server.

When the preferred-lifetime expires for the address, the client sends the server a Renew message to extend the lease time. If the server is willing to renew the address, it sends a DHCP Reply message. If the client does not get a response from the server that owns its current address, it multicasts a DHCP Rebind message if, for example, the server has been moved from one network to another. If the client has not renewed its address after the valid-lifetime, the address is removed from the interface and the process starts over. This cycle prevents multiple clients on a network from being assigned the same address.

9.7.1 DHCPv6 Server

9.7.1.1 Creating DHCPv6 address Pool

The DHCP pool is a group of IP addresses that will be assigned to DHCP clients by DHCP server. You can create various DHCP pools that can be configured with a different network, default gateway and range of IP addresses. This allows the network administrators to effectively handle multiple DHCP environments.

To create a DHCPv6 pool, use the following command.

Command	Mode	Description
ipv6 dhcp pool *POOLNAME*	Global	Creates a DHCPv6 pool and opens *DHCPv6 Pool Configuration* mode.
no ipv6 dhcp pool *POOLNAME*		Removes the specified DHCPv6 pool.

The following is an example of creating the DHCPv6 pool as *sample*.

```
SWITCH(config)# ipv6 dhcp pool sample
SWITCH(config-dhcp6[sample])#
```

To display a DHCPv6 pool configuration, use the following command.

Command	Mode	Description
show ipv6 dhcp pool [*POOLNAME*]	Enable Global	Shows the DHCPv6 address pool information POOL: DHCPv6 pool name

9.7.1.2 DHCPv6 Database

To specifie DHCP for IPv6 binding database agent parameters and stores binding entries in TFTP server, use the following command.

Command	Mode	Description
ipv6 dhcp database *A.B.C.D* **<**120-315360000**>**	Global	Configures DHCP for IPv6 binding database agent parameters. A.B.C.D: IPv4 address for database backup to tftp server **<**120-315360000**>:** interval time for backup (unit: second)
no ipv6 dhcp database		Removes the specified DHCPv6 parameters for database backup.

9.7.1.3 DHCPv6 unique identifier (DUID)

Each DHCPv6 client and server is identified by a DHCP unique identifier (DUID).

Command	Mode	Description
ipv6 dhcp filter-duid *CLIENT-DUID* **type**		Configures DHCPv6 duid filter function. type: DHCPv6 message type
ipv6 dhcp filter-duid *CLIENT-DUID* **type {confitm | decline | inform-req | rebind | release | renew | request | solicit }**	Global	
no ipv6 dhcp filter-duid *CLIENT-DUID*		Disables dhcp6 duid filter function.
no ipv6 dhcp filter-duid *CLIENT-DUID* **type {confitm | decline | inform-req | rebind | release | renew | request | solicit }**		

9.7.1.4 Domain Name

To set a domain name, use the following command.

Command	Mode	Description
domain-name *DOMAIN*	DHCPv6	Sets a domain name.

	Pool	DOMAIN: a domain name
no domain-name		Deletes the configured domain name.

9.7.1.5 DNS Server

The DNS server option is used to inform clients of DNS server addresses. The address of the DNS server should be statically configured in the DHCPv6 server configuration.

To specify a DNS server to inform DHCP clients, use the following command.

Command	Mode	Description
dns-server *X:X::X:X*	DHCPv6 Pool	Specifies a DNS server. X:X::X:X: DNS server IPv6 address
no dns-server *X:X::X:X*		Deletes a specified DNS server.

9.7.1.6 Range of IPv6 Address

To specify a range of IP addresses that will be assigned to DHCP clients, use the following command.

Command	Mode	Description
range *X:X::X:X X:X::X:X* [{**second** <60-315360000> <60-315360000> | **minute** <1-5256000> <1-5256000>}]	DHCPv6 Pool	Specifies a range of IPv6 addresses. X:X::X:X : start/end IPv6 address 60-315360000: valid life time (unit: second, default: 2592000) 60-315360000: preferred life time (unit: second, default: 604800) 1-5256000: valid life time (unit: minute, default: 43200) 1-5256000: preferred life time (unit: minute, default: 10080)
no range *X:X::X:X X:X::X:X*		Deletes the specified range of IP addresses.

9.7.1.7 DHCPv6 Options

DHCPv6 can be used in two ways. The first way of using DHCPv6 is to grant clients addresses from a pool while also using DHCPv6 to push configuration options. This is called stateful configuration. The other option is to use DHCPv6 combined with SLAAC for addressing, while using DHCPv6 for configuration options. This is called stateless configuration. DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients. To configure the NIS server DHCPv6 option, use the following command.

Command	Mode	Description
nis domain-name *DOMAIN*	DHCPv6 Pool	Sets a domain name of a NIS server. DOMAIN: a domain name of the NIS server for client to use

nis address X:X::X:X		Specifies the NIS server address to be sent to the client. X:X::X:X: NIS server IPv6 address
no nis domain-name		Removes the NIS domain name.
no nis address X:X::X:X		Removes the NIS server address.

To configure the NIS+ server DHCPv6 option, use the following command.

Command	Mode	Description
nisp domain-name *DOMAIN*	DHCPv6 Pool	Sets a domain name of a NIS+ server. DOMAIN: a domain name of the NIS+ server for client to use
nisp address X:X::X:X		Specifies the NIS+ server address to be sent to the client.
no nisp domain-name		Removes the NIS+ domain name.
no nisp address X:X::X:X		Removes the NIS+ server address.

To configure the SIP server DHCPv6 option, use the following command.

Command	Mode	Description
sip domain-name *DOMAIN*	DHCPv6 Pool	Sets a domain name of a SIP server. DOMAIN: a domain name of the SIP server for client to use
sip address X:X::X:X		Specifies the SIP server address to be sent to the client.
no sip domain-name		Removes the SIP domain name.
no sip address X:X::X:X		Removes the SIP server address.

9.7.1.8 Enabling DHCPv6 Server on Interface

After a DHCPv6 address pool is created, you need to apply/enable the specified pool to an interface. To configure DHCPv6 server functionality on an interface, use the following command.

Command	Mode	Description
ipv6 dhcp server *POOL* [**rapid-commit**] [**preference** <0-255>]	Interface	Enables DHCPv6 server functionality on an interface. POOL: DHCPv6 pool name containing stateless and/or prefix delegation parameters rapid-commit: an option that allows for an abbreviated exchange between the client and server 0-255: value used by clients to determine preference between multiple DHCPv6 servers
no ipv6 dhcp server		Disables the DHCPv6 server functionality.

9.7.1.9 Displaying DHCPv6 Information

To display a DHCPv6 pool configuration, use the following command.

Command	Mode	Description
show ipv6 dhcp pool [*POOLNAME*]	Enable Global	Shows the DHCPv6 address pool information POOL: DHCPv6 pool name

A DHCPv6 Unique Identifier (DUID) is used to identify the device when exchanging DHCPv6 messages.

To display the DUID of the local device, use the following command.

Command	Mode	Description
show ipv6 dhcp	Enable Global	Shows this device’s DUID.

To display the DHCPv6 interface configuration, use the following command.

Command	Mode	Description
show ipv6 dhcp interface	Enable Global	Shows the DHCPv6 information for all relevant interfaces or the specified interface.

To display information about user-defined local IPv6 address pools, use the following command.

Command	Mode	Description
show ipv6 local pool [*PREFIX-POOL*]	Enable Global	Shows information about any defined IPv6 address local pools.

To display DHCP binding information from the DHCPv6 server binding table, use the following command.

Command	Mode	Description
show ipv6 dhcp binding	Enable Global	Shows all automatic client bindings for the specific IP address from the DHCPv6 server binding table.

To delete/reset the configured bindings of DHCPv6 server, use the following command.

Command	Mode	Description
clear ipv6 dhcp binding	Enable Global	Clears an automatic address binding from the DHCP server database.

9.7.2 DHCPv6 Snooping

For enhanced security, the LD3032 provides the DHCP snooping feature. The DHCP snooping filters untrusted DHCP messages and maintains a DHCP snooping binding table. An untrusted message is a message received from outside the network, and an untrusted interface is an interface configured to receive DHCP messages from outside the network.

The DHCP snooping basically permits all the trusted messages received from within the network and filters untrusted messages. In case of untrusted messages, all the binding entries are recorded in a DHCP snooping binding table. This table contains a hardware address, IP address, lease time, VLAN ID, interface, etc. It also gives you a way to differentiate between untrusted interfaces connected to the end-user and trusted interfaces connected to the DHCP server or another switch.

9.7.2.1 Enabling DHCPv6 Snooping

DHCPv6 snooping should be enabled to allow clients to obtain IPv6 addresses from an authorized DHCPv6 server. To enable the DHCPv6 snooping on the system, use the following command

Command	Mode	Description
ipv6 dhcp snooping	Global Interface [XE/GE/br/ CG/GPON]	Enables the DHCPv6 snooping on the system.
no ipv6 dhcp snooping		Disables the DHCPv6 snooping on the system. (default)

To enable the DHCPv6 snooping on a VLAN, use the following command

Command	Mode	Description
ipv6 dhcp snooping vlan *VLANS*	Global	Enables the DHCPv6 snooping on a specific VLAN.
no ipv6 dhcp snooping vlan *VLANS*		Disables the DHCPv6 snooping on a specific VLAN.

! You must enable DHCPv6 snooping on the system before enabling DHCPv6 snooping on a VLAN.

9.7.2.2 DHCPv6 Snooping Port State

To define a state of a port as trusted or untrusted, use the following command.

Command	Mode	Description
ipv6 dhcp snooping trust *PORTS*	Global	Configures the specified port as a DHCPv6 snooping trusted port.
no ipv6 dhcp snooping trust *PORTS*		Configures the specified port as a DHCPv6 snooping untrusted port.

9.7.2.3 DHCP Rate Limit

To set the number of DHCPv6 packet per second (pps) that an interface can receive, use the following command.

Command	Mode	Description
ipv6 dhcp snooping limit-rate *PORTS* <1-255>	Global	Sets a rate limit for DHCPv6 packets. (unit: pps)
no ipv6 dhcp snooping limit-rate *PORTS*		Deletes a rate limit for DHCPv6 packets.

ℹ Normally, the DHCP rate limit is specified to untrusted interfaces and 15 pps is recommended for a proper value. However, if you want to set a rate limit for trusted interfaces, keep in mind that trusted interfaces aggregate all DHCP traffic in the switch, and you will need to adjust the rate limit to a higher value.

9.7.2.4 DHCP Lease Limit

The number of entry registration in DHCP snooping binding table can be limited. If there are too many DHCP clients on an interface and they request IP address at the same time, it may cause IP pool exhaustion.

To set the number of entry registration in DHCP snooping binding table, use the following command.

Command	Mode	Description
ipv6 dhcp snooping limit-lease *PORTS* <1-2147483637>	Global	Enables a DHCP lease limit on a specified untrusted port. 1-2147483637: the number of entry registration
no ipv6 dhcp snooping limit-lease *PORTS*		Deletes a DHCP lease limit.

⚠ You can limit the number of entry registration only for untrusted interfaces, because the DHCP snooping binding table only contains the information for DHCP messages from untrusted interfaces.

9.7.2.5 Specifying DHCPv6 Snooping Binding Entry

The DHCPv6 snooping binding table contains a hardware address, IPv6 address, lease time, VLAN ID, and port information that correspond to the valid interfaces of the system.

To manually add DHCPv6 snooping binding entry, use the following command.

Command	Mode	Description
ipv6 dhcp snooping binding <1-4094> *X:X::X:X MAC-ADDR* <120-2147483637>	Interface [XE/GE/GPON]	Adds the static entry to the DHCPv6 snooping binding table. 1-4094: VLAN ID X:X::X:X: IPv6 address

		MAC-ADDR: DHCPv6 client's MAC address 120-2147483637: Expiry time (unit: second)

To remove the configured entry from DHCPv6 snooping binding table, use the following command.

Command	Mode	Description
clear ipv6 dhcp snooping binding {*X:X::X:X* | **all**}	Interface [XE/GE/CG/GPON]	Removes the static entry from the DHCPv6 snooping table. X:X::X:X: IPv6 address

9.7.2.6 DHCP Snooping Option

DHCP snooping-enabled switch may receive DHCP messages with various different options from clients, which cause DHCP server hard to manage client's information in the perspective of data consistency. That's why this function is necessary.

The switch operating DHCP snooping can modify or attach an option field of the DHCP messages with the defined snooping option and can forward them to DHCP server. The snooping option can be applied on a port basis or on entire ports.

Before using this function, a global DHCPv6 option format should be created and configured. For details of setting the DHCP option format, refer to the 9.7.4 DHCPv6 Option.

To enter the DHCPv6 option mode, use the following command.

Command	Mode	Description
ipv6 dhcp option format *NAME*	Global	Enters the DHCPv6 option mode to configure the DHCPv6 option format. NAME: DHCPv6 option format name
no ipv6 dhcp option format *NAME*		Deletes the given DHCPv6 option format.

To set a DHCP snooping option for a specific port, use the following command.

Command	Mode	Description
ipv6 dhcp snooping opt-code <1-254> **format** *NAME*	Interface	Specifies a snooping option format on a port. opt-code: DHCPv6 option code NAME: DHCPv6 option format name
ipv6 dhcp snooping opt-code <1-254> **policy** {**keep** | **replace**}		Configures a policy against DHCP option belonging to a DHCP message (default: replace) keep: forwards a DHCP message to DHCP server without any modification. replace: deletes the DHCP message's option and adds the snooping option if both of them are same. However, if they are different each other, **replace** option just adds the snooping option.
no ip dhcp snooping opt-code <1-254>		Removes the DHCP snooping option for a given port.

In case there is not a DHCP snooping option for a specific port, DHCP snooping switch finds the snooping default option. If it exists, DHCP snooping switch sends a DHCP server DHCP messages by replacing their options with the snooping default option.

To specify a DHCP server default option, use the following command.

Command	Mode	Description
ipv6 dhcp snooping default-option code <1-254> **format** *NAME*	Global	Specifies a snooping default option format for a switch. NAME: DHCPv6 option format name
ipv6 dhcp snooping default-option code <1-254> **policy** <**keep** | **replace**>		Configures a policy against DHCP option belonging to a DHCP message (default: replace) keep: forwards a DHCP message to DHCP server without any modification. replace: deletes the DHCP message's option and adds the snooping default option if both of them are same. However, if they are different each other, **replace** option just adds the snooping default option.
no ipv6 dhcp snooping default-option code <1-254>		Removes the DHCP snooping default option for a given port.

9.7.2.7 Displaying DHCPv6 Snooping Configuration

To display DHCPv6 snooping table, use the following command.

Command	Mode	Description
show ipv6 dhcp snooping	Enable Global	Shows a DHCPv6 snooping configuration.
show ipv6 dhcp snooping binding		Shows DHCP snooping binding entries for IPv6.

9.7.3 DHCPv6 Relay Agent

9.7.3.1 DHCPv6 Relay Agent Destination

To specify a destination address to which client messages are forwarded and enable DHCP for IPv6 relay service on the interface, use the following command.

Command	Mode	Description
ipv6 dhcp relay destination *X:X::X:X* [*INTERFACE*]	Interface [XE/GE/br/GPON]	Specifies relay destination address on an interface. X:X::X:X: IPv6 destination address for DHCPv6 packet forwarding INTERFACE: interface name
no ipv6 dhcp relay destination {**all** | *X:X::X:X* [*INTERFACE*] }		Deletes the specified relay destination address.

9.7.3.2 DHCP Relay Agent Option

The switch operating DHCP server can include DHCP option information in the DHCP communication. Before using this function, a global DHCP option format should be created. For details of setting the DHCPv6 option format, refer to the 9.7.4 DHCPv6 Option.

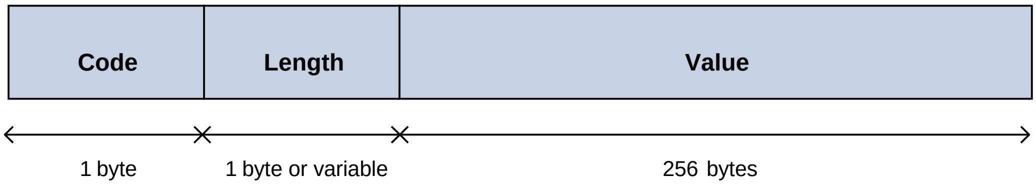
To specify a DHCPv6 server option, use the following command.

Command	Mode	Description
ipv6 dhcp relay option code <1-254> **format** *NAME*	Interface [XE/GE/br/ GPON]	Specifies a DHCPv6 option format for a DHCP server. code: DHCP option code NAME: DHCPv6 option format name
no ipv6 dhcp relay option code <1-254> **format**		Removes a specified DHCPv6 option for a DHCP server.

9.7.4 DHCPv6 Option

This function enables administrators to define DHCP options that are carried in the DHCP communication between DHCP server and client or relay agent. The following indicates the format of the DHCP options field.

DHCP Option Format



A code identifies each DHCP option. It can be expressed in value 0 to 255 by user configuration and some of them are predefined in the standards. (128 ~ 254 is site specific) A length can be variable according to value or can be fixed. A value contains actual information such an IPv6 address, string, or index, which is inserted into the DHCP packet.

Administrators can configure a DHCPv6 option format in *DHCPv6 Option* mode, which is globally used over the DHCP functions.

9.7.4.1 Entering DHCPv6 Option Mode

To enter the DHCPv6 option mode, use the following command.

Command	Mode	Description
ipv6 dhcp option format *NAME*	Global	Enters the DHCPv6 option mode. NAME: DHCPv6 option format name

9.7.4.2 Configuring DHCPv6 Option Format

To configure a DHCPv6 option format, use the following command.

Command	Mode	Description
attr <1-32> **type** <0-255> **length** {<1-256> | **variable**} **value** {**hex** | **index** | **ipv6** | **if_ipv6** | **string**} *VALUE*	DHCPv6 Option	Sets the type, length, and value of an attribute for a DHCPv6 option. attr: They can be made in a DHCPv6 option and are applied in order of attribute value (1-32). type: The type of a value length: The length of a value. It could be a fixed length by user input or a variable length according to the actual value length. value: The actual value of an option
attr <1-32> **type** <0-255> **length-hidden** {<1-256> | **variable**} **value** {**hex** | **index** | **ipv6** | **if_ipv6** | **string**} *VALUE*		
attr <1-32> **length variable value** {**hex** | **index** | **ipv6** | **if_ipv6** | **string**} *VALUE*		Sets the length and value of an attribute for a DHCPv6 option.
attr <1-32> **length** <1-256> **value** {**hex** | **index** | **ipv6** | **if_ipv6** | **string**} *VALUE*		
attr <1-32> **length-hidden variable value** {**hex** | **index** | **ipv6** | **if_ipv6** | **string**} *VALUE*		Sets the value of an attribute for a DHCPv6 option.
attr <1-32> **length-hidden** <1-256> **value** {**hex** | **index** | **ipv6** | **if_ipv6** | **string**} *VALUE*		
no attr <1-32>		Deletes the given attribute.

i

The packets can be mapped to the option format string that defined by variable values with special character (%).

%DEVICE-NAME: device name
%VENDOR-NAME: vendor name
%MODEL-NAME: product model name
%FIRMWARE-VERSION: firmware version
%PORT-NUM: input port number
%IN_IF_IPv6: input interface IPv6 address
%ONT-SERIAL: ONT serial number

9.7.4.3 Deleting DHCPv6 Option Format

To delete a specified DHCPv6 option format, use the following command.

Command	Mode	Description
no ipv6 dhcp option format *NAME*	Global	Deletes the given DHCPv6 option format.

9.7.4.4 Displaying DHCPv6 option

To print a specified DHCPv6 option format, use the following command.

Command	Mode	Description

show ipv6 dhcp option format *NAME*	Enable Global DHCPv6 Option	Shows the information of a given DHCPv6 option format.

9.7.5 DHCPv6 Filtering

To enable the DHCPv6 server packet filtering, use the following command.

Command	Mode	Description
dhcp6-server-filter on	Interface [XE/GE /GPON/CG]	Enables the DHCP server packet filtering.
dhcp6-server-filter off		Disables the DHCP server packet filtering.

To display a status of the DHCPv6 server packet filtering, use the following command.

Command	Mode	Description
show dhcp6-server-filter	Enable Global	Show a status of the DHCP server packet filtering.

9.7.6 Debugging DHCPv6

To enable/disable a DHCPv6 debugging, use the following command.

Command	Mode	Description
debug ipv6 dhcp [**detail**]	Enable	Enables DHCPv6 debugging.
no debug ipv6 dhcp [**detail**]		Disables DHCPv6 debugging.

To display the debugging information, use the following command.

Command	Mode	Description
show debugging ipv6 dhcp	Enable Global Bridge	Shows the debugging information of DHCP.

9.8 Virtual Router Redundancy Protocol (VRRP)

Virtual router redundancy protocol (VRRP) is configuring Virtual router (VRRP Group) consisted of VRRP routers to prevent network failure caused by one dedicated router. You can configure maximum 255 VRRP routers in VRRP group of LD3032. First of all, decide which router plays a roll as Master Virtual Router. The other routers will be Backup Virtual Routers. After you give priority to these backup routers, the router serves for Master Virtual Router when there are some problems in Master Virtual router. When you configure VRRP, configure all routers in VRRP with unified Group Id and assign unified Associated IP to them. After that, decide Master Virtual Router and Backup Virtual Router. A router that has the highest priority is supposed to be Master and Backup Virtual Routers also get orders depending on priority.

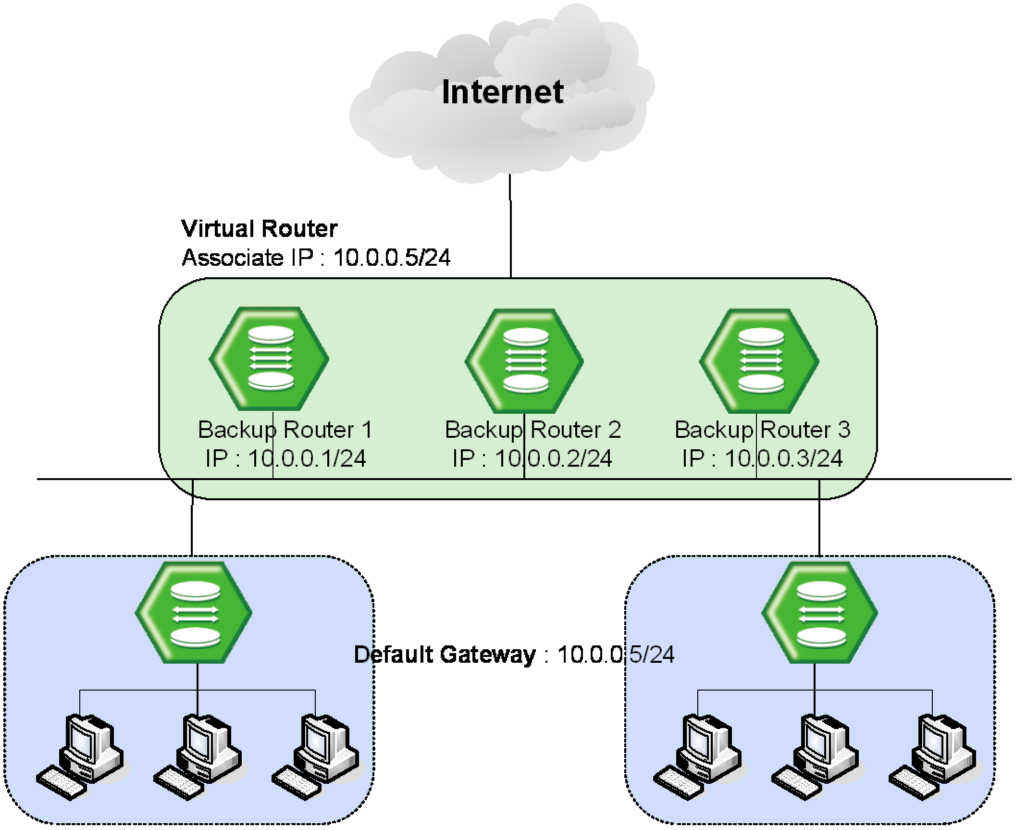


Fig. 9.43 VRRP Operation

In case routers have same priorities, then a router, which has lower IP address, gets the precedence. Fig. 9.43 shows an example of configuring three routers which have IP addresses, 10.0.0.1/24, 10.0.0.2/24 and 10.0.0.3/24 for each one as Virtual router by Associated IP, 10.0.0.5/24. If these three routers have same Priority, a router, which has the smallest IP, address, 10.0.0.1/24 is decided to be Master Router. Also, switches and PCs connected to the Virtual Router are to have IP address of Virtual Router, 10.0.0.5/24 as default gateway.

9.8.1 Configuring VRRP

To configure the LD3032 as device in Virtual Router, use the following command on *Global Configuration* mode. Then you can configure VRRP by opening *VRRP Configuration* mode.

Command	Mode	Description
router vrrp *INTERFACE* <1-255>	Global	Configures Virtual Router (VRRP Group). 1-255: VRRP virtual server ID

To delete the VRRP configuration, use the following command.

Command	Mode	Description
no router vrrp {**all** | <1-255>}	Global	Deletes current configuration of specific VRRP virtual server ID or all VRRP virtual servers. 1-255: VRRP virtual server ID

9.8.1.1 Associated IP Address

After configuring a virtual router, you need to assign an associated IP address to the virtual router. Assign unified IP address to routers in one group.

To assign an associate IP address to routers to a virtual router or delete a configured associate IP address, use the following command.

Command	Mode	Description
associate *A.B.C.D*	VRRP	Assigns an associated IP address to a virtual router. A.B.C.D: virtual router IP address
no associate {*A.B.C.D* | **all**}		Deletes an assigned associated IP address from a virtual router.

9.8.1.2 Access to Associated IP Address

If you configure the function of accessing Associated IP address, you can access to Associated IP address by the commands such as ping.

To configure the function of accessing Associated IP address, use the following command.

Command	Mode	Description
vip-access enable	VRRP	Enables the function of accessing associated IP address.
vip-access disable		Disables the function of accessing associated IP address.

9.8.1.3 Master Router and Backup Router

The LD3032 can be configured as Master Router and Backup Router by comparing Priority and IP address of devices in Virtual Router. First of all, it compares Priority. A device, which has higher Priority, is to be higher precedence. And when devices have same Priority, then it compares IP address. A device, which has lower IP address, is to be lower precedence. If a problem occurs on Master Router and there are more than two routers, one of them is selected as new Master Router according to their precedence.

To configure Priority of Virtual Router or delete the configuration, use the following commands.

Command	Mode	Description
vr-priority <1-254>	VRRP	Configures Priority of Virtual Router.
no vr-priority		Deletes configured Priority of Virtual Router.

i

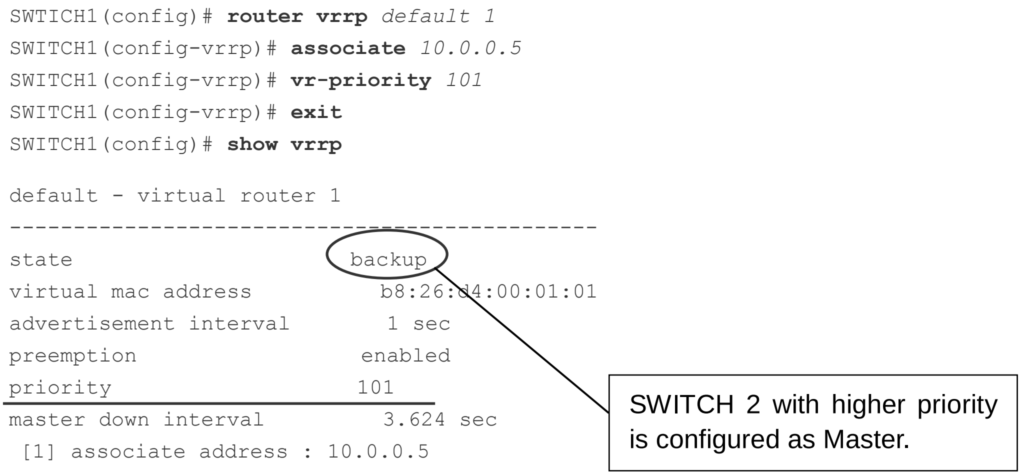
Priority of Virtual Backup Router can be configured from 1 to 254.

To set VRRP advertisement timers or delete the configuration, use the following command.

Command	Mode	Description
vr-timers advertisement <1-10>	VRRP	Sets VRRP advertisement timers. 1-10: advertisement time in the unit of second
no vr-timers advertisement		Clears a configured VRRP time.

The following is an example of configuring Master Router and Backup Router by comparing their Priorities: Virtual Routers, Layer 3 SWITCH 1 – 101 and Layer 3 SWITCH 2 – 102. Then, regardless of IP addresses, one that has higher Priority, Layer 3 SWITCH 2 becomes Master Router.

<Layer 3 SWITCH1: IP Address - 10.0.0.1/24>



```
SWTICH1(config)# router vrrp default 1
SWITCH1(config-vrrp)# associate 10.0.0.5
SWITCH1(config-vrrp)# vr-priority 101
SWITCH1(config-vrrp)# exit
SWITCH1(config)# show vrrp

default - virtual router 1
----------------------------------------------
state                    backup
virtual mac address        b8:26:d4:00:01:01
advertisement interval      1 sec
preemption                 enabled
priority                  101
master down interval        3.624 sec
 [1] associate address : 10.0.0.5
```

SWITCH 2 with higher priority is configured as Master.

<Layer 3 SWITCH 2: IP Address - 10.0.0.2/24>

```
SWTICH2(config)# router vrrp default 1
SWITCH2(config-vrrp)# associate 10.0.0.5
SWITCH2(config-vrrp)# vr-priority 102
SWITCH2(config-vrrp)# exit
SWITCH2(config)# show vrrp

default - virtual router 1
---------------------------------------------
state                        master
virtual mac address           b8:26:d4:00:01:01
advertisement interval         1 sec
preemption                   enabled
priority                     102
master down interval           3.620 sec
 [1] associate address : 10.0.0.5
```

SWITCH 2 with higher priority is configured as Master.

By default, Priority of the LD3032 is configured as “100”. Therefore, unless you configure specific Priority, this switch becomes Master Router because a device, which has higher IP address, has higher precedence.

Also, when there are more than two Backup Routers, IP addresses are compared to decide order. The following is an example of configuring Master Router and Backup Router by comparing IP addresses: Virtual Routers, Layer 3 SWITCH 1 – 10.0.0.1 and Layer 3 SWITCH 2 – 10.0.0.2.

<Layer 3 SWITCH 1: IP address - 10.0.0.1/24>

```
SWTICH1(config)# router vrrp default 1
SWITCH1(config-vrrp)# associate 10.0.0.5
SWITCH1(config-vrrp)# exit
SWITCH1(config)# show vrrp

default - virtual router 1
---------------------------------------------
state                        master
virtual mac address           b8:26:d4:00:01:01
advertisement interval         1 sec
preemption                   enabled
priority                     100
master down interval           3.624 sec
 [1] associate address : 10.0.0.5
```

<Layer 3 SWITCH 2: IP Address - 10.0.0.2/24>

```
SWTICH2(config)# router vrrp default 1
SWITCH2(config-vrrp)# associate 10.0.0.5
SWITCH2(config-vrrp)# exit
SWITCH2(config)# show vrrp

default - virtual router 1
---------------------------------------------
state                        backup
virtual mac address           b8:26:d4:00:01:01
advertisement interval         1 sec
```

In case of same priorities, SWITCH 1 with higher IP address is configured as Master.

```
preemption                    enabled
priority                     100
master down interval           3.620 sec
 [1] associate address : 10.0.0.5
```

9.8.1.4 VRRP Track Function

When the link connected to Master Router of VRRP is off as below, if link of Master Router is not recognized, the users on the interface are not able to communicate because the interface is not able to access to Master Router.

In the condition that Link to VRRP's master router is down as the figure shown below, or the link of Master Router cannot be recognized, the communication would be impossible.

For the LD3032, you can configure Master Router to be changed by giving lower Priority to Master Router when the link of Master Router is disconnected. This function is VRRP Track.

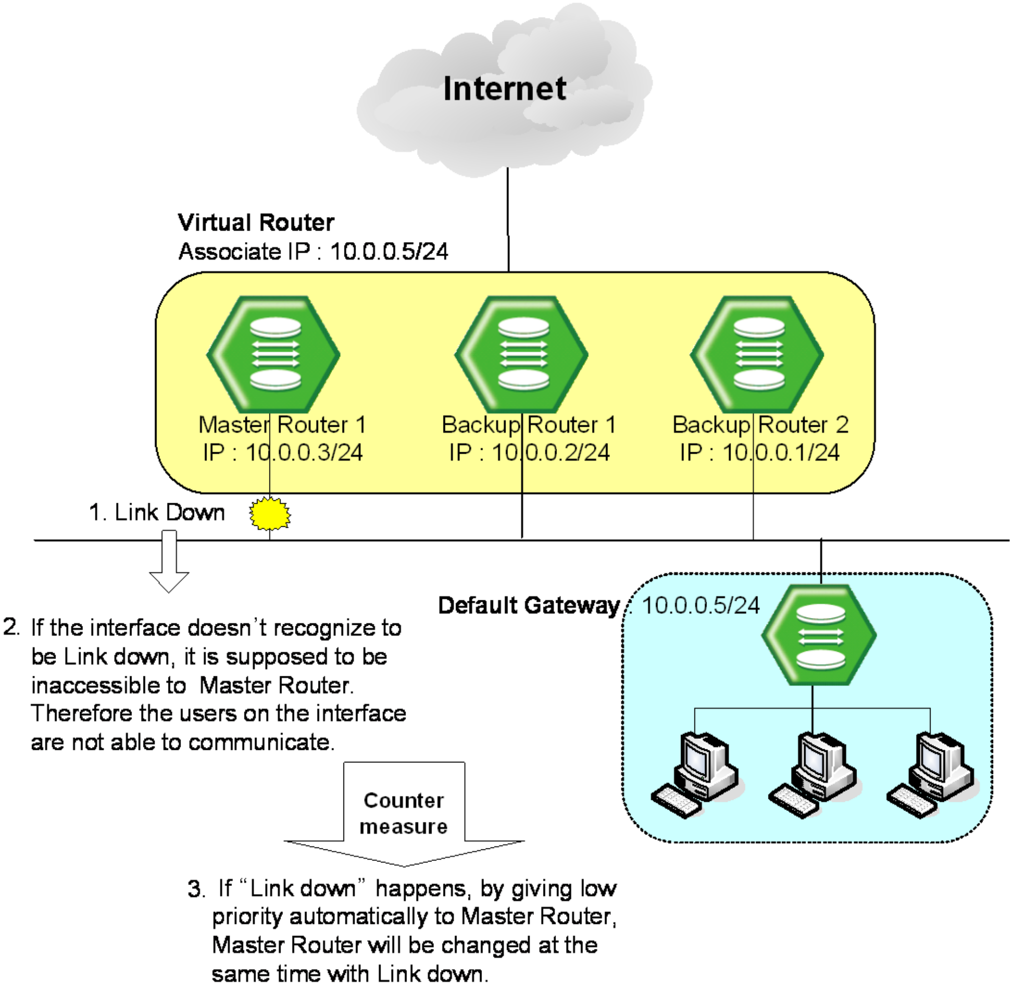

Internet
Virtual Router
Associate IP : 10.0.0.5/24
Master Router 1
IP : 10.0.0.3/24
Backup Router 1
IP : 10.0.0.2/24
Backup Router 2
IP : 10.0.0.1/24
1. Link Down
Default Gateway
10.0.0.5/24
2. If the interface doesn't recognize to be Link down, it is supposed to be inaccessible to Master Router. Therefore the users on the interface are not able to communicate.
Counter measure
3. If "Link down" happens, by giving low priority automatically to Master Router, Master Router will be changed at the same time with Link down.

Fig. 9.44 VRRP Track

To configure VRRP Track, use the following command.

Command	Mode	Description
track interface *INTERFACE* **priority** <1-254>	VRRP	Configures VRRP Track. The Priority becomes lower as the configured value.

To release VRRP Track configuration, use the following command.

Command	Mode	Description
no track interface *INTERFACE*	VRRP	Disables VRRP Track configuration.

9.8.1.5 Authentication Password

If anyone knows Group ID and Associated IP address, he can configure another device as a Virtual Router. To prevent this, user needs to configure a password, named authentication password that can be used only in Virtual Router user configured.

To configure an authentication password for security of Virtual Router, use the following command on VRRP configuration mode.

Command	Mode	Description
authentication clear_text *PASSWORD*	VRRP	Configures an authentication password.
no authentication		Deletes a configured authentication password.

i

Authentication password can be configured with maximum 7 digits.

The following is an example of configuring Authentication password in Virtual Router as network and showing it.

```
SWITCH(config-vrrp)# authentication clear_text network
SWITCH(config-vrrp)# show running-config
Building configuration...
(Omitted)
vrrp default 1
 authentication clear_text network
 associate 10.0.0.5
no snmp
SWITCH(config-vrrp)#
```

9.8.1.6 Preempt

Preempt is a function that an added device with the highest Priority user gave is automatically configured as Master Router without rebooting or specific configuration.

To configure Preempt, use the following command.

Command	Mode	Description
preempt	VRRP	Enables Preempt. (default: enable)
preempt delay <1-3600>		Specifies the number of seconds the router delays before issuing an advertisement claiming virtual IP address ownership to be the master router.

To disable Preempt and return to as default setting of delay time, use the following command.

Command	Mode	Description
no preempt	VRRP	Deletes the former configuration of Preempt to enable it.
no preempt delay		Returns to the default setting.

9.8.2 VRRP Monitoring and Management

You can view all kinds of statistics and database recorded in IP routing table. The information can be used to enhance system utility and solve problem in case of trouble. You can check network connection and data routes through the transmission.

9.8.2.1 Displaying VRRP Protocol Information

To display a configuration of VRRP, use the following command.

Command	Mode	Description
show vrrp	Enable Global VRRP	Shows current configuration of VRRP.
show vrrp vrid [<1-255> | **all**]		Shows a specified or all configured virtual servers.
show vrrp interface {*INTERFACE* | **all**}		Shows current configuration of specified interface VRRP.

9.8.2.2 VRRP Statistics

To display the VRRP statistics that packets have been sent and received, use the following command.

Command	Mode	Description
show vrrp stat	Enable Global VRRP	Shows statistics of packets in Virtual Router Group.

To clear the VRRP statistics information, use the following command.

Command	Mode	Description
clear vrrp stat	Enable/Global/VRRP	Clears statistics of packets in Virtual Router Group.

9.8.2.3 VRRP Debug

To enable VRRP debugging, use the following command.

Command	Mode	Description
debug vrrp [**all**]	Enable	Enables VRRP debugging. all: all VRRP debugging
debug vrrp nsm [**interface** | **bfd**]		Enables VRRP debugging. nsm: NSM notifications debugging interface: interface information bfd: BFD detection
debug vrrp packet [**send** | **recv** | **detail**]		Enables VRRPv2 packets debugging. packet: VRRPv2 packets send: outgoing packets recv: incoming packets detail: detail information
debug vrrp sm [**events** | **status** | **timers**]		Enables VRRP state machine debugging. sm: state machine events: SM events status: SM status timers: SM timers

To disable VRRP debugging, use the following command.

Command	Mode	Description
no debug vrrp [**all**]	Enable	Disables VRRP debugging.
no debug vrrp nsm [**interface** | **bfd**]		
no debug vrrp packet [**send** | **recv** | **detail**]		
no debug vrrp sm [**events** | **status** | **timers**]		

To display the debugging information, use the following command.

Command	Mode	Description
show debugging vrrp	Enable Global VRRP	Shows the debugging information of VRRP.

9.9 Rate Limit

User can customize port bandwidth according to user’s environment. By this configuration, you can prevent a certain port to monopolize whole bandwidth so that all ports can use bandwidth equally. Egress and ingress can be configured both to be same and to be different.

The LD3032 can apply the rate limit with 64 Kbps unit for GE port, and support ingress policing and egress shaping.

To set a rate limit for ports, use the following command.

Command	Mode	Description
rate-limit rate *RATE* {**egress** | **ingress dot3x** {**shape** | **drop**}}	Interface [XE/GE/GPON]	Sets a rate limit for ports. If you input egress or ingress, you can configure outgoing packet or incoming packet. The unit is 64 Kbps.
no rate-limit {**egress** | **ingress dot3x**}		Clears a specified rate limit for port.

⚠ For the ingress rate limit, the flow control should be enabled on a specified port! For more information of the flow control, see Section 5.9.7.

To display a configured rate limit, use the following command.

Command	Mode	Description
show rate-limit	Enable Global	Shows a configured rate limit.

9.10 Flood Guard

Flood guard limits number of packets, how many packets can be transmitted, in configured bandwidth, whereas Rate limit controls packets through configuring width of bandwidth, which packets pass through. This function prevents receiving packets more than configured amount without enlarging bandwidth.

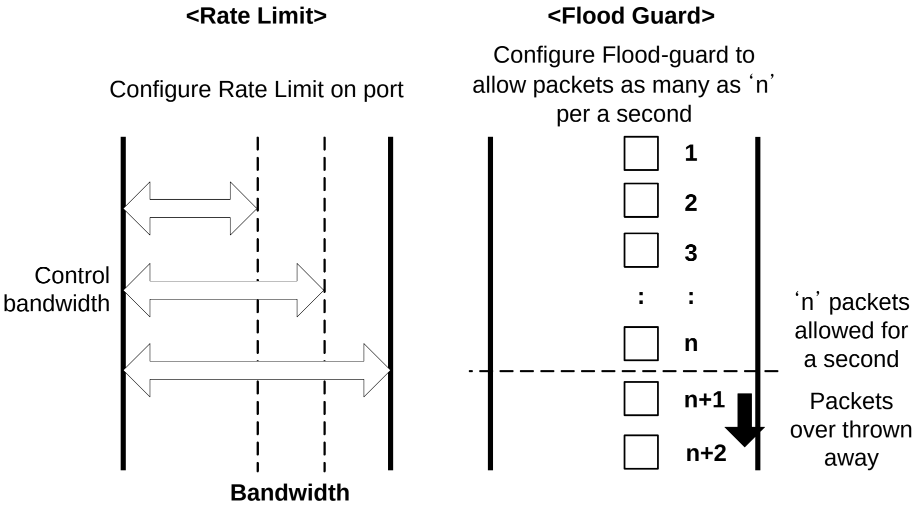

<Rate Limit>
Configure Rate Limit on port
Control bandwidth
Bandwidth
<Flood Guard>
Configure Flood-guard to allow packets as many as 'n' per a second
1
2
3
:
:
n
n+1
n+2
'n' packets allowed for a second
Packets over thrown away

Fig. 9.45 Rate Limit and Flood Guard

9.10.1 MAC Flood Guard

MAC flood guard controls the number of incoming packets per second, which have the same MAC address. Using this function, you can protect malicious attacks such as Denial of Service (DoS) from unauthorized user.

To configure the MAC flood guard, use the following command.

Command	Mode	Description
mac-flood-guard <1-6000>	Interface [XE/GE/GPON/CG]	Enables the MAC flood guard on a port by specifying the number of incoming packets with the same MAC address per second. 1-6000: the number of packets per second
no mac-flood-guard		Disables the MAC flood guard.

To display the configured MAC flood guard, use the following command.

Command	Mode	Description
show mac-flood-guard	Enable Global	Shows the configured MAC flood guard.
show mac-flood-guard macs		Shows the MAC addresses blocked by the MAC flood guard.

9.10.2 CPU Flood Guard

CPU flood guard controls the number of broadcast and multicast packets per second, which is coming to CPU to prevent CPU overload. If the number of those packets exceeds the threshold, the system generates an SNMP trap.

To enable/disable the CPU flood guard, use the following command.

Command	Mode	Description
cpu-flood-guard {**enable** | **disable**}	Global	Enables/disables the CPU flood guard.

To specify the number of broadcast and multicast packets per second, which is coming to CPU, use the following command.

Command	Mode	Description
cpu-flood-guard <1-6000>	Interface [XE/GE/GPON/CG]	Specifies the number of broadcast and multicast packets toward CPU per second. 1-6000: the number of packets per second
no cpu-flood-guard		Deletes a specified number of packets.

You can also enable the blocking option. When the blocking option for CPU flood guard is running, if the number of incoming broadcast and multicast packets per second exceeds a configured value, the port will discard those packets during a specified time.

To enable the blocking option, use the following command.

Command	Mode	Description
cpu-flood-guard timer <10-3600>	Interface [XE/GE/ GPON/CG]	Enables the blocking option. 10-3600: blocking time (unit: second)
cpu-flood-guard unblock		Forces the state of a blocked port to change to NORMAL.

To display the configured CPU flood guard, use the following command.

Command	Mode	Description
show cpu-flood-guard	Enable Global	Shows the configured CPU flood guard.

9.10.3 System Flood Guard

A packet flooding occurs unexpectedly when a large number of broadcast or multicast packets are received on a port, which may cause unnecessary network congestion. The LD3032 provides the system flood guard function that controls traffic for a port by given threshold. If the number of incoming packets exceeds the threshold, the system generates a syslog message/SNMP trap or discards those packets.

To enable/disable the system flood guard, use the following command.

Command	Mode	Description
system-flood-guard {**enable** | **disable**}	Global	Enables/disables the system flood guard.

You can also enable the blocking timer option. When the blocking timer option for system flood guard is running, if the number of incoming packets per second exceeds the configured threshold, the port will discard those packets during a specified time.

To specify the number of packets per second according to the type of packets, which is transmitted to a specific port, use the following command.

Command	Mode	Description
system-flood-guard packet-type { **multicast** | **broadcast** | **arp** | **dhcp** | **dlf** | **all**} <1-2147483647> **timer** <10-3600> **block**	Interface [XE/GE/GPON/CG]	Specifies the number of incoming packets to a port per second according to the packets' type. Discards the packets which exceeds given threshold. 1-2147483647: the number of packets per 1 second 10-3600: blocking time (default:60, unit: second)
no system-flood-guard packet-type { **multicast** | **broadcast** | **arp** | **dhcp** | **dlf** | **all**}		Deletes a specified number of packets.

To generate the trap message when the number of incoming packets is less than a configured value, use the following command.

Command	Mode	Description
system-flood-guard packet-type { **multicast** | **broadcast** | **arp** | **dhcp** | **dlf** | **all**} <1-2147483647> **timer** <10-3600> **unblock**	Interface [XE/GE/GPON/CG]	Enables the system to display a trap message when the number of incoming packets per second is less than the threshold. 1-2147483647: the number of packets per 1 second 10-3600: blocking time (default:60, unit: second)

To disable the blocking option for the blocked port to permit the packet transmission, use the following command.

Command	Mode	Description
system-flood-guard un-block	Interface [XE/GE/GPON/CG]	Disables the blocking option.

To display the configured system flood guard, use the following command.

Command	Mode	Description
show system-flood-guard	Enable Global	Shows the configured system flood guard.

i

BPDU is still transmitted even if the specific port is blocked by system flood guard.

9.10.4 Invalid Traffic Guard

A packet storm may occur unexpectly if a large number of invalid packets are received on a port. It can cause the network to slow down or to time out. The LD3032 provides the traffic guard function that controls the port's traffic by threshold value. The threshold (%) rate is based on the number of packets per second (pps). Basically, a maximum pps is usually calculated when all Ethernet frames are of 64-bytes in length, or the minimum size frame. Because of the Inter-Packet Gap (12 bytes) and preamble (8 bytes), the minimum packet size becomes 84 bytes.

The following table shows the performance numbers in packets per second (pps) for 100M, 1G and 10G Ethernet port.

Port Speed	Bytes/second	PPS for 64-byte	PPS for 1518-byte
100M Port	12,500,000	148,809	8,234
1G Port	125,000,000	1,488,095	82,345
10G Port	1,250,000,000	14,880,952	823,451

The invalid traffic guard function is configured with the threshold rate (%) that is based on pps of the maximum Ethernet port's bandwidth.

	Frame size for PPS calculation	Packet Type which are counted	Threshold Rate (%) based on PPS
Attack-guard	64-byte	Multicast, Unicast, Broadcast	1G port: 100% (=1,488,095 pps) 10G port: 100% (=14,880,952 pps) Default: High-80%, Low-20%
Error-guard	64-byte	Error packets	1G port: 100% (=1,488,095 pps) 10G port: 100% (=14,880,952 pps) Default: 1%

i

To generate a SNMP trap of invalid traffic guard (attack/error), SNMP trap mode should be "alarm-report" mode.

9.10.4.1 Attack Guard

A packet storm may unexpectedly occur if a large number of broadcast, unicast, or multicast packets are received on a port. Forwarding these packets can cause the network to slow down or to time out. The LD3032 provides the attack guard function that controls traffic for a specified port by threshold value. The threshold (%) rate of attack guard is based on the number of packets per second (pps) that is calculated by 64-byte frame size. If the number of incoming packets exceeds a given threshold, the system can shut down the port or generate SNMP trap messages for warning when attack guard function is enabled on this port. If the threshold (%) comes down to a given low threshold, it generates traps. You can specify the packet type, a high threshold value and a low threshold for a port.

To enable/disable the attack guard function, use the following command.

Command	Mode	Description
attack-guard {**broadcast** | **multicast** | **unicast**} <0-100> <0-100> [*PORTS*]	Interface [XE/GE/GPON/CG]	Enables the attack guard function according to its packet type and sets the threshold. PORTS: port number 0-100: high rate threshold percent (default: 80%) 0-100: low rate threshold percent (default: 20%)
no attack-guard {**broadcast** | **multicast** | **unicast**} [*PORTS*]		Disable the attack guard function.

If the high threshold is set to 85% for 1G Ethernet port, the LD3032 monitors the number of configured packet type. The number of those packets exceeds 1,264,880 pps (=14,880,95 * 0.85), the shutdown/trap action will be performed.

To determine the policy to take action when the incoming broadcast/multicast/unicast packets exceed the configured threshold, use the following command.

Command	Mode	Description
attack-guard action shutdown [*PORTS*]	Interface [XE/GE/GPON/CG]	Shuts down the port if the amount of traffic exceeds a high threshold.
attack-guard action trap [*PORTS*]		Generates a trap message when the amount of traffic exceeds a high threshold.
no attack-guard action {**shutdown** | **trap** } [*PORTS*]		Disables the shutdown action or trap action on a port when the attack guard function is enabled.

To display the attack guard configuration, use the following command.

Command	Mode	Description
show attack-guard	Interface [XE/GE/GPON/CG]	Displays the attack guard configuration.

9.11 PPS Control

A packet storm occurs unexpectedly when a large number of broadcast, unicast, or multicast packets are received on a port, which may cause unnecessary network congestion. The LD3032 provides the PPS control function that controls traffic for a port by given threshold. If the number of incoming packets exceeds the threshold, the system generates a syslog message and SNMP trap.

To set the threshold for PPS control, use the following command.

Command	Mode	Description
pps-control *THRESHOLD* {**5** | **60** | **600**}	Interface [XE/GE/GPON]	Sets the threshold for PPS control. THRESHOLD: number of packets per second (pps) 5 | 60 | 600: time interval (unit: second)
no pps-control		Deletes the configured threshold for PPS control.

When the blocking option for PPS control is running, if the number of incoming packets exceeds a configured threshold, the traffic is discarded during specified time.

To enable the blocking option, use the following command.

Command	Mode	Description
pps-control block timer <10-3600>	Interface [XE/GE/GPON]	Enables the blocking option. 10-3600: blocking time (unit: second)
no pps-control block		Disables the blocking option.

To display current incoming packet statistics and configurations for PPS control, use the following command.

Command	Mode	Description
show pps-control [**interface** {**gigabitethernet** | **tengigabitethernet** | **gpon** } *IFPORT*]	Enable Global Interface [XE/GE/GPON]	Shows current incoming packet statistics and configurations for PPS control.

9.12 Storm Control

The LD3032 provides a storm control feature for mass broadcast, multicast, and destination lookup failure (DLF). Generally, wrong network configuration, hardware malfunction, virus and so on cause these kinds of mass packets. Packet storm occupies most of the bandwidth of the network, and that causes the network very unstable.

To enable/disable the storm control, use the following command.

Command	Mode	Description
storm-control {**broadcast** | **multicast** | **dlf**} **level** *LEVEL*	Interface [XE/GE/GPON]	Enables broadcast, multicast or DLF storm control respectively in a port with a user defined rate. level: threshold level

		LEVEL: Rate (unit: Packet/s), range: FE(0-262142), GE(0-2097150)
no storm-control {**broadcast** | **multicast** | **dlf**}		Disables broadcast, multicast or DLF storm control respectively.

By default, DLF storm control is enabled and multicast storm control is disabled.

To display a configuration of the storm control, use the following command.

Command	Mode	Description
show storm-control [**interface** {**gigabitethernet** | **tengigabitethernet** | **gpon** } *IFPORT*]	Enable Global Interface [XE/GE/GPON]	Displays a configuration of the storm control.

9.13 Jumbo Frame Capacity

The packet range that can be capable to accept is from 64 bytes to 1518 bytes. Therefore, packets not between these ranges will not be taken. However, the LD3032 can accept jumbo frame larger than 1518 bytes through user’s configuration.

To enable/disable the jumbo frame capacity, use the following command.

Command	Mode	Description
jumbo-frame <1518-12288>	Interface [XE/GE/GPON]	Configures to accept jumbo frame between specified ranges. (default: 1518)
no jumbo-frame		Disables configuration to accept jumbo frame on specified port.

To display the configuration of jumbo frame, use the following command.

Command	Mode	Description
show jumbo-frame	Enable Global Interface [XE/GE/GPON]	Shows a configuration of jumbo frame.

9.14 Configuring PPPoE Tag Option Format

PPP over Ethernet (PPPoE) provides the ability to connect a network of hosts over a simple bridging access device to a remote Access Concentrator (AC). By using PPPoE with vendor tag, switch in the host network can include the additional information about itself before sending PPPoE packets to the AC.

9.14.1 PPPoE Vendor Tag Option

9.14.1.1 Entering PPPoE Vendor Tag Option Mode

To enter the PPPoE vendor tag option mode, use the following command.

Command	Mode	Description
pppoe tag-format *NAME*	Global	Enters the PPPoE vendor tag option mode. NAME: PPPoE vendor tag option format name

9.14.1.2 Configuring PPPoE Vendor Tag Option Format

To configure a PPPoE vendor tag option format, use the following command.

Command	Mode	Description
attr <1-32> **type** <0-255> **length** {<1-128> | **variable**} **value** {**hex** | **index** | **ip** | **string** | **tag-format**} *VALUE*	PPPoE Option	Sets the type, length, and value of an attribute for a PPPoE Vendor Tag option. attr: They can be made in a PPPoE vendor tag option and are applied in order of attribute value (1-32). type: The type of a value length: The length (size) of a value field. It could be a fixed length by user input or a variable length according to the actual value length. 1-128: 1 to 128 bytes fixed length (size) of the value field value: The actual value of an option.
attr <1-32> **type** <0-255> **length-hidden** {<1-128> | **variable**} **value** {**hex** | **index** | **ip** | **string** | **tag-format** } *VALUE*		
attr <1-32> **length variable value** {**hex** | **index** | **ip** | **string** | **tag-format** } *VALUE*		Sets the length and value of an attribute for a PPPoE Vendor Tag option.
attr <1-32> **length** <1-128> **value** {**hex** | **index** | **ip** | **string** | **tag-format** } *VALUE*		
attr <1-32> **length-hidden variable value** {**hex** | **index** | **ip** | **string** | **tag-format** } *VALUE*		Sets the value of an attribute for a PPPoE vendor tag option.
attr <1-32> **length-hidden** <1-128> **value** {**hex** | **index** | **ip** | **string** | **tag-format** } *VALUE*		
no attr <1-32>		Deletes the given attribute.

The packets can be mapped to the option format string that defined by variable values with special character (%).

%FRAME: frame (chassis) number for receiving PPPoE packets
%SLOT: slot number for receiving PPPoE packets
%PORT: port number for receiving PPPoE packets
%VID: VLAN ID tagged on packets
%IN VID: inner VLAN ID
%BANDWIDTH: bandwidth
%MGMT IP: MGMT interface’s IP address
%HOST NAME: host name
%IN_IF_IP: input interface IP address
%REAL_PORT: port number (slot#/port#)
%CPU-MAC: system MAC address
%ONU-ID: ONU ID
%ONU_PORT_NUM: ONU’s UNI port number
%ONU_DESCRIPTION: ONU description written by administrator
%ONU_PORT_DESCRIPTION: ONU port description written by administrator
%ONU_SERIAL_NUM: ONU’s serial number
%BLANK: blank

9.14.1.3 Deleting PPPoE Vendor Tag Option Format

To delete the given PPPoE vendor tag option format, use the following command.

Command	Mode	Description
no pppoe tag-format *NAME*	Global	Deletes the given PPPoE vendor tag option format.

9.14.1.4 Displaying PPPoE Vendor Tag option

To display the specified PPPoE vendor tag option format, use the following command.

Command	Mode	Description
show pppoe tag-format *NAME* **port** *PORT* **vlan** *VLANS*	Enable Global	Shows information about the PPPoE vendor tag format. NAME: PPPoE vendor tag format name

9.14.2 PPPoE Vendor Tag Filtering

9.14.2.1 PPPoE Snooping Mode

To enable/disable PPPoE snooping, use the following command.

Command	Mode	Description
pppoe snooping	Global	Enables PPPoE snooping function.
no pppoe snooping		Disables PPPoE snooping function.

9.14.2.2 Configuring PPPoE Vendor Tag Filtering

The PPPoE filter will decide the way that PPPoE packet is forwarded. Each filter has a unique filter ID. This ID is also used as a priority. The filter having the highest priority will be chosen. The filter can be applied for all ports in switch or some specific ports, all VLANs or some specific VLAN IDs, and chose action drop or permit.

To create a PPPoE packet filter and define the filter, use the following command.

Command	Mode	Description
flt-id <1-16> **port** {**any** | *PORTS*} **vid** {**any** | *VLANS*} **action** {**drop** | **permit**}	PPPoE Snooping	Creates a PPPoE filter ID and selects a port number, VLAN ID and filter action policy (drop/permit). 1-16: PPPoE filter ID
no flt-id <1-16>		Removes the configured PPPoE filter ID.

PPPoE tag operation is the action applied on the PPPoE tag field of the permitted PPPoE packet. The tag operation has lower priority than filter action and can select one action from remove, keep, add, update and replace.
To set the tag operation which will be applied to the PPPoE vendor tag field of the permitted PPPoE packets, use the following command.

Command	Mode	Description
tag-opr-id <1-16> **type** *CODE* **port** {**any** | *PORTS*} **vid** {**any** | *VLANS*} **action** {**remove** | **keep** | **add** | **update** | **replace**} **format** *NAME*	PPPoE Snooping	Specifies a PPPoE tag operation on a port and VLAN. 1-16: tag operation ID CODE: PPPoE Vendor tag type code (e.g. 0x0105 for Vendor-specific) remove: Remove the vendor tag from the PPPoE packets. keep: Keep the vendor tag in the PPPoE packets. add: Add the vendor tag the PPPoE packet if it is not existed. update: Update or add the vendor tag to PPPoE packet regardless of the existence of the tag. replace: Replace the vendor tag if it exist. NAME: PPPoE vendor tag format name
no tag-opr-id <1-16>		Removes the PPPoE tag operation.

9.14.3 PPPoE Debug

To enable debugging of all PPPoE or a specific feature of PPPoE, use the following command.

Command	Mode	Description
debug pppoe { **all** | **func** | **pkt** }	Global	Enables PPPoE debugging. all: all PPPoE features func: PPPoE function pkt: PPPoE packet
no debug pppoe { **all** | **func** | **pkt** }		Disables PPPoE debugging.

To display the debugging status of PPPoE, use the following command.

Command	Mode	Description
show debug pppoe	Global	Shows the debugging status of PPPoE.

9.15 Bandwidth

Routing protocol uses bandwidth information to measure routing distance value. To configure bandwidth of interface, use the following command.

Command	Mode	Description
bandwidth *BANDWIDTH*	Interface	Configures bandwidth of interface. BANDWIDTH: <1-999> k|m for 1 to 999 kilo bits or mega bits <1-10> g for 1 to 10 giga bits
no bandwidth *BANDWIDTH*		Deletes configured bandwidth of interface.

i This bandwidth is valid only for forwarding routing information and it does not concern any physical bandwidth.

9.16 Maximum Transmission Unit (MTU)

Maximum value for the length of the data payload can be transmitted. You can set a maximum transmission unit (MTU) with below command.

Command	Mode	Description
mtu <68-9170>	Interface [XE/GE/GPON]	Sets a MTU size.
no mtu		Returns to the default MTU size.

9.17 Source Address Validation

The Reverse Path filter (rp_filter) can reject incoming packets if their source address doesn't match the network interface that they're arriving on, which helps to prevent IP spoofing. When source and destination traffic to the same IP using different interface occurs, the Linux kernel drops the traffic as potentially spoofed. This is called reverse-path filtering.

To enable/disable reverse-path filtering, use the following command.

Command	Mode	Description
ip configuration all rp_filter <0-2>	Global	Enables reverse-path filtering for source validation. 0: no source validation (default) 1: strict mode- Each incoming packet is tested against the FIB and if the interface is not the best reverse path and the packet check will fail. The failed packets are discarded. 2: loose mode- Each incoming packet's source address is also tested against the FIB and if the source address is not reachable via any interface the packet check will fail.
no ip configuration all rp_filter		Disables reverse-path filtering for source validation.
ip configuration rp_filter <0-2>	Interface [VLAN]	Enables reverse-path filtering for source validation on the interface.
no ip configuration rp_filter		Disables reverse-path filtering for source validation.

To display reverse-path filtering status, use the following command.

Command	Mode	Description
show ip configuration all rp_filter	Global	Shows reverse-path filtering status.

9.18 Blocking Direct Broadcasting Packets

RFC 2644 recommends that system blocks broadcast packet of same network bandwidth with interface of equipment, namely direct broadcast packet. Hereby, LD3032 is supposed to block direct broadcast packet by default setting. However, you can enable or disable it in LD3032.

To block/unblock the direct broadcast packet forwarding, use the following command.

Command	Mode	Description
no ip forward direct-broadcast	Global	Enables the system to block the direct broadcast packets. (Default)
ip forward direct-broadcast		Disables the system to block the direct broadcast packets.

9.19 Blocking Packet Flooding

If the broadcast/DLF flooding block function is enabled on the some ports/interfaces, the broadcast /DLF packets are blocked between the those ports. This configuration does not apply to the broadcast /DLF flooding from/to uplink ports.

To configure port blocking for broadcast or DLF packet flooding, use the following command.

Command	Mode	Description
flood-block broadcast	Interface [XE/GE/GPON]	Enables the interface/port to be blocked for broadcast packet flooding.
flood-block dlf		Enables the interface/port to be blocked for destination lookup failure (DLF) packet flooding.
no flood-block {**broadcast** | **dlf**}		Disables the interface/port to be blocked for DLF/broadcast packet flooding.

To display the configured port blocking function, use the following command.

Command	Mode	Description
show flood-block	Enable Global Interface-all	Shows the DLF/broadcast packet blocking configuration.

10 IP Multicast

IP communication provides three types of packet transmission: unicast, broadcast and multicast. Unicast is the communication for a single source host to a single destination host. This is still the most common transmission form in the IP network. Broadcast is the communication for a single source host to all destination hosts on a network segment. This transmission is also widely used especially by network protocols, but it sometimes may not be efficient for those hosts in the subnet who are not participating in the broadcast. Multicast is the communication for a single or many source hosts to a specific group of destination hosts, which is interested in the information from the sources. This type of packet transmission can be deployed for a number of applications with more efficient utilization of the network infrastructure.

The point of implementing multicast is how to deliver source traffic to specific destinations without any burden on the sources or receivers using the minimized network bandwidth. The solution is to create a group of hosts with addressing the group, and to let the network determine how to replicate the source traffic to the receivers. The traffic will then be addressed to the multicast address and replicated to the multiple receivers by network devices. Standard multicast protocols such as IGMP and PIM provides most of these capabilities.

IP multicast features on the LD3032 consist of the group membership management, Layer 2 multicast forwarding, and Layer 3 multicast routing, which allow network administrators to successfully achieve the effective and flexible multicast deployment.

Fig. 10.1 an example of the IP multicast network. In this case, the LD3032 is configured only with IGMP snooping (L2 multicast forwarding feature) in the Layer 2 network.

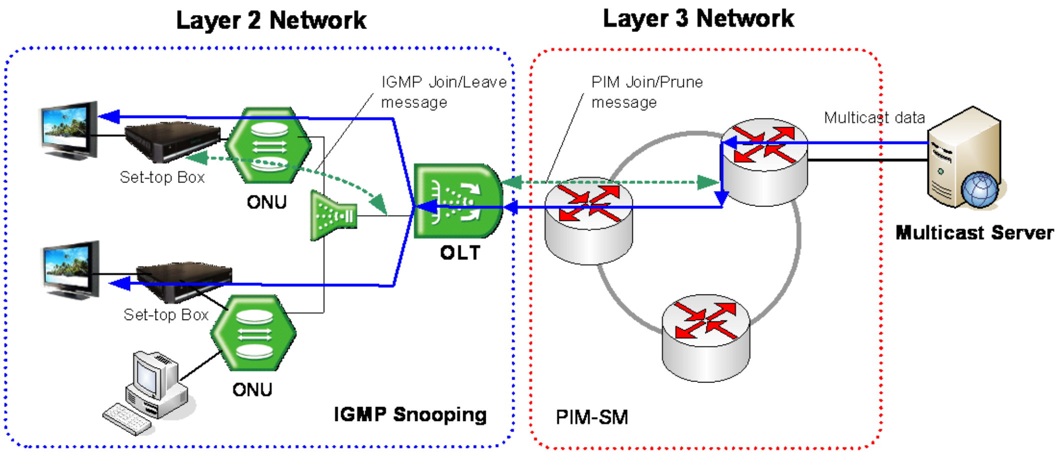


Fig. 10.1 The LD3032 with IGMP Snooping

When installed within the Layer 3 network as a router, the LD3032 should be configured with a multicast routing protocol. However, an additional switch performing IGMP snooping is needed for subscribers in the Layer 2 network. Fig. 10.2 shows an example of the LD3032 with PIM-SM (L3 multicast routing protocol) in the Layer 3 network.

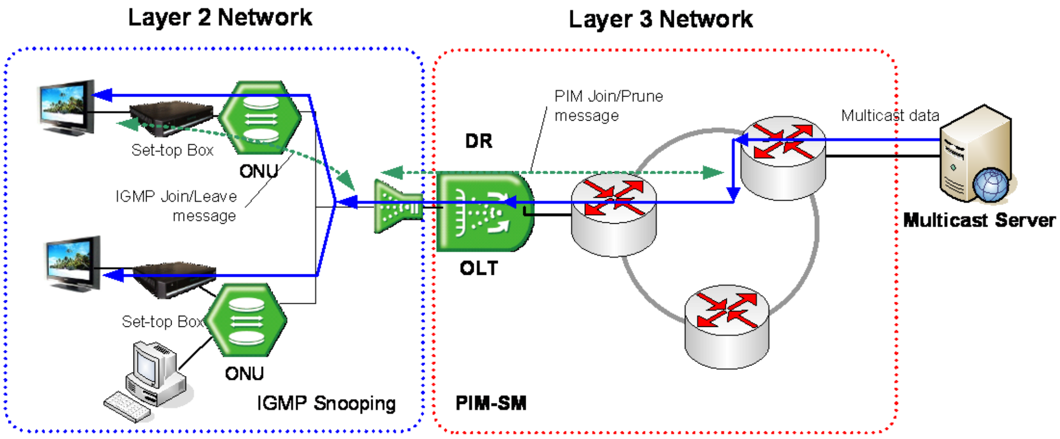


Fig. 10.2 The LD3032 with PIM-SM

If more than one port are on the same Layer 2 interface and the LD3032 is a border router of the Layer 3 network, you should configure the LD3032 with both IGMP snooping and PIM-SM together. Fig. 10.3 shows the example of the multicast network with the LD3032 configured with both IGMP snooping and PIM-SM.

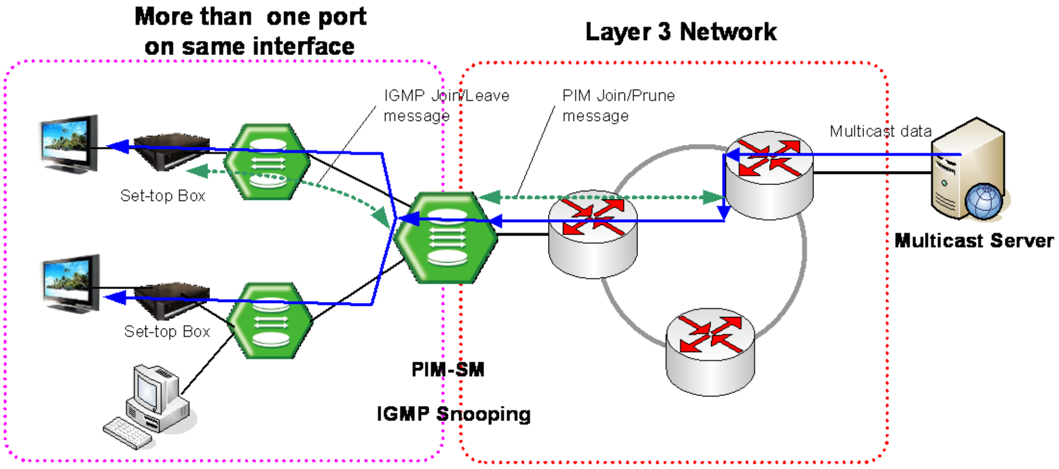


Fig. 10.3 The LD3032 with IGMP Snooping and PIM-SM

10.1 Multicast Group Membership

The most important implementation of the multicast is the group membership management. The multicast group membership allows a router to know which host is interested in receiving the traffic from a certain multicast group and to forward the multicast traffic corresponding to the group to that host. Even if there is more than one host interested in the group, the router forwards only one copy of the traffic stream to minimize the use of network bandwidth.

Internet Group Management Protocol (IGMP) is a protocol used by routers and hosts to manage the multicast group membership. Using IGMP, hosts express an interest in a certain multicast group, and routers maintain the multicast group membership database by collecting the interests from the hosts.

The LD3032 supports IGMP version 1, 2, and 3 each defined in RFC 1112, 2236, and 3376.

10.1.1 IGMP Basic

Internet Group Management Protocol (IGMP) manages the host membership in multicast groups. The hosts inform a neighboring multicast router that they are interested in receiving the traffic from a certain multicast group by sending the membership report (join a group). The router then forwards the multicast traffic corresponding to the report to the hosts.

A multicast router called as a querier is responsible for keeping track of the membership state of the multicast groups by sending periodic general query messages to current interested hosts. If there are no responses to the query from the hosts for a given time (leave a group), the router then stops forwarding the traffic. During the above transaction between hosts and routers, they are using IGMP messages to report or query the group membership.

IGMP has three versions that are supported by hosts and routers. The followings are the simple definitions of each version:

- **IGMP Version 1**
  The basic query-response mechanism for the group membership management is introduced. Routers, however, should use the timeout-based mechanism to discover members with no longer interests in the groups since there is no leave process.

- **IGMP Version 2**
  IGMP messages such as leave group and specific-group query are added for the explicit leave process. This process greatly reduces the leave latency compared to IGMP version 1. Unwanted and unnecessary traffic can be constrained much faster.

- **IGMP Version 3**
  The source filtering is supported. That is, hosts now can join a group with specifying including/excluding a set of sources, allowing supporting the source-specific multicast (SSM). It also increases the multicast address capability, and enhances the security from unknown multicast sources.

10.1.1.1 IGMP Version

By default, the LD3032 runs IGMP version 2. To change the IGMP protocol version on a current interface, use the following command.

Command	Mode	Description
ip igmp version <1-3>	Interface [VLAN]	Sets an IGMP version on a current interface. 1-3: IGMP version (default: 2)
no ip igmp version		Sets to the default setting.

i Routers running different versions of IGMP negotiate the lowest common version of IGMP that is supported by hosts on their subnet and operate in that version.

10.1.1.2 Querier's Robustness Variable

You can statically configure the Querier's Robustness Variable (QRV) field in the membership query message for IGMP version 2 and 3. The QRV allows tuning for the expected packet loss on a network. If a network is expected to be lossy, the QRV value may be increased. When receiving the query message that contains a certain QRV value from a querier, a host returns the report message as many as the specified QRV value.

To configure the QRV value on an interface, use the following command.

Command	Mode	Description
ip igmp robustness-variable <2-7>	Interface [VLAN]	Configures the Querier's Robustness Variable (QRV) value on an interface. (default: 2)
no ip igmp robustness-variable		Deletes a specified QRV value.

10.1.1.3 Clearing IGMP Entry

To clear IGMP entries, use the following command.

Command	Mode	Description
clear ip igmp	Enable Global	Deletes all IGMP entries.
clear ip igmp interface *INTERFACE*		Deletes the IGMP entries learned from a specified interface. INTERFACE: interface name
clear ip igmp group {***** | *A.B.C.D* [*INTERFACE*]}		Deletes IGMP entries in a specified IGMP group. *: all IGMP group A.B.C.D: IGMP group address

10.1.1.4 IGMP Debug

To enable debugging of all IGMP or a specific feature of IGMP, use the following command.

Command	Mode	Description
debug igmp {**all** | **decode** | **encode** | **events** | **fsm** | **tib**}	Enable	Enables IGMP debugging. all: all IGMP decode: IGMP decoding encode: IGMP encoding events: IGMP events fsm: IGMP Finite State Machine (FSM) tib: IGMP Tree Information Base (TIB)
no debug igmp {**all** | **decode** | **encode** | **events** | **fsm** | **tib**}		Disables IGMP debugging.

i

Tree Information Base (TIB) is the collection of state at a router that has been created by receiving IGMP messages from local hosts.

To display the debugging information, use the following command.

Command	Mode	Description
show debugging igmp	Enable Global	Shows the debugging information of IGMP.

10.1.2 IGMP Version 2

In IGMP version 2, the new extensions such as the leave process, election of an IGMP querier, and membership report suppression are added. New IGMP messages, the leave group and group-specific query can be used by hosts to explicitly leave groups, resulting in great reduction of the leave latency.

IGMPv2 Messages

There are three types of IGMPv2 messages of concern to the host-router interaction as shown below:

- **Membership query**
  A multicast router determines if any hosts are listening to a group by sending membership queries. The membership queries have two subtypes.
  – **General query**: This is used to determine if any hosts are listening to any group.
  – **Group-specific query**: This is used to determine if any hosts are listening to a particular group.

- **Version 2 membership report**
  This is used by hosts to join a group (unsolicited) or to respond to membership queries (solicited).

- **Leave group**
  This is used to explicitly leave a group.

IGMPv2 Operation

An IGMP querier is the only router that sends membership query messages for a network segment. In IGMP version 2, the querier is a router with the lowest IP address on the subnet. If the router hears no queries during the timeout period, it becomes the querier.

A host joins multicast groups by sending unsolicited membership report messages indicating its wish to receive multicast traffic for those groups (indicating that the host wants to become a member of the groups).

The querier sends general query messages periodically to discover which multicast groups have members on the attached networks of the router. The messages are addressed to the all-hosts multicast group, which has the address of 224.0.0.1 with a time-to-live (TTL) value of 1. If hosts do not respond to the received query messages for the maximum response time advertised in the messages, a multicast router discovers that no local hosts are members of a multicast group, and then stops forwarding multicast traffic onto the local network from the source for the group.

When hosts respond to membership queries from an IGMP querier, membership reports from the hosts other than the first one are suppressed to avoid increasing the unnecessary traffic. For an IGMP querier, it is sufficient to know that there is at least one interested member for a group on the network segment.

When a host is not interested in receiving the multicast traffic for a particular group any more, it can explicitly leave the group by sending leave group messages. Upon receiving a leave message, a querier then sends out a group-specific query message to determine if there is still any host interested in receiving the traffic. If there is no reply, the querier stops forwarding the multicast traffic.

10.1.2.1 IGMP Static Join

When there are no more group members on a network segment or a host cannot report its group membership using IGMP, multicast traffic is no longer transmitted to the network segment. However, you may want to pull down multicast traffic to a network segment to reduce the time from when an IGMP join request is made to when the requested stream begins arriving at a host, which is called the zapping time.

The IGMP static join feature has been developed to reduce the zapping time by statically creating a virtual host that behaves like a real on a port, even if there is no group member in the group where the port belongs. As a result, a multicast router realizes there is still group member, allowing multicast traffic to be permanently reachable on the group.

To configure the IGMP static join, use the following command.

Command	Mode	Description
ip igmp join-group *A.B.C.D* **vlan** *VLAN_NAME* **port** *PORT* [**reporter** *A.B.C.D*]	Global	Configures the IGMP static join group. A.B.C.D: IGMP group address VLAN_NAME: VIAN name reporter: host address
no ip igmp join-group		Deletes the configured IGMP static join group. *: all addresses
no ip igmp join-group {*A.B.C.D* |		

vlan *VLAN*}		
no ip igmp join-group *A.B.C.D* **vlan** *VLAN_NAME* [**port** *PORT*]		
no ip igmp join-group *A.B.C.D* **vlan** *VLAN_NAME* **port** *PORT* **reporter** {*A.B.C.D* | *}		

To configure the IGMP static join for a range of IGMP groups by access lists, use the following command.

Command	Mode	Description
ip igmp join-group list {<1-99> | <1300-1999> | WORD} **vlan** *VLAN_NAME* **port** *PORT* [**reporter** *A.B.C.D*]	Global	Configures the IGMP static join for a range of IGMP groups by access lists. 1-99: IP standard access list 1300-1999: IP standard access list (extended range) WORD: access list name VLAN_NAME: VLAN name reporter: host address
no ip igmp join-group list {<1-99> | <1300-1999> | WORD}		Deletes the configured IGMP static join for a range of IGMP groups. *: all addresses
no ip igmp join-group list {<1-99> | <1300-1999> | WORD} **vlan** *VLAN_NAME* [**port** *PORT*]		
no ip igmp join-group list {<1-99> | <1300-1999> | WORD} **vlan** *VLAN_NAME* **port** *PORT* **reporter** {*A.B.C.D* | *}		

To display the IGMP static join group list, use the following command.

Command	Mode	Description
show ip igmp join-group	Enable Global	Shows the IGMP static join group list. 1-99: IP standard access list 1300-1999: IP standard access list (extended range) WORD: access list name VLAN_NAME: VLAN name
show ip igmp join-group list		
show ip igmp join-group list {<1-99> | <1300-1999> | WORD} [**vlan** *VLAN_NAME*]		

If you do not specify the **reporter** option, the IP address configured on the VLAN is used as the source address of the membership report by default. If no IP address is configured on the VLAN, 0.0.0.0 is then used.

This feature only supports an IGMPv2 host; it does not support IGMPv3 host.

10.1.2.2 IGMP Access Control

Multicast routers send membership query messages to determine which multicast groups have members in the attached local networks of the router. If hosts respond to the queries, the routers then forward all packets addressed to the multicast group to these group members. You can restrict hosts on a network to join multicast groups on the specified access list.

To control an access to multicast groups on an interface, use the following command.

Command	Mode	Description
ip igmp access-group {<1-99> | *WORD*}	Interface [VLAN]	Enables an IGMP access control on an interface. 1-99: IP standard access list WORD: access list name
no ip igmp access-group		Disables a configured IGMP access control.

10.1.2.3 IGMP Querier Configuration

An IGMP querier is the only router that sends membership query messages for a network segment. In IGMP version 2, the querier is a router with the lowest IP address on the subnet. If the router hears no queries for the timeout period, it becomes the querier.

IGMP Query Interval

The querier (a multicast router) sends general query messages periodically to discover which multicast groups have members on the attached networks of the router.

To specify an interval to send general query messages, use the following command.

Command	Mode	Description
ip igmp query-interval <1-18000>	Interface [VLAN]	Specifies a general query interval. 1-18000: query interval (default: 125 seconds)
no ip igmp query-interval		Deletes a specified general query interval.

IGMP Startup Query Interval

The LD3032 needs to acquire information of its multicast members for the updated membership when it becomes the querier on the specified IGMP interface. For the updated membership, LD3032 sends general query messages as a querier. You can specify the interval to send this query messages as many as the configured QRV value.

To specify the interval to send general query messages, use the following command.

Command	Mode	Description
ip igmp startup-query-interval <1-18000>	Interface [VLAN]	Specifies a startup query interval. 1-18000: startup query interval (Default: 31 seconds)
no ip igmp startup-query-interval		Deletes a specified startup query interval.

IGMP Query Response Time

In IGMP version 2 and 3, membership query messages include the maximum query response time field. This field specifies the maximum time allowed before sending a responding report. The maximum query response time allows a router to quickly detect that there are no more directly connected group members on a network segment.

To specify a maximum query response time advertised in membership query messages, use the following command.

Command	Mode	Description
ip igmp query-max-response-time <1-240>	Interface [VLAN]	Specifies a maximum query response time. 1-240: maximum response time (default: 10 seconds)
no ip igmp query-max-response-time		Deletes a specified maximum query response time.

IGMP Querier Timeout

There should be a single querier on a network segment to prevent duplicating multicast traffic for connected hosts. When there are several routers, if the router has the lowest IP address or if the router hears no queries during the timeout period, it becomes the querier.

To specify a timeout period before a router takes over as a querier for the interface after the previous querier has stopped querying, use the following command.

Command	Mode	Description
ip igmp querier-timeout <60-300>	Interface [VLAN]	Specifies an IGMP queier timeout period. 60-300: timeout period (default: 255 seconds)
no ip igmp querier-timeout		Deletes a specified IGMP queier timeout period.

IGMP Last Member Query Count and Interval

When a host is not interested in receiving the multicast traffic for a particular group any more, it can explicitly leave the group by sending leave group messages.

Upon receiving a leave message, a querier then sends out a group-specific (IGMPv2) or group-source-specific query (IGMPv3) message to determine if there is still any host interested in receiving the traffic. If there is no reply, the querier stops forwarding the multicast traffic. However, IGMP messages may get lost for various reasons, so you can specify the number of sending query messages and its interval.

To specify the number of sending group-specific or group-source-specific query messages, use the following command.

Command	Mode	Description
ip igmp last-member-query-count <2-7>	Interface [VLAN]	Specifies a last member query count. 2-7: last member query count value (default: 2)
no ip igmp last-member-query-count		Deletes a specified last member query count.

To specify the interval to send group-specific or group-source-specific query messages, use the following command.

Command	Mode	Description
ip igmp last-member-query-interval <1000-25500>	Interface [VLAN]	Specifies a last member query interval. 1000-25500: last member query interval (default: 1000 milliseconds)
no ip igmp last-member-query-interval		Deletes a specified last member query interval.

IGMP Unsolicited Report Interval

When one of its hosts joins a multicast address group to which none of its other hosts belong, sends unsolicited group membership reports to that group. You can specify the interval to send this unsolicited report messages as many as the configured QRV value.

To specify the interval to send unsolicited report messages, use the following command.

Command	Mode	Description
ip igmp unsolicited-report-interval <1-18000>	Interface [VLAN]	Specifies an unsolicited report interval. 1-18000: unsolicited report interval (default: 10 seconds)
no ip igmp unsolicited-report-interval		Deletes a specified unsolicited report interval.

10.1.2.4 IGMP Immediate Leave

Normally, a querier sends a group-specific or group-source-specific query message upon receipt of a leave message from a host. If you want to set a leave latency as 0 (zero), you can omit the querying procedure. When the querying procedure is omitted, the router immediately removes the interface from the IGMP cache for that group, and informs the multicast routing protocols.

To enable the immediate leave feature on a current interface, use the following command.

Command	Mode	Description
ip igmp immediate-leave group-list {<1-99> | <1300-1999> | *WORD*}	Interface [VLAN]	Enables the IGMP immediate leave. 1-99: IP standard access list 1300-1999: IP standard access list (extended range) WORD: access list name
no ip igmp immediate-leave		Disables the IGMP immediate leave.

Use this command only on IGMPv2 and IGMPv3 interfaces to which one IGMP host is connected. If there is more than one IGMP host connected to a network segment through the same interface, and a certain host sends a leave group message, the router will remove all hosts on the interface from the multicast group. The router will lose contact with the hosts that should remain in the multicast group until they send join requests in response to the router's next general query.

10.1.3 IGMP Version 3

IGMP version 3 provides support for the source filtering, which is to receive multicast traffic for a group from specific source addresses, or from except specific source addresses, allowing the Source-Specific Multicast (SSM) model.

The source filtering is implemented by the major revision of the membership report. IGMPv3 membership reports contain two types of the record: current-state and state-change. Each record specifies the information of the filter mode and source list. The report can contain multiple group records, allowing reporting of full current state using fewer packets.

The LD3032 runs IGMPv3 by default, and there are no additional IGMPv3 parameters you need to configure. IGMPv3 snooping features are provided.

IGMPv3 Messages

There are two types of IGMPv3 messages of concern to the host-router interaction as shown below:

- **Membership query**
  A multicast router determines if any hosts are listening to a group by sending membership queries. There are three variants of the membership queries.
  – **General query**: This is used to determine if any hosts are listening to any group.
  – **Group-specific query**: This is used to determine if any hosts are listening to a particular group.
  – **Group-source-specific query**: This is used to determine if any hosts are listening to a particular group and source.

- **Version 3 membership report**
  This is used by hosts to report the current multicast reception state, or changes in the multicast reception state, of their interfaces. IGMPv3 membership reports contain a group record that is a block of fields containing information of the host's membership in a single multicast group on the interface from which the report is sent. A single report may also contain multiple group records. Each group record has one of the following information:
  – **Current-state**: This indicates the current filter mode including/excluding the specified multicast address.
  – **Filter-mode-change**: This indicates a change from the current filter mode to the other mode.
  – **Source-list-change**: This indicates a change allowing/blocking a list of the multicast sources specified in the record.

IGMPv3 Operation

Basically, IGMPv3 has the same join/leave (allow/block in the IGMPv3 terminology) and query-response mechanism as IGMPv2’s. Due to the major revision of the membership report, however, leave group messages are not used for the explicit leave process any longer. In IGMPv3 concept, membership reports with state-change records are used to allow or block multicast sources, and those with current-state records are used to respond to membership queries. Membership report suppression feature has been removed for multicast routers to keep track of membership state per host.

10.1.4 Displaying IGMP Information

To display current IGMP groups and relevant information, use the following command.

Command	Mode	Description
show ip igmp groups [**detail**]	Enable Global	Shows the multicast groups with receivers directly connected to the router and learned through IGMP. A.B.C.D: IGMP group address IFPORT: physical interface port number (SLOT#/PORT#, e.g. 0/1, 0/2, 1/1)
show ip igmp groups *A.B.C.D* [**detail**]		
show ip igmp groups { **gigabitethernet** | **tengigabitethernet** | **gpon** | **channelgroup**} *IFPORT* [**detail**]		
show ip igmp groups vlan *VLAN* [**detail**]		
show ip igmp groups *INTERFACE A.B.C.D* [**detail**]		
show ip igmp groups summary		
show ip igmp groups { **gigabitethernet** | **tengigabitethernet** | **gpon** | **channelgroup**} *IFPORT* {*A.B.C.D* [**detail**] | **summary**}		
show ip igmp interface		Shows multicast-related information on an interface.
show ip igmp inter*face* { **gigabitethernet** | **tengigabitethernet** | **gpon** | **channelgroup**} *IFPORT*		

10.2 Multicast Functions

The LD3032 provides various multicast functions including Layer 2 multicast forwarding, which allow you to achieve the fully effective and flexible multicast deployment.

10.2.1 Multicast Forwarding Database

Internally, the LD3032 forwards the multicast traffic referred to the multicast forwarding database (McFDB). The McFDB maintains multicast forwarding entries collected from multicast protocols and features, such as PIM, IGMP, etc.

The McFDB has the same behavior as the Layer 2 FDB. When certain multicast traffic comes to a port, the switch looks for the forwarding information (the forwarding entry) for the traffic in the McFDB. If the McFDB has the information for the traffic, the switch forwards it to the proper ports. If the McFDB does not have the information for the traffic, the switch learns the information on the McFDB, and then floods it to all ports. If the information is not referred to forward another multicast traffic during the given aging time, it is aged out from the McFDB.

10.2.1.1 Blocking Unknown Multicast Traffic

When certain multicast traffic comes to a port and the McFDB has no forwarding information for the traffic, the multicast traffic is flooded to all ports by default. You can configure the switch not to flood unknown multicast traffic.

To configure the switch to discard unknown multicast traffic, use the following command.

Command	Mode	Description
ip unknown-multicast [**port** *PORTS*] **block**	Global	Configures the switch to discard unknown multicast traffic. PORTS: port number (1/1, 1/2, 2/1, …)
no ip unknown-multicast [**port** *PORTS*] **block**		Configures the switch to flood unknown multicast traffic. (default)

⚠ This command should not be used for the ports to which a multicast router is attached!

10.2.1.2 Forwarding Entry Aging

To specify the aging time for forwarding entries on the McFDB, use the following command.

Command	Mode	Description
ip mcfdb aging-time <10-10000000>	Global	Specifies the aging time for forwarding entries on the McFDB. 10-10000000: aging time (default: 300 seconds)
no ip mcfdb aging-time		Deletes the specified aging time for forwarding entries.

To specify the maximum number of forwarding entries on the McFDB, use the following command.

Command	Mode	Description
ip mcfdb aging-limit <256-65535>	Global	Specifies the maximum number of forwarding entries on the McFDB. 256-65535: number of entries (default: 5000)
no ip mcfdb aging-limit		Deletes the specified maximum number of forwarding entries.

10.2.1.3 Displaying McFDB Information

To display McFDB information, use the following command.

Command	Mode	Description
show ip mcfdb	Enable Global	Shows the current aging time and maximum number of forwarding entries.
show ip mcfdb aging-entry [**vlan** *VLAN* | **group** *A.B.C.D*] [**mac-based** | **detail**]		Shows the current forwarding entries. VLAN: VLAN ID (1-4094) A.B.C.D: multicast group address mac-based: lists entries on a MAC address basis

To clear multicast forwarding entries, use the following command.

Command	Mode	Description
clear ip mcfdb {* | **vlan** *VLAN*}	Enable Global	Clears multicast forwarding entries. *: all forwarding entries VLAN: VLAN ID (1-4094)
clear ip mcfdb vlan *VLAN* **group** *A.B.C.D* **source** *A.B.C.D*		Clears a specified forwarding entry. group: multicast group source: multicast source

10.2.2 IGMP Snooping Basic

Layer 2 switches normally flood multicast traffic within the broadcast domain, since it has no entry in the Layer 2 forwarding table for the destination address. Multicast addresses never appear as source addresses, therefore the switch cannot dynamically learn multicast addresses. This multicast flooding causes unnecessary bandwidth usage and discarding unwanted frames on those nodes which did not want to receive the multicast transmission. To avoid such flooding, IGMP snooping feature has been developed.

The purpose of IGMP snooping is to constrain the flooding of multicast traffic at Layer 2. IGMP snooping, as implied by the name, allows a switch to snoop the IGMP transaction between hosts and routers, and maintains the multicast forwarding table which contains the information acquired by the snooping. When the switch receives a join request from a host for a particular multicast group, the switch then adds a port number connected to the host and a destination multicast group to the forwarding table entry; when the switch receives a leave message from a host, it removes the entry from the table.

By maintaining this multicast forwarding table, the LD3032 dynamically forward multicast traffic only to those interfaces that want to receive it as nominal unicast forwarding does.

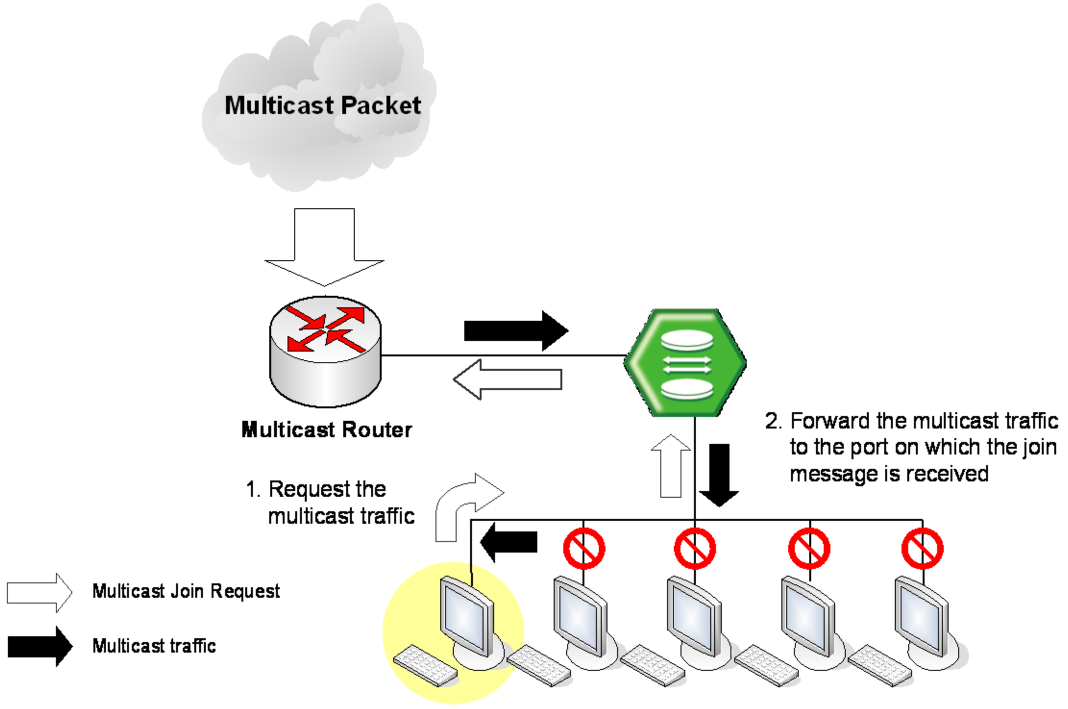

Multicast Packet
Multicast Router
2. Forward the multicast traffic to the port on which the join message is received
1. Request the multicast traffic
Multicast Join Request
Multicast traffic

Fig. 10.4 IGMP Snooping

10.2.2.1 Enabling IGMP Snooping

You can enable IGMP snooping globally or on each VLAN respectively. By default, IGMP snooping is globally disabled.

To enable IGMP snooping, use the following command.

Command	Mode	Description
ip igmp snooping	Global	Enables IGMP snooping globally.
ip igmp snooping vlan *VLANS*		Enables IGMP snooping on a VLAN. VLANS: VLAN ID (1-4094)

To disable IGMP snooping, use the following command.

Command	Mode	Description
no ip igmp snooping	Global	Disables IGMP snooping globally.
no ip igmp snooping vlan *VLANS*		Disables IGMP snooping on a VLAN. VLANS: VLAN ID (1-4094)

10.2.2.2 IGMP Snooping Version

The membership reports sent to the multicast router are sent based on the IGMP snooping version of the interface. If you statically specify the version on a certain interface, the reports are always sent out only with the specified version. If you do not statically specify the version, and a version 1 query is received on the interface, the interface dynamically sends out a version 1 report. If no version 1 query is received on the interface for the version 1 router present timeout period (400 seconds), the interface version goes back to its default value (3).

To specify the static IGMP snooping version, use the following command.

Command	Mode	Description
ip igmp snooping version <1-3>	Global	Configures the IGMP snooping version globally. 1-3: IGMP snooping version (default: 3)
ip igmp snooping vlan *VLANS* **version** <1-3>		Configures the IGMP snooping version on a VLAN interface. VLANS: VLAN ID (1-4094)

To delete the specified static IGMP snooping version, use the following command.

Command	Mode	Description
no ip igmp snooping version	Global	Deletes the specified IGMP snooping version.
no ip igmp snooping vlan *VLANS* **version**		

i

Dynamic IGMPv3 snooping is configured by default.

10.2.2.3 IGMP Snooping Robustness Value

The robustness variable allows tuning for the expected packet loss on a network. If a network is expected to be lossy, the robustness variable may be increased. When receiving the query message that contains a certain robustness variable from an IGMP snooping querier, a host returns the report message as many as the specified robustness variable.

To configure the robustness variable, use the following command.

Command	Mode	Description
ip igmp snooping robustness-variable <1-7>	Global	Configures the robustness variable. (default: 2)
ip igmp snooping vlan *VLANS* **robustness-variable** <1-7>		Configures the robustness variable on a VLAN. VLANS: VLAN ID (1-4094)

To delete a specified robustness variable, use the following command.

Command	Mode	Description
no ip igmp snooping robustness-variable	Global	Deletes a specified robustness variable.
no ip igmp snooping vlan *VLANS* **robustness-variable**		

10.2.2.4 IGMP Snooping R-APS

To enable R-APS (Ring Automatic Protection Switching) packet to protect and recovery switching for Ethernet traffic in a ring topology, use the following command.

Command	Mode	Description
ip igmp snooping r-aps	Global	Enables the IGMP snooping R-APS.
no ip ip igmp snooping r-aps		Disables the IGMP snooping R-APS.

10.2.2.5 IGMP Snooping Source IP Verification

In case that the IGMP source IP address of packets is 0.0.0.0 or 255.255.255.255, the switch handles the packets according to the user-defined configuration.

To discard/forward the IGMP packets according to the source IP address, use the following command.

Command	Mode	Description
ip igmp snooping verify-sip	Global	Discards the IGMP packets if the IGMP source IP address is 0.0.0.0 or 255.255.255.255.
no ip igmp snooping verify-sip		Forwards the IGMP packets even if the IGMP source IP address is 0.0.0.0 or 255.255.255.255.

10.2.3 IGMPv2 Snooping

10.2.3.1 IGMP Snooping Querier Configuration

IGMP snooping querier should be used to support IGMP snooping in a VLAN where PIM and IGMP are not configured.

When the IGMP snooping querier is enabled, the IGMP snooping querier sends out periodic general queries that trigger membership report messages from a host that wants to receive multicast traffic. The IGMP snooping querier listens to these membership reports to establish appropriate forwarding.

Enabling IGMP Snooping Querier

To enable the IGMP snooping querier, use the following command.

Command	Mode	Description
ip igmp snooping querier [**address** *A.B.C.D*]	Global	Enables the IGMP snooping querier globally. A.B.C.D: source address of IGMP snooping query
ip igmp snooping vlan *VLANS* **querier** [**address** *A.B.C.D*]		Enables the IGMP snooping querier on a VLAN. VLANS: VLAN ID (1-4094)

To disable the IGMP snooping querier, use the following command.

Command	Mode	Description
no ip igmp snooping querier [**address**]	Global	Disables the IGMP snooping querier. address: source address of IGMP snooping query
no ip igmp snooping vlan *VLANS* **querier** [**address**]		

If you do not specify a source address of an IGMP snooping query, the IP address configured on the VLAN is used as the source address by default. If no IP address is configured on the VLAN, 0.0.0.0 is then used.

IGMP Snooping Query Interval

An IGMP snooping querier periodically sends general query messages to trigger membership report messages from a host that wants to receive IP multicast traffic.

To specify an interval to send general query messages, use the following command.

Command	Mode	Description
ip igmp snooping querier query-interval <1-1800>	Global	Specifies an IGMP snooping query interval in the unit of second. 1-1800: query interval (default: 125)
ip igmp snooping vlan *VLANS* **querier query-interval** <1-1800>		Specifies an IGMP snooping query interval on a VLAN. VLANS: VLAN ID (1-4094)

To delete a specified interval to send general query messages, use the following command.

Command	Mode	Description
no ip igmp snooping querier query-interval	Global	Disables a specified IGMP snooping query interval.
no ip igmp snooping vlan *VLANS* **querier query-interval**		

IGMP Snooping Query Response Time

Membership query messages include the maximum query response time field. This field specifies the maximum time allowed before sending a responding report. The maximum query response time allows a router to quickly detect that there are no more hosts interested in receiving multicast traffic.

To specify a maximum query response time advertised in general query messages, use the following command.

Command	Mode	Description
ip igmp snooping querier max-response-time <1-25>	Global	Specifies a maximum query response time. 1-25: maximum response time (default: 10 seconds)
ip igmp snooping vlan *VLANS* **querier max-response-time** <1-25>		Specifies a maximum query response time. VLANS: VLAN ID (1-4094)

To delete a specified maximum query response time, use the following command.

Command	Mode	Description
no ip igmp snooping querier max-response-time	Global	Deletes a specified maximum query response time.
no ip igmp snooping vlan *VLANS* **querier max-response-time**		

Displaying IGMP Snooping Querier Information

To display IGMP querier information and configured parameters, use the following command.

Command	Mode	Description
show ip igmp snooping [**vlan** *VLANS*] **querier** [**detail**]	Enable Global	Shows IGMP querier information and configured parameters.

10.2.3.2 IGMP Snooping Last Member Query Interval

Upon receiving a leave message, a switch with IGMP snooping then sends out a group-specific (IGMPv2) or group-source-specific query (IGMPv3) message to determine if there is still any host interested in receiving the traffic. If there is no reply, the switch stops forwarding the multicast traffic. However, IGMP messages may get lost for various reasons, so you can specify an interval to send query messages.

To specify an interval to send group-specific or group-source-specific query messages, use the following command.

Command	Mode	Description
ip igmp snooping last-member-query-interval <100-10000>	Global	Specifies a last member query interval. 100-10000: last member query interval (default: 1000 milliseconds)
ip igmp snooping vlan *VLANS* **last-member-query-interval** <100-10000>		Specifies a last member query interval. VLANS: VLAN ID (1-4094)

To delete a specified an interval to send group-specific or group-source-specific query messages, use the following command.

Command	Mode	Description
no ip igmp snooping last-member-query-interval	Global	Deletes a specified last member query interval.
no ip igmp snooping vlan *VLANS* **last-member-query-interval**		

10.2.3.3 IGMP Snooping Immediate Leave

Normally, an IGMP snooping querier sends a group-specific or group-source-specific query message upon receipt of a leave message from a host. If you want to set a leave latency as 0 (zero), you can omit the querying procedure. When the querying procedure is omitted, the switch immediately removes the entry from the forwarding table for that VLAN, and informs the multicast router.

To enable the IGMP snooping immediate leave, use the following command.

Command	Mode	Description
ip igmp snooping immediate-leave	Global	Enables the IGMP snooping immediate leave globally.
ip igmp snooping port *PORTS* **immediate-leave**		Enables the IGMP snooping immediate leave on a port. PORTS: port number (1/1, 1/2, 2/1, …)
ip igmp snooping vlan *VLANS* **immediate-leave**		Enables the IGMP snooping immediate leave on a VLAN. VLANS: VLAN ID (1-4094)

To disable the IGMP snooping immediate leave, use the following command.

Command	Mode	Description
no ip igmp snooping immediate-	Global	Disables the IGMP snooping immediate leave.

leave		
no ip igmp snooping port *PORTS* **immediate-leave**		
no ip igmp snooping vlan *VLANS* **immediate-leave**		

Use this command with the explicit host tracking feature. If you don't, when there is more than one IGMP host belonging to a VLAN, and a certain host sends a leave group message, the switch will remove all host entries on the forwarding table from the VLAN. The switch will lose contact with the hosts that should remain in the forwarding table until they send join requests in response to the switch's next general query message.

10.2.3.4 IGMP Snooping Report Suppression

If an IGMP querier sends general query messages, and hosts are still interested in the multicast traffic, the hosts should return membership report messages. For a multicast router, however, it is sufficient to know that there is at least one interested member for a group on the network segment. Responding a membership report per each of group members may unnecessarily increase the traffic on the network; only one report per group is enough.

When the IGMP snooping report suppression is enabled, a switch suppresses membership reports from hosts other than the first one, allowing the switch to forward only one membership report in response to a general query from a multicast router.

To enable the IGMP snooping report suppression, use the following command.

Command	Mode	Description
ip igmp snooping report-suppression	Global	Enables the IGMP snooping report suppression globally.
ip igmp snooping vlan *VLANS* **report-suppression**		Enables the IGMP snooping report suppression on a VLAN. VLANS: VLAN ID (1-4094)

To disable the IGMP snooping report suppression, use the following command.

Command	Mode	Description
no ip igmp snooping report-suppression	Global	Disables the IGMP snooping report suppression.
no ip igmp snooping vlan *VLANS* **report-suppression**		

The IGMP snooping report suppression is supported only IGMPv1 and IGMPv2 reports. In case of an IGMPv3 report, a single membership report can contain the information for all the groups which a host is interested in. Thus, there is no need for the report suppression since the number of reports would be generally equal to the number of hosts only.

10.2.3.5 IGMP Snooping S-Query Report Agency

If IGMP snooping switch receives IGMP group-specific query messages from the multicast router, it just floods them into all of its ports. The hosts received the group-specific queries send the report messages according to their IGMP membership status. However, LD3032 is enabled as IGMP snooping S-Query report agency, the group-specific queries are not sent downstream. When the switch receives a group-specific query, the switch terminates the query and sends an IGMP report if there is a receiver for the group.

To enable IGMP snooping S-Query Report Agency, use the following command.

Command	Mode	Description
ip igmp snooping s-query-report-agency	Global	Enables IGMP snooping s-query-report agency.

To disable IGMP snooping S-Query Report Agency, use the following command.

Command	Mode	Description
no ip igmp snooping s-query-report-agency	Global	Disables IGMP snooping s-query-report agency.

10.2.3.6 Explicit Host Tracking

Explicit host tracking is one of the important IGMP snooping features. It has the ability to build the explicit tracking database by collecting the host information via the membership reports sent by hosts. This database is used for the immediate leave for IGMPv2 hosts, the immediate block for IGMPv3 hosts, and IGMP statistics collection.

To enable explicit host tracking, use the following command.

Command	Mode	Description
ip igmp snooping explicit-tracking	Global	Enables explicit host tracking globally.
ip igmp snooping explicit-tracking s-query-suppression		Enables IGMP group specific query suppression under explicit host tracking

To disable explicit host tracking, use the following command.

Command	Mode	Description
no ip igmp snooping explicit-tracking	Global	Disables explicit host tracking globally.
ip igmp snooping explicit-tracking s-query-suppression		Disables IGMP group specific query suppression under explicit host tracking

You can also restrict the number of hosts on a port for the switch performance and enhanced security.

To specify the maximum number of hosts on a port, use the following command.

Command	Mode	Description
ip igmp snooping explicit-tracking max-hosts port *PORTS* **count** <1-65535>	Global	Specifies the maximum number of hosts on a port. PORTS: port number (1/1, 1/2, 2/1, …) 1-65535: maximum number of hosts (default: 1024)
no ip igmp snooping explicit-tracking max-hosts port *PORTS*		Deletes the specified maximum number of hosts

To display the explicit tracking information, use the following command.

Command	Mode	Description
show ip igmp snooping explicit-tracking	Enable Global	Shows the explicit host tracking information globally.
show ip igmp snooping explicit-tracking summary { **vlan** *VLANS* | **port** *PORTS* }		Shows the summary of IGMP snooping explicit-tracking information.
show ip igmp snooping explicit-tracking vlan *VLANS*		Shows the explicit host tracking information per VLAN. VLANS: VLAN ID (1-4094)
show ip igmp snooping explicit-tracking port *PORTS*		Shows the explicit host tracking information per port. PORTS: port number (1/1, 1/2, 2/1, …)
show ip igmp snooping explicit-tracking group *A.B.C.D*		Shows the explicit host tracking information per group. A.B.C.D: multicast group address

i

Explicit host tracking is enabled by default.

10.2.3.7 Multicast Router Port Configuration

The multicast router port is the port which is directly connected to a multicast router. A switch adds multicast router ports to the forwarding table to forward membership reports only to those ports. Multicast router ports can be statically specified or dynamically learned by incoming IGMP queries and PIM hello packets.

Static Multicast Router Port

You can statically configure Layer 2 port as the multicast router port which is directly connected to a multicast router, allowing a static connection to a multicast router.

To specify a multicast router port, use the following command.

Command	Mode	Description
ip igmp snooping mrouter port {*PORTS* | **cpu**}	Global	Specifies a multicast router port globally. PORTS: port number (1/1, 1/2, 2/1, …) cpu: CPU port
ip igmp snooping vlan *VLANS* **mrouter port** {*PORTS* | **cpu**}		Specifies a multicast router port on a VLAN. VLANS: VLAN ID (1-4094)

To delete a specified multicast router port, use the following command.

Command	Mode	Description
no ip igmp snooping mrouter port {*PORTS* | **cpu**}	Global	Deletes a specified multicast router port.
no ip igmp snooping vlan *VLANS* **mrouter port** {*PORTS* | **cpu**}		

Multicast Router Port Learning

Multicast router ports are added to the forwarding table for every Layer 2 multicast entry. The switch dynamically learns those ports through snooping on PIM hello packets.

To enable the switch to learn multicast router ports through PIM hello packets, use the following command.

Command	Mode	Description
ip igmp snooping mrouter learn pim	Global	Enables to learn multicast router ports through PIM hello packets globally.
ip igmp snooping vlan *VLANS* **mrouter learn pim**		Enables to learn multicast router ports through PIM hello packets on a VLAN. VLANS: VLAN ID (1-4094)

To disable the switch to learn multicast router ports through PIM hello packets, use the following command.

Command	Mode	Description
no ip igmp snooping mrouter learn pim	Global	Disables to learn multicast router ports through PIM hello packets.
no ip igmp snooping vlan *VLANS* **mrouter learn pim**		

Multicast Router Port Forwarding

The multicast traffic should be forwarded to IGMP snooping membership ports and multicast router ports because the multicast router needs to receive muticast source information. To enable the switch to forward the traffic to multicast router ports, use the following command.

Command	Mode	Description
ip multicast mrouter-pass-through	Global	Enables to forward multicast traffic to the multicast router ports.
no ip multicast mrouter-pass-through		Disables to forward multicast traffic to the multicast router ports.

Displaying Multicast Router Port

To display a current multicast router port for IGMP snooping, use the following command.

Command	Mode	Description
show ip igmp snooping mrouter	Enable Global	Shows a current multicast router port for IGMP snooping globally.
show ip igmp snooping vlan *VLANS* **mrouter**		Shows a current multicast router port for IGMP snooping on a specified VLAN. VLANS: VLAN ID (1-4094)

10.2.3.8 TCN Multicast Flooding

When a network topology change occurs, the protocols for a link layer topology – such as spanning tree protocol (STP), Ethernet ring protection (ERP), etc – notify switches in the topology using a topology change notification (TCN).

When TCN is received, the switch where an IGMP snooping is running will flood multicast traffic to all ports in a VLAN, since a network topology change in a VLAN may invalidate previously learned IGMP snooping information. However, this flooding behavior is not desirable if the switch has many ports that are subscribed to different groups. The traffic could exceed the capacity of the link between the switch and the end host, resulting in packet loss. Thus, a period of multicast flooding needs to be controlled to solve such a problem.

Enabling TCN Multicast Flooding

To enable the switch to flood multicast traffic when TCN is received, use the following command.

Command	Mode	Description
ip igmp snooping tcn flood	Global	Enables the switch to flood multicast traffic when TCN is received.
ip igmp snooping tcn vlan *VLANS* **flood**		Enables the switch to flood multicast traffic on a VLAN when TCN is received. VLANS: VLAN ID (1-4094)

To disable the switch to flood multicast traffic when TCN is received, use the following command.

Command	Mode	Description
no ip igmp snooping tcn flood	Global	Disables the switch to flood multicast traffic when TCN is received
no ip igmp snooping tcn vlan *VLANS* **flood**		

TCN Flooding Suppression

When TCN is received, the switch where an IGMP snooping is running will flood multicast traffic to all ports until receiving two general queries, or during two general query intervals by default. You can also configure the switch to stop multicast flooding according to a specified query count or query interval.

To specify a query count to stop multicast flooding, use the following command.

Command	Mode	Description
ip igmp snooping tcn flood query count <1-10>	Global	Specifies a query count to stop multicast flooding. 1-10: query count value (default: 2)
no ip igmp snooping tcn flood query count		Deletes a specified query count to stop multicast flooding.

To specify a query interval to stop multicast flooding, use the following command.

Command	Mode	Description
ip igmp snooping tcn flood query interval <1-1800>	Global	Specifies a query interval to stop multicast flooding in the unit of second. An actual stop-flooding interval is calculated by (query count) x (query interval). 1-1800: query interval value (default: 125)
no ip igmp snooping tcn flood query interval		Deletes a specified query interval to stop multicast flooding.

TCN Flooding Query Solicitation

Typically, if a network topology change occurs, the spanning tree root switch issues a query solicitation which is actually a global leave message with the group address 0.0.0.0. When a multicast router receives this solicitation, it immediately sends out IGMP general queries to hosts, allowing the fast convergence. You can direct the switch where an IGMP snooping is running to send a query solicitation when TCN is received.

To enable the switch to send a query solicitation when TCN is received, use the following command.

Command	Mode	Description
ip igmp snooping tcn query solicit [**address** *A.B.C.D*]	Global	Enables the switch to send a query solicitation when TCN is received. address: source IP address for query solicitation

To disable the switch to send a query solicitation when TCN is received, use the following command.

Command	Mode	Description
no ip igmp snooping tcn query solicit [**address**]	Global	Disables the switch to send a query solicitation when TCN is received.

IGMP Snooping TCN Debug

To enable debugging of all IGMP snooping TCN, use the following command.

Command	Mode	Description
debug igmp snooping tcn	Enable	Enables IGMP snooping Topology Change Notification (TCN) debugging.

no debug igmp snooping tcn		Disables IGMP snooping Topology Change Notification (TCN) debugging.

10.2.4 IGMPv3 Snooping

Immediate Block

IGMPv3 immediate block feature allows a host to block sources with the block latency, 0 (zero) by referring to the explicit tracking database. When receiving a membership report with the state-change record from a host that is no longer interested in receiving multicast traffic from a certain source, the switch compares the source list for the host in the explicit tracking database with the source list in the received membership report. If both are matching, the switch removes the source entry from the list in the database, and stops forwarding the multicast traffic to the host; no group-source-specific query message is needed for the membership leave process.

To enable IGMPv3 immediate block, use the following command.

Command	Mode	Description
ip igmp snooping immediate-block	Global	Enables immediate block globally.
ip igmp snooping vlan *VLANS* **immediate-block**		Enables immediate block on a VLAN. VLANS: VLAN ID (1-4094)

To disable IGMPv3 immediate block, use the following command.

Command	Mode	Description
no ip igmp snooping immediate-block	Global	Disables immediate block globally.
no ip igmp snooping vlan *VLANS* **immediate-block**		Disables immediate block on a VLAN. VLANS: VLAN ID (1-4094)

i IGMPv3 immediate block is enabled by default.

10.2.5 Displaying IGMP Snooping Information

To display a current IGMP snooping configuration, use the following command.

Command	Mode	Description
show ip igmp snooping [**vlan** *VLANS*]	Enable Global	Shows a current IGMP snooping configuration. VLAN: VLAN ID (1-4094)
show ip igmp snooping info [**vlan** *VLANS*]		

To display the IGMP snooping table, use the following command.

Command	Mode	Description
show ip igmp snooping groups [*A.B.C.D* | **mac-based**]	Enable Global	Shows the IGMP snooping table globally. mac-based: lists groups on a MAC address basis.
show ip igmp snooping groups port {*PORTS* | **cpu**} [**mac-based**]		Shows the IGMP snooping table per port. PORTS: port number (1/1, 1/2, 2/1, …)
show ip igmp snooping groups vlan *VLANS* [**mac-based**]		Shows the IGMP snooping table per VLAN. VLANS: VLAN ID (1-4094)
show ip igmp snooping groups summary [**port** *PORTS* | **vlan** *VLANS*]		Show the summary of IGMP snooping group membership information per port or VLAN ID

To display the IGMP snooping membership table, use the following command.

Command	Mode	Description
show ip igmp snooping table vlan *VLANS*	Enable Global	Shows the IGMP snooping membership table of specific VLAN ID.
show ip igmp snooping table port *PORTS*		Shows the IGMP snooping membership table of a port number.
show ip igmp snooping table group *A.B.C.D*		Shows the IGMP snooping membership table of specific multicast group address.
show ip igmp snooping table reporter *A.B.C.D*		Shows the IGMP snooping membership table of specific reporter's IP address.

To display the collected IGMP snooping statistics, use the following command.

Command	Mode	Description
show ip igmp snooping stats port {*PORTS* | **cpu**}	Enable Global	Shows the collected IGMP snooping statistics. PORTS: port number (1/1, 1/2, 2/1, …)

To clear the collected IGMP snooping statistics, use the following command.

Command	Mode	Description
clear ip igmp snooping stats port [*PORTS* | **cpu**]	Enable Global	Clears the collected IGMP snooping statistics PORTS: port number (1/1, 1/2, 2/1, …)

Multicast VLAN Registration (MVR)

Multicast VLAN registration (MVR) is designed for applications using multicast traffic across an Ethernet network. MVR allows a multicast VLAN to be shared among subscribers remaining in separate VLANs on the network. It guarantees the Layer 2 multicast flooding instead of the forwarding via Layer 3 multicast, allowing to flood multicast streams in the multicast VLAN, but to isolate the streams from the subscriber VLANs for bandwidth and security reasons. This improves bandwidth utilization and simplifies multicast group management.

MVR also provides the fast convergence for topology changes in the Ethernet ring-based service provider network with STP and IGMP snooping TCN, guaranteeing stable multicast services.

MVR implemented for the LD3032 has the following restrictions, so you must keep in mind those, before configuring MVR.

⚠

- All receiver ports must belong to the both subscriber and multicast VLANs as untagged.
- IGMP snooping must be enabled before enabling MVR.
- A single group address cannot belong to more than two MVR groups.
- MVR and multicast routing cannot be enabled together.
- MVR only supports IGMPv2.

10.2.5.1 Enabling MVR

To enable MVR on the system, use the following command.

Command	Mode	Description
mvr	Global	Enables MVR.
no mvr		Disables MVR.

10.2.5.2 MVR Group

To configure MVR, you need to specify an MVR group and group address. If you specify several MVR groups, IGMP packets from the receiver ports are sent to the source ports belonging to the corresponding MVR group according to the group address specified in the packets.

To specify an MVR group and group address, use the following command.

Command	Mode	Description
mvr vlan *VLAN* **group** *A.B.C.D*	Global	Specifies an MVR group and group address. VLAN: VLAN ID (1-4094) A.B.C.D: IGMP group address
no mvr vlan *VLAN* **group** *A.B.C.D*		Deletes a specified MVR group and group address.

10.2.5.3 Source/Receiver Port

You need to specify the source and receiver ports for MVR. The followings are the definitions for the ports.

- **Source Port**
  This is connected to multicast routers or sources as an uplink port, which receives and sends the multicast traffic. Subscribers cannot be directly connected to source ports. All source ports belong to the multicast VLAN as tagged.
- **Receiver Port**
  This is directly connected to subscribers as a subscriber port, which should only receive the multicast traffic. All receiver ports must belong to the both subscriber and multicast VLANs as untagged for implementation reasons.

To specify a port as the source or receiver port, use the following command.

Command	Mode	Description
mvr port *PORTS* **type** {**receiver** | **source**}	Global	Specifies an MVR port. PORTS: port number (1/1, 1/2, 2/1, …)
no mvr port *PORTS*		Deletes a specified MVR port.

10.2.5.4 MVR Helper Address

When being in a different network from an MVR group’s, a multicast router sends the multicast traffic to each MVR group using Layer 3 multicast routing. In such an environment, when an IGMP packet from a subscriber is transmitted to the multicast router via the MVR group (multicast VLAN interface), the source address of the IGMP packet may not match the network address of the MVR group. In this case, the multicast router normally discards the IGMP packet. To avoid this behavior, you can configure the switch to replace the source address with a specified helper address. The helper address must belong to the MVR group’s network.

To specify an MVR helper address to replace a source address of an IGMP packet, use the following command.

Command	Mode	Description
mvr vlan *VLAN* **helper** *A.B.C.D*	Global	Specifies an MVR helper address. VLAN: VLAN ID (1-4094) A.B.C.D: helper address
no mvr vlan *VLAN* **helper**		Deletes a specified MVR helper address.

10.2.5.5 Displaying MVR Configuration

To display an MVR configuration, use the following command.

Command	Mode	Description
show mvr	Enable Global	Shows an MVR configuration.
show mvr port		
show mvr vlan *VLANS*		

10.2.6 IGMP Filtering and Throttling

IGMP filtering and throttling control the distribution of multicast services on each port. IGMP filtering controls which multicast groups a host on a port can join by associating an IGMP profile that contains one or more IGMP groups and specifies whether an access to the group is permitted or denied with a port. For this operation, configuring the IGMP profile is needed before configuring the IGMP filtering. IGMP throttling limits the maximum number of IGMP groups that a host on a port can join.

Note that both IGMP filtering and throttling control only membership reports (join messages) from a host, and do not control multicast streams.

10.2.6.1 IGMP Filtering

Creating IGMP Profile

You can configure an IGMP profile for IGMP filtering in *IGMP Profile Configuration* mode. The system prompt will be changed from SWITCH(config)# to SWITCH(config-igmp-profile[N])#.

To create/modify an IGMP profile, use the following command.

Command	Mode	Description
ip igmp profile <1-2147483647>	Global	Creates/modifies an IGMP profile. 1-2147483647: IGMP profile number
no ip igmp profile <1-2147483647>		Deletes a created IGMP profile.

IGMP Group Range

To specify an IGMP group range to apply to IGMP filtering, use the following command.

Command	Mode	Description
range *A.B.C.D* [*A.B.C.D*]	IGMP Profile	Specifies a range of IGMP groups. A.B.C.D: low multicast address A.B.C.D: high multicast address
no range *A.B.C.D* [*A.B.C.D*]		Deletes a specified range of IGMP groups.

i

A single IGMP group address is also possible.

IGMP Filtering Policy

To specify an action to permit or deny an access to an IGMP group range, use the following command.

Command	Mode	Description
{**permit** | **deny**}	IGMP Profile	Specifies an action for an IGMP group range.

Enabling IGMP Filtering

To enable IGMP filtering for a port, a configured IGMP profile needs to be applied to the port.

To apply an IGMP profile to ports to enable IGMP filtering, use the following command.

Command	Mode	Description
ip igmp filter port *PORTS* **profile** <1-2147483647>	Global	Applies an IGMP profile to ports PORTS: port number (1/1, 1/2, 2/1, …) 1-2147483647: IGMP profile number
no ip igmp filter port *PORTS*		Releases an applied IGMP profile.

Before enabling IGMP filtering, please keep in mind the following restrictions.

- Plural IGMP profiles cannot be applied to a single port.
- IGMP snooping must be enabled before enabling IGMP filtering.
- To delete a created IGMP profile, all ports where the profile applied must be released.
- IGMP filtering only supports IGMPv2.

By the following command, LD3032 can permit or deny the IGMP packets by referring to its DHCP snooping binding table. This reference enables the system to permit IGMP messages only when the source IP address and MAC address of host have identified from the DHCP snooping binding table.

To permit/discard IGMP packets for the hosts authorized by the DHCP snooping, use the following command.

Command	Mode	Description
ip igmp filter port *PORTS* **permit dhcp-snoop-binding**	Global	Adds the entry to IGMP snooping table when it exists on the DHCP snooping binding table.
no ip igmp filter port *PORTS* **permit dhcp-snoop-binding**		Adds the entry to IGMP snooping table irrespective of DHCP snooping binding table.

To allow or discard IGMP messages by message type on a port, use the following command.

Command	Mode	Description
ip igmp filter port *PORTS* **packet–type** {**reportv1** | **reportv2** | **reportv3** | **query** | **leave** | **all**}	Global	Filters the specified IGMP messages on a port.
no ip igmp filter port *PORTS* **packet–type** {**reportv1** | **reportv2** | **reportv3** | **query** | **leave** | **all**}		Disables filtering the specified IGMP messages on a port.

10.2.6.2 IGMP Throttling

You can configure the maximum number of multicast groups that a host on a port can join. To specify the maximum number of IGMP groups per port, use the following command.

Command	Mode	Description
ip igmp max-groups port *PORTS* **count** <1-2147483647>	Global	Specifies the maximum number of IGMP groups for a port. PORTS: logical port number 1-2147483647: number of IGMP groups
ip igmp max-groups port sum count <1-2147483647>		Specifies the sum of IGMP groups for all of ports. sum: sum of all port counters
no ip igmp max-groups port {*PORTS* | **sum**}		Deletes a specified maximum number of IGMP groups.

To specify the maximum number of IGMP groups for the system, use the following command.

Command	Mode	Description
ip igmp max-groups system count <1-2147483647>	Global	Specifies the maximum number of IGMP groups for the system. 1-2147483647: number of IGMP groups
no ip igmp max-groups system		Deletes a specified maximum number of IGMP groups.

10.2.6.3 Displaying IGMP Filtering and Throttling

To display a configuration for IGMP filtering and throttling, use the following command.

Command	Mode	Description
show ip igmp filter [**port** *PORTS*]	Enable Global	Shows a configuration for IGMP filtering and throttling. PORTS: port number (1/1, 1/2, 2/1, …)

To display existing IGMP profiles, use the following command.

Command	Mode	Description
show ip igmp profile [<1-2147483647>]	Enable Global	Shows existing IGMP profiles. 1-2147483647: IGMP profile number

10.2.7 IGMP Proxy

IGMP Proxy enables this L3 switch to issue IGMP host messages on behalf of hosts that the switch discovered through standard IGMP interfaces. The switch acts as a proxy for its hosts. The LD3032 supports IGMPv2.

IGMP Proxy can only work in a simple tree topology; where traffic is distributed to explicit upstream and downstream. You need to manually designate upstream and downstream interface on IGMP proxy switch. There are no multicast routers within the tree and the root of the tree is expected to be connected to a wider multicast infrastructure.

The IGMP proxy-enabled switch can deliver multicast traffic to the downward LANs or direct hosts without performing complex multicast routing protocol.

IGMP Proxy function is implemented with the following restrictions, so you must keep them in mind before setting IGMP Proxy related commands or parameters.

- It must be used only in a simple tree topology.
- User should manually set upstream and downstream interface for IGMP proxy operation.
- IGMP proxy and PIM on an interface cannot work together.
- It doesn’t support IGMPv3; if IGMPv3 runs on the interface, that interface should not be designated upstream and downstream interface of IGMP proxy switch. At the same time, if a certain interface is configured as upstream or downstream interface, IGMPv3 setting should not be made on that interface.
- It doesn’t work with SSM mapping.
- IGMP proxy is a L3 feature and requires L3 interfaces to use for that function. Also, the **no shutdown** command should be preceded before configuring IGMP proxy interfaces.
- If **ip igmp proxy-service sip first-reporter** is configured, the first reporter’s source IP address of a group remains even though it leaves from the group. The information will be maintained until the group membership record is deleted.

10.2.7.1 Designating Downstream Interface

To specify the downstream interface for IGMP proxy operation, use the following command.

Command	Mode	Description
ip igmp mroute-proxy {**gigabitethernet** | **tengigabitethernet** | **gpon** | **channelgroup**} *IFPORT*	Interface [VLAN]	Designates the downstream interface of mroute proxy.
ip igmp mroute-proxy vlan *VLANS*		
no ip igmp mroute-proxy {**gigabitethernet** | **tengigabitethernet** | **gpon** | **channelgroup**} *IFPORT*		Release the downstream interface of mrouter proxy.
no ip igmp mroute-proxy vlan *VLANS*		

10.2.7.2 Designating Upstream Interface

To specify the upstream interface for IGMP proxy operation, use the following command.

Command	Mode	Description
ip igmp proxy-service	Interface [VLAN]	Designates the upstream interfaces of mroute proxy.
no ip igmp proxy-service		Releases the upstream interface of mroute proxy.

10.2.7.3 Configuring Upstream Interface Mode

When a single downstream interface is specified with multiple upstream interfaces, LD3032 supports two methods of IGMP proxy operation that are priority mode and load balancing mode. You can choose the way how to handle multicast traffic going to upstream interfaces. The priority mode is configured by default.

There are two modes for handling the multicast traffic toward upstream interfaces

- Priority mode: Each downstream interface joins one upstream interface of the highest priority based on its credit, priority and vid.
- Load balancing mode: It distributes multicast packets across multiple links of upstream interfaces with the largest credit value according to hash-threshold algorithm for IGMP group.

i

Every upstream interface has a credit unit value (default :100) and a priority. The upstream interfaces are specified a priority based on its credit value, the configured priority value and vid. The highest upstream interface has larger credit, higher priority and lower vid than other ones.

To specify the priority on an upstream interface, use the following command.

Command	Mode	Description
ip igmp proxy-service priority <0-255>	Interface [VLAN]	Specifies the priority on an upstream interface (default :0)
no ip igmp proxy-service priority		Deletes the configured priority of upstream interface.

To choose the upstream interface mode for IGMP proxy operation, use the following command.

Command	Mode	Description
ip igmp proxy-service multipath grpip	Global	Specifies load balancing mode for upstream interface
no ip igmp proxy-service multipath grpip		Specifies priority mode for upstream interface.

10.2.7.4 IGMP-Proxy IF Flap Discredit

IGMP IF is IGMP Proxy-enabled upstream or downstream interface that is used for IGMP proxy implementation.

IGMP IF flap discredit function is intended to apply a traffic flow penalty in IGMP interface due to its link down-up (Flap). All of IGMP IFs have 100 credit values by default.

An IGMP IF loses the specified credit value in case the flapping happens on this interface. Therefore, the forwarding path for the flow must be recalculated, causing low multicast forwarding performance.

Under the ECMP environment, if IGMP Proxy multi-uplink interface is load-balancing mode, a multicast traffic flow is split across the multipath according to the priority based on its credit unit value and configurations. The upstream interfaces with the largest credit would get the highest proxy-service priority.

If IGMP Proxy multi-uplink interface is specified the priority mode, one upstream interface of the highest priority based on its credit value, priority and vid handles a multicast traffic flow.

IGMP IF flap discredit function has been designed to minimize such a path recalculation caused by the IF flapping, which can increase the stability and quality for multicast service. Using this function, the LD3032 gives a discredit to a IGMP IF for every flapping time, and then the IF is not selected as a forwarding path until its credit is regenerated.

IGMP Proxy IF flap discredit function is implemented with the following restrictions, so you must keep them in mind before setting the related commands or parameters.

- If you configure recover-interval value as 0, the decreased IGMP IF credit is not recovered.
- If the credit unit becomes 0 because of the continuous flapping of IGMP IF, the credit is not recovered until **clear ip igmp if flap discredit** command is configured.

To enable/disable the IGMP IF flap discredit function, use the following command.

Command	Mode	Description
ip igmp if flap discredit	Global	Enables the IGMP IF flap discredit. (default)
no ip igmp if flap discredit		Disables the IGMP IF flap discredit.

To specify the discredit value in case of IGMP IF flapping, use the following command.

Command	Mode	Description
ip igmp if flap discredit unit <1-50>	Global	Specifies the discredit value for the IF flapping and decreases the credit unit as much as a specified value. (default: 5)
no ip igmp if flap discredit unit		Deletes a configured discredit value.

To set the IGMP IF flap credit regenerating rate, use the following command.

Command	Mode	Description
ip igmp if flap recover-interval <0-3600>	Global	Specifies the interval of recovering its credit as much as a specified value. (default: 10 seconds)
ip igmp if flap recover-unit <1-50>		Sets the regenerating value of the IF credit. (default: 5)
no ip igmp if flap {**recover-interval** | **recover-unit**}		Deletes a configured IF credit regenerating rate.

⚠ If you configure this rate as 0, the IGMP IF credit is not regenerated!

To set the current IGMP IF credit as the default (100), use the following command.

Command	Mode	Description
clear ip igmp if flap discredit [{**gigabitethernet** | **tengigabitethernet** | **gpon** | **channelgroup**} *IFPORT*]	Enable Global	Restores the current credit to a default value (100).
clear ip igmp if flap discredit vlan *VLANS*		

10.2.7.5 Disabling Verification of Source IP of IGMP Packets

RPF (Reverse Path Forwarding) Check is basic operation to correctly forward multicast traffic down the distribution tree. A multicast router checks if the packet is received on the interface it would used to forward a unicast packet back to the source. If the RPF check is successful, the packet is forwarded. Otherwise, it is dropped.

However, IGMP Proxy switches do not perform RPF check on multicast traffic and only can verify if IGMP packets are received from connected network.

To disable the IGMP packet’s source IP verification function, use the following command.

Command	Mode	Description
no ip igmp verify-sip	Global	Disable the RPF check over IGMP packets.
ip igmp verify-sip		Enable the RPF check over IGMP packets (default).

10.2.7.6 Specifying IGMP Report/Leave’s Source IP Address

In IGMP proxy operation, the switch interacts with the router on its upstream interface through the exchange of IGMP messages on behalf of hosts and acts as the proxy. It performs the host portion of the IGMP task on the upstream interface by replacing the source IP address of IGMP messages, a membership report and leave group, with its own.

To specify the source IP address of IGMP membership report and leave group messages that is sent by IGMP proxy-service (upstream) interface, use the following command.

Command	Mode	Description
ip igmp proxy-service sip {*A.B.C.D* | **first-reporter**}	Interface [VLAN]	Configures the source IP address of IGMP membership report and leave group messages that is sent by proxy-service interface. A.B.C.D: Source IP address that manually entered by user first-reporter: Source IP address of the host that sent the first IGMP membership report. last-reporter: Source IP of the host that sent the last IGMP membership report. (Default : proxy-service interface IP address)
no ip igmp proxy-service sip		Removes the source IP configuration for IGMP membership report and leave group messages.

10.2.7.7 Querying with Real Querirer's Source IP Address

To send hosts queries with the actual source IP addresses, not with mroute-proxy interface's IP address, use the following command.

Command	Mode	Description
ip igmp mroute-proxy querier address proxy-service	Interface [VLAN]	Sets IGMP queries with original query's source IP address that is received on the mroute-proxy interface
no ip igmp mroute-proxy querier address proxy-service		Deletes the query's source IP configuration.

10.2.7.8 Displaying IGMP Proxy Information

To display IGMP proxy-service information, use the following command.

Command	Mode	Description
show ip igmp-proxy groups [**detail**]	Enable Global	Shows the IGMP group membership information of upstream interfaces. detail: IGMPv3 source information A.B.C.D: multicast group address
show ip igmp-proxy groups *A.B.C.D* [**detail**]		
show ip igmp-proxy groups {**gigabitethernet** | **tengigabitethernet** | **gpon** | **channelgroup**} *IFPORT* [**detail**]		
show ip igmp-proxy groups vlan *VLANS*		

To display IGMP proxy group membership information, use the following command.

Command	Mode	Description
show ip igmp proxy groups	Enable Global	Shows the IGMP proxy group membership information. detail: IGMPv3 source information A.B.C.D: multicast group address
show ip igmp proxy groups *A.B.C.D* **detail**		
show ip igmp proxy groups channelgroup | tengigabitethernet | **gpon**} *IFPORT* [**detail**]		
show ip igmp proxy groups detail		

10.2.8 IGMP State Limit

You can use IGMP State Limit feature to limit the number of IGMP states that can be joined to a router on a per-interface or global level. Membership reports exceeding the configured limits are not entered into the IGMP cache and traffic for the excess membership reports is not forwarded.

To configure the IGMP State limit globally, use the following command.

Command	Mode	Description
ip igmp limit <1-2097152> [**except** {<1-99> | <1300-1999> | WORD}]	Global	Limits the number of IGMP membership reports globally: 1-2097152: the number of IGMP states allowed on a router 1-99: IP standard access list 1300-1999: IP standard access list (expanded) WORD: access list name
no ip igmp limit		Disables the globally configured IGMP state limit.

i If you want to exclude certain groups or channels from being counted against the IGMP limit so that they can be joined to an interface, use **except** option.

To configure the IGMP State limit on an interface, use the following command.

Command	Mode	Description
ip igmp limit <1-2097152> [**except** {<1-99> | <1300-1999> | WORD}]	Interface [VLAN]	Limits the number of IGMP membership reports on an interface: 1-2097152: the number of IGMP states allowed on a router (default:0) 1-99: IP standard access list 1300-1999: IP standard access list (expanded) WORD: access list name
no ip igmp limit		Disables a configured IGMP state limit per interface.

10.2.9 Multicast-Source Trust Port

Any port of LD3032 can be specified as a multicast-source trust port which is registered in the multicast forwarding table. Only multicast-source trust ports can be received the multicast traffic.

However, the reserved multicast packets should be sent to CPU even if these packets pass through a multicast-source trust port. This feature helps the switch to distinguish between general traffic receivers and multicast traffic receivers, and is a more efficient use of system resources because it sends the multicast traffic to specific hosts which want to receive the traffic.

To configure a specified port as a multicast-source trust port, use the following command.

Command	Mode	Description
ip multicast-source trust port *PORTS*	Global	Specifies multicast-source trust ports
no ip multicast-source trust port *PORTS*		Deletes the configured multicast-source trust ports

10.3 Multicast Routing

When receivers join a certain group, multicast routers must deliver the multicast traffic corresponding to the group to those receivers. To determine the appropriate forwarding path and to replicate the multicast traffic to multiple destinations, multicast routing protocols are needed.

The multicast routing protocols establish the distribution tree by building a forwarding table in its own way. The forwarding table contains the information of sources, groups, interfaces, and how to forward multicast packets. Note that the multicast has the different routing method from the unicast's.

Reverse Path Forwarding (RPF)

Routers typically forward unicast packets with the destination lookup. When unicast packets come to interfaces, routers forward the packets to the interfaces toward the destinations of those packets by referring to the routing table. If the routing table does not contain the information of the destinations, the routers forward the packets to the default gateway.

On the other hand, routers forward multicast packets based on the source of the packets. When multicast packets come to an interface, routers validate whether the interface on which the packets are received is directly toward the source of those packets by referring to the existing unicast routing table. This procedure is called the reverse path forwarding (RPF) check. If incoming multicast packets pass the RPF check, routers forward the packets to the outgoing interface. If not, routers drop the packets.

In the multicast routing, routers must forward packets away from the sources to prevent routing loops. Finally, the distribution tree established by RPF follows the shortest path tree (SPT) topology.

10.3.1 Multicast Routing

10.3.1.1 Enabling Multicast Routing

By default, multicast routing is disabled. To configure the LD3032 to forward multicast traffic via Layer 3 network, you need to enable multicast routing.

To enable Layer 3 multicast routing, use the following command.

Command	Mode	Description
ip multicast-routing	Global	Enables multicast routing.
no ip multicast-routing		Disables multicast routing. (default)

To enable/disable Layer 3 multicast routing for IPv6, use the following command.

Command	Mode	Description
ipv6 multicast-routing	Global	Enables IPv6 multicast routing.
no ipv6 multicast-routing		Disables IPv6 multicast routing. (default)

10.3.1.2 TTL Threshold

You can specify a TTL threshold for multicast packets on an interface. This configuration is used on a border router which limits a multicast domain, since only the multicast packets with a TTL value greater than a TTL specified on an interface are forwarded to outgoing interfaces. If you intend the router to operate as a border router, the TTL threshold must be a very high value.

To specify a TTL threshold for multicast packets, use the following command.

Command	Mode	Description
ip multicast ttl-threshold <0-255>	Interface [VLAN]	Specifies a TTL threshold for multicast packets. 0-255: TTL value (default: 1)
no ip multicast ttl-threshold		Deletes a specified TTL threshold for multicast packets.

10.3.1.3 ECMP Load Splitting

Multicast routing protocols have different forwarding policies for the equal cost multipath (ECMP). In case of PIM, the interface with highest IP address is used to forward multicast traffic over the equal cost multipath.

The purpose of this feature is load splitting for forwarding multicast traffic over ECMP, allowing more efficient use of network resources and preventing traffic congestion. With this feature, multicast traffic is split across the equal cost multipath based on either its source address or its source and group address.

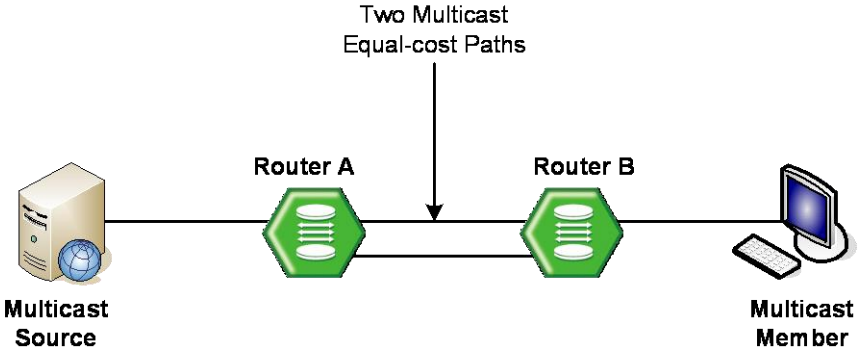


Fig. ?.5 Multicast Equal Cost Multipath (ECMP)

ECMP load splitting has two options for next hop decision:

- **srcip** selects next hop based on source address.
- **srcgrpip** selects next hop based on both source and group address.

To enable ECMP load splitting, use the following command.

Command	Mode	Description
ip multicast multipath [**srcip** | **srcgrpip**]	Global	Enables ECMP load splitting. srcip: source address (default) srcgrpip: source and group address
no ip multicast multipath		Disables ECMP load splitting.

10.3.1.4 MRIB Entry Limit

You can limit the maximum number of multicast routing entries in the multicast routing table in the multicast routing information base (MRIB), and then the system generates an error message when the number of the entries exceeds the limit. If the warning threshold is specified, the system generates a warning message when the number of the entries exceeds the threshold.

To specify the maximum number of multicast routing entries, use the following command.

Command	Mode	Description
ip multicast route-limit *LIMIT* [*THRESHOLD*]	Global	Specifies the limit of the maximum number of multicast routing entries. LIMIT: number of routing entries (1-214783647) THRESHOLD: warning threshold (1-214783647)
no ip multicast route-limit		Deletes a specified limit.

The warning threshold must not exceed the maximum number of multicast routing entries.

10.3.1.5 Static Multicast Route Configuration

Static mroutes are similar to unicast static routes but differ in the ways that static mroutes are used to calculate RPF information, not to forward traffic and cannot be redistributed.

When static mroutes are configured, they are stored on the device in a separate table referred to as the static mroute table.

To configure the static multicast routing, use the following command.

Command	Mode	Description
ip mroute *A.B.C.D/M* **{***A.B.C.D* | **interface}** [<1-255>]	Enable Global	Configure static multicast routes A.B.C.D/M: group address and prefix A.B.C.D: RPF neighbor address or route static: static routes <1-255>: administrative distance
ip mroute *A.B.C.D/M* **{bgp | isis | ospf | rip | static }** **{***A.B.C.D* | **interface }** [<1-255>]		

10.3.1.6 Displaying MRIB Entry

To display the multicast routing entries in the MRIB, use the following command.

Command	Mode	Description
show ip mroute [**summary**]	Enable Global	Shows all multicast routing entries. summary: abbreviated display
show ip mroute {**dense** | **sparse**} [**summary**]		Shows the multicast routing entries for a given PIM mode. dense: dense mode

		sparse: sparse mode
show ip mroute *A.B.C.D* [**dense** | **sparse**] [**summary**]		Shows the multicast routing entries for a given group. A.B.C.D: group address
show ip mroute *A.B.C.D A.B.C.D* [**dense** | **sparse**] [**summary**]		Shows the multicast routing entries for a given group and source. A.B.C.D: group/source address
show ip mroute *A.B.C.D/M* [**dense** | **sparse**] [**summary**]		Shows the multicast routing entries for a given group range. A.B.C.D/M: group address and prefix

If you use the **clear ip mroute** command, the MRIB clears the multicast routing entries in its multicast routing table, and removes the entries from the multicast forwarder.

To delete the multicast routing entries in the MRIB, use the following command.

Command	Mode	Description
clear ip mroute *	Enable Global	Deletes all multicast route entries.
clear ip mroute *A.B.C.D* [*A.B.C.D*]		Deletes a specified multicast route entry. A.B.C.D: group/source address

To clear the multicast forwarding cache (MFC) and tree information base (TIB) entries in the PIM-SM protocol level, use the following command.

Command	Mode	Description
clear ip mroute * [**pim sparse-mode**]	Enable Global	Deletes all MFC and TIB entries in the PIM-SM protocol.
clear ip mroute *A.B.C.D* [*A.B.C.D*] [**pim sparse-mode**]		Deletes a specified MFC and TIB entry in the PIM-SM protocol. A.B.C.D: group/source address

When clearing the MRIB entries, you must specify the group address prior to the source address.

10.3.1.7 Displaying RPF information

To display RPF (Reverse Path Forwarding) information for multicast source, use the following command.

Command	Mode	Description
show ip rpf *A.B.C.D*	Enable Global	Shows RPF information. A.B.C.D: IP address of multicast source

10.3.1.8 Displaying MRIB Statistics

To display the multicast routing statistics entries in the MRIB, use the following command.

Command	Mode	Description
show ip mroute count	Enable Global	Shows all multicast routing statistics entries.
show ip mroute {**dense** | **sparse**} **count**		Shows the multicast routing statistics entries for a given PIM mode. dense: dense mode sparse: sparse mode
show ip mroute *A.B.C.D* [**dense** | **sparse**] **count**		Shows the multicast routing statistics entries for a given group. A.B.C.D: group address
show ip mroute *A.B.C.D A.B.C.D* [**dense** | **sparse**] **count**		Shows the multicast routing statistics entries for a given group and source. A.B.C.D: group/source address
show ip mroute *A.B.C.D/M* [**dense** | **sparse**] **count**		Shows the multicast routing statistics entries for a given group range. A.B.C.D/M: group address and prefix

To delete the multicast routing statistics entries from the multicast routing table, use the following command.

Command	Mode	Description
clear ip mroute statistics *	Enable Global	Deletes all multicast routing statistics entries.
clear ip mroute statistics *A.B.C.D* [*A.B.C.D*]		Deletes a specific multicast routing statistics entry. A.B.C.D: group/source address

10.3.1.9 Displaying MFIB Information

The multicast forwarding information base (MFIB) is the group of the information to forward multicast traffic in Layer 3, which is maintained by currently running multicast routing protocol. You can verify the forwarding entries in the MFIB with the **show ip mfib** command.

To display the multicast forwarding entries in the MFIB, use the following command.

Command	Mode	Description
show ip mfib [**vlan** *VLANS* | **group** *A.B.C.D*] [**detail**]	Enable Global	Shows the multicast forwarding entries in the MFIB. VLANS: VLAN ID (1-4094) A.B.C.D: multicast group address

10.3.1.10 MRIB Debug

To debug events in the MRIB, use the following command.

Command	Mode	Description
debug nsm mcast {**all** | **fib-msg** | **mrt** | **register** | **stats** | **vif**}	Enable	Debugs events in the MRIB. all: all multicast debugging fib-msg: MFIB messages

		mrt: multicast routes register: multicast PIM register messages stats: multicast statistics vif: multicast interface
no debug nsm mcast {**all** | **fib-msg** | **mrt** | **register** | **stats** | **vif**}		Disables the debug event.

10.3.2 PIM Basic

Protocol Independent Multicast (PIM) is the most widely deployed multicast routing protocol. It may use the underlying unicast routing information base, but is not dependent on any particular unicast routing protocol. PIM has two operation modes, which are called PIM Sparse Mode (PIM-SM) and PIM Dense Mode (PIM-DM), each optimized for a different environment.

PIM-SM is a multicast routing protocol efficient for multicast groups that may span wide-area (and inter-domain) internets. In the sparse mode, routers forward multicast packets only when they receives explicit join messages from neighboring routers that have downstream group members. PIM-SM uses a unidirectional shared tree per group to deliver multicast traffic, and optionally uses the shortest path tree per source.

PIM-DM is a multicast routing protocol efficient for multicast groups that are densely populated across a network. In the dense mode, routers initially flood multicast datagrams to all multicast routers, since they assume that all downstream systems want to receive multicast packets. Prune messages are then used to prevent from propagating to routers with no group members. Both PIM protocols use the same message formats.

The LD3032 currently support PIM-SM only.

PIM Messages

The followings are simple descriptions of PIM control messages:

- **Hello**
  PIM routers periodically send hello messages on all interfaces to discover neighboring PIM routers and to determine which router will be the DR for each subnet.

- **Register**
  Register messages are sent by the DR to the RP when a multicast packet needs to be transmitted on the RPT. These messages may contain the encapsulated multicast traffic. Both register and register-stop messages are unicast.

- **Register-stop**
  When receiving the register-stop message, routers stop sending register messages. These messages are sent from the RP to the sender of the register messages.

- **Join/prune**
  Join/prune messages are sent by routers towards upstream sources or RPs. Join messages are sent to receive the multicast traffic by building shared trees (RPT) or source trees (SPT). Prune messages are sent to prune established distribution trees when there are no more interests in the traffic.

- **Bootstrap**
  The bootstrap router (BSR) sends bootstrap messages to elect the Rendezvous Point

(RP), which contain a set of the information for each candidate RP (RP-set).

- **Assert**
  Assert messages are used to resolve forwarding conflicts among routers.
- **Candidate RP advertisement**
  Each candidate RP unicasts these messages containing its own information to the BSR. The BSR then includes a set of that information in the bootstrap message.

10.3.2.1 PIM Mode

To enable PIM-SM on an interface, use the following command.

Command	Mode	Description
ip pim sparse-mode	Interface [VLAN]	Enables PIM-SM on an interface.
no ip pim sparse-mode		Disables PIM-SM on an interface.

You can also enable PIM-SM as the passive mode. The passive mode operation is for local members. The passive mode disables sending/receiving PIM packets on an interface, allowing only IGMP mechanism to be active.

To enable PIM-SM passive mode on an interface, use the following command.

Command	Mode	Description
ip pim sparse-mode passive	Interface [VLAN]	Enables PIM-SM passive mode on an interface.
no ip pim sparse-mode passive		Disables PIM-SM passive mode on an interface.

To clear the collected PIM-SM packet statistics, use the following command.

Command	Mode	Description
clear ip pim sparse-mode packet	Enable	Clears the PIM-SM packet statistics.

10.3.2.2 DR Priority

In PIM-SM, the designated router (DR) is normally the first-hop router of receivers (hosts), which is responsible to periodically send PIM join/prune messages toward the RP to inform it of the host group membership.

When there are multiple routers on the same subnet, one of them must be selected to act as the DR. To elect the DR, each PIM router examines PIM hello messages received from other neighbor PIM routers and compares its DR priority in those from neighbors. The router with the highest priority then is elected as the DR. In case of more than one router with the same highest priority value, the one with the higher IP address is elected. If no PIM hello message is received from the DR for a certain period of time, another DR election is held.

In PIM-DM, however, the DR only plays a role of the alternative IGMP querier using this DR election when multiple routers exist with IGMPv1, since IGMPv1 does not define any IGMP querier election process. To specify the DR priority on an interface, use the following command.

Command	Mode	Description
ip pim dr-priority **<**0-4294967294>	Interface [VLAN]	Specifies the DR priority on an interface. 0-4294967294: priority value (default: 1)
no ip pim dr-priority **<**0-4294967294>		Deletes the specified DR priority.
no ip pim dr-priority		

i The DR and the IGMP querier may be different routers in IGMPv2, while those are typically the same router in IGMPv1. In IGMPv2, the DR is the router with the highest IP address on the subnet, whereas the IGMP querier is the router with the lowest IP address.

10.3.2.3 Neighbor Filtering

If necessary, you can filter neighbor routers using access lists. When you enable this feature, PIM establishes adjacency without neighbor routers specified as deny in access lists. To enable filtering neighbor routers in PIM, use the following command.

Command	Mode	Description
ip pim neighbor-filter {<1-99> | *WORD*}	Interface [VLAN]	Enables filtering neighbor routers in PIM. 1-99: IP standard access list WORD: access list name
no ip pim neighbor-filter {<1-99> | *WORD*}		Disables filtering neighbor routers in PIM.

To display the information of PIM neighbor routers, use the following command.

Command	Mode	Description
show ip pim neighbor [**detail**]	Enable Global	Shows the information for PIM neighbor routers.

10.3.2.4 PIM Join/Prune Message Group Filtering

If necessary, you can filter PIM join/prune messages from separate group using access lists. When you enable this feature, a specified PIM group of PIM join/prune messages from the trusted neighbor are denied by a specified range of access lists.

To enable PIM group filtering, use the following command.

Command	Mode	Description
ip pim group-filter {<1-99> | *WORD*}	Interface [VLAN]	Enables PIM group filtering to block PIM join/prune messages using a specified access list. 1-99: IP standard access list WORD: access list name
ip pim group-filter range {<1-1024> | *WORD*}		Enables PIM group filtering to block PIM join/prune messages using a specified range of access lists. 1-1024: IP standard access list range WORD: IP access-list-range name

no ip pim group-filter [**range**]		Disables PIM group filtering.

For more information of Standard Access List and Access List Range, see Section 7.17.1 Standard Access List and 7.17.5 Access List Range.

10.3.2.5 PIM Hello Message

PIM routers periodically send PIM hello messages to discover neighboring PIM routers and to determine which router will be the DR for each subnet. PIM hello messages are also the multicast packets using the group address 224.0.0.13 (all PIM routers group).

To specify an interval to send PIM hello messages, use the following command.

Command	Mode	Description
ip pim query-interval <1-18724>	Interface [VLAN]	Specifies an interval to send PIM hello messages. 1-18724: hello message interval (unit: second)
no ip pim query-interval		Deletes a specified interval to send PIM hello messages.

PIM hello messages may contain the hold time value in the option fields, which specifies how long the information is valid. The default hold time is 3.5 times of the interval of the PIM hello messages. If a hold time you specified is less than the current interval of those, the hold time will be ignored and return to the default value.

To specify a hold time of PIM hello messages, use the following command.

Command	Mode	Description
ip pim query-holdtime <1-65535>	Interface [VLAN]	Specifies a hold time of PIM hello messages. 1-65535: hello message hold time (unit: second)
no ip pim query-holdtime		Deletes a specified hold time of PIM hello messages.

10.3.2.6 PIM Join/Prune Interval

PIM routers periodically send PIM join/prune messages to a group. If a router does not send the join message during 3 times of the specified interval, it will be pruned from the group.

To specify an interval to send PIM join/prune messages, use the following command.

Command	Mode	Description
ip pim message-interval <1-65535>	Global	Specifies an interval to send join/prune messages. 1-65535: join/prune message interval (unit: second)
no ip pim message-interval		Deletes a specified interval to send join/prune messages.

10.3.2.7 PIM VIF Flap Discredit

PIM VIF is a PIM-specific virtual interface that is used to send or receive PIM control packets in the implementation level. It includes the methods for processing and composing PIM control messages, as well as various states per interface.

PIM routers are internally connected with PIM VIFs, and the equal cost multipath (ECMP) can also exist between them. Under the ECMP environment, a traffic flow is split across the multipath based on its source and group address as the physical interface's case. However, if a VIF flapping happens, the forwarding path for the flow must be recalculated, causing low multicast forwarding performance.

PIM VIF flap discredit function has been designed to minimize such a path recalculation caused by the VIF flapping, which can increase the stability and quality for multicast service. Using this function, the LD3032 gives a discredit to a VIF for every flapping time, and then the VIF is not selected as a forwarding path until its credit is regenerated.

To enable/disable the PIM VIF flap discredit function, use the following command.

Command	Mode	Description
ip pim vif flap discredit	Global	Enables the PIM VIF flap discredit. (default)
no ip pim vif flap discredit		Disables the PIM VIF flap discredit.

To set the discredit value for the VIF flapping, use the following command.

Command	Mode	Description
ip pim vif flap discredit unit <10-50>	Global	Sets the discredit value for the VIF flapping. (default: 10)
no ip pim vif flap discredit unit		Deletes a configured discredit value.

To set the VIF credit regenerating rate, use the following command.

Command	Mode	Description
ip pim vif flap discredit half-recover-time <0-3600>	Global	Sets the VIF credit regenerating rate. (default: 10 seconds)
no ip pim vif flap discredit half-recover-time		Deletes a configured VIF credit regenerating rate.

If you configure this rate as 0, the VIF credit is not regenerated!

To set the current credit as the default (100), use the following command.

Command	Mode	Description
clear ip pim vif flap discredit [**vif** <0-127>]	Enable Global	Sets the current credit as the default (100). 0-127: VIF index

10.3.2.8 PIM Static Join

The IGMP static join feature supports an IGMPv2 host only. PIM static join has been also developed to reduce the zapping time by statically creating a virtual host that behaves like a real on a port. However, IGMP static join feature can not be used by Layer 3 device (Core switch) that is incapable of IGMP feature with no group member (host). In this case, you can use PIM static join instead of IGMP static join.

To configure the PIM static join, use the following command.

Command	Mode	Description
ip pim static-group *A.B.C.D*	Interface [VLAN]	Configures the PIM static join. A.B.C.D: Start/End multicast group address
ip pim static-group range *A.B.C.D A.B.C.D*		
no ip pim static-group [*A.B.C.D* | *]		Deletes the configured PIM static join. *: all addresses
no ip pim static-group range *A.B.C.D A.B.C.D*		

10.3.2.9 Displaying PIM-SM Information

To display current PIM-SM information, use the following command.

Command	Mode	Description
show ip pim sparse-mode interface [**detail**]	Enable Global	Shows PIM-SM interface information. detail: includes VIF information
show ip pim sparse-mode local-members [*SHORT_IF_NAME*]		Shows PIM local membership information. SHORT_IF_NAME: interface name
show ip pim sparse-mode mroute *A.B.C.D* [*A.B.C.D* **detail** | **detail**]		Shows the multicast routing table. A.B.C.D: multicast group or source address
show ip pim sparse-mode neighbor *SHORT_IF_NAME* [*A.B.C.D* **detail | detail**]		Shows the neighbor information. SHORT_IF_NAME: interface name A.B.C.D: neighbor address
show ip pim sparse-mode neighbor detail		
show ip pim sparse-mode rp mapping		Shows group-to-RP mappings.

10.3.3 PIM-SM

Rendezvous Point Tree (RPT)

PIM-SM mainly uses a shared tree to deliver multicast traffic, called the RP tree (RPT). As its name implies, it relies on a core router called the Rendezvous Point (RP) that receives all multicast traffic from the sources and forwards that traffic to the receivers. Other routers do not need to know the information of the sources. All they need to know is the address of the RP, because the RP surely knows the information of the sources for all multicast groups. Thus, receivers who are interested in a certain multicast group only send PIM join messages with (*, G) state toward the RP. That is, the RPT prevent each router from maintaining source and group (S, G) states for every multicast source. This mechanism shifts the burden of finding the multicast sources from each router to the network itself.

The shared tree is unidirectional, which means all multicast traffic flows only from the RP to the receivers. Thus, there is no guarantee that the shared tree (RPT) is the shortest path tree to the source, and most likely it is not, resulting in longer delays, but less forwarding states to maintain. Each multicast group has only one RP that may be different; each multicast group may have the different distribution tree.

Fig. 10.6 shows an example of the RPT network. The multicast traffic from the source A flows through the router B to the router D which is the RP. Note that, even in the RPT, RPs must receive multicast traffic from the sources via the shortest path. The RP then distributes the traffic to the receiver E and F that indicate the interest in the multicast group. Consequently, the distribution tree for the receiver E is **A→B→D→E**, and the one for the receiver F is **A→B→D→C→F**.

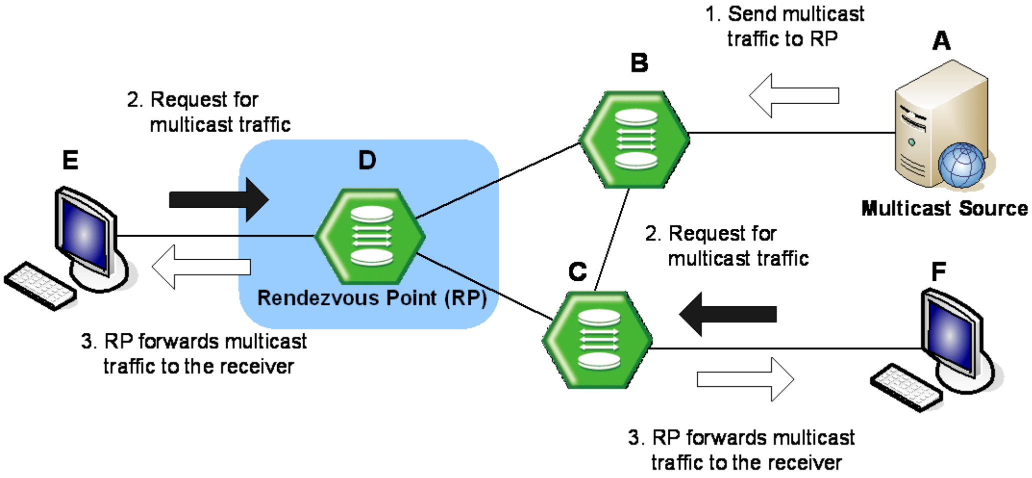

1. Send multicast traffic to RP
A
B
2. Request for multicast traffic
E
D
Multicast Source
2. Request for multicast traffic
C
F
Rendezvous Point (RP)
3. RP forwards multicast traffic to the receiver
3. RP forwards multicast traffic to the receiver

Fig. 10.6 Rendezvous Point Tree

Shortest Path Tree (SPT)

When the number of receivers increases, a shared tree may not be entirely efficient, so PIM-SM also provides the option to switch to receive multicast traffic on a shortest path tree (SPT). When this option is enabled, on receiving the first multicast packet from the RP in response to the PIM join message, the switchover to the SPT then occurs.

To establish the SPT to the multicast source, the DR sends the join message with (S, G) state toward that source. When the SPT between the receiver and source is established, and multicast traffic is sent via that distribution tree, the DR sends the prune message with (*, G) state toward the RP to prune the existing shared tree to receive the traffic.

SPT is established based on the existing unicast routing table by performing the RPF check. It has a different distribution tree for every multicast source, allowing the efficient network traffic flows, but more resources are needed for each multicast routers to maintain (S, G) states.

Fig. 10.7 shows an example of the SPT switchover. The multicast traffic from the source A initially attempts to flow through the router B and C to the receiver D that indicates the interest in the multicast group. Once the traffic arrives at the router C which is the DR, it sends the join message with (S, G) state toward the source A to build the SPT between the source and receiver. The source A then sends the multicast traffic to the receiver D via the SPT by deleting unnecessary hops. Finally, the distribution tree (SPT) built by the

RPF check is **A→C→D**.

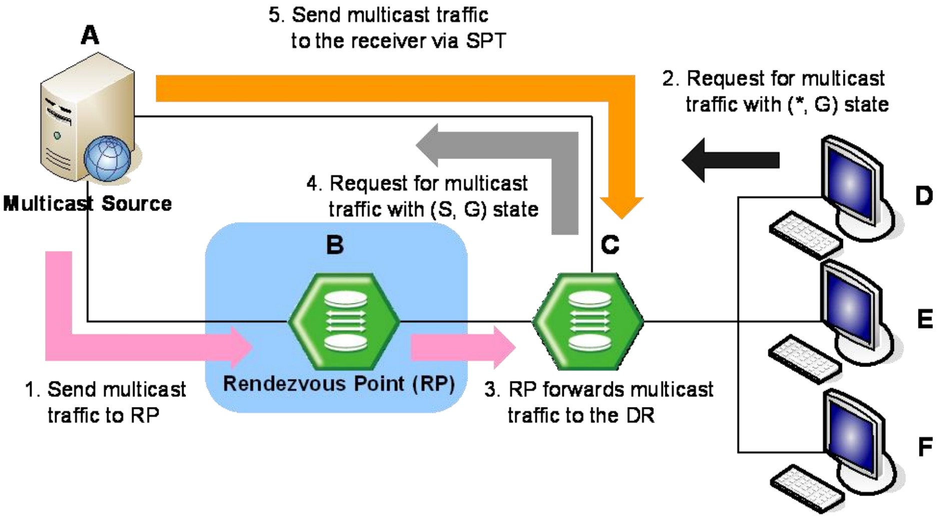

A
Multicast Source
5. Send multicast traffic to the receiver via SPT
2. Request for multicast traffic with (*, G) state
4. Request for multicast traffic with (S, G) state
B
C
D
E
F
Rendezvous Point (RP)
1. Send multicast traffic to RP
3. RP forwards multicast traffic to the DR

Fig. 10.7 Shortest Path Tree

PIM-SM Operation

When multicast receivers indicate their interests in certain multicast groups, the DR of the receivers sends PIM join messages with (*, G) state toward the RP for those groups. While the join messages flow hop-by-hop toward the RP, each PIM router along the path adds the interface on which the join messages are received to the outgoing interface (OIF) list with the join state, and sends the messages to the interface toward the RP.

If the RP has receivers interested in the group, the RP must receive the multicast traffic from the source of that group via the SPT to deliver the traffic to those receiver. The DR of the source encapsulates the multicast packets in the PIM register messages, and starts to unicast them to the RP. On receipt of the register messages, the RP sends the join message with (S, G) state toward the source to establish the SPT. When receiving the multicast traffic via the established SPT, the RP forwards the traffic toward those receivers.

Multicast traffic may be directly delivered from sources to receivers via the SPT using the switchover mechanism.

10.3.3.1 Rendezvous Point

In a shared tree, Rendezvous Point (RP) is a means for receivers to discover the sources that send to a particular multicast group. It is responsible to receive all multicast traffic from the sources and to forward that traffic to the receivers.

Static RP

To elect the RP among candidate RPs in the shared tree, the LD3032 supports the BSR mechanism and static RP, and also supports the simultaneous use of those. You can configure a router to use the static RP either for all the multicast groups (default) or for specific multicast groups (with access lists). If multiple static RPs are available for a single multicast group, the one with the highest IP address will be elected.

To statically specify an RP address for multicast groups, use the following command.

Command	Mode	Description
ip pim rp-address *A.B.C.D* [<1-99> | <1300-1999>] [**override**]	Global	Specifies an RP address for multicast groups. A.B.C.D: RP address 1-99: IP standard access list 1300-1999: IP standard access list (extended range)
no ip pim rp-address *A.B.C.D*		Deletes a specified RP address for multicast groups

i

When the static RP and the RP elected through the BSR are both available for a multicast group, the one elected through the BSR is chosen by default. If you, however, want to choose the static RP for a multicast group in that situation, use the **override** option that gives the higher priority to the static RP.

Anycast RP

Using Anycast RP is an implementation strategy that provides load sharing and redundancy in Protocol Independent Multicast sparse mode (PIM-SM) networks. Anycast RP allows two or more rendezvous points (RPs) to share the load for source registration and the ability to act as hot backup routers for each other.

To specify an anycast RP address to provide redundancy and RP load sharing, use the following command.

Command	Mode	Description
ip pim anycast-rp *A.B.C.D A.B.C.D*	Global	Configures the shared anycast address A.B.C.D: anycast RP address A.B.C.D: anycast member RP address
no ip pim anycast-rp *A.B.C.D A.B.C.D*		Deletes a specified anycast RP address A.B.C.D: anycast RP address A.B.C.D: anycast member RP address

Keep Alive Time

After a multicast source registers with the RP, the DR of the multicast source periodically sends the PIM null-register message to the RP to keep the (S, G) state between the router and RP. The null-register message is the one without encapsulated multicast traffic. If there is no null-register message during a given keep alive time (KAT), the multicast routing entry with (S, G) state is expired, and the source registration process will restart.

To specify the keep alive time for (S, G) states at the RP, use the following command.

Command	Mode	Description
ip pim rp-register-kat <1-65535>	Global	Specifies the KAT for (S, G) states at the RP. 1-65535: KAT value(unit: second)
no ip pim rp-register-kat		Deletes the specified KAT value.

Interface for Candidate RP

To elect the RP, each candidate RP sends its information to the BSR. This advertisement contains the IP address and priority of the candidate RP and the multicast groups that it can service. The BSR then periodically distributes the bootstrap message that includes a set of the information received from each candidate RP (RP-set) to all the routers in the PIM-SM domain.

To configure an interface to send the candidate RP advertisement to the BSR, use the following command.

Command	Mode	Description
ip pim rp-candidate *INTERFACE* [**group-list** <1-99>] [**interval** <1-16383>] [**priority** <0-255>]	Global	Configures an interface to send the candidate RP advertisement. INTERFACE: interface name 1-99: IP standard access list 1-16383: advertising interval (unit: second) 0-255: priority value
no ip pim rp-candidate *INTERFACE* **group-list** <1-99>		Deletes specified multicast groups which an interface can service.
no ip pim rp-candidate *INTERFACE*		Configures an interface not to send the candidate RP advertisement.
no ip pim rp-candidate		Configures an interface not to send the candidate RP advertisement as well as deletes specified candidate RP information.

i The access list with this command specifies the multicast groups that an advertising router can service. The candidate RP information without the access lists means that the router will service all the multicast groups.

Ignoring RP Priority

Normally, when choosing the RP among candidate RPs, routers examine the bootstrap messages sent from the BSR, and then choose the one has the highest priority among the RP-set. You can configure a router to only use the hash mechanism for the RP choice instead of the RP priority. This feature is used to interoperate with a router that cannot recognize the RP priority.

To configure a router to use the hash mechanism for the RP choice, use the following command.

Command	Mode	Description
ip pim ignore-rp-set-priority	Global	Enables ignoring the PR priority for the RP choice.
no ip pim ignore-rp-set-priority		Disables ignoring the PR priority for the RP choice.

Displaying RP Information

To display the RP information, use the following command.

Command	Mode	Description

show ip pim rp-hash *A.B.C.D*		Shows the RP to be chosen for a specified group. A.B.C.D: multicast group address

10.3.3.2 Bootstrap Router

The bootstrap router (BSR) mechanism is one way that a multicast router can learn the set of group-to-RP mappings required in order to function.

All multicast routers in PIM-SM domain can be potentially the bootstrap router (BSR); they are all considered as candidate BSRs. To elect the BSR among the candidate BSRs, each candidate BSR floods the bootstrap messages with its information to the domain. When receiving the bootstrap messages, the candidate BSRs examine the messages, and then the one with the highest priority is elected as the BSR. If more than one candidate with the same highest priority, the one with the higher IP address is elected.

The elected BSR is responsible to periodically send out bootstrap messages including the RP-set, allowing all the routers in the PIM-SM domain determine which router is the RP that covers given multicast groups.

Interface for Candidate BSR

To configure an interface to flood the candidate BSR advertisement, use the following command.

Command	Mode	Description
ip pim bsr-candidate *INTERFACE*	Global	Configures an interface to flood the candidate BSR advertisement. INTERFACE: interface name 0-32: hash mask length for RP selection 0-255: priority for candidate BSR
ip pim bsr-candidate *INTERFACE* <0-32>		
ip pim bsr-candidate *INTERFACE* <0-32> <0-255>		
no ip pim bsr-candidate		Configures an interface not to flood the candidate BSR advertisement.

Clearing RP-Set

The BSR periodically distributes the bootstrap message that includes a set of the information received from each candidate RP (RP-set) to all the routers in the PIM-SM domain. You can also clear all RP-set to reset.

To clear all RP-set, use the following command.

Command	Mode	Description
clear ip pim sparse-mode bsr rp-set *	Global	Clears all RP-set.

Displaying BSR Configuration

To display the BSR information, use the following command.

Command	Mode	Description
show ip pim bsr-router	Enable Global	Shows the BSR information.

10.3.3.3 Source Registration

Multicast sources do not need any join process to send multicast traffic, since the DR of the multicast sources just receives the traffic from the sources without any information. Even in the RPT, RPs must receive multicast traffic from the sources via the shortest path while receivers receive multicast traffic via the shared tree. Thus, the DR needs to inform the RP about the information for the source, and the SPT must be established between the DR and RP via (S, G) states.

In case of the registration for a source, when receiving multicast traffic from the source, the DR encapsulates the multicast traffic in the PIM register message, and constantly unicasts it to the RP. The RP receives the register message, and then sends the PIM join message with (S, G) state back toward the DR to establish the SPT between them. Once the DR receives the join message, the SPT is then established, and the DR begins sending the multicast traffic without an encapsulation to the RP. When receiving the native multicast traffic, the RP unicasts the PIM register-stop message back to the DR. The DR then stops encapsulating the multicast traffic in the register message.

Registration Rate Limit

You can limit the maximum number of the PIM register message packets per second. If you enable this feature, both DR and RP will discard the register messages that exceed the limit.

To enable the rate limit for PIM register message, use the following command.

Command	Mode	Description
ip pim register-rate-limit <1-65535>	Global	Enables the rate limit for PIM register message. 1-65535: maximum number of packets that can be sent per second
no ip pim register-rate-limit		Disables the rate limit for PIM register message.

Registration Suppression Time

Once a multicast routing entry with (S, G) state is established by the source registration, the periodic reregistration is needed to keep the state for the entry. After the registration, the DR periodically sends the PIM null-register message that does not contain the encapsulated multicast traffic to the RP, and the RP returns the register-stop message. If there is no response to the null-register message during a given period, the multicast routing entry with (S, G) state is expired, and the source registration process will start again.

You can specify the interval to send the PIM null-register message which is also called the registration suppression time. When you specify this value at the RP, the configuration modifies the keep alive time (KAT) for the RP, if the **ip pim rp-register-kat** command is not used. To specify the registration suppression time, use the following command.

Command	Mode	Description

ip pim register-suppression <1-65535>	Global	Specifies the registration suppression time. 1-65535: null-register message interval (unit: second)
no ip pim register-suppression		Deletes the specified the registration suppression time.

Register Message Filtering

You can enable the router to filter multicast sources specified in access lists at the RP. This filtering will permit/deny the PIM register messages for the specified sources. If unauthorized sources try to register with the RP, the RP then drops the PIM register messages from those sources. You can specify the either multicast source or source's DR address in access lists.

To enable the router to filter multicast sources, use the following command.

Command	Mode	Description
ip pim accept-register list {<100-199> | <2000-2699> | *WORD*}	Global	Enables the router to filter multicast sources. 100-199: IP extended access list 2000-2699: IP extended access list (extended range) WORD: access list name
no ip pim accept-register		Disables the router to filter multicast sources.

RP Reachability Validation

To enable the RP reachability validation for the source registration process at the first-hop router, use the following command.

Command	Mode	Description
ip pim register-rp-reachability	Global	Enables the RP reachability validation.
no ip pim register-rp-reachability		Disables the RP reachability validation. (default)

Source Address of Register Message

You can specify the source IP address of PIM register messages sent by the DR. This address is used to send corresponding PIM register-stop messages in response. By default, the source address of register messages is the IP address of the interface toward the RP. This address must be able to be learned by unicast routing protocols on the DR.

To specify the source IP address of PIM register messages, use the following command.

Command	Mode	Description
ip pim register-source {*A.B.C.D* | *INTERFACE*}	Global	Specifies the source IP address of register messages. A.B.C.D: source IP address INTERFACE: interface name
no ip pim register-source		Deletes a specified source IP address of register messages.

10.3.3.4 SPT Switchover

PIM-SM provides the switching option to deliver multicast traffic on the SPT. Multicasting over the SPT may be more efficient than multicasting over the RPT, since it can substantially reduce the network latency.

When the switching option is enabled, once multicast traffic from sources arrives at the DR, the switchover to the SPT then occurs. This option only provides the binary option, meaning that the switching to the SPT occurs either when receiving the first multicast packet, or not at all; it is not rate-based. You can enable this option only for specified multicast groups using access lists.

To enable the switchover to the SPT, use the following command.

Command	Mode	Description
ip pim spt-threshold	Global	Enables the switchover to SPT.
ip pim spt-threshold group-list {<1-99> | <1300-1999> | *WORD*}		Enables the switchover to SPT for specified multicast groups. 1-99: IP standard access list 1300-1999: IP standard access list (extended range) WORD: access list name

To disable the switchover to the SPT, use the following command.

Command	Mode	Description
no ip pim spt-threshold	Global	Disables the switchover to SPT.
no ip pim spt-threshold group-list {<1-99> | <1300-1999> | *WORD*}		

i The switchover to the SPT to deliver multicast traffic is disabled by default.

10.3.3.5 Cisco’s Router Interoperability

Register Message Checksum

When a multicast source registers with the RP, the DR encapsulates the multicast traffic from the source in the PIM register message, and unicasts it to the RP. The standard PIM protocol specifies that the checksum field in the register message contains the checksum for the entire register message excluding the data portion, the encapsulated multicast traffic.

The Cisco’s routers, however, validate the checksum for the whole register message including the data portion, resulting in incompatibility with the standard-based routers. To guarantee compatibility with the Cisco’s routers, the LD3032 provides the checksum option, which expands the range of the checksum calculation.

To enable the Cisco checksum option, use the following command.

Command	Mode	Description
ip pim cisco-register-checksum	Global	Enables the Cisco checksum option.
ip pim cisco-register-checksum group-list {<1-99> | <1300-1999> | *WORD*}		Enables the Cisco checksum option for specified multicast groups. 1-99: IP standard access list 1300-1999: IP standard access list (extended range) WORD: access list name

To disable the Cisco checksum option, use the following command.

Command	Mode	Description
no ip pim cisco-register-checksum	Global	Disables the Cisco checksum option.

Candidate RP Message

Some Cisco's BSRs do not comply with the BSR standards; they do not accept candidate RPs with a group prefix number of zero. You can configure the router to send candidate RP messages with the option for the compatibility with the Cisco's BSR.

To enable the candidate RP message option for the Cisco compatibility, use the following command.

Command	Mode	Description
ip pim crp-cisco-prefix	Global	Enables the candidate RP message option for the Cisco compatibility.
no ip pim crp-cisco-prefix		Disables the candidate RP message option for the Cisco compatibility.

Excluding GenID Option

PIM hello messages may contain the generation ID (GenID) in the option fields, which is a random value for the interface on which the hello message is sent. The GenID is regenerated whenever PIM forwarding is started or restarted on the interface. It enables neighbors to quickly detect a router's reboot and thus to synchronize RP-set information and forwarding states by triggering the bootstrap and join/prune messages to the rebooted router. The rebooted router then is able to quickly recover from the reboot.

Some older Cisco's routers cannot recognize the GenID option in the hello messages, so the LD3032 provides the exclude-GenID option for the compatibility with the Cisco's routers.

To exclude the GenID option from the PIM hello messages, use the following command.

Command	Mode	Description
ip pim exclude-genid	Interface [VLAN]	Excludes the GenID from the hello messages.
no ip pim exclude-genid		Includes the GenID from the hello messages.

10.3.3.6 Debugging PIM-SM

To enable PIM-SM debugging, use the following command.

Command	Mode	Description
debug pim sparse-mode {**all** | **events** | **mfc** | **mib** | **mtrace** | **nexthop** | **nsm** | **state** | **packet** [**in** | **out**]}	Enable	Enables PIM-SM debugging. all: all PIM-SM debugging events: events debugging mfc: MFC add/delete/update debugging mib: MIBs debugging mtrace: Mtrace messages nexthop: nexthop communications debugging nsm: NSM communications debugging state: debugging of state transition on all FSMs packet: incoming and/or outgoing packets debugging
no debug pim sparse-mode {**all** | **events** | **mfc** | **mib** | **mtrace** | **nexthop** | **nsm** | **state** | **packet** [**in** | **out**]}		Disables PIM-SM debugging.

To enable PIM-SM timer debugging, use the following command.

Command	Mode	Description
debug pim sparse-mode timer	Enable	Enables PIM-SM timer debugging.
debug pim sparse-mode timer assert [**at**]		Enables PIM-SM assert timer debugging.
debug pim sparse-mode timer bsr [**bst** | **crp**]		Enables PIM-SM BSR timer debugging. bst: bootstrap debugging timer crp: candidate RP debugging timer
debug pim sparse-mode timer hello [**ht** | **nlt** | **tht**]		Enables PIM-SM hello timer debugging. ht: hello timer nlt: neighbor liveness timer tht: triggered hello timer
debug pim sparse-mode timer joinprune [**jt** | **et** | **ppt** | **kat** | **ot**]		Enables PIM-SM join/prune timer debugging. jt: join timer et: expiry timer ppt: prune pending timer kat: keep alive timer ot: override timer
debug pim sparse-mode timer register [**rst**]		Enables PIM-SM register timer debugging.

To disable PIM-SM timer debugging, use the following command.

Command	Mode	Description
no debug pim sparse-mode timer	Enable	Disables PIM-SM timer debugging.
no debug pim sparse-mode timer assert [**at**]		

no debug pim sparse-mode timer bsr [**bst** | **crp**]		
no debug pim sparse-mode timer hello [**ht** | **nlt** | **tht**]		
no debug pim sparse-mode timer joinprune [**jt** | **et** | **ppt** | **kat** | **ot**]		
no debug pim sparse-mode timer register [**rst**]		

10.3.4 Source Specific Multicast (SSM)

Multicast supports both many-to-many and one-to-many models, which are also known as Any Source Multicast (ASM). In this model, receivers may join and leave multicast groups with (*, G) state that indicates any source and group G. Since there is no means to specify the source’s information, source discovery such as the RP mechanism in PIM-SM is needed, which is the key feature of ASM. Each group address is identified as 224.0.0.0 to 239.255.255.255 (224/4).

Source-Specific Multicast (SSM) is another multicast model especially for one-to-many. In the SSM service model, receivers can receive multicast traffic by subscribing to channel (S, G) that indicates specific source S and group G. Since SSM assumes that receivers already know the source’s information, no further source discovery is provided. Thus, receivers need to know the source’s information using an out of band mechanism. The SSM group address range is defined as 232.0.0.0 to 232.255.255.255 (232/8) by default.

10.3.4.1 PIM-SSM

PIM Source-Specific Multicast (PIM-SSM) is a subset of PIM-SM. It is much simpler than PIM-SM, because it only considers one-to-many multicast service model. PIM-SSM only use a shortest path tree (SPT) to deliver multicast traffic, so the PIM-SM’s complex mechanisms such as RP, BSR, SPT switchover and a shared tree are not necessary any more. PIM-SSM uses the same PIM messages as PIM-SM’s for its operation.

If all routers are configured with PIM-SM and IGMPv3, only by using the **ip pim ssm** command, PIM-SSM will be enabled. You can also define an additional SSM group other than the default SSM group range 232/8.

To enable PIM-SSM, use the following command.

Command	Mode	Description
ip pim ssm default	Global	Enables PIM-SSM for the group range 232/8.
ip pim ssm range {<1-99> | *WORD*}		Enables PIM-SSM for a specified group range. 1-99: standard access list WORD: access list name
no ip pim ssm		Disables PIM-SSM.

10.3.4.2 Static SSM Mapping

The purpose of static SSM mapping is to provide SSM service on IGMPv1 and IGMPv2 messages. It means that it enables a multicast host to signal to a router which groups it wants to receive multicast traffic from, and from which sources this traffic is expected. You can specify a source address of multicast server to receive the multicast traffic from specified sources. If LD3032 receives IGMPv1 or IGMPv2 report message from the host when static SSM mapping is enabled, it handles as if it receives IGMPv3 report messages.

Static SSM mapping implemented for the LD3032 has the following restriction, so you must keep it in mind, before configuring static SSM mapping.

IGMP proxy and static SSM mapping cannot be enabled together. It means that SSM mapping cannot be enabled when the system is already configured with upstream or downstream interface with IGMP proxy feature.
Before configuring static SSM mapping, you should first globally enable SSM mapping. To enable static SSM mapping, use the following command.

Command	Mode	Description
ip igmp ssm-map enable	Global	Enables SSM mapping for groups in a configured SSM range.
no ip igmp ssm-map enable		Disables SSM mapping for groups.

To configure the switch to statically map groups that match specified ACL to source address, use the following command.

Command	Mode	Description
ip igmp ssm-map static {<1-99> | <1300-1999> | *WORD*} *A.B.C.D*	Global	Enables a static SSM mapping for the group that matches specified ACL and source address. 1-99: standard access list number 1300-1999: extended range of standard access list WORD: IP named standard access list A.B.C.D: source address to use for static map group
no ip igmp ssm-map static {<1-99> | <1300-1999> | *WORD*} *A.B.C.D*		Disables a static SSM mapping for the group that matches specified ACL and source address.

To display the sources that SSM mapping uses for a particular group, use the following command.

Command	Mode	Description
show ip igmp ssm-map [*A.B.C.D*]	Enable Global	Shows a static SSM mapping information A.B.C.D: multicast group address

10.4 IP Multicast Interface

To display information about IP multicast interface configuration parameters, use the following command.

Command	Mode	Description
show ip mvif channelgroup *IFPORT*	Enable Global	Shows information about IP multicast interface configured. IFPORT: interface port number VLANID: VLAN ID
show ip mvif gpon *IFPORT*		
show ip mvif tengigabitethernet *IFPORT*		
show ip mvif vlan *VLANID*		

11 IPv6 Multicast

Multicast is the communication for a single or many source hosts to a specific group of destination hosts, which is interested in the information from the sources. This type of packet transmission can be deployed for a number of applications with more efficient utilization of the network infrastructure.

The point of implementing multicast is how to deliver source traffic to specific destinations without any burden on the sources or receivers using the minimized network bandwidth. The solution is to create a group of hosts with addressing the group, and to let the network determine how to replicate the source traffic to the receivers. The traffic will then be addressed to the multicast address and replicated to the multiple receivers by network devices.

An IPv6 multicast group is an arbitrary group of receivers that want to receive a particular data stream. This group has no physical or geographical boundaries--receivers can be located anywhere on the Internet or in any private network. Receivers that are interested in receiving data flowing to a particular group must join the group by signaling their local router. If you use these features IGMP in IPv4, This signaling is achieved with the MLD protocol in IPv6.

Routers use the MLD protocol to learn whether members of a group are present on their directly attached subnets. Hosts join multicast groups by sending MLD report messages. The network then delivers data to a potentially unlimited number of receivers, using only one copy of the multicast data on each subnet. IPv6 hosts that wish to receive the traffic are known as group members.

Packets delivered to group members are identified by a single multicast group address. Multicast packets are delivered to a group using best-effort reliability, just like IPv6 unicast packets.

The multicast environment consists of senders and receivers. Any host can send to a group. However, only the members of a group receive the message. A multicast address is chosen for the receivers in a multicast group. Senders use that address as the destination address of a datagram to reach all members of the group.

Membership in a multicast group is dynamic; hosts can join and leave at any time. There is no restriction on the location or number of members in a multicast group. A host can be a member of more than one multicast group at a time.

11.1 Multicast Listener Discovery (MLD)

The Multicast Listener Discovery (MLD) protocol is the multicast group management protocol for IPv6 and is used to exchange group information between multicast hosts and routers.

Multicast Listener Discovery (MLD) enables the IPv6 router to discover the presence of multicast listeners (that is, nodes wishing to receive multicast packets) on its directly attached links, and to discover specifically which multicast addresses are of interest to those neighboring nodes.

MLDv1 (RFC2710) is designed based on Internet Group Management Protocol version 2 (IGMPv2). MLDv2 (RFC3810) is designed based on IGMPv3. One important difference to note is that MLD uses ICMPv6 (IP Protocol 58) message types.

MLD Messages

There are three types of MLD messages of concern to the host-router interaction as shown below:

- **Query Message**
  A multicast router determines of any hosts are listening to a group by sending membership queries. The membership queries have two subtypes.
  - **General query**: In a query message, the multicast address field is set to 0 when MLD sends a general query. This is used to determine if any hosts are listening to any group.
  - **Multicast-address-specific query**: This is used to determine if any hosts are listening to a particular group. A group address is a multicast address.
- **Report Message**
  This is used by hosts to response to a query. The multicast address field is that of the specific IPv6 multicast address to which the sender is listening.
- **Done Message**
  This is used to indicate that a host stopped listening to a multicast address. The multicast address field is that of the specific IPv6 multicast address to which the source of the MLD message is no longer listening.

MLD has two versions that are supported by hosts and routers. MLD messages for each version are Query and Report types. Additionally, Done message is added to the version1.

The followings are the simple definitions of each version:

- **MLD Version 1**

MLDv1 is based on IGMP2.

<table>
<tr><th>0</th><th>4</th><th>8</th><th>16</th><th>32</th></tr>
<tr><td colspan="2"><b>Type</b></td><td><b>Code</b></td><td colspan="2"><b>Checksum</b></td></tr>
<tr><td colspan="3"><b>Maximum Response Delay</b></td><td colspan="2"><b>Reserved</b></td></tr>
<tr><td colspan="5"><b>Multicast Address (128 bits)</b></td></tr>
</table>

Fig. 11.1 MLDv1 Message Format

MLDv1 Messages

- **Type**: MLD message types
  – **General query / Multicast-address-specific query message (ICMPv6 #130)**
  – **Multicast Listener report message (ICMPv6 #131)**
  – **Multicast Listener done message (ICMPv6 #132)**
- **Code**: This field is set to zero by the sender and ignored by receivers.
- **Checksum**: The standard ICMPv6 checksum, covering the entire MLD message of IPv6 header fields.
- **Maximum Response Delay**: This field is used only in Query messages, and specifies the maximum allowed delay before sending a responding Report, in units of milliseconds.
- **Multicast Address**
  – **In a Query message**: This field is set to zero when sending a General Query, and set to a specific IPv6 multicast address when sending a multicast-address-specific query.
  – **In a Report or Done message:** This field holds a specific IPv6 multicast address to which the message sender is listening to is ceasing to listen, respectively.

- **MLD Version 2**

MLDv2 is based on IGMP3. MLD v2 message consists of two messages as Listener Query and Listener Report. In addition, Query messages are classified into three types as General, Multicast-address-specific, Multicast-address-source-specific Query.

0 4 8 16 32

<table>
<tr><td colspan="3"><b>Type</b></td><td><b>Code</b></td><td><b>Checksum</b></td></tr>
<tr><td colspan="4"><b>Maximum Response Delay</b></td><td><b>Reserved</b></td></tr>
<tr><td colspan="5"><b>Multicast Address (128 bits)</b></td></tr>
<tr><td><b>Reserved</b></td><td><b>S</b></td><td><b>QRV</b></td><td><b>QQIC</b></td><td><b>Number of Sources (n)</b></td></tr>
<tr><td colspan="5"><b>Source Address [1] 128bits</b></td></tr>
<tr><td colspan="5"><b>…</b></td></tr>
<tr><td colspan="5"><b>Source Address [n] 128bits</b></td></tr>
</table>

Fig. 11.2 MLDv2 Query Message Format

MLDv2 Messages

- **S (S Flag; Suppress Router-Side Processing):** When a router sends or receives a query, it must update router’s timer to reflect to correct timeout values for the multicast address or sources being queried. When set to one, the S Flag indicates to any receiving multicast routers that they have to suppress the normal timer updates they perform upon hearing a query.

- **QRV (Querier’s Robustness Variable):** If this is non-zero, it contains the Robustness Variable value used by the sender of the Query. Routers should update their Robustness Variable to match the most recently received Query unless the value is zero.

- **QQIC (Querier’s Query Interval Code):** This code is used to specify the Query Interval value used by the querier.

- **Number of Sources (n):** This field specifies how many source addresses are present in the Query. This number is zero in a General Query or a Multicast Address Specific Query, and non-zero in a Multicast Address and Source Specific Query. This number is limited by the network’s MTU.

- **Source Address:** This fields are a vector of n IP unicast address, where n is the value in the value in the Number of Sources (N) field.

11.1.1 MLD Version

By default, this system runs MLDv2. To change the MLD protocol version on a current interface, use the following command.

Command	Mode	Description
ipv6 mld version <1-2>	Interface	Sets MLD version on a current interface. 1-2: MLD version (default: 2)
no ipv6 mld version		Returns to the default setting.

11.1.2 MLD Querier's Robustness Variable

You can statically configure the Querier's Robustness Variable (QRV) field in the query message. The MLD QRV allows tuning for the expected packet loss on a network. If a network is expected to be lossy, the QRV value may be increased. When receiving the query message that contains a certain QRV value from a querier, a host returns the report message as many as the specified QRV value.

To configure the QRV value on an interface, use the following command.

Command	Mode	Description
ipv6 mld robustness-variable <2-7>	Interface	Configures the MLD Querier's Robustness Variable (QRV) value on an interface. (default: 2)
no ipv6 mld robustness-variable		Deletes a specified MLD QRV value.

11.1.3 Clearing MLD Entry

To clear MLD entries, use the following command.

Command	Mode	Description
clear ipv6 mld	Enable Global	Deletes all MLD entries.
clear ipv6 mld interface *IFNAME*		Deletes the MLD entries learned from a specified interface. IFNAME: interface name
clear ipv6 mld group {***** | *X:X::X:X* [*IFNAME*]}		Deletes MLD entries in a specified MLD group. *: all MLD groups *X:X::X:X*: MLD IPv6 group address

11.1.4 MLD Debug

To enable debugging of all MLD or a specific feature of MLD, use the following command.

Command	Mode	Description
debug mld {**all** | **decode** | **encode** | **events** | **fsm** | **tib**}	Enable	Enables MLD debugging. all: all MLD decode: MLD decoding encode: MLD encoding

		events: MLD events fsm: MLD Finite State Machine (FSM) tib: MLD Tree Information Base (TIB)
no debug mld {**all** | **decode** | **encode** | **events** | **fsm** | **tib**}		Disables MLD debugging.

Tree Information Base (TIB) is the collection of state at a router that has been created by receiving MLD messages from local hosts.

To display the debugging information, use the following command.

Command	Mode	Description
show debugging mld snooping	Enable	Shows the debugging status of MLD.

11.1.5 MLD Access Control

Multicast routers send membership query messages to determine which multicast groups have members in the attached local networks of the router. If hosts respond to the queries, the routers then forward all packets addressed to the multicast group to these group members.

You can restrict hosts on a network to join multicast groups on the specified access list.

To control an access to multicast groups on an interface, use the following command.

Command	Mode	Description
ipv6 mld access-group *WORD*	Interface	Enables an MLD access-group control on an interface. WORD: IPv6 access list name
no ipv6 mld access-group		Disables a configured MLD access-group control.

11.1.6 MLD Querier Configuration

An MLD querier is the router periodically sends a General Query message for managing the multicast group. In MLD version1, the querier is a router with the lowest IPv6 address on the subnet. If the router hears no queries for the timeout period, it becomes the MLD querier.

11.1.6.1 MLD Query Interval

The MLD querier sends general query messages periodically to discover which multicast groups have members on the attached networks of the router.

To specify an interval to send MLD query messages, use the following command.

Command	Mode	Description

Command	Mode	Description
ipv6 mld query-interval <1-18000>	Interface	Specifies a general query interval. 1-18000: query interval (default: 125 seconds)
no ipv6 mld query-interval		Deletes a specified general query interval.

11.1.6.2 MLD Query Response Time

In MLD version 1 and 2, membership query messages include the maximum query response time field. This field specifies the maximum time allowed before sending a responding report. The maximum query response time allows a router to quickly detect that there are no more directly connected group members on a network segment.

To specify a maximum query response time advertised in membership query messages, use the following command.

Command	Mode	Description
ipv6 mld query-max-response-time <1-240>	Interface	Specifies a maximum query response time. 1-240: maximum response time (default: 10 seconds)
no ipv6 mld query-max-response-time		Deletes a specified maximum query response time.

11.1.6.3 MLD Querier Timeout

There should be a MLD querier on a network segment to prevent duplicating multicast traffic for connected hosts. When there are several routers, if the router has the lowest IPv6 address or if the router hears no queries during the timeout period, it becomes the querier.

To specify a timeout period before a router takes over as a querier for the interface after the previous querier has stopped querying, use the following command.

Command	Mode	Description
ipv6 mld querier-timeout <60-300>	Interface	Specifies an MLD queier timeout period. 60-300: MLD previous querier-timeout value (default: 255 seconds)
no ipv6 mld querier-timeout		Deletes a specified MLD queier timeout value.

11.1.6.4 MLD Last Member Query Count and Interval

When a host is not interested in receiving the multicast traffic for a particular group any more, it can explicitly leave the group by sending leave group messages.

Upon receiving a done message, a querier then sends out a Multicast-address-specific (MLDv1) or Multicast-address-source-specific query (MLDv2) message to determine if there is still any host interested in receiving the traffic. If there is no reply, the querier stops forwarding the multicast traffic. However, MLD messages may get lost for various reasons, so you can specify the number of sending query messages and its interval.

To specify the number of sending Multicast-address-specific or Multicast-address-source-specific query messages, use the following command.

Command	Mode	Description
ipv6 mld last-member-query-count <2-7>	Interface	Specifies a last member query count. 2-7: last member query count value (default: 2)
no ipv6 mld last-member-query-count		Deletes a specified last member query count.

To specify the interval to send group-specific or group-source-specific query messages, use the following command.

Command	Mode	Description
ipv6 mld last-member-query-interval <1000-25500>	Interface	Specifies a last member query interval. 1000-25500: last member query interval (default: 1000 milliseconds)
no ipv6 mld last-member-query-interval		Deletes a specified last member query interval.

11.1.6.5 MLD Immediate Leave

Normally, a querier sends a Multicast-address-specific or Multicast-address-source-specific query message upon receipt of a done message from a host. If you want to set a leave latency as 0 (zero), you can omit the querying procedure. When the querying procedure is omitted, the router immediately removes the interface from the MLD cache for that group, and informs the multicast routing protocols.

To enable the MLD immediate leave feature on a current interface, use the following command.

Command	Mode	Description
ipv6 mld immediate-leave group-list *WORD*	Interface	Enables the MLD immediate leave. 1-99: IP standard access list 1300-1999: IP standard access list (extended range) WORD: IPv6 access list name
no ipv6 mld immediate-leave		Disables the IGMP immediate leave.

Use this command only on MLDv1 and MLDv2 interfaces to which one host is connected. If there is more than one host connected to a network segment through the same interface, and a certain host receives a done message, the router will remove all hosts on the interface from the multicast group. The router will lose contact with the hosts that should remain in the multicast group until they send join requests in response to the router's next general query.

11.1.7 Displaying MLD Information

To display current MLD groups and relevant information, use the following command.

Command	Mode	Description
show ipv6 mld groups detail	Enable Global	Shows the multicast groups with receivers directly connected to the router and learned through MLD. X:X::X:X: IPv6 multicast group address IFNAME: interface name
show ipv6 mld groups X:X::X:X [**detail**]		
show ipv6 mld groups *IFNAME* [**detail**]		
show ipv6 mld groups *IFNAME* X:X::X:X [**detail**]		
show ipv6 mld interf*ace* *IFNAME*		

To display IPv6 MLD proxy information, use the following command.

Command	Mode	Description
show ipv6 mld-proxy	Enable Global	Shows the IPv6 MLD proxy information,

11.1.8 Debugging ICMPv6

To enable/disable a ICMPv6 debugging, use the following command.

Command	Mode	Description
debug ipv6 icmp	Enable	Enables ICMPv6 debugging.
no debug ipv6 icmp		Disables ICMPv6 debugging.

To display the debugging information, use the following command.

Command	Mode	Description
show debugging ipv6 icmp	Enable	Shows the debugging information of ICMPv6.

11.2 IPv6 Multicast Functions

This system provides various multicast functions including Layer 2 multicast forwarding, which allow you to achieve the fully effective and flexible multicast deployment.

11.2.1 Multicast Forwarding Database

Internally, this system forwards the multicast traffic referred to the multicast forwarding database (McFDB). The McFDB maintains multicast forwarding entries collected from multicast protocols and features, such as PIM, MLD etc.

11.2.1.1 Blocking Unknown Multicast Traffic

When certain multicast traffic comes to a port and the McFDB has no forwarding information for the traffic, the IPv6 multicast traffic is flooded to all ports by default. You can configure the switch not to flood unknown IPv6 multicast traffic.

To configure the switch to discard unknown IPv6 multicast traffic, use the following command.

Command	Mode	Description
ipv6 unknown-multicast block	Global	Configures the switch to discard unknown IPv6 multicast traffic. PORTS: unknown IPv6 multicast port number
ipv6 unknown-multicast port *PORTS*		
ipv6 unknown-multicast port *PORTS* **block**		
no ipv6 unknown-multicast block		Configures the switch to flood unknown IPv6 multicast traffic. (default) PORTS: unknown IPv6 multicast port number
no ipv6 unknown-multicast port *PORTS*		
no ipv6 unknown-multicast port *PORTS* **block**		

This command should not be used for the ports to which a multicast router is attached!

11.2.1.2 Forwarding Entry Aging

To specify the aging time for forwarding entries on the McFDB, use the following command.

Command	Mode	Description
ipv6 mcfdb aging-time <10-10000000>	Global	Specifies the aging time for forwarding entries on the McFDB. 10-10000000: IPv6 aging time (default: 300)
no ipv6 mcfdb aging-time		Deletes the specified aging time for forwarding entries.

To specify the maximum number of forwarding entries on the McFDB, use the following command.

Command	Mode	Description
ipv6 mcfdb aging-limit <256-65535>	Global	Specifies the maximum number of forwarding entries on the McFDB. 256-65535: number of entries (default: 5000)
no ipv6 mcfdb aging-limit		Deletes the specified maximum number of forwarding entries.

11.2.1.3 Displaying McFDB Information

To display McFDB information, use the following command.

Command	Mode	Description
show ipv6 mcfdb	Enable Global Bridge	Shows the current aging time and maximum number of forwarding entries.
show ipv6 mcfdb aging-entry [**vlan** *VLAN* | **group** *X:X::X:X*] [**mac-based** | **detail**]		Shows the current forwarding entries. VLAN: VLAN ID (1-4094) X:X::X:X: IPv6 multicast group address mac-based: lists entries on a MAC address basis

To clear multicast forwarding entries, use the following command.

Command	Mode	Description
clear ipv6 mcfdb [* | **vlan** *VLAN*]	Enable Global	Clears multicast forwarding entries. *: all forwarding entries VLAN: VLAN ID (1-4094)
clear ipv6 mcfdb vlan *VLAN* **group** *X:X::X:X* **source** *X:X::X:X*		Clears a specified forwarding entry. group: : IPv6 multicast group address source: IPv6 address

11.2.2 MLD Snooping Basic

Layer 2 switches normally flood multicast traffic within the broadcast domain, since it has no entry in the Layer 2 forwarding table for the destination address. Multicast addresses never appear as source addresses, therefore the switch cannot dynamically learn multicast addresses. This multicast flooding causes unnecessary bandwidth usage and discarding unwanted frames on those nodes which did not want to receive the multicast transmission. To avoid such flooding, MLD snooping feature has been developed.

The purpose of MLD snooping is to constrain the flooding of multicast traffic at Layer 2. MLD snooping, as implied by the name, allows a switch to snoop the MLD transaction between hosts and routers, and maintains the multicast forwarding table which contains the information acquired by the snooping. When the switch receives a join request from a host for a particular multicast group, the switch then adds a port number connected to the host and a destination multicast group to the forwarding table entry; when the switch receives a done message from a host, it removes the entry from the table.

11.2.2.1 Enabling MLD Snooping

You can enable MLD snooping globally or on each interface respectively. By default, MLD snooping is globally disabled.

To enable MLD snooping, use the following command.

Command	Mode	Description
ipv6 mld snooping	Global	Enables MLD snooping globally.
	Interface	Enables MLD snooping on the interface.

To disable MLD snooping, use the following command.

Command	Mode	Description
no ipv6 mld snooping	Global	Disables MLD snooping globally.
	Interface	Disables MLD snooping on the interface.

11.2.2.2 MLD Snooping Version

The membership reports sent to the multicast router are sent on the basis of the MLD snooping version of each interface. If you statically specify the MLD snooping version on a certain interface, the reports are always sent out only with the specified version.

If you do not statically specify the MLD snooping version, and a MLD version 1 query is received on the interface, the interface actively sends out a version 1 report to the router. If MLD snooping version 1 query is not consistently received on the interface for a timeout period (400 seconds), the interface version goes back to its default version (2).

To specify the static MLD snooping version, use the following command.

Command	Mode	Description
ipv6 mld snooping version <1-2>	Interface	Configures the MLD snooping version globally. 1-2: MLD snooping version (default: 2)

To delete the specified static MLD snooping version, use the following command.

Command	Mode	Description
no ipv6 mld snooping version	Interface	Deletes the specified MLD snooping version and returns to the default version.

11.2.2.3 MLD Snooping Robustness Value

The robustness variable allows you can tune to reflect expected packet loss on a congested network. If a network is expected to be lossy, you can increase the robustness variable to increase the number of times that packets are resent.

When receiving the query message that contains a certain robustness variable from an MLD snooping querier, a host returns the report message as many as the specified robustness variable.

To configure the robustness variable, use the following command.

Command	Mode	Description
ipv6 mld snooping robustness-variable <2-7>	Interface	Configures the robustness variable. (default: 2)

To delete a specified robustness variable, use the following command.

Command	Mode	Description
no ipv6 mld snooping robustness-variable	Interface	Deletes a specified robustness variable.

11.2.3 MLD Snooping

11.2.3.1 MLD Snooping Querier Configuration

MLD snooping querier should be used to support MLD snooping in a VLAN where PIM and MLD are not configured.

When the MLD snooping querier is enabled, the MLD snooping querier sends out periodic general queries that trigger membership report messages from a host that wants to receive multicast traffic. The MLD snooping querier listens to these membership reports to establish appropriate forwarding.

Enabling MLD Snooping Querier

To enable the MLD snooping querier, use the following command.

Command	Mode	Description
ipv6 mld snooping querier	Interface	Enables the MLD snooping querier.

To disable the MLD snooping querier, use the following command.

Command	Mode	Description
no ipv6 mld snooping querier	Interface	Disables the MLD snooping querier.

i

If you do not specify a source address of an MLD snooping query, the IP address configured on the VLAN is used as the source address by default.

MLD Snooping Query Response Time

MLDv1/v2 membership query messages include the maximum query response time field. This field specifies the maximum time allowed before sending a responding report. The maximum query response time allows a router to quickly detect that there are no more hosts interested in receiving multicast traffic.

To specify a maximum query response time advertised in general query messages, use the following command.

Command	Mode	Description
ipv6 mld snooping query-max-response-time <1-240>	Interface	Specifies a maximum query response time. 1-240: maximum response time (default: 10 seconds)

To delete a specified maximum query response time, use the following command.

Command	Mode	Description
no ipv6 mld snooping query-max-response-time	Interface	Deletes a specified maximum query response time and resets the default.

11.2.3.2 MLD Snooping Fast Leave

Fast-leave can be used to speed up the reaction to MLD leave announcements.

This minimizes the leave latency of group memberships on an interface, as the switch does not send group-specific queries. As a result, the group entry is removed from the forwarding table as soon as a group done message is received.

To enable the MLD snooping fast leave, use the following command.

Command	Mode	Description
ipv6 mld snooping fast-leave	Interface	Enables the MLD snooping fast leave.

⚠ The MLD snooping fast-leave function is available only in the MLDv1 host.

⚠ In fast-leave processing, when there is more than one MLD host belonging to a group, and a certain host sends a done message, the MLD snooping querier will remove all host entries from the forwarding table. The switch lose contact with the hosts that should remain from the forwarding table until they send join requests in response to the switch's next general query message.

So, it is recommended that you use the fast leave command only if there is one receiver behind the interface for a given group.

To disable the MLD snooping fast leave, use the following command.

Command	Mode	Description
no ipv6 mld snooping fast-leave	Interface	Disables the MLD snooping fast leave.

11.2.3.3 MLD Snooping Last Member Query Interval

Upon receiving a done message, a switch with MLD snooping then sends out a multicast-address-specific query (MLDv1) or multicast-address-source-specific query (MLDv2) message to determine if there is still any host interested in receiving the traffic. If there is no reply, the switch stops forwarding the multicast traffic. However, MLD messages may get lost for various reasons, so you can specify an interval to send query messages.

To specify an interval to send multicast-address-specific or multicast-address-source-specific query messages, use the following command.

Command	Mode	Description
ipv6 mld snooping last-member-query-interval <1000-25500>	Interface	Specifies a last member query interval. 1000-25500: last member query interval value (default: 1000 milliseconds)

To delete a specified an interval to send multicast-address-specific or multicast-address-source-specific query messages, use the following command.

Command	Mode	Description
no ipv6 mld snooping last-member-query-interval	Interface	Deletes a specified last member query interval.

11.2.3.4 MLD Snooping Report Suppression

If an MLD querier sends general query messages, and hosts are still interested in the multicast traffic, the hosts should return membership report messages. For a multicast router, however, it is sufficient to know that there is at least one interested member for a group on the network segment. Responding a membership report per each of group members may unnecessarily increase the traffic on the network; only one report per group is enough.

When the MLD snooping report suppression is enabled, a switch suppresses membership reports from hosts other than the first one, allowing the switch to forward only one membership report in response to a general query from a multicast router.

To enable the MLD snooping report suppression, use the following command.

Command	Mode	Description
ipv6 mld snooping report-suppression	Interface	Enables the MLD snooping report suppression.

To disable the MLD snooping report suppression, use the following command.

Command	Mode	Description
no ipv6 mld snooping report-suppression	Interface	Disables the MLD snooping report suppression.

11.2.3.5 Multicast Router Port Configuration

The multicast router port is the port which is directly connected to a multicast router. A switch adds multicast router ports to the forwarding table to forward membership reports only to those ports.

Static Multicast Router Port

You can statically configure Layer 2 port as the multicast router port which is directly connected to a multicast router, allowing a static connection to a multicast router.

To specify a multicast router port, use the following command.

Command	Mode	Description
ipv6 mld snooping mrouter port *PORTS*	Interface	Specifies a multicast router port. PORTS: port number

To delete a specified multicast router port, use the following command.

Command	Mode	Description
no ipv6 mld snooping mrouter port *PORTS*	Interface	Deletes a specified multicast router port.

Displaying Multicast Router Port

To display a current multicast router port for MLD snooping, use the following command.

Command	Mode	Description
show ipv6 mld snooping mrout-	Enable	Shows a current multicast router port for MLD snooping

er *IFNAME*	Global	globally. IFNAME: VLAN interface name

11.2.4 MLD State Limit

You can use MLD State Limit feature to limit the number of MLD states that can be joined to a router on a per-interface or global level. The MLD group limits feature provides protection against DoS (denial of service) attacks caused by MLD packets. Membership reports exceeding the configured limits are not entered into the MLD cache and traffic for the excess membership reports is not forwarded.

To limit the number of MLD state globally, use the following command.

Command	Mode	Description
ipv6 mld limit <1-2097152> [**except** *WORD*]	Global	Limits the number of MLD membership reports globally. 1-2097152: the number of MLD states allowed on a router. (Default: 0) WORD: IPv6 access list name
no ipv6 mld limit		Disables the globally configured MLD state limit.

If you want to exclude certain groups or channels from being counted against the MLD limit so that they can be joined to an interface, use **except** option.

To limit the number of MLD state on an interface, use the following command.

Command	Mode	Description
ipv6 mld limit <1-2097152> **[except** *WORD* **]**	Interface	Limits the number of MLD membership reports on an interface. 1-2097152: the number of MLD states allowed on an interface (default:0) WORD: IPv6 access list name
no ipv6 mld limit		Disables the configured MLD state limit per interface.

11.2.5 MLD Snooping Debug

To enable the debugging of all MLD or a specific feature of the MLD, use the following command.

Command	Mode	Description
debug mld snooping {all | decode | encode | fsm | tib | events}	Enable	Enables MLD snooping debugging.

To disable the MLD snooping debugging, use the following command.

Command	Mode	Description
no debug mld snooping {all | decode | encode | fsm | tib | events}	Enable	Disables MLD snooping debugging.

To display the debugging information, use the following command.

Command	Mode	Description
show debugging mld snooping	Enable	Shows the debugging status of MLD.

11.3 IPv6 Multicast Routing

When receivers join a certain group, multicast routers must deliver the multicast traffic corresponding to the group to those receivers. To determine the appropriate forwarding path and to replicate the multicast traffic to multiple destinations, multicast routing protocols are needed.

The multicast routing protocols establish the distribution tree by building a forwarding table in its own way. The forwarding table contains the information of sources, groups, interfaces, and how to forward multicast packets.

Reverse Path Forwarding (RPF)

Routers typically forward unicast packets with the destination lookup. When unicast packets come to interfaces, routers forward the packets to the interfaces toward the destinations of those packets by referring to the routing table. If the routing table does not contain the information of the destinations, the routers forward the packets to the default gateway.

On the other hand, routers forward multicast packets based on the source of the packets. When multicast packets come to an interface, routers validate whether the interface on which the packets are received is directly toward the source of those packets by referring to the existing unicast routing table. This procedure is called the reverse path forwarding (RPF) check. If incoming multicast packets pass the RPF check, routers forward the packets to the outgoing interface. If not, routers drop the packets.

In the multicast routing, routers must forward packets away from the sources to prevent routing loops. Finally, the distribution tree established by RPF follows the shortest path tree (SPT) topology.

11.3.1 Multicast Routing

11.3.1.1 Enabling Multicast Routing

By default, multicast routing is disabled. To configure the system to forward multicast traffic via Layer 3 network, you need to enable multicast routing.

To enable/disable Layer 3 multicast routing for IPv6, use the following command.

Command	Mode	Description
ipv6 multicast-routing	Global	Enables IPv6 multicast routing.
no ipv6 multicast-routing		Disables IPv6 multicast routing. (default)

11.3.1.2 ECMP Load Splitting

Multicast routing protocols have different forwarding policies for the equal cost multipath (ECMP). In case of PIM, the interface with highest IPv6 address is used to forward multicast traffic over the equal cost multipath.

The purpose of this feature is load splitting for forwarding multicast traffic over ECMP, allowing more efficient use of network resources and preventing traffic congestion. With this feature, multicast traffic is split across the equal cost multipath based on either its source address or its source and group address.

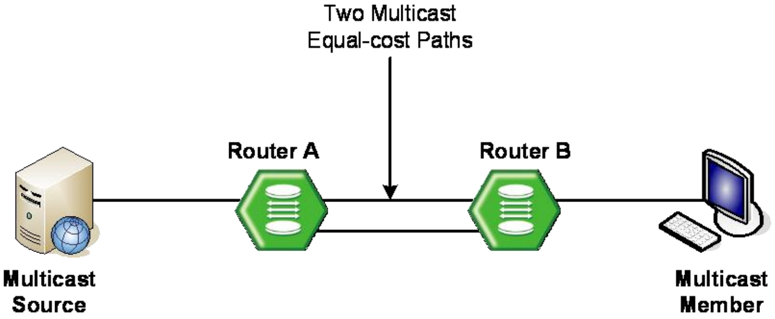


Fig. 11.3 Multicast Equal Cost Multipath (ECMP)

ECMP load splitting has two options for next hop decision:

- **srcip** selects next hop based on source address.
- **srcgrpip** selects next hop based on both source and group address.

To enable ECMP load splitting for IPv6, use the following command.

Command	Mode	Description
ipv6 multicast multipath [**srcip** | **srcgrpip**]	Global	Enables IPv6 ECMP load splitting. srcip: source address (default) srcgrpip: source and group address
no ip multicast multipath		Disables ECMP load splitting.

To disable ECMP load splitting for IPv6, use the following command.

Command	Mode	Description
no ipv6 multicast multipath	Global	Disables IPv6 ECMP load splitting.

11.3.1.3 MRIB Entry Limit

You can limit the maximum number of multicast routing entries in the multicast routing table in the multicast routing information base (MRIB), and then the system generates an error message when the number of the entries exceeds the limit. If the warning threshold is specified, the system generates a warning message when the number of the entries exceeds the threshold.

To specify the maximum number of multicast routing entries, use the following command.

Command	Mode	Description
ipv6 multicast route-limit *LIMIT* [*THRESHOLD*]	Global	Specifies the limit of the maximum number of multicast routing entries.

		LIMIT: number of routing entries (1-214783647) THRESHOLD: warning threshold (1-214783647)
no ipv6 multicast route-limit		Deletes a specified limit.

The warning threshold must not exceed the maximum number of multicast routing entries.

11.3.1.4 Displaying MRIB Entry

To display the multicast routing entries in the MRIB, use the following command.

Command	Mode	Description
show ipv6 mroute [**summary** | **count**]	Enable Global	Shows all multicast routing entries. summary: abbreviated display count: route and packet count data
show ipv6 mroute [**dense** | **sparse**] [**count** | **summary**]		Shows the multicast routing entries for a given PIM mode. dense: dense mode sparse: sparse mode count: route and packet count data summary: abbreviated display
show ipv6 mroute *X:X::X:X* [**dense** | **sparse**] [**count** [**summary**]		Shows the multicast routing entries for a given group. X:X::X:X: IPv6 source/group address
show ipv6 mroute *X:X::X:X* *X:X::X:X* [**dense** | **sparse**] [**count** | **summary**]		Shows the multicast routing entries for a given group and source. X:X::X:X: IPv6 source/group address

If you use the **clear ipv6 mroute** command, the MRIB clears the multicast routing entries in its multicast routing table, and removes the entries from the multicast forwarder.

11.3.1.5 Clearing MRIB Entry

To delete the multicast routing entries in the MRIB, use the following command.

Command	Mode	Description
clear ipv6 mroute *	Enable Global	Deletes all multicast route entries.
clear ipv6 mroute *X:X::X:X* [*X:X::X:X*]		Deletes a specified multicast route entry. X:X::X:X: IPv6 source/group address

To clear the multicast forwarding cache (MFC) and tree information base (TIB) entries in the PIM-SM protocol level, use the following command.

Command	Mode	Description
clear ipv6 mroute * [**pim sparse-mode**]	Enable Global	Deletes all MFC and TIB entries in the PIM-SM protocol.
clear ipv6 mroute *X:X::X:X* [*X:X::X:X*] [**pim sparse-mode**]		Deletes a specified MFC and TIB entry in the PIM-SM protocol. X:X::X:X: IPv6 source/group address

When clearing the MRIB entries, you must specify the group address prior to the source address.

11.3.1.6 Displaying MRIB Statistics

To display the multicast routing statistics entries in the MRIB, use the following command.

Command	Mode	Description
show ipv6 mroute count	Enable Global	Shows all multicast routing statistics entries.
show ipv6 mroute {**dense** | **sparse**} **count**		Shows the multicast routing statistics entries for a given PIM mode. dense: dense mode sparse: sparse mode
show ipv6 mroute *X:X::X:X* [**dense** | **sparse**] **count**		Shows the multicast routing statistics entries for a given group. X:X::X:X: group IPv6 address
show ipv6 mroute *X:X::X:X* *X:X::X:X* [**dense** | **sparse**] **count**		Shows the multicast routing statistics entries for a given group and source. X:X::X:X: group/source IPv6 address

To delete the multicast routing statistics entries from the multicast routing table, use the following command.

Command	Mode	Description
clear ipv6 mroute statistics *	Enable Global	Deletes all multicast routing statistics entries.
clear ipv6 mroute statistics *X:X::X:X* [*X:X::X:X*]		Deletes a specific multicast routing statistics entry. X:X::X:X: group/source IPv6 address

11.3.1.7 Displaying MFIB Information

The multicast forwarding information base (MFIB) is the group of the information to forward multicast traffic in Layer 3, which is maintained by currently running multicast routing protocol. You can verify the forwarding entries in the MFIB with the **show ipv6 mfib** command.

To display the multicast forwarding entries in the MFIB, use the following command.

Command	Mode	Description
show ipv6 mfib [**vlan** *VID* | **group** *X:X::X:X*] [**detail**]	Enable Global Bridge	Shows the multicast forwarding entries in the MFIB. VID: VLAN ID (1-4094) *X:X::X:X*: IPv6 multicast group address

11.3.1.8 Displaying RPF information

To display RPF (Reverse Path Forwarding) information for IPv6 multicast source, use the following command.

Command	Mode	Description
show ipv6 rpf *X:X::X:X*	Enable	Shows RPF information. X:X::X:X: IPv6 address of multicast source

11.3.1.9 MRIB Debug

To debug events in the MRIB, use the following command.

Command	Mode	Description
debug nsm mcast6 {**all** | **fib-msg** | **mif | mrt** | **register** | **stats**}	Enable	Debugs events in the MRIB. all: all IPv6 multicast debugging fib-msg: MFIB messages mif: multicast interface mrt: multicast routes register: multicast PIM register messages stats: multicast statistics
no debug nsm mcast6 {**all** | **fib-msg** | **mif** | **mrt** | **register** | **stats**}		Disables the debug event.

11.3.2 PIMv6 Basic

Protocol Independent Multicast (PIM) is the most widely deployed multicast routing protocol. It may use the underlying unicast routing information base, but is not dependent on any particular unicast routing protocol. PIM has two operation modes, which are called PIM Sparse Mode (PIM-SM) and PIM Dense Mode (PIM-DM), each optimized for a different environment. IPv6 PIM supports the PIM-SM only.

PIM-SM is a multicast routing protocol efficient for multicast groups that may span wide-area (and inter-domain) internets. In the sparse mode, routers forward multicast packets only when they receives explicit join messages from neighboring routers that have downstream group members. PIM-SM uses a unidirectional shared tree per group to deliver multicast traffic, and optionally uses the shortest path tree per source.

PIM-DM is a multicast routing protocol efficient for multicast groups that are densely populated across a network. In the dense mode, routers initially flood multicast datagrams to all multicast routers, since they assume that all downstream systems want to receive multicast packets. Prune messages are then used to prevent from propagating to routers with no group members. Both PIM protocols use the same message formats.

i This switch currently supports PIM-SM only.

PIM-SM Operation

When multicast receivers indicate their interests in certain multicast groups, the DR of the receivers sends PIM join messages with (*, G) state toward the RP for those groups. While the join messages flow hop-by-hop toward the RP, each PIM router along the path adds the interface on which the join messages are received to the outgoing interface (OIF) list with the join state, and sends the messages to the interface toward the RP.

If the RP has receivers interested in the group, the RP must receive the multicast traffic from the source of that group via the SPT to deliver the traffic to those receiver. The DR of the source encapsulates the multicast packets in the PIM register messages, and starts to unicast them to the RP. On receipt of the register messages, the RP sends the join message with (S, G) state toward the source to establish the SPT. When receiving the multicast traffic via the established SPT, the RP forwards the traffic toward those receivers.

Multicast traffic may be directly delivered from sources to receivers via the SPT using the switchover mechanism. For more information, see Section 11.3.6 IPv6 SPT Switchover

Rendezvous Point Tree (RPT)

PIM-SM mainly uses a shared tree to deliver multicast traffic, called the RP tree (RPT). As its name implies, it relies on a core router called the Rendezvous Point (RP) that receives all multicast traffic from the sources and forwards that traffic to the receivers. Other routers do not need to know the information of the sources. All they need to know is the address of the RP, because the RP surely knows the information of the sources for all multicast groups. Thus, receivers who are interested in a certain multicast group only send PIM join messages with (*, G) state toward the RP.

The shared tree is unidirectional, which means all multicast traffic flows only from the RP to the receivers. Thus, there is no guarantee that the shared tree (RPT) is the shortest path tree to the source, and most likely it is not, resulting in longer delays, but less forwarding states to maintain.

Fig. 11.4 shows an example of the RPT network. The multicast traffic from the source A flows through the router B to the router D which is the RP. Note that, even in the RPT, RPs must receive multicast traffic from the sources via the shortest path. The RP then distributes the traffic to the receiver E and F that indicate the interest in the multicast group. Consequently, the distribution tree for the receiver E is **A→B→D→E**, and the one for the receiver F is **A→B→D→C→F**.

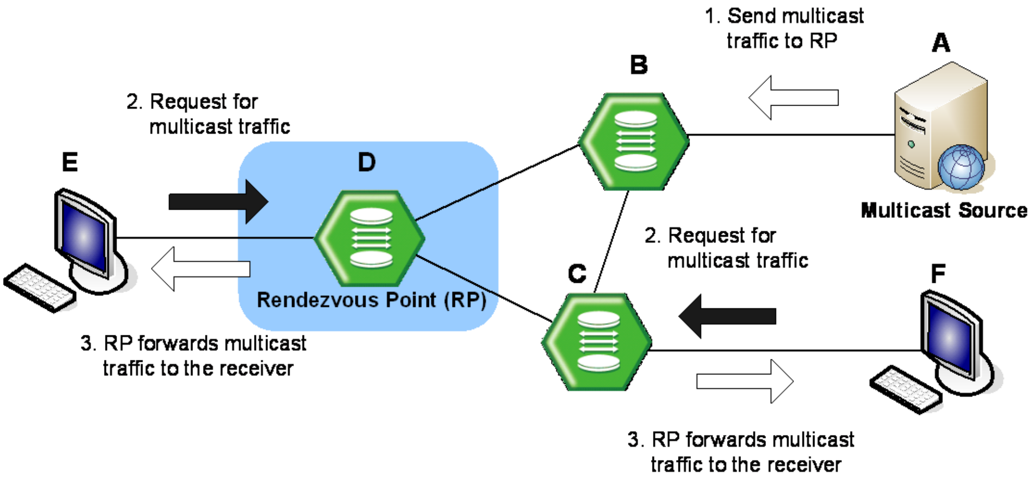

1. Send multicast traffic to RP
A
B
2. Request for multicast traffic
E
D
Multicast Source
2. Request for multicast traffic
C
F
Rendezvous Point (RP)
3. RP forwards multicast traffic to the receiver
3. RP forwards multicast traffic to the receiver

Fig. 11.4 Rendezvous Point Tree

Shortest Path Tree (SPT)

When the number of receivers increases, a shared tree may not be entirely efficient, so PIM-SM also provides the option to switch to receive multicast traffic on a shortest path tree (SPT). When this option is enabled, on receiving the first multicast packet from the RP in response to the PIM join message, the switchover to the SPT then occurs.

To establish the SPT to the multicast source, the DR sends the join message with (S, G) state toward that source. When the SPT between the receiver and source is established, and multicast traffic is sent via that distribution tree, the DR sends the prune message with (*, G) state toward the RP to prune the existing shared tree to receive the traffic.

SPT is established based on the existing unicast routing table by performing the RPF check. It has a different distribution tree for every multicast source, allowing the efficient network traffic flows, but more resources are needed for each multicast routers to maintain (S, G) states.

Fig. 11.5 shows an example of the SPT switchover. The multicast traffic from the source A initially attempts to flow through the router B and C to the receiver D that indicates the interest in the multicast group. Once the traffic arrives at the router C which is the DR, it sends the join message with (S, G) state toward the source A to build the SPT between the source and receiver. The source A then sends the multicast traffic to the receiver D via the SPT by deleting unnecessary hops. Finally, the distribution tree (SPT) built by the RPF check is **A→C→D**.

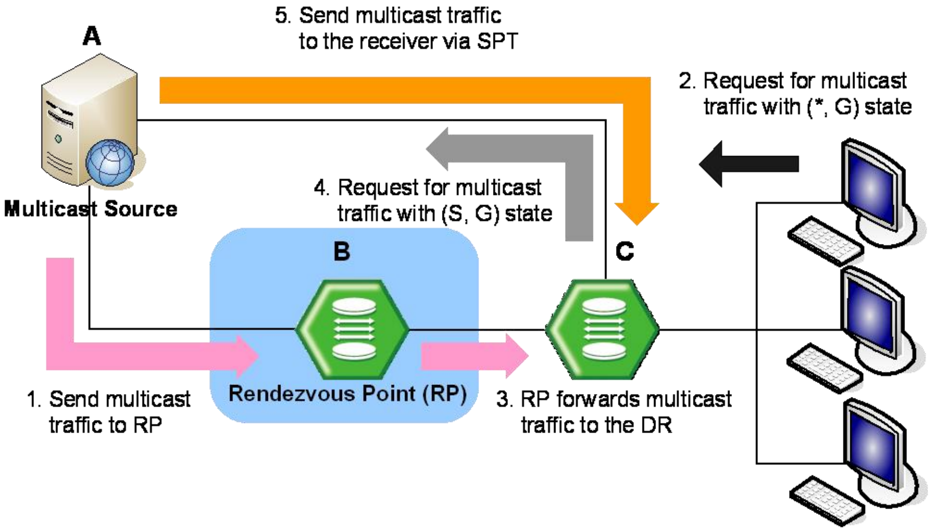

A
5. Send multicast traffic to the receiver via SPT
2. Request for multicast traffic with (*, G) state
Multicast Source
4. Request for multicast traffic with (S, G) state
B
C
D
E
F
Rendezvous Point (RP)
1. Send multicast traffic to RP
3. RP forwards multicast traffic to the DR

Fig. 11.5 Shortest Path Tree

PIM Messages

The followings are simple descriptions of PIM control messages:

- **Hello**
  PIM routers periodically send hello messages on all interfaces to discover neighboring PIM routers and to determine which router will be the DR for each subnet.
- **Register**
  Register messages are sent by the DR to the RP when a multicast packet needs to be transmitted on the RPT. These messages may contain the encapsulated multicast traffic. Both register and register-stop messages are unicast.
- **Register-stop**
  When receiving the register-stop message, routers stop sending register messages. These messages are sent from the RP to the sender of the register messages.
- **Join/prune**
  Join/prune messages are sent by routers towards upstream sources or RPs. Join messages are sent to receive the multicast traffic by building shared trees (RPT) or source trees (SPT). Prune messages are sent to prune established distribution trees when there are no more interests in the traffic.
- **Bootstrap**
  The bootstrap router (BSR) sends bootstrap messages to elect the Rendezvous Point (RP), which contain a set of the information for each candidate RP (RP-set).
- **Assert**
  Assert messages are used to resolve forwarding conflicts among routers.
- **Candidate RP advertisement**
  Each candidate RP unicasts these messages containing its own information to the BSR. The BSR then includes a set of that information in the bootstrap message.

11.3.2.1 PIMv6 Mode

To enable PIM-SM on an interface, use the following command.

Command	Mode	Description
ipv6 pim sparse-mode	Interface	Enables PIM-SM on an interface.
no ipv6 pim sparse-mode		Disables PIM-SM on an interface.

You can also enable PIM-SM as the passive mode. The passive mode operation is for local members. The passive mode disables sending/receiving PIM packets on an interface, allowing only MLD mechanism to be active.

To enable PIM-SM passive mode on an interface, use the following command.

Command	Mode	Description
ipv6 pim sparse-mode passive	Interface	Enables PIM-SM passive mode on an interface.
no ipv6 pim sparse-mode passive		Disables PIM-SM passive mode on an interface.

11.3.2.2 DR Priority

In PIM-SM, the designated router (DR) is normally the first-hop router of receivers (hosts), which is responsible to periodically send PIM join/prune messages toward the RP to inform it of the host group membership.

When there are multiple routers on the same subnet, one of them must be selected to act as the DR. To elect the DR, each PIM router examines PIM hello messages received from other neighbor PIM routers and compares its DR priority in those from neighbors. The router with the highest priority then is elected as the DR. In case of more than one router with the same highest priority value, the one with the higher IPv6 address is elected. If no PIM hello message is received from the DR for a certain period of time, another DR election is held.

To specify the DR priority on an interface, use the following command.

Command	Mode	Description
ipv6 pim dr-priority **<**0-4294967294>	Interface	Specifies the DR priority on an interface. 0-4294967294: priority value (default: 1)
no ipv6 pim dr-priority **[<**0-4294967294>]		Deletes the specified DR priority.

11.3.2.3 Neighbor Filtering

If necessary, you can filter neighbor routers using access lists. When you enable this feature, PIM establishes adjacency without neighbor routers specified as deny in access lists.

To enable filtering neighbor routers in PIM, use the following command.

Command	Mode	Description
ipv6 pim neighbor-filter *WORD*	Interface	Enables filtering neighbor routers in PIM. WORD: access list name
no ipv6 pim neighbor-filter *WORD*		Disables filtering neighbor routers in PIM. WORD: access list name

To display the information of PIM neighbor routers, use the following command.

Command	Mode	Description
show ipv6 pim neighbor [**detail**]	Enable Global	Shows the information for PIM neighbor routers.

11.3.2.4 PIMv6 Hello Message

PIM routers periodically send PIM hello messages to discover neighboring PIM routers and to determine which router will be the Designated Router (DR) for each subnet. PIM hello messages are also the multicast packets using the group address ff02::d (all PIM routers group).

To specify an interval to send PIM hello messages, use the following command.

Command	Mode	Description
ipv6 pim hello-interval <1-65535>	Interface	Specifies an interval to send PIM hello messages. 1-65535: hello message interval (unit: second)
no ipv6 pim hello-interval		Deletes a specified interval to send PIM hello messages.

PIM hello messages may contain the hold time value in the option fields, which specifies how long the information is valid. The default hold time is 3.5 times of the interval of the PIM hello messages. If you sets 10 seconds, the hold time of the PIM hello message will be 10 x 3.5 = 35 seconds

⚠ If a hold time you specified is less than the current interval of those, the hold time is ignored and return to the default value.

To specify a hold time of PIM hello messages, use the following command.

Command	Mode	Description
ipv6 pim hello-holdtime <1-65535>	Interface	Specifies a hold time of PIM hello messages. 1-65535: hello message hold time (unit: second)
no ipv6 pim hello-holdtime		Deletes a specified hold time of PIM hello messages.

11.3.2.5 PIMv6 Join/Prune Interval

Router sends the PIM join/prune message to the upstream RPF neighbor. PIM multicast traffic can join or be removed from the shortest path tree (SPT) or rendezvous point tree (RPT).

To specify an interval to send PIM join/prune messages, use the following command.

Command	Mode	Description
ipv6 pim jp-timer <1-65535>	Global	Specifies an interval to send join/prune messages. 1-65535: join/prune message interval (unit: second)
no ipv6 pim jp-timer [<1-65535>]		Deletes a specified interval to send join/prune messages.

11.3.2.6 Displaying PIMv6 Information

To display current PIM information, use the following command.

Command	Mode	Description
show debugging ipv6 pim sparse-mode	Enable/ Global/ Bridge	Shows PIM-SMv6 debugging status
show ipv6 pim interface [**detail**]	Enable Global	Shows PIMv6 interface information. detail: detailed interface information
show ipv6 pim local-members [*IFNAME*]		Shows PIMv6 local membership information. IFNAME: interface name
show ipv6 pim mroute *X:X::X:X* [*X:X::X:X*]		Shows the multicast routing table. X:X::X:X: multicast group or source address
show ipv6 pim mroute [summary]		Shows the summary of multicast routing table entry information.
show ipv6 pim nexthop		Shows the next hop information

11.3.3 PIMv6 Rendezvous Point (RP)

In a shared tree, Rendezvous Point (RP) is a means for receivers to discover the sources that send to a particular multicast group. It is responsible to receive all multicast traffic from the sources and to forward that traffic to the receivers.

11.3.3.1 Static RP

To elect the RP among candidate RPs in the shared tree, the system supports the BSR mechanism and static RP, and also supports the simultaneous use of those. You can configure a router to use the static RP either for all the multicast groups (default) or for specific multicast groups (with access lists). If multiple static RPs are available for a single multicast group, the one with the highest IPv6 address will be elected.

To statically specify an RP address for multicast groups, use the following command.

Command	Mode	Description
ipv6 pim rp-address *X:X::X:X* WORD	Global	Specifies an RP address for IPv6 multicast groups. X:X::X:X: RP address WORD: access list name (1~99)
no ipv6 pim rp-address *X:X::X:X*		Deletes a specified RP address for multicast groups

11.3.3.2 Keep Alive Time

After a multicast source registers with the RP, the DR of the multicast source periodically sends the PIM null-register message to the RP to keep the (S, G) state between the router and RP. The null-register message is the one without encapsulated multicast traffic. If there is no null-register message during a given keep alive time (KAT), the multicast routing entry with (S, G) state is expired, and the source registration process will restart.

To specify the keep alive time for (S, G) states at the RP, use the following command.

Command	Mode	Description
ipv6 pim rp-register-kat <1-65535>	Global	Specifies the KAT for (S, G) states at the RP. 1-65535: KAT value(unit: second)
no ipv6 pim rp-register-kat		Deletes the specified KAT value.

11.3.3.3 Interface for Candidate RP

To elect the RP, each candidate RP sends its information to the BSR. This advertisement contains the IP address and priority of the candidate RP and the multicast groups that it can service. The BSR then periodically distributes the bootstrap message that includes a set of the information received from each candidate RP (RP-set) to all the routers in the PIM-SM domain.

To configure an interface to send the candidate RP advertisement to the BSR, use the following command.

Command	Mode	Description
ipv6 pim rp-candidate *IFNAME* [**group-list** *WORD* [**interval** <1-	Global	Configures an interface to send the candidate RP advertisement.

Command	Mode	Description
16383>] [**priority** <0-255>]		IFNAME: interface name WORD: IPv6 access list name 1-16383: advertising interval (unit: second) 0-255: priority value
no ipv6 pim rp-candidate *IFNAME* **group-list** *WORD*		Deletes specified multicast groups which an interface can service. WORD: IPv6 access list name
no ipv6 pim rp-candidate *IFNAME*		Configures an interface not to send the candidate RP advertisement.
no ipv6 pim rp-candidate		Configures an interface not to send the candidate RP advertisement as well as deletes specified candidate RP information.

The access list with this command specifies the multicast groups that an advertising router can service. The candidate RP information without the access lists means that the router will service all the multicast groups.

11.3.3.4 Ignoring RP Priority

Normally, when choosing the RP among candidate RPs, routers examine the bootstrap messages sent from the BSR, and then choose the one has the highest priority among the RP-set. You can configure a router to only use the hash mechanism for the RP choice instead of the RP priority. This feature is used to interoperate with a router that cannot recognize the RP priority.

To configure a router to use the hash mechanism for the RP choice, use the following command.

Command	Mode	Description
ipv6 pim ignore-rp-set-priority	Global	Enables ignoring the PR priority for the RP choice.
no ipv6 pim ignore-rp-set-priority		Disables ignoring the PR priority for the RP choice.

Displaying RP Information

To display the RP information, use the following command.

Command	Mode	Description
show ipv6 pim rp mapping	Enable Global	Shows group-to-RP mappings and the RP-set.
show ipv6 pim rp-hash *X:X::X:X*		Shows the RP to be chosen for a specified group. X:X::X:X: multicast group address

11.3.4 Bootstrap Router

The bootstrap router (BSR) mechanism is one way that a multicast router can learn the set of group-to-RP mappings required in order to function.

All multicast routers in PIM-SM domain can be potentially the bootstrap router (BSR); they are all considered as candidate BSRs. To elect the BSR among the candidate BSRs, each candidate BSR floods the bootstrap messages with its information to the domain. When receiving the bootstrap messages, the candidate BSRs examine the messages, and then the one with the highest priority is elected as the BSR. If more than one candidate with the same highest priority, the one with the higher IP address is elected.

The elected BSR is responsible to periodically send out bootstrap messages including the RP-set, allowing all the routers in the PIM-SM domain determine which router is the RP that covers given multicast groups.

11.3.4.1 Interface for Candidate BSR

To configure an interface to the candidate BSR, use the following command.

Command	Mode	Description
ipv6 pim bsr-candidate *IFNAME*	Global	Configures an interface to the candidate BSR. IFNAME: interface name 0-128: hash mask length for RP selection 0-255: priority for candidate BSR
ipv6 pim bsr-candidate *IFNAME* <0-128>		
ipv6 pim bsr-candidate *IFNAME* <0-128> <0-255>		
no ipv6 pim bsr-candidate *IFNAME*		Configures an interface not to the candidate BSR.

11.3.4.2 Clearing RP-Set

The BSR periodically distributes the bootstrap message that includes a set of the information received from each candidate RP (RP-set) to all the routers in the PIM-SM domain. You can also clear all RP-set to reset.

To clear all RP-set, use the following command.

Command	Mode	Description
clear ipv6 pim sparse-mode bsr rp-set *	Enable Global	Clears all RP-set.

11.3.4.3 Displaying BSR Configuration

To display the BSR information, use the following command.

Command	Mode	Description
show ipv6 pim bsr-router	Enable Global	Shows the BSR information.

11.3.5 Source Registration

Multicast sources do not need any join process to send multicast traffic, since the DR of the multicast sources just receives the traffic from the sources without any information. Even in the RPT, RPs must receive multicast traffic from the sources via the shortest path while receivers receive multicast traffic via the shared tree. Thus, the DR needs to inform the RP about the information for the source, and the SPT must be established between the DR and RP via (S, G) states.

In case of the registration for a source, when receiving multicast traffic from the source, the DR encapsulates the multicast traffic in the PIM register message, and constantly unicasts it to the RP. The RP receives the register message, and then sends the PIM join message with (S, G) state back toward the DR to establish the SPT between them. Once the DR receives the join message, the SPT is then established, and the DR begins sending the multicast traffic without an encapsulation to the RP. When receiving the native multicast traffic, the RP unicasts the PIM register-stop message back to the DR. The DR then stops encapsulating the multicast traffic in the register message.

11.3.5.1 Registration Rate Limit

You can limit the maximum number of the PIM register message packets per second. If you enable this feature, both DR and RP will discard the register messages that exceed the limit.

To enable the rate limit for PIM register message, use the following command.

Command	Mode	Description
ipv6 pim register-rate-limit <1-65535>	Global	Enables the rate limit for PIM register message. 1-65535: maximum number of packets that can be sent per second
no ipv6 pim register-rate-limit		Disables the rate limit for PIM register message.

11.3.5.2 Registration Suppression Time

Once a multicast routing entry with (S, G) state is established by the source registration, the periodic reregistration is needed to keep the state for the entry. After the registration, the DR periodically sends the PIM null-register message that does not contain the encapsulated multicast traffic to the RP, and the RP returns the register-stop message. If there is no response to the null-register message during a given period, the multicast routing entry with (S, G) state is expired, and the source registration process will start again.

You can specify the interval to send the PIM null-register message which is also called the registration suppression time. When you specify this value at the RP, the configuration modifies the keep alive time (KAT) for the RP, if the **ipv6 pim rp-register-kat** command is not used.

To specify the registration suppression time, use the following command.

Command	Mode	Description

Command	Mode	Description
ipv6 pim register-suppression <1-65535>	Global	Specifies the registration suppression time. 1-65535: null-register message interval (unit: second)
no ipv6 pim register-suppression		Deletes the specified the registration suppression time.

11.3.5.3 Register Message Filtering

You can enable the router to filter multicast sources specified in access lists at the RP. This filtering will permit/deny the PIM register messages for the specified sources. If unauthorized sources try to register with the RP, the RP then drops the PIM register messages from those sources. You can specify the either multicast source or source's DR address in access lists.

To enable the router to filter multicast sources, use the following command.

Command	Mode	Description
ipv6 pim accept-register list *WORD*	Global	Enables the router to filter multicast sources. WORD: access list name - 100-199: IP extended access list - 2000-2699: IP extended access list (extended range)
no ipv6 pim accept-register		Disables the router to filter multicast sources.

11.3.5.4 RP Reachability Validation

To enable the RP reachability validation for the source registration process at the first-hop router, use the following command.

Command	Mode	Description
ipv6 pim register-rp-reachability	Global	Enables the RP reachability validation.
no ipv6 pim register-rp-reachability		Disables the RP reachability validation. (default)

11.3.5.5 Source Address of Register Message

You can specify the source IPv6 address of PIM register messages sent by the designated router (DR). This address is used to send corresponding PIM register-stop messages in response. By default, the source IPv6 address of register messages is the IP address of the interface toward the RP. This address must be able to be learned by routing protocols on the DR.

To specify the source IPv6 address of PIM register messages, use the following command.

Command	Mode	Description
ipv6 pim register-source {*X:X::X:X* | *IFNAME*}	Global	Specifies the source IPv6 address of register messages.

Command	Mode	Description
		X:X::X:X: source IP address IFNAME: interface name
no ipv6 pim register-source		Deletes a specified source IPv6 address of register messages.

11.3.6 IPv6 SPT Switchover

PIM-SM provides the switching option to deliver multicast traffic on the SPT. Multicasting over the SPT may be more efficient than multicasting over the RPT, since it can substantially reduce the network latency.

When the switching option is enabled, once multicast traffic from sources arrives at the DR, the switchover to the SPT then occurs. This option only provides the binary option, meaning that the switching to the SPT occurs either when receiving the first multicast packet, or not at all; it is not rate-based. You can enable this option only for specified multicast groups using access lists.

To enable the switchover to the IPv6 SPT, use the following command.

Command	Mode	Description
ipv6 pim spt-threshold	Global	Enables the switchover to IPv6 SPT.
ipv6 pim spt-threshold group-list *WORD*		Enables the switchover to IPv6 SPT for specified multicast groups. WORD: IPv6 access list name (<1-99>)

To disable the switchover to the IPv6 SPT, use the following command.

Command	Mode	Description
no ipv6 pim spt-threshold	Global	Disables the switchover to IPv6 SPT. WORD: IPv6 access list name (<1-99>)
no ipv6 pim spt-threshold group-list *WORD*		

i

The switchover to the IPv6 SPT to deliver multicast traffic is disabled by default.

11.3.7 IPv6 Cisco's Router Interoperability

11.3.7.1 Register Message Checksum

When a multicast source registers with the RP, the DR encapsulates the multicast traffic from the source in the PIM register message, and unicasts it to the RP. The standard PIM protocol specifies that the checksum field in the register message contains the checksum for the entire register message excluding the data portion, the encapsulated multicast traffic.

The Cisco's routers, however, validate the checksum for the whole register message including the data portion, resulting in incompatibility with the standard-based routers. To guarantee compatibility with the Cisco's routers, the system provides the checksum option, which expands the range of the checksum calculation.

To enable the Cisco checksum option, use the following command.

Command	Mode	Description
ipv6 pim cisco-register-checksum	Global	Enables the Cisco checksum option.
ipv6 pim cisco-register-checksum group-list *WORD*		Enables the Cisco checksum option for specified multicast groups. WORD: IPv6 access list name <1-99>

To disable the Cisco checksum option, use the following command.

Command	Mode	Description
no ipv6 pim cisco-register-check-sum	Global	Disables the Cisco checksum option.
no ipv6 pim cisco-register-check-sum group-list *WORD*		

11.3.7.2 Candidate RP Message

Some Cisco's BSRs do not comply with the BSR standards; they do not accept candidate RPs with a group prefix number of zero. You can configure the router to send candidate RP messages with the option for the compatibility with the Cisco's BSR.

To enable the candidate RP message option for the Cisco compatibility, use the following command.

Command	Mode	Description
ipv6 pim crp-cisco-prefix	Global	Enables the candidate RP message option for the Cisco compatibility.
no ipv6 pim crp-cisco-prefix		Disables the candidate RP message option for the Cisco compatibility.

11.3.7.3 Excluding GenID Option

PIM hello messages may contain the generation ID (GenID) in the option fields, which is a random value for the interface on which the hello message is sent. The GenID is regenerated whenever PIM forwarding is started or restarted on the interface. It enables neighbors to quickly detect a router's reboot and thus to synchronize RP-set information and forwarding states by triggering the bootstrap and join/prune messages to the rebooted router. The rebooted router then is able to quickly recover from the reboot.

Some older Cisco's routers cannot recognize the GenID option in the hello messages, so this system provides the exclude-GenID option for the compatibility with the Cisco's routers.

To exclude the GenID option from the PIM hello messages, use the following command.

Command	Mode	Description
ipv6 pim exclude-genid	Interface	Excludes the GenID from the hello messages.
no ipv6 pim exclude-genid		Includes the GenID from the hello messages.

11.3.8 IPv6 PIM Debug

To enable IPv6 PIM-SM debugging, use the following command.

Command	Mode	Description
debug ipv6 pim sparse-mode {**all** | **events** | **nexthop** | **mib** | **mfc** | **nsm** | **state** | **packet** [**in** | **out**]}	Enable	Enables PIM-SM debugging. all: all PIM-SM debugging events: events debugging nexthop: nexthop communications debugging mib: MIBs debugging mfc: MFC add/delete/update debugging nsm: NSM communications debugging state: debugging of state transition on all FSMs packet: incoming and/or outgoing packets debugging
no debug ipv6 pim sparse-mode {**all** | **events** | **nexthop** | **mib** | **mfc** | **nsm** | **state** | **packet** [**in** | **out**]}		Disables PIM-SM debugging.

To enable IPv6 PIM-SM timer debugging, use the following command.

Command	Mode	Description
debug ipv6 pim sparse-mode timer	Enable	Enables PIM-SM timer debugging.
debug ipv6 pim sparse-mode timer assert [**at**]		Enables PIM-SM assert timer debugging.
debug ipv6 pim sparse-mode timer bsr [**bst** | **crp**]		Enables PIM-SM BSR timer debugging. bst: bootstrap debugging timer crp: candidate RP debugging timer
debug ipv6 pim sparse-mode timer hello [**ht** | **nlt** | **tht**]		Enables PIM-SM hello timer debugging. ht: hello timer nlt: neighbor liveness timer tht: triggered hello timer
debug ipv6 pim sparse-mode timer joinprune [**jt** | **et** | **ppt** | **kat** | **ot**]		Enables PIM-SM join/prune timer debugging. jt: join timer et: expiry timer ppt: prune pending timer kat: keep alive timer ot: override timer
debug ipv6 pim sparse-mode timer register [**rst**]		Enables PIM-SM register timer debugging.

To disable IPv6 PIM-SM timer debugging, use the following command.

Command	Mode	Description
no debug ipv6 pim sparse-mode timer	Enable	Disables PIM-SM timer debugging.
no debug ipv6 pim sparse-mode		

Command	Mode	Description
timer assert [**at**]		
no debug ipv6 pim sparse-mode timer bsr [**bst** | **crp**]		
no debug ipv6 pim sparse-mode timer hello [**ht** | **nlt** | **tht**]		
no debug ipv6 pim sparse-mode timer joinprune [**jt** | **et** | **ppt** | **kat** | **ot**]		
no debug ipv6 pim sparse-mode timer register [**rst**]		

11.3.9 Source Specific Multicast (SSM)

Multicast supports both many-to-many and one-to-many models, which are also known as Any Source Multicast (ASM). In this model, receivers may join and leave multicast groups with (*, G) state that indicates any source and group G. Since there is no means to specify the source's information, source discovery such as the RP mechanism in PIM-SM is needed, which is the key feature of ASM. IPv6 multicast address have the prefix ff00::/8.

Source-Specific Multicast (SSM) is especially suit for one-to-many multicast network. In the SSM service model, receivers can receive multicast traffic by subscribing to channel (S, G) that indicates specific IPv6 unicast source S and multicast group address G.

Since SSM assumes that receivers already know the source's information, no further source discovery is provided. Thus, receivers need to know the source's information using an out of band mechanism. The SSM group address range is defined as ff33::/32 ~ ff3f::/21 by default.

11.3.9.1 PIMv6-SSM

PIM Source-Specific Multicast (PIM-SSM) is a subset of PIM-SM. It is much simpler than PIM-SM, because it only considers one-to-many multicast service model. PIM-SSM only use a shortest path tree (SPT) to deliver multicast traffic, so the PIM-SM's complex mechanisms such as RP, BSR, SPT switchover and a shared tree are not necessary any more. PIM-SSM uses the same PIM messages as PIM-SM's for its operation.

If all routers are configured with PIM-SM and MLDv2, only by using the **ipv6 pim ssm** command, PIM-SSM will be enabled. You can also define an additional SSM group other than the default SSM group range.

To enable PIM-SSM, use the following command.

Command	Mode	Description
ipv6 pim ssm default	Global	Enables PIM-SSM for the IPv6 group range.
ipv6 pim ssm range *WORD*		Enables PIM-SSM for a specified group range.: WORD: standard access list (<1-99>)
no ipv6 pim ssm		Disables PIM-SSM.

11.3.9.2 Static SSM Mapping

The purpose of static SSM mapping is to provide SSM service only for MLDv1 and MLDv2 report messages. It means that a multicast host can receive multicast traffic from the specified group and you can set the source which this traffic is expected from. You can specify a source address of multicast server to receive the multicast traffic from specified sources.

If this system receives MLDv1 report message from the host when static SSM mapping is enabled, it handles as if it receives MLDv2 report messages.

Static SSM mapping implemented for the LD3032 has the following restriction, so you must keep it in mind, before configuring static SSM mapping.

IGMP proxy and static SSM mapping cannot be enabled together. It means that SSM mapping cannot be enabled when the system is already configured with upstream or downstream interface with IGMP proxy feature.

Before configuring static SSM mapping, you should first globally enable SSM mapping.

To enable static SSM mapping, use the following command.

Command	Mode	Description
ipv6 mld ssm-map enable	Global	Enables SSM mapping for groups in a configured SSM range.
no ipv6 mld ssm-map enable		Disables SSM mapping for groups.

To specify the Source IPv6 address for static SSM mapping, depending on the specified ACL, use the following command.

Command	Mode	Description
ipv6 mld ssm-map static *WORD X:X::X:X*	Global	Enables a static SSM mapping for the MLDv1 group that matches specified ACL and IPv6 source address. WORD: IPv6 standard access list (<1-99>) X:X::X:X: source address to use for static map group
no ipv6 mld ssm-map static *WORD X:X::X:X*		Disables a static SSM mapping for the MLDv1 group that matches specified ACL and IPv6 source address.

To display information about configured SSM mapping, use the following command.

Command	Mode	Description
show ipv6 mld ssm-map [*X:X::X:X*]	Enable Global	Shows a static SSM mapping information X:X::X:X: IPv6 multicast group address

11.3.10 IPv6 Prefix Lists

Filtering through prefix list processes routing information in specific order by applying policy defined in filter list. It is similar to access list but there are more detail rules as follow.

- Allows all network information if there is no defined policy in prefix list.
- Rejects specified network information unless policy applied to network in defined in prefix list.
- Distinguishes each policy with the assigned number and applies policy which has the lowest number when there is more than one policy applied to one network.

Routers search policy in prefix list in order. For faster operation, user can make quick search list by using **seq** provided from ip prefix-list. In order to view assigned number to policy, use the **show ipv6 prefix-list** command.

Policies configured by user are automatically assigned number. If you do not configure it, you should assign number to each policy by using the command, **ipv6 prefix-list seq** <1-4294967295>.

11.3.10.1 Creating prefix list

To create an entry of IPv6 prefix list, use the following command.

Command	Mode	Description
ipv6 prefix-list *WORD* {**deny** | **permit**} *X:X::X:X/M* **ge** <0-128> [**le** <0-128>]	Global	Creates an entry of IPv6 prefix list. WORD: name of IPv6 prefix list deny: denies access of packet if conditions are matched. permit: permits access of packet if conditions are matched. X:X::X:X/M: IPv6 prefix to be matched (e.g. 3ffe::/16 <network/length>) any: any IPv6 prefix to match. (same as "::0/0 le 128") ge: minimum prefix length to be matched le: maximum prefix length to be matched 0-128: minimum/maximum prefix length
ipv6 prefix-list *WORD* {**deny** | **permit**} *X:X::X:X/M* **le** <0-128> [**ge** <0-128>]		
ipv6 prefix-list *WORD* {**deny** | **permit**} {*X:X::X:X/M* | **any**}		
ipv6 prefix-list *WORD* **description** *LINE*		Writes comments for the prefix list. LINE: prefix list description up to 80 characters

By default, the sequence numbers are automatically generated in increments of 5.

To delete the entries in the prefix list, use the following command.

Command	Mode	Description
no ipv6 prefix-list *WORD*	Global	Deletes the entries of the prefix list. WORD: name of IPv6 prefix list deny: denies access of packet if conditions are matched. permit: permits access of packet if conditions are matched. X:X::X:X/M: IPv6 prefix to be matched (e.g. 3ffe::/16 <network/length>) any: any IPv6 prefix to match. (same as "::0/0
no ipv6 prefix-list *WORD* {**deny** | **permit**} *X:X::X:X/M* **ge** <0-128> [**le** <0-128>]		
no ipv6 prefix-list *WORD* {**deny** | **permit**} *X:X::X:X/M* **le** <0-128> [**ge** <0-128>]		
no ipv6 prefix-list *WORD* {**deny** | **permit**} { *X:X::X:X/M* | **any**}		
no ipv6 prefix-list *WORD* **description**		

Command	Mode	Description
[*LINE*]		le 128") ge: minimum prefix length to be matched le: maximum prefix length to be matched 0-128: minimum/maximum prefix length

11.3.10.2 Creating prefix list policy

Sequence numbers are automatically generated by default. To configure the sequence numbers manually, you can use the **seq** <1-4294967295> argument of the **ipv6 prefix-list** command.

To add policy to prefix list one by one and assign a sequence number to the policy, use the following command.

Command	Mode	Description
ipv6 prefix-list *WORD* **seq** <1-4294967295> {**deny** | **permit**} { *X:X::X:X/M* | **any**}	Global	Creates an entry in an IPv6 prefix list and assigns a sequence number to the entry. WORD: name of IPv6 prefix list 1-4294967295: sequence number of an entry deny: denies access of packet if conditions are matched. permit: permits access of packet if conditions are matched. X:X::X:X/M: IPv6 prefix to be matched (e.g. 3ffe::/16 <network/length>) any: any IPv6 prefix to match. (same as "::0/0 le 128") ge: minimum prefix length to be matched le: maximum prefix length to be matched 0-128: minimum/maximum prefix length
ipv6 prefix-list *WORD* **seq** <1-4294967295> {**deny** | **permit**} *X:X::X:X/M* **ge** <0-128> [**le** <0-128>]		
ipv6 prefix-list *WORD* **seq** <1-4294967295> {**deny** | **permit**} *X:X::X:X/M* **le** <0-128> [**ge** <0-128>]		

You can input **ge** and **le** optionally, and they are used when you configure more than one network. If you do use neither **ge** nor **le**, network range is more clearly configured. When only **ge** attribute is configured, network range is configured from **ge** value, and when only **le** attribute is configured, network range is configured from netmask to **le** value.

To delete the configured policy of prefix list, use the following command.

Command	Mode	Description
no ipv6 prefix-list *WORD* **seq** <1-4294967295> {**deny** | **permit**} { *X:X::X:X/M* | **any**}	Global	Deletes the entry in an IPv6 prefix list and removes a sequence number from the entry.
no ipv6 prefix-list *WORD* **seq** <1-4294967295> {**deny** | **permit**} *X:X::X:X/M* **ge** <0-32> [**le** <0-32>]		
no ipv6 prefix-list *WORD* **seq** <1-4294967295> {**deny** | **permit**} *X:X::X:X/M* **le** <0-32> [**ge** <0-32>]		

With sequenced prefix lists, each prefix list entry is associated with a sequence number. Sequence numbers can be used to insert a prefix list into the middle of an existing list or to delete an existing statement in the list.

To include the sequence numbers in the configuration, use the following command.

Command	Mode	Description
ipv6 prefix-list sequence-number	Global	Includes sequence numbers in non-volatile generation (NVGEN).

To exclude the sequence numbers, use the following command.

Command	Mode	Description
no ipv6 prefix-list sequence-number	Global	Excludes sequence numbers in non-volatile generation (NVGEN).

11.3.10.3 Displaying Prefix List Entries

To display the information about a prefix list or prefix list entries, use the following command.

Command	Mode	Description
show ipv6 prefix-list [*WORD*]	Enable Global	Shows information about all prefix lists.
show ipv6 prefix-list *WORD X:X::X:X/M* [**first-match** | **longer**]		Shows the prefix list entry according to the parameter. longer: all entries of a prefix list that are more specific than the given network and length first-match: the entry of a prefix list that matches the given prefix
show ipv6 prefix-list *WORD* **seq** <1-4294967295>		Shows the prefix list entry with a given sequence number.
show ipv6 prefix-list {**detail** | **summary**} [*WORD*]		Shows a table showing the entries in a prefix list identified by name.

To clear the existing prefix list entries, use the following command.

Command	Mode	Description
clear ipv6 prefix-list [*WORD*]	Enable Global	Clears the counters of all IPv6 prefix lists or an IPv6 prefix with a specified name and prefix.
clear ipv6 prefix-list *WORD X:X::X:X/M*		

11.3.11 Creating IPv6 Prefix Pool

All pool names muse be unique. Once a pool is configured, it cannot be changed. To change the configuration, the pool must be removed and recreated. All prefixes already allocated will also be freed.

To configure a local IPv6 prefix pool, use the following command.

Command	Mode	Description
ipv6 local pool *PREFIX-POOLNAME X:X::X:X/M* <2-64>	Global	Sets a domain name. PREFIX-POOLNAME: prefix-pool name X:X::X:X/M: IPv6 prefix address <2-64>: assugbed length (bits)
show ipv6 local pool		Displays information about any defined IPv6 address pools.

11.4 IPv6 Multicast Interface

To display information about IPv6 multicast interface configuration parameters, use the following command.

Command	Mode	Description
show ipv6 mif channelgroup *IFPORT*	Enable Global	Shows information about IPv6 multicast interface configured. IFPORT: interface port number VLANID: VLAN ID
show ipv6 mif gpon *IFPORT*		
show ipv6 mif tengigabitethernet *IFPORT*		
show ipv6 mif vlan *VLANID*		

12 IP Routing Protocol

12.1 Border Gateway Protocol (BGP)

The Border Gateway Protocol (BGP) is an exterior gateway protocol (EGP) that is used to exchange routing information among routers in different autonomous systems (AS). BGP routing information includes the complete route to each destination. BGP uses the routing information to maintain a database of network reachability information, which it exchanges with other BGP systems. BGP uses the network reachability information to construct a graph of AS connectivity, thus allowing BGP to remove routing loops and en-force policy decisions at the AS level.

Multiprotocol BGP (MBGP) extensions enable BGP to support IPv6. MBGP defines the attributes MP_REACH_NLRI and MP_UNREACH_NLRI, which are used to carry IPv6 reachability information. Network layer reachability information (NLRI) update messages carry IPv6 address prefixes of feasible routes.

BGP allows for policy-based routing. You can use routing policies to choose among multiple paths to a destination and to control the redistribution of routing information.

BGP uses the Transmission Control Protocol (TCP) as its transport protocol, using port 179 for establishing connections. Running over a reliable transport protocol eliminates the need for BGP to implement update fragmentation, retransmission, acknowledgment, and sequencing.

The routing protocol software supports BGP version 4. This version of BGP adds support for classless interdomain routing (CIDR), which eliminates the concept of network classes. Instead of assuming which bits of an address represent the network by looking at the first octet, CIDR allows you to explicitly specify the number of bits in the network address, thus providing a means to decrease the size of the routing tables. BGP version 4 also supports aggregation of routes, including the aggregation of AS paths

An Autonomous System (AS) is a set of routers that are under a single technical administration and normally use a single interior gateway protocol and a common set of metrics to propagate routing information within the set of routers. To other ASs, an AS appears to have a single, coherent interior routing plan and presents a consistent picture of what destinations are reachable through it.

The two most important consequences are the need for interior routing protocols to reach one hop beyond the AS boundary, and for BGP sessions to be fully meshed within an AS. Since the next-hop contains the IP address of a router interface in the next autonomous system, and this IP address is used to perform routing, the interior routing protocol must be able to route to this address. This means that interior routing tables must include entries one hop beyond the AS boundary. When a BGP routing update is received from a neighboring AS, it must be relayed directly to all other BGP speakers in the AS. Do not expect to relay BGP paths from one router, through another, to a third, all within the same AS.

12.1.1 Basic Configuration

12.1.1.1 Configuration Type of BGP

When configuring BGP, you can select BGP configuration type between standard BGP and ZebOS BGP for the LD3032.

The standard BGP is one of the general BGP configuration type, which includes the following restrictions.

- **Manual transmission of community information**
  You should send the community information or message to neighbors directly using the **neighbor** {*A.B.C.D* **|** *WORD*} **send-community** command.
- **No synchronization**
  Standard configuration type does not support a synchronization between IGP and eBGP. In this type, BGP network disables IGP synchronization in BGP by default.
- **No auto-summary**
  Standard configuration type does not support auto summary feature. By default, the system disables the automatic network number summarization.

The ZebOS type requires no specific configuration for sending out BGP community and extended community attributes. ZebOS type is the default for the LD3032.

To select configuration type of the BGP router, use the following command.

Command	Mode	Description
bgp config-type {**standard** | **zebos**}	Global	Sets the BGP configuration type between standard and ZebOS.
no bgp config-type		Deletes the recent BGP configuration type and returns to default.

The community attributes group destinations in a certain community and applies routing decisions according to those communities. On receiving community attributes the router re-announces them to the neighbor. To specify a community attribute to be sent to a neighbor, use the following command.

Command	Mode	Description
neighbor {*A.B.C.D* | *WORD*} **send-community** [**both** | **extended** | **standard**]	Router AF	Specifies that a community attributes are sent to a BGP neighbor. A.B.C.D: BGP neighbor IP address WORD: name of existing peer-group both: standard and extended community attributes (default) extended: extended community attributes standard: standard community attributes
no neighbor {*A.B.C.D* | *WORD*} **send-community** [**both** | **extended** | **standard**]		Specifies that the community attributes are not re-announced to the neighbor.

12.1.1.2 Enabling BGP Routing

Step 1 To define an AS number and open *Router Configuration* mode, use the following command.

Command	Mode	Description
router bgp {<1-65535> | <1.0-XX.YY>}	Global	Assigns AS number to configure BGP routing and opens *Router Configuration* mode. 1-65535: AS number 1.0-XX.YY: ASnumber

Step 2 To specify a network to operate with BGP, use the following command.

Command	Mode	Description
network *A.B.C.D/M*	Router	Adds BGP network to operate. A.B.C.D/M: network address with netmask (<network>/<lengh>) A.B.C.D: network address NETMASK: subnet mask
network *A.B.C.D* **mask** *NETMASK*		

Step 1 To delete a specified network to operate with BGP, use the following command.

Command	Mode	Description
no network *A.B.C.D/M*	Router	Deletes BGP network. A.B.C.D/M: network address with netmask A.B.C.D: network address NETMASK: subnet Mask
no network *A.B.C.D* **mask** *NETMASK*		

Step 2 Go back to *Global Configuration* mode using the **exit** command.

Step 3 To disable BGP routing of the chosen AS, use the following command.

Command	Mode	Description
no router bgp <1-65535>	Global	Deletes assigned AS number to configure BGP routing, enter the AS number. 1-65535: AS number

12.1.1.3 Router ID

In case the loopback interface is configured the router-id is set to the IP address of a loopback interface. If not, the highest IP address is the router-id.

To manually configure a fixed router ID as a BGP router identifier, use the following command.

Command	Mode	Description
bgp router-id *A.B.C.D*	Router	Configures the router identifier. A.B.C.D: router ID

no bgp router-id [*A.B.C.D*]		Deletes a configured router ID.

12.1.1.4 Enabling ASN Capabilities

In case of attempt to change the AS capability from 2 to 4 or 4 to 2, a prompt occurs to remove the VRF configuration because the route distinguisher (RD) configuration whould have been created with the current capability.

To be Not changed while loading from a saved configuration with AS4 capability and BGP VRF configuration, use the following command.

Command	Mode	Description
bgp extended-asn-cap	Global	Configures a BGP router to send 4-octet ASN capabilies.
no bgp extended-asn-cap		Disables a BGP router to send 4-octet ASN capabilities.

12.1.1.5 Registering BGP Neighbor

To assign IP address or peer group name for BGP Neighboring router within specified AS number, use the following command.

Command	Mode	Description
neighbor {*A.B.C.D* | *WORD*} **remote-as** <1-65535>	Router	Configures BGP neighboring router and specify AS number of BGP Neighbors. A.B.C.D: neighbor IP address WORD: peer group name or neighbor tag 1-65535: remote AS Number
no neighbor { *A.B.C.D* | *WORD*} **remote-as** <1-65535>		Deletes the configured BGP Neighbor within specified AS number.

12.1.1.6 IPv4 Unicast Address

By default, a peer or peer group is activated only for IPv4 unicast address family. To manually enable/disable the automatic exchange of IPv4 address family prefixes, use the following command.

Command	Mode	Description
bgp default ipv4-unicast	Router	Sets the IPv4 unicast address family for BGP peering session establishment. (default)
no bgp default ipv4-unicast		Disables default IPv4 unicast address family for peering session establishment.

12.1.1.7 Maximum Path

To set the maximum number of parallel paths for the BGP table, use the following command.

Command	Mode	Description

maximum-paths <1-8>	Router	Forwards packets over multiple paths. <1-8>: the numbers of multipath supported (defualt:1) ibgp: iBGP over multiple paths
maximum-paths ibgp <1-8>		
no maximum-paths [**ibgp**]		Deletes the configured number of parallel paths.

12.1.1.8 BGP Aggregation

To set the BGP option to perform aggregation only when next-hop matches the specified IP address, use the following command.

Command	Mode	Description
bgp aggregate-nexthop-check	Global	Performs the BGP aggregation only when next-hop matches the specified IP address.
no bgp aggregate-nexthop-check		Disables the configured BGP aggregation.

12.1.1.9 BGP Path Selection

To set the RFC1771 compatible path selection mechanism, use the following command.

Command	Mode	Description
bgp rfc1771-path-select	Global	Sets the RFC1771 compatible path selection mechanism.
no bgp rfc1771-path-select		Deletes the configured RFC1771 compatible path selection mechanism.

To configure the strict RFC1771 setting, use the following command.

Command	Mode	Description
bgp rfc1771-strict	Global	Sets the strict RFC1771 setting.
no bgp rfc1771-strict		Deletes the configured strict RFC1771 setting.

12.1.2 IGP Synchronization in BGP

The synchronization in BGP is when a BGP router does not advertise external destinations learned from iBGP unless those destinations are also learned from an IGP. If synchronization is enabled, an iBGP peer does not advertise an external destination learned from another iBGP peer, unless it is also learned from the IGP (OSPF). To enable/disable the IGP synchronization in BGP, use the following command.

Command	Mode	Description
synchronization	Router	Enables the IGP synchronization in BGP.
no synchronization		Disables the IGP synchronization in BGP.

12.1.3 BGP Autonomous System Number Formatting

To change the default display and regular expression match format of Border Gateway Protocol (BGP) 4-byte autonomous system numbers from asplain (decimal values) to dot notation, use the bgp asnotation dot command in router configuration mode.

To change the default display 4-byte autonomous system numbers in the asdot format, use the following command.

Command	Mode	Description
bgp asnotation {dot | dotplus}	Router	Changes the display and regulat expression format of BGP.
no bgp asnotation		Resets the configured.

12.1.4 Enforcing the First AS Path Feature

To configure a router to deny an update received from an external BGP (eBGP) peers that do not list their autonomous system (AS) number at the first of the AS_PATH attribute of the incoming route, use the following command.

Command	Mode	Description
bgp enforce-first-as	Router	Enforces the first AS for eBGP route.
no bgp enforce-first-as		Disables the configured.

12.1.5 External BGP Peering Session Reset

To configure a BGP routing process to immediately reset external BGP peering sessions if the link used to reach these peers goes down, use the following command.

Command	Mode	Description
bgp fast-external-failover	Router	Resets eBGP peering sessions if the link goes down
no bgp fast-external-failover		Disables the configured.

12.1.6 BGP Scan Time

To configure scanning intervals of BGP routers for validation or to decrease import processing time of Virtual Private Network version 4 (VPNv4) routing information, use the following command.

Command	Mode	Description
bgp scan-time <0-60>	Router	Configures background scan interval. (Default: 60, Disables: 0)
no bgp scan-time		Disables the configured.

12.1.7 BGP Update Delay

To set the maximum initial delay period before a BGP speaking networking device sends its first updates, use the following command.

Command	Mode	Description
bgp update-delay <1-3600>	Router	Configures maximum initial delay period. 1-3600: dalay value (seconds)
no bgp update-delay [<1-3600>**]**		Disables the configured.

12.1.8 Network Aggregate

Aggregation combines the characteristics of several different routes and advertises a single route. In the example of 2 routes information of 172.16.0.0/24 and 172.16.1.0/24, the **as-set** parameter creates an aggregate entry advertising the path for a single route of 172.16.0.0/23, consisting of all elements contained in all paths being summarized. Use this feature to reduce the size of path information by listing the AS number only once, even if it was included in multiple paths that were aggregated. And it's useful when aggregation of information results in incomplete path information. Using the **summary-only** parameter transmits the IP prefix only, suppressing the more-specific routes to all neighbors. Using the **as-set** parameter transmits a single AS path information only, one of AS numbers of each path.

To summarize route's information for the transmission, use the following command.

Command	Mode	Description
aggregate-address *A.B.C.D/M* **as-set** [**summary-only**]	Router	Summarizes the information of routes and transmits it to the other routers. A.B.C.D/M: network address summary-only: transmits IP prefix only. as-set: transmits one AS-path information.
aggregate-address *A.B.C.D/M* **summary-only** [**as-set**]		

To delete the route's information of specific network address, use the following command.

Command	Mode	Description
no aggregate-address *A.B.C.D/M* **as-set** [**summary-only**]	Router	Disables the summarization function of routes.
no aggregate-address *A.B.C.D/M* **summary-only** [**as-set**]		

12.1.9 Route Reflector

Route reflectors are a solution for the explosion of iBGP peering within an autonomous system. By route reflection the number of iBGP peers within an AS is reduced. To configure the local router as the route reflector and specify neighbors as its client, use the following command.

Command	Mode	Description
neighbor {*A.B.C.D* | *WORD*} **route-reflector-client**	Router	Configures BGP route reflector and specifies a neighbor as its client. A.B.C.D: BGP neighbor address in IPv4 format WORD: existing peer group name or neighbor tag
no neighbor { *A.B.C.D* | *WORD*} **route-reflector-client**		Deletes the configured BGP route reflector and the specified neighbor as its client.

An AS can have more than one route reflector. One route reflector treats the other route reflector as another BGP speaker.

A cluster includes route reflectors and its clients. Usually, each cluster is identified by the router ID of its single route reflector but to increase redundancy sometimes a cluster may have more than one route reflector. All router reflectors in such a cluster are then identified by a cluster ID.

To configure the cluster ID if the BGP cluster has more than one route reflector, use the following command.

Command	Mode	Description
bgp cluster-id {<1-4294967295> | *A.B.C.D*}	Router	Specifies the cluster ID of this router acting as a route reflector. 1-4294967295: route reflector cluster-id
no cluster-id [*A.B.C.D*]		Removes the cluster ID.

The client-to-client reflection is used to configure routers as route reflectors. Route reflectors are used when all Interior BGP (iBGP) speaker are not fully meshed. To enable/disable the client-to-client reflection, use the following command.

Command	Mode	Description
bgp client-to-client reflection	Router	Enables the client-to-client reflection.
no bgp client-to-client reflection		Disables the client-to-client reflection.

When a router is configured as a route reflector, client-to-client reflection is enabled by default.

To display BGP network information, use the following command.

Command	Mode	Description
show ip bgp	Enable Global	Shows network information.
show ipv6 bgp		Shows IPv6 BGP network information.
show ip prorocols bgp		Shows a current status of bgp prorocol and its information.
show ipv6 protocols bgp		Shows a current status of ipv6 bgp protocol and its information.

12.1.10 Confederation

A confederation allows an AS to be divided into ASs. The AS is given a confederation identifier. External routers view only the whole confederation as one AS. Each AS is fully meshed within itself and is visible internally to the confederation.

To specify a BGP confederation identifier, use the following command.

Command	Mode	Description
bgp confederation identifier <1-65535>	Router	Specifies a BGP confederation identifier. 1-65535: routing domain confederation AS number
no bgp confederation identifier <1-65535>		Deletes a specified BGP confederation identifier.

To define the list of confederation peers, use the following command.

Command	Mode	Description
bgp confederation peers <1-65535> [1-65535]	Router	Configures the Autonomous System (AS) that belongs to the confederation. 1-65535: AS numbers of eBGP peers under same confederation but in a different sub-AS
no bgp confederation peers <1-65535>		Removes an AS form the confederation.

12.1.11 Advanced Configuration

The LD3032 is possibly configured for the additional configurations related BGP.

12.1.11.1 Automatic Summarization of Path

Automatic summarization is new feature to expend the route information up to the class of specified IP address on interface connected directly to BGP router. For example, A class is fundamentally had “/8” as the subnet mask in case IP address assigned 100.1.1.1 in A class. It can generate route information of 100.0.0.0/8.

To enable/disable automatic summarization of the route, use the following command.

Command	Mode	Description
auto-summary	Router	Enables automatic network summarization of a route.
no auto-summary		Disables automatic network summarization of a route.

Please note that, use this feature when you use the basic classes in network.

12.1.11.2 BGP Next-Hop Address Tracking

BGP prefixes are automatically tracked as peering sessions are established. BGP next-hop address tracking feature significantly improves the response time of BGP to next-hop changes for routes installed in the RIB.

To enable/disable BGP next-hop address tracking, use the following command.

Command	Mode	Description
bgp nexthop trigger disable	Router	Enables BGP next-hop address tracking. (default)
bgp nexthop trigger enable		Disables BGP next-hop address tracking.

To set the delay interval between routing table walks for BGP next-hop address tracking, use the following command.

Command	Mode	Description
bgp nexthop trigger delay <2-30>	Router	Configures the delay interval between routing table walks for next-hop address tracking.
no bgp nexthop trigger delay		Deletes the configured delay interval.

12.1.11.3 Local Preference

The local preference indicates the preferred path when there are multiple paths to the same destination. The path having a higher preference is preferred.

To define preference of a particular path, use the following command.

Command	Mode	Description
bgp default local-preference luster-id <1-4294967295>	Router	Defines preference of a particular path and it is sent to all routers and access servers in the local AS. 1-4294967295: local preference value (default: 100)
no bgp default local-preference luster-id [1-4294967295]		Deletes the defined preference and reverts to the default setting.

12.1.11.4 Multi-Exit Discriminator (MED)

During the best-path selection process, the switch compares weight, local preference and AS-path in turn among the similar parameters of BGP routers. Then, the MED is considered when selecting the best path among many alternative paths.

The LD3032, MED comparison is configured only among all paths from the autonomous system. You can configure the comparison of MEDs among all BGP routers within autonomous system. In addition, MED is used when comparing of routes from the neighboring routers placed within different AS.

To find the best route by comparing MED values, use the following command.

Command	Mode	Description
bgp always-compare-med	Router	Configures the router to consider the comparison of MEDs in choosing the best path from among paths.
no bgp always-compare-med		Chooses the best path regardless of the comparison of MEDs.

Meanwhile, when the best-path is selected among the neighbor routers within same Autonomous System, it doesn't compare MED values of them. However, in case the paths have same AS-path information, it does compare MED values. If there are two paths with different AS-path each other, the comparison of MED is unnecessary work. Other parameter's path information can be used to find the best path.

To compare MED values in order to choose the best path among lots of alternative paths included same AS-path value, use the following command.

Command	Mode	Description
bgp deterministic-med	Router	Configures the router to compare MEDs in choosing the best path when paths have same AS-path information.
no bgp deterministic-med		Configures the router not to compare MEDs even if the paths have same AS-path.

i

During the best-path selection process, use the **bgp always-compare-med** command in case of comparing MED values regardless of AS-path. Otherwise, use the **bgp deterministic-med** command if it compares MED values of lots of paths contained same AS-path information.

12.1.11.5 Choosing Best Path

There are a lot of path parameters BGP protocol, which are IP address, AS, MED value and router ID. Even if two paths look same under the condition of IP address, they are actually different when other parameters are compared with each other.

To ignore AS-path for selecting the best path, use the following command.

Command	Mode	Description
bgp bestpath as-path ignore	Router	Ignores the information of AS-path as a factor in the algorithm for choosing the best route.
no bgp bestpath as-path ignore		Considers the information of AS-path as a factor in the algorithm for choosing the best route.

i

If you would like to configure to select the best route by considering AS-path length of Confederation, you should configure the router first to ignore AS-path for choosing the best route using the **bgp bestpath as-path ignore** command before implementing the following command.

To consider AS-path length of Confederation during the best-path selection process, use the following command.

Command	Mode	Description
bgp bestpath compare-confed-aspath	Router	Considers the information of AS-path length of confederation as a factor in the algorithm for choosing the best route.

no bgp bestpath compare-confed-aspath		Ignores AS-path length of confederation as a factor in the algorithm for choosing the best route.

When comparing similar routes from more than 2 peers the BGP router does not consider router ID of the routes. It selects the first received route. The LD3032 uses router ID in the selection process; similar routes are compared and the route with lowest router ID is selected as the best route. Router ID can be manually set by using the following command.

To select the best path by comparing router ID, use the following command. However, the default condition is that BGP receives routes with identical eBGP paths from eBGP peers.

Command	Mode	Description
bgp bestpath compare-routerid	Router	Selects the best path using the router ID for identical eBGP paths.
no bgp bestpath compare-routerid		Disables selecting the best path using the router ID.

The LD3032 is basically configured not to compare MED values of the path information that exchanges between the Confederation Peers. But just in case, it can be configured to compare MED values of the path information that exchanges between Confederation Peers.

To compare MED values on the exchange of path information between Confederation Peers, use the following command.

Command	Mode	Description
bgp bestpath med confed [**missing-as-worst**]	Router	Configures the router to consider the MED in choosing a path from among the paths on the exchange of information between confederation peers.
bgp bestpath med missing-as-worst [**confed**]		

To ignore MED values of paths on the exchange of information between confederation peers, use the following command.

Command	Mode	Description
no bgp bestpath med confed [**missing-as-worst**]	Router	Ignores MEDs of paths on the exchange of their information between confederation peers.
no bgp bestpath med missing-as-worst [**confed**]		

If there are several equal paths, one of them has no MED value. Because this path is considered as “zero” without MED value, it will be chosen the best path. But the path would be the worst one if it has no MED value after **missing-as-worst** is set.

After **missing-as-worst** parameter is configured in the system, the path will be recognized as the worst path without MED value.

12.1.11.6 Graceful Restart

Graceful restart allows a router undergoing a restart to inform its adjacent neighbors and peers of its condition. The restarting router requests a grace period from the neighbor or peer, which can then cooperate with the restarting router. With a graceful restart, the restarting router can still forward traffic during the restart period, and convergence in the network is not disrupted. The restart is not visible to the rest of the network, and the restarting router is not removed from the network topology.

The main benefits of graceful restart are uninterrupted packet forwarding and temporary suppression of all routing protocol updates. Graceful restart thus allows a router to exchange path information with the neighboring router.

To configure graceful restart specifically for BGP, use the following command.

Command	Mode	Description
bgp graceful-restart	Router	Sets to use graceful restart in BGP protocol.
no bgp graceful-restart		Disables the restart time value setting.

Therefore, 2 options of the time can be used to speed up routing convergence by its peer in case that BGP doesn’t come back after a restart.

- **Restart Time**
  It’s the waiting time for the restarting of Neighboring router’s BGP process. Restart time allows BGP process time to restart and implement the internal connection (The session). However, if it’s not working properly, it is considered as the router stops operating.
- **Stalepath Time**
  After BGP process of Neighboring router is restarted, it holds the time until BGP up dates the path information. In case that the information of BGP routes is not updated until the stalepath time, the switch discards this BGP routes information.

To set restart time or stalepath time on Graceful Restarting algorithm, use the following command.

Command	Mode	Description
bgp graceful-restart restart-time <1-3600>	Router	Sets the restart time of Graceful Restart configuration in the unit of second. 1-3600: restart time (default: 120)
bgp graceful-restart stalepath-time <1-3600>		Sets the stalepath-time of Graceful Restart configuration in the unit of second. 1-3600: stalepath time (default: 30)

If you don’t use Graceful Restart feature or want to return the default value for restart time or stalepath time, use the following command.

Command	Mode	Description

no bgp graceful-restart restart-time [<1-3600>]	Router	Restores the default value for restart time.
no bgp graceful-restart stalepath-time [<1-3600>]		Restores the default value for stalepath time.

You can restart configured graceful for BGP, OSPF and RIP in *Privileged EXEC Enable* mode, use the following command.

Command	Mode	Description
restart bgp graceful	Enable	Restarts the configured BGP graceful.
restart ospf graceful grace-period <1-1800>		Restarts the configured OSPF graceful in the unit of second. 1-1800: grace-period (unit: seconds)
restart rip graceful grace-period <1-65535>		Restarts the configured RIP graceful in the unit of second. 1-65535: grace-period (unit: seconds)

12.1.12 Administrative Distance for BGP

An administrative distance is a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. Numerically, an administrative distance is an integer between 1 and 255. In general, the higher the value is, the lower the trust rating is. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored.

To configure the administrative distance for BGP, use the following command.

Command	Mode	Description
distance <1-255> *A.B.C.D/M*	Router	Configures the administrative distance for BGP routes. 1-255: the administrative distance A.B.C.D/M: IP source prefix WORD: name of the access list
distance <1-255> *A.B.C.D/M WORD*		
distance bgp <1-255> <1-255> <1-255>		Specifies the administrative distance for BGP routes. 1-255: the administrative distance for BGP external routes (default: 20) 1-255: the administrative distance for BGP internal routes (default: 200) 1-255: the administrative distance for BGP local routes (default: 200)

To remove an administrative distance, use the following command.

Command	Mode	Description
no distance <1-255> *A.B.C.D/M*	Router	Removes the configured administrative distance.
no distance <1-255> *A.B.C.D/M*		

WORD		
no distance bgp		

12.1.13 IP Address Family

The LD3032 recently supports both unicast and multicast as address-family. Use the following command in choosing either unicast or multicast to enter the *Address-Family Configuratio*n mode allowing configuration of address-family specific parameters.

Use the following command in order to enable address family routing process, which open you in *Address-Family Configuration* mode.

Command	Mode	Description
address-family ipv4 [**multicast** | **unicast**]	Router	Opens the *Address-Family Configuration* mode to configure sessions for IPv4 prefixes.
address-family vpnv4 [**multicast** | **unicast**]		Opens the *Address-Family Configuration* mode to configure sessions for VPNv4 prefixes.
exit-address-family	Address-Family	Exits to *Router Configuration* mode.

12.1.14 Route Flap Dampening

The route dampening minimizes the instability caused by route flapping. A penalty is added for every flap in a flapping route. As soon as the total penalty reaches the “suppress” limit the advertisement of the route is suppressed. This penalty is decayed according to the configured “half time” value. Once the penalty is lower than the “reuse” limit, the route advertisement is un-suppressed.

To enable the route-flap dampening, use the following command.

Command	Mode	Description
bgp dampening	Router AF	Enables the route-flap dampening.

To configure BGP dampening parameters, use the following command.

Command	Mode	Description
bgp dampening <1-45>	Router AF	Configures BGP dampening parameters.
bgp dampening <1-45> <1-20000> <1-255>		1-45: reachability half-life time in minute (default: 15 minutes) 1-20000: reuse limit value (default: 750) 1-20000: suppress limit value (default: 2000) 1-255: max-suppress-time (default: 60 minutes) 1-45: un-reachability half-life time for penalty
bgp dampening <1-45> <1-20000> <1-20000> <1-255> <1-45>		
bgp dampening route-map *WORD*		Specifies the route-map criteria for dampening. WORD: route-map name

When the penalty for a suppressed route decays below the “reuse value”, the routes become unsuppressed. When the penalty for a route exceeds the “suppress value”, the route is suppressed.

i

The “reachability half-life time” is for the penalty to decrease to one-half of its current value. The “max-suppress-time is the maximum time that a dampened route is suppressed. This value is 4 times the half-life time.

To delete the configured BGP dampening parameters, use the following command.

Command	Mode	Description
no bgp dampening <1-45>	Router AF	Deletes the configured BGP dampening parameters.
no bgp dampening <1-45> <1-20000> <1-255>		
no bgp dampening <1-45> <1-20000> <1-20000> <1-255> <1-45>		
no bgp dampening route-map [*WORD*]		

To display detailed information about dampening, use the following command.

Command	Mode	Description
show ip bgp dampening dampened-paths	Enable Global	Shows paths suppressed due to dampening.
show ip bgp dampening flap-statistics		Shows flap statistics of routes
show ip bgp dampening parameters		Shows details of configured dampening parameters.

To reset all dampened BGP routes, use the following command.

Command	Mode	Description
clear ip bgp dampening	Enable Global	Resets all dampened BGP routes.
clear ip bgp dampening {*A.B.C.D* | *A.B.C.D/M*}		

To clear the flap count and history duration for all the prefixes under the specified address family, use the following command.

Command	Mode	Description
clear ip bgp flap-statistics	Enable Global	Clears the collected BGP flap statistics.
clear ip bgp flap-statistics {*A.B.C.D* | *A.B.C.D/M*}		

12.1.15 BGP Session Reset

When you manage BGP network, you can use the command to reset the session for all peers occasionally. Because the internal connections are re-established newly after resetting, the route information of the connected routers is restored by default.

You can reset the session in specified condition. The LD3032 is available with several parameters to reset the BGP connections.

12.1.15.1 Session Reset of All Peers

To reset the sessions with all BGP peers, use the following command.

Command	Mode	Description
clear bgp *	Enable Global	Resets all sessions with BGP peer groups.
clear ip bgp *	Enable Global Bridge	
clear ipv6 bgp *		

When the route parameters restore to the default value by reset command, you can configure the specific parameters for its initialization. If you would like to reset/clear the outgoing advertised routes only, you should use **out** parameter. Otherwise, if you'd like to reset/clear the incoming advertised routes only, you should use **in** parameter.

Meanwhile, if **prefix-filter** is configured with **in** option, ORF (Outbound Route Filtering) and incoming route can be reset. By using **soft** option, you can configure the switch to update route information only when the session is still connected.

To reset the sessions of all peers and initialize the details of route configurations, use the following command.

Command	Mode	Description
clear bgp * in [**prefix-filter**]	Enable Global	Resets the session of specific group under * condition. in: clears incoming advertised routes. prefix-filter: pushes out prefix-list ORF and does inbound soft reconfiguration. *: the conditional option (peer group name or AS number or IP address) WORD: view name
clear bgp * in [**prefix-filter**]		
clear bgp view *WORD* *** in**		
clear ipv6 bgp * in [**prefix-filter**]		
clear ip bgp * {**unicast** | **multicast**} **in** [**prefix-filter**]		
clear bgp out		Resets the session of specific group under * condition. *: the conditional option (peer group name or AS number or IP address) out: clears outgoing advertised routes. unicast | multicast: address family modifier WORD: view name
clear bgp view *WORD* *** out**		
clear ip bgp out		
clear ipv6 bgp out		
clear ip bgp * {**unicast** | **multicast**} **out**		
clear bgp * soft [**in** | **out**]		Updates the route information only while the session is

clear ip bgp * soft [**in** | **out**]		possible for specific group under * condition. Apply the route either incoming or outgoing routes. *: the conditional option (peer group name or AS number or IP address)
clear ipv6 bgp * soft [**in** | **out**]		
clear ip bgp * {**unicast** | **multicast**} **soft** [**in** | **out**]		

12.1.15.2 Session Reset of Peers within Particular AS

To reset the session with all neighbor router which are connected to a particular AC, use the following command.

Command	Mode	Description
clear bgp <1-4294967295>	Enable Global	Resets the session with all members of neighbor routers which are configured a particular AC number.
clear ip bgp <1-4294967295>	Enable Global Bridge	
clear ipv6 bgp <1-4294967295> **soft**		

See Section 12.1.15.1 when you configure the detail parameters.

To reset the sessions of BGP neighboring routers which are belong to specific AS number and initialize the details of route configurations, use the following command.

and initialize the details of route configurations, use the following command.

Command	Mode	Description
clear bgp <1-4294967295> **in** [**prefix-filter**]	Enable Global	Resets the session of BGP neighboring routers which are configured a particular AC number. in: clears incoming advertised routes. prefix-filter: pushes out prefix-list ORF and does inbound soft reconfiguration. 1-65535: AS number
clear ip bgp <1-4294967295> **in** [**prefix-filter**]		
clear ipv6 bgp <1-4294967295> **in** [**prefix-filter**]		
clear ip bgp <1-4294967295> {**unicast** | **multicast**} **in** [**prefix-filter**]		
clear bgp <1-4294967295> **out**		Resets the session of BGP neighboring routers which are configured a particular AC number. 1-65535: AS number out: clears outgoing advertised routes. unicast | multicast: address family modifier
clear ip bgp <1-4294967295> **out**		
clear ipv6 bgp <1-4294967295> **out**		
clear ip bgp <1-4294967295> {**unicast** | **multicast**} **out**		
clear bgp <1-4294967295> **soft** [**in** | **out**]	Global	Updates the route information only while the session is possible of BGP neighboring routers which are configured a particular AC number. Apply the route either incoming or outgoing routes. 1-65535: AS number
clear ip bgp <1-4294967295> **soft** [**in** | **out**]		
clear ipv6 bgp <1-4294967295>		

soft [**in** | **out**]		
clear ip bgp <1-4294967295> {**unicast** | **multicast**} **soft** [**in** | **out**]		

12.1.15.3 Session Reset of Specific Route

To reset the sessions of BGP neighboring router with specified IP address, use the following command.

Command	Mode	Description
clear bgp {*A.B.C.D* | *X:X::X:X* }	Enable Global	Resets the sessions of BGP neighboring router with specified IP address.
clear ip bgp *A.B.C.D*	Enable Global Bridge	
clear ipv6 bgp *X:X::X:X*}		

See Section 12.1.15.1when you configure the detail parameters.

To reset the sessions of BGP neighboring router with specified IP address and initialize the details of route configurations, use the following command.

Command	Mode	Description
clear bgp {*A.B.C.D* | *X:X::X:X* } **in** [**prefix-filter**]	Enable Global	Resets the session of BGP neighboring router contained specified IP address. in: clears incoming advertised routes. prefix-filter: pushes out prefix-list ORF and does inbound soft reconfiguration. A.B.C.D: route IP address
clear ip bgp *A.B.C.D* **in** [**prefix-filter**]		
clear ipv6 bgp *X:X::X:X* **in** [**prefix-filter**]		
clear ip bgp *A.B.C.D* {**unicast** | **multicast**} **in** [**prefix-filter**]		
clear bgp {*A.B.C.D* | *X:X::X:X* } **out**		Resets the session of BGP neighboring router with specified IP address. A.B.C.D: route IP address out: clears outgoing advertised routes. unicast | multicast: address family modifier
clear ip bgp *A.B.C.D* **out**		
clear ipv6 bgp *X:X::X:X* **out**		
clear ip bgp *A.B.C.D* {**unicast** | **multicast**} **out**		
clear bgp {*A.B.C.D* | *X:X::X:X* } **soft** [**in** | **out**]		Updates the route information only while the session is possible of BGP neighboring router with specified IP address. Apply the route either incoming or outgoing routes. A.B.C.D: route IP address
clear ip bgp *A.B.C.D* **soft** [**in** | **out**]		
clear ipv6 bgp *X:X::X:X* **soft** [**in** | **out**]		
clear ip bgp *A.B.C.D* {**unicast** |		

multicast} **soft** [**in** | **out**]		

12.1.15.4 Session Reset of External Peer

You can reset the session of BGP router connected to external AS. To reset a BGP connection for all external peers, use the following command.

Command	Mode	Description
clear bgp external	Enable Global	Resets the session of all external AS peers.
clear ip bgp external	Enable Global Bridge	
clear ipv6 bgp external		

See Section 12.1.15.1 when you configure the detail parameters.

To reset the sessions of BGP router connected to external AS and initialize the details of route configurations, use the following command.

Command	Mode	Description
clear bgp external in [**prefix-filter**]	Enable Global	Resets the session of BGP router connected to external AS. in: clears incoming advertised routes. prefix-filter: pushes out prefix-list ORF and does inbound soft reconfiguration. external: clears all external peers.
clear ip bgp external in [**prefix-filter**]		
clear ipv6 bgp external in prefix-filter		
clear ip bgp external {**unicast** | **multicast**} **in** [**prefix-filter**]		
clear bgp external out		Resets the session of BGP router connected to external AS. external: clears all external peers. out: clears outgoing advertised routes. unicast | multicast : address family modifier
clear ip bgp external out		
clear ipv6 bgp external *WORD* **out**		
clear ip bgp external {**unicast** | **multicast**} **out**		
clear bgp external soft [**in** | **out**]		Updates the route information only while the session is possible of BGP router connected to external AS. Apply the route either incoming or outgoing routes. external: clears all external peers.
clear ip bgp external soft [**in** | **out**]		
clear ipv6 bgp external soft [**in** | **out**]		
clear ip bgp external {**unicast** | **multicast**} **soft** [**in** | **out**]		

12.1.15.5 Session Reset of Peer Group

To reset the session for all members of a peer group, use the following command.

Command	Mode	Description
clear bgp peer-group *GROUP*	Enable Global	To reset the session for all configured routers of specified peer group. GROUP: peer group name
clear ip bgp peer-group *GROUP*	Enable Global Bridge	
clear ipv6 bgp peer-group *GROUP*		

See Section 12.1.15.1 when you configure the detail parameters.

To reset the sessions of BGP routers which are members of specified peer group and initialize the details of route configurations, use the following command.

Command	Mode	Description
clear ip bgp peer-group *GROUP* **in** [**prefix-filter**]	Global	Resets the session for all members of specified peer group. in: clears incoming advertised routes. prefix-filter: pushes out prefix-list ORF and does inbound soft reconfiguration. GROUP: peer group name
clear ip bgp peer-group *GROUP* {**unicast** | **multicast**} **in** [**prefix-filter**]		
clear ip bgp peer-group *GROUP* **out**		Resets the session for all members of specified peer group. GROUP: peer group name out: clears outgoing advertised routes. unicast | multicast: address family modifier
clear ip bgp peer-group *GROUP* {**unicast** | **multicast**} **out**		
clear ip bgp peer-group *GROUP* **soft** [**in** | **out**]		Resets the route information only while the session is possible for all members of specified peer group. Apply the route either incoming or outgoing routes. GROUP: peer group name
clear ip bgp peer-group *GROUP* {**unicast** | **multicast**} **soft** [**in** | **out**]		

12.1.16 BGP AS-path Access List

Autonomous System (AS) is one of the essential element of BGP. AS framework provides distance vector metric and loop detection to BGP. An AS path access list can be spcified on both inbound and outbound BGP routes.

To define a new Autonomous System (AS) path access-list, use the following command.

Command	Mode	Description
ip as-path access-list *WORD* {**deny** | **permit** } *LINE*	Global	Specifies a BGP AS path access list to be used in filtering. WORD: regular expression AS path access list name deny: specify packets to reject permit: specify packets to forward

		LINE: a regular expression to match the BGP AS paths
no ip as-path access-list *WORD* [{**deny** | **permit** } *LINE*]		Deletes the configured BGP AS path access list.

To display the defined BGP Autonomous System (AS) path access list, use the following command.

Command	Mode	Description
show ip as-path-access-list	Enable Global Bridge	Shows information about BGP AS path access list.
show ip as-path-access-list *NAME*		

An AS path access list must be done within a route map and then referred to within a protocol. And AS path access lists can be used in match conditions in route-maps to match on access lists attached to BGP routes.

12.1.17 Configuring BGP Neighbor

12.1.17.1 Default Route

The LD3032 can be configured that particular neighboring BGP routers or peer group is assigned by default route as 0.0.0.0. Then, neighboring router or member of peer group is able to receive the information of default route from the designated routers.

The following command allows neighboring BGP routers or Peer Group to transmit 0.0.0.0 as the default route.

To generate the default route to BGP neighbor or peer group, use the following command.

Command	Mode	Description
neighbor {*A.B.C.D* | *WORD*} **default-originate** [**route-map** *NAME*]	Router	Generates the default route to BGP Neighbor. NEIGHBOR-IP: neighbor IP address WORD: peer group name or neighbor tag 1-65535: remote AS number NAME: route map name
no neighbor {*A.B.C.D* | *WORD*} **default-originate** [**route-map** *NAME*]		Removes the default route for BGP Neighbor or peer group.

12.1.17.2 Peer Group

As the number of external BGP groups increases, the ability to support a large number of BGP sessions may become a scaling issue. In principle all members of BGP routers within a single AS must connect to other neighboring routers. The preferred way to configure a large number of BGP neighbors is to configure a few groups consisting of multiple neighbors per group. Supporting fewer BGP groups generally scales better than supporting a large number of BGP groups. This becomes more evident in the case of dozens of BGP neighboring groups when compared with a few BGP groups with multiple peers in each group. If the routers belong to same group, they can be applied by same configuration. This group is called as Peer Group.

After peer relationships have been established, the BGP peers exchange update message to advertise network reachability information. You can arrange BGP routers into groups of peers.

To create a BGP Peer Group, use the following command.

Command	Mode	Description
neighbor *NAME* **peer-group**	Router	Create a BGP peer group. NAME: peer group name
no neighbor *NAME* **peer-group**		Delete the BGP peer group created before.

To specify neighbor to the created peer group, use the following command.

Command	Mode	Description
neighbor *A.B.C.D* **peer-group** *NAME*	Router	Includes BGP neighbor to specified peer group using IP address. A.B.C.D: neighbor IP address NAME: peer group name
no neighbor *A.B.C.D* **peer-group** *NAME*		Removes BGP neighbor from the specified Peer Group.

12.1.17.3 Route Map

You can apply the specific route map on neighboring router that the exchange route information between routers or blocking the IP address range is configured on route map.

To make BGP Neighbor router exchange the routing information using Route-map, use the following command.

Command	Mode	Description
neighbor { *A.B.C.D* | *WORD*} **route-map** *NAME* {**in** | **out**}	Router	Applies a route map to incoming or outgoing routes on neighboring router or peer group and exchange the route information. A.B.C.D : neighbor IP address WORD: peer group name NAME: route map name
no neighbor { *A.B.C.D* | *WORD*} **route-map** *NAME* {**in** | **out**}		Removes the connection with configured route-map.

12.1.17.4 Force Shutdown

The LD3032 supports the feature to force to shutdown any active session for the specified BGP router or peer group and to delete the routing data between them. It shutdowns all connections and deletes the received path information from neighboring router or peer group.

To disable the exchange information with a specified router or peer group, use the following command.

Command	Mode	Description
neighbor {*A.B.C.D* | *WORD*} **shutdown**	Router	Shutdowns any active session for the specified router or peer group and delete all related routing data. A.B.C.D: neighbor IP address WORD: peer group name or neighbor tag
no neighbor {*A.B.C.D* | *WORD*} **shutdown**		Enables the sessions with a previously existing neighbor or peer group that had been disabled.

12.1.17.5 Changing the Nexthop Information

When you use the command to change the nexthop information that is sent to the iBGP peer, the nexthop information is set the IP address of the interface used to communicate with the neighbor. To configure the router as the next hop for a BGP-speaking router or peer group, use the following command.

Command	Mode	Description
neighbor {*A.B.C.D* | *WORD*} **next-hop-self**	Router AF	Configures the router as the next hop for a BGP-speaking router or peer group. A.B.C.D: BGP neighbor IP address WORD: peer group name or neighbor tag
no neighbor {*A.B.C.D* | *WORD*} **next-hop-self**		Deletes the configured router as the next hop for a BGP-speaking router or peer group.

12.1.17.6 Neighbor Password

To enable/disable MD5 authentication on a TCP connection between BGP neighbors, use the following command.

Command	Mode	Description
neighbor {*A.B.C.D* | *WORD*} **password** *PASSWORD*	Router	Sets password to the neighbor. A.B.C.D: BGP neighbor IP address WORD: neighbor tag PASSWORD: password 0-7: encryption type LINE: alphanumeric string of characters
neighbor {*A.B.C.D* | *WORD*} **password** <0-7> *LINE*		
no neighbor {*A.B.C.D* | *WORD*} **password** [*PASSWORD*]		Deletes a configured password.
no neighbor {*A.B.C.D* | *WORD*} **password** [<0-7> *LINE*]		

12.1.17.7 Neighbor Description

A specific neighbor's description is useful for an ISP that has multiple neighbor relationships. To associate a description with a neighbor, use the following command.

Command	Mode	Description
neighbor {*A.B.C.D* | *WORD*} **description** *LINE*	Router AF	Specifies a description on a neighbor. A.B.C.D: BGP neighbor IP address WORD: neighbor tag LINE: 80-character text that describes the neighbor
no neighbor {*A.B.C.D* | *WORD*} **description** [*LINE*]		Deletes a specified description.

12.1.17.8 Source of Routing Updates

The loopback interface is that is most commonly used with the following command. The use of loopback interface eliminates a dependency and BGP doest not have to rely on the availability of a particular interface for making TCP connection. It is used in conjunction with any specified interface on the router

To allow internal BGP sessions to use any operation interface for TCP connection, use the following command.

Command	Mode	Description
neighbor {*A.B.C.D* | *WORD*} **update-source** *INTERFACE*	Router	Allows internal BGP sessions to use any operation interface for TCP connections. A.B.C.D: BGP neighbor IP address WORD: neighbor tag INTERFACE: loopback interface name or IP address
no neighbor {*A.B.C.D* | *WORD*} **update-source**		Restores the interface assignment to the closest interface.

12.1.17.9 Updates for Inbound Soft Reconfiguration

Soft-reconfiguration may be used in lieu of BGP route refresh capability. The LD3032 can store updates for inbound soft reconfiguration. When a soft reset (inbound) is done on this neighbor, the locally stored routes are reprocessed according to the inbound policy.

To enable/disable local storage of all the received routes and their attributes, use the following command.

Command	Mode	Description
neighbor {*A.B.C.D* | *WORD*} **soft-reconfiguration inbound**	Router	Enables the local storage of updates. A.B.C.D: BGP neighbor IP address WORD: neighbor tag
no neighbor {*A.B.C.D* | *WORD*} **soft-reconfiguration inbound**		Disables the local storage of updates.

12.1.18 BGP Community List

The community-lists specify BGP community attributes. The community attribute is used for implementing policy routing. It is an optional, transitive attribute and facilitates transfer of local policies through different autonomous systems (ASs). It includes community values that are 32 bits long.

There are two kinds of community-lists: the expanded and standard. The *standard community-list* defines the community attributes in a specified format and not with regular expressions. The *expanded community-list* defines the community attributes with regular expressions.

Use the ip **community-list standard** command to add a standard community-list entry. The standard community-list is compiled into binary format and is directly compared with the BGP communities attribute in the BGP updates. The comparison is faster than the expanded community-list. Any community value that does not match the standard community value is automatically treated as expanded.

To add a community list entry, use the following command.

Command	Mode	Description
ip community-list <1-99> {**deny | permit**} [*LINE*]	Global	Specifies a deny or permit statement of the community-list. 1-99: standard community list numbers 100-199: expanded community list numbers WORD: community list name deny: specify community to reject. permit: specify community to accept. LINE: Community number in aa:nn format or internet | local-AS | no-advertise | no-export AA:NN: the valid value for the community number (format: 32 bit communities value) internet: specifies routes not to be advertised to the internet local-AS: specifies routes not to be advertised to external BGP peers no-advertise: specifies routes not to be advertised to other BGP peers no-export: specifies routes not to be advertised outside of Autonomous System boundary
ip community-list <100-199> {**deny | permit**} [*LINE*]		
ip community-list *WORD* {**deny | permit**} [*LINE*]		
ip community-list standard *WORD* {**deny | permit**} [*LINE*]		Creates a standard community list.
ip community-list expanded *WORD* {**deny | permit**} *LINE*		Creates a expanded community list.

Add entries to the list by repeating the command for different IP addresses.

To delete an entry in the community list, use the following command.

Command	Mode	Description

no ip community-list {<1-99> | <100-199> | *WORD*}	Global	Deletes an entry of the community-list.
no ip community-list {<1-99> | <100-199> | *WORD*} {**deny | permit**} *LINE*		
no ip community-list standard *WORD* [{**deny | permit**} *LINE*]		
no ip community-list expanded *WORD* [{**deny | permit**} *LINE*]		

To display the entry information of the community list, use the following command.

Command	Mode	Description
show ip community-list	Enable Global Bridge	Shows an entry of the community-list.
show ip community-list {<1-99> | <100-199> | *WORD*}		

To create an extended community-list and control access to it, use the following command.

Command	Mode	Description
ip extcommunity-list <1-99> {**deny | permit**}	Global	Specifies a deny or permit statement of the extended community-list. 1-99: standard extended community list number deny: specify extended community to reject. permit: specify extended community to accept. LINE: extended community attribute in 'rt aa:nn_or_IPaddr:nn' OR 'soo aa:nn_or_IPaddr:nn' format
ip extcommunity-list <1-99> {**deny | permit**} *LINE*		
ip extcommunity-list <100-199> {**deny | permit**} *LINE*		Specifies a deny or permit statement of the extended community-list. 100-199: expanded extended community list number LINE: An ordered list as a regular-expression
ip extcommunity-list standard *WORD* {**deny | permit**} [*LINE*]		Creates a standard extcommunity-list. WORD: extended community list name
ip extcommunity-list expanded *WORD* {**deny | permit**} *LINE*		Creates a expanded extcommunity-list. WORD: extended community list name

To delete an entry in the extended community list, use the following command.

Command	Mode	Description
no ip extcommunity-list {<1-99> | <100-199>}	Global	Deletes an entry of the extended community-list.
no ip extcommunity-list {<1-99> | <100-199>} {**deny | permit**} *LINE*		
no ip extcommunity-list stand-		

ard *WORD* [{**deny | permit**} *LINE*]		
no ip extcommunity-list expanded *WORD* [{**deny | permit**} *LINE*]		

To display the entry information of the extended community list, use the following command.

Command	Mode	Description
show ip extcommunity-list	Enable Global Bridge	Shows an entry of the extended community-list.
show ip extcommunity-list {<1-99> | <100-199> | *WORD*}		

Route tagging with communities is always done with a route-map. You can attach up to 32 communities to a single route with one route-map set statement. And community-lists can be used in match conditions in route-maps to match on communities attached to BGP routes.

To display the BGP routes matching the communities, use the following command.

Command	Mode	Description
show ip bgp community-list *WORD* [**exact-match**]	Enable Global Bridge	Shows all networks that are permitted by the community-list. WORD: community-list name exact-match: routes that have exactly the same specified communities unicast: IPv4 unicast address family multicast: IPv4 multicast address family
show ip bgp {**unicast** | **multicast**} **community-list** *WORD* [**exact-match**]		
show [**ip**] **bgp community**		Shows all routes in a BGP table that all the specified communities attached.
show [**ip**] **bgp community** {*AA:NN* | **internet** | **local-AS** | **no-advertise** | **no-export**} [**exact-match**]		
show [**ip**] **bgp** {**unicast** | **multicast**} **community**		
show [**ip**] **bgp** {**unicast** | **multicast**} **community** {*AA:NN* | **internet** | **local-AS** | **no-advertise** | **no-export**} [**exact-match**]		
show ip bgp community-info		Shows the list of all bgp communities' information

12.1.19 BGP Timers

BGP keepalive timer indicates that the frequency with which the keepalive messages are sent to the neighbors. And holdtime is the interval which the neighbor is considered dead if keepalive messages are not received.

To set the BGP keepalive and holdtime timer values for all the neighbors, use the following command.

Command	Mode	Description
timers bgp <0-65535> <0-65535>	Router	Configures the period of finding in the unit of second. 0-65535: keepalive timer value (default: 60 seconds) 0-65535: holdtime value (default: 180 seconds)

To reset the values, use the following command.

Command	Mode	Description
no timers bgp [0-65535] [0-65535]	Router	Resets timers to default value.

12.1.20 BGP Network

To specify a backdoor route to a BGP-learned prefix that provides better information about the network, use the following command.

Command	Mode	Description
network *A.B.C.D/M* **backdoor**	Router	Specifies a backdoor route to a BGP-learnd prefix. A.B.C.D/M: IP prefix <network>/<length>
no network *A.B.C.D/M*		Disables the configured.
no network *A.B.C.D/M* **backdoor**		

To specify the networks to be advertised by the BGP and multiprotocol BGP routing processes, use the following command.

Command	Mode	Description
network *A.B.C.D/M* **route-map** *WORD* [**backdoor**]	Router	Specifies the networks backdoor route to a BGP-learnd prefix. A.B.C.D/M: IP prefix <network>/<length> WORD: route map name
no network *A.B.C.D/M* **route-map** *WORD* [**backdoor**]		Disables the configured.

12.1.21 External Routes to BGP Network

The redistribution is used by routing protocols to advertise routes that are learned by some other means, such as by another routing protocol or by static routes. Since all internal routes are dumped into BGP, careful filtering should be applied to make sure that only routes to be advertised reach the internet, not everything. To inject routes from on routing process into another, use the following command.

Command	Mode	Description
redistribute { **connected** | **kernel** | **static** | **rip** | **ospf**}	Router	Configures the external route transmission.

redistribute { **connected** | **kernel** | **static** | **rip** | **ospf**} **route-map** *MAP-NAME*		

To delete a configured external route transmission, use the following command.

Command	Mode	Description
no redistribute { **connected** | **kernel** | **static** | **rip** | **ospf**}	Router	Deletes a configured external route transmission.
no redistribute { **connected** | **kernel** | **static** | **rip** | **ospf**} **route-map** [*MAP-NAME*]		

12.1.22 BGP Monitoring and Management

12.1.22.1 Displaying OSPF Protocol Information

BGP network information or configurations provided can be used to determine resource utilization and enable BGP troubleshooting functions to solve network problems.

To see the configurations involved in BGP routing protocol, use the following command.

Command	Mode	Description
show ip bgp summary	Enable Global	Shows the summarized network status of BGP neighboring routers.
show ip bgp [**ipv4** {**unicast** | **multicast**}] **summary**		

12.1.22.2 BGP Neighbor

To show detailed information on BGP neighbor router's session, use the following command.

Command	Mode	Description
show ip bgp neighbors	Enable Global	Shows general information on BGP neighbor connections of all neighboring routers.
show ip bgp ipv4 {**unicast** | **multicast**} **neighbors**		
show ip bgp neighbors *NEIGHBOR-IP*		Shows information of a specified neighbor router by its IP address. NEIGHBOR-IP: neighbor router' s IP address
show ip bgp ipv4 {**unicast** | **multicast**} **neighbors** *NEIGHBOR-IP*		
show ip bgp neighbors *NEIGHBOR-IP* **advertised-routes**		The **advertised-routes** option displays all the routes the router has advertised to the neighbor.
show ip bgp ipv4 {**unicast** | **multicast**} **neighbors** *NEIGHBOR-IP* **advertised-routes**		
show ip bgp neighbors *NEIGHBOR-IP* **received prefix-filter**		Displays all received routes from neighbor router, both accepted and rejected.
show ip bgp ipv4 {**unicast** | **multicast**} **neighbors** *NEIGHBOR-IP* **received prefix-filter**		
show ip bgp neighbors *NEIGHBOR-IP* **re-**		The **received-routes** option displays all

ceived-routes		received routes (both accepted and rejected) from the specified neighbor. To implement this feature, BGP soft reconfiguration is set.
show ip bgp ipv4 {**unicast** | **multicast**} **neighbors** *NEIGHBOR-IP* **received-routes**		
show ip bgp neighbors *NEIGHBOR-IP* **routes**		The **routes** option displays the available routes only that are received and accepted.
show ip bgp ipv4 {**unicast** | **multicast**} **neighbors** *NEIGHBOR-IP* **routes**		

12.1.22.3 Logging Neighbor Changes

To enable/disable logging of status change messages without turning on BGP debugging, use the following command.

Command	Mode	Description
bgp log-neighbor-changes	Router	Enables logging of BGP neighbor status changes
no bgp log-neighbor-changes		Disables logging of BGP neighbor status changes

The LD3032 logs the following events using the above command.

- BGP notification received
- Erroneous BGP update received
- User reset request
- Peer time-out / Peer closing down the session / Member added to peer group
- Interface flap
- Router ID changed
- Neighbor deleted
- Remote AS changed
- Administrative shutdown

12.1.22.4 Checking the BGP Network Route

To check that the BGP network route is reachable through IGP, use the following command.

Command	Mode	Description
bgp network import-check	Router	Checks BGP network route exists in IGP.
no bgp network import-check		Disables the function.

12.1.23 BGP Filtering through Prefix Lists

Prefix lists were introduced in BGP because they are efficient forms of filtering. Because they search on the prefix of the address as defined by the administrator, the lookup is very fast. This is particularly important in the potentially huge routing tables that can be generated in BGP networks. When you restrict BGP route, prefix list is preferred than access list because of the following reason:

- saves time to search and apply in case of massive filter lists
- unlimited registration in filter lists
- easy to use

Before applying prefix list, user should configure prefix list. User can assign a sequence number to each policy registered in prefix list.

Traffic filtering operation through prefix lists

Filtering through prefix list processes routing information in specific order by applying policy defined in filter list. It is similar to access list but there are more detail rules as follow.

- Allows all network information if there is no defined policy in prefix list.
- Rejects specified network information unless policy applied to network in defined in prefix list.
- Distinguishes each policy with the assigned number and applies policy which has the lowest number when there is more than one policy applied to one network.

Routers search policy in prefix list in order. For faster operation, user can make quick search list by using **seq** provided from ip prefix-list. In order to view assigned number to policy, use the **show ip prefix-list** command.

Policies configured by user are automatically assigned number. If you do not configure it, you should assign number to each policy by using the command, **ip prefix-list seq** <1-4294967295>.

12.1.23.1 Creating prefix list

To create an entry of IPv4 prefix list, use the following command.

Command	Mode	Description
ip prefix-list *WORD* {**deny** | **permit**} *A.B.C.D/M* **ge** <0-32> [**le** <0-32>]	Global	Creates an entry of IPv4 prefix list. WORD: name of IP prefix list deny: denies access of packet if conditions are matched. permit: permits access of packet if conditions are matched. A.B.C.D/M: IPv4 prefix to be matched (e.g. 35.0.0.0/8) any: any IPv4 prefix to match. (same as 0.0.0.0/0 le 32) ge: minimum prefix length to be matched le: maximum prefix length to be matched 0-32: minimum/maximum prefix length
ip prefix-list *WORD* {**deny** | **permit**} *A.B.C.D/M* **le** <0-32> [**ge** <0-32>]		
ip prefix-list *WORD* {**deny** | **permit**} {*A.B.C.D/M* | **any**}		
ip prefix-list *WORD* **description**		Writes comments for the prefix list.

LINE		LINE: prefix list description up to 80 characters

i By default, the sequence numbers are automatically generated in increments of 5.

To delete the entries in the prefix list, use the following command.

Command	Mode	Description
no ip prefix-list *WORD*	Global	Deletes the entries of the prefix list.
no ip prefix-list *WORD* {**deny** | **permit**} *A.B.C.D/M* **ge** <0-32> [**le** <0-32>]		
no ip prefix-list *WORD* {**deny** | **permit**} *A.B.C.D/M* **le** <0-32> [**ge** <0-32>]		
no ip prefix-list *WORD* {**deny** | **permit**} {*A.B.C.D/M* | **any**}		
no ip prefix-list *WORD* **description** [*LINE*]		

12.1.23.2 Creating prefix list policy

Sequence numbers are automatically generated by default. To configure the sequence numbers manually, you can use the **seq** <1-4294967295> argument of the **ip prefix-list** command.

To add policy to prefix list one by one and assign a sequence number to the policy, use the following command.

Command	Mode	Description
ip prefix-list *WORD* **seq** <1-4294967295> {**deny** | **permit**} {*A.B.C.D/M* | **any**}	Global	Creates an entry in an IPv4 prefix list and assigns a sequence number to the entry. WORD: name of IP prefix list 1-4294967295: sequence number of an entry deny: denies access of packet if conditions are matched. permit: permits access of packet if conditions are matched. A.B.C.D/M: IPv4 prefix to match (e.g. 35.0.0.0/8) any: any IP prefix to match. (same as 0.0.0.0/0 le 32) ge: minimum prefix length to be matched le: maximum prefix length to be matched 0-32: minimum/maximum prefix length
ip prefix-list *WORD* **seq** <1-4294967295> {**deny** | **permit**} *A.B.C.D/M* **ge** <0-32> [**le** <0-32>]		
ip prefix-list *WORD* **seq** <1-4294967295> {**deny** | **permit**} *A.B.C.D/M* **le** <0-32> [**ge** <0-32>]		

You can input **ge** and **le** optionally, and they are used when you configure more than one network. If you do use neither **ge** nor **le**, network range is more clearly configured. When only **ge** attribute is configured, network range is configured from **ge** value, and when only **le** attribute is configured, network range is configured from netmask to **le** value.

To delete the configured policy of prefix list, use the following command.

Command	Mode	Description
no ip prefix-list *WORD* **seq** <1-4294967295> {**deny** | **permit**} {*A.B.C.D/M* | **any**}	Global	Deletes the entry in an IPv4 prefix list and removes a sequence number from the entry.
no ip prefix-list *WORD* **seq** <1-4294967295> {**deny** | **permit**} *A.B.C.D/M* **ge** <0-32> [**le** <0-32>]		
no ip prefix-list *WORD* **seq** <1-4294967295> {**deny** | **permit**} *A.B.C.D/M* **le** <0-32> [**ge** <0-32>]		

With sequenced prefix lists, each prefix list entry is associated with a sequence number. Sequence numbers can be used to insert a prefix list into the middle of an existing list or to delete an existing statement in the list.

To include the sequence numbers in the configuration, use the following command.

Command	Mode	Description
ip prefix-list sequence-number	Global	Includes sequence numbers in non-volatile generation (NVGEN).

To exclude the sequence numbers, use the following command.

Command	Mode	Description
no ip prefix-list sequence-number	Global	Excludes sequence numbers in non-volatile generation (NVGEN).

12.1.23.3 Displaying Prefix List Entries

To display the information about a prefix list or prefix list entries, use the following command.

Command	Mode	Description
show ip prefix-list [*WORD*]	Enable Global	Shows information about all prefix lists.
show ip prefix-list *WORD* *A.B.C.D/M* [**first-match** | **longer**]		Shows the prefix list entry according to the parameter. longer: all entries of a prefix list that are more specific than the given network and length first-match: the entry of a prefix list that matches the given prefix
show ip prefix-list *WORD* **seq** <1-4294967295>		Shows the prefix list entry with a given sequence number.
show ip prefix-list {**detail** | **summary**} [*WORD*]		Shows a table showing the entries in a prefix list identified by name.

To clear the existing prefix list entries, use the following command.

Command	Mode	Description
clear ip prefix-list [*WORD*]	Enable Global	Clears the counters of all IPv4 prefix lists or an IPv4 prefix with a specified name and prefix.
clear ip prefix-list *WORD*		

A.B.C.D/M		

12.1.24 BGP Debug

To enable BGP debugging, use the following command.

Command	Mode	Description
debug bgp	Enable	Enables BGP debugging.
debug bgp { **all** | **dampening** | **events** | **filters** | **fsm** | **keepalives** | **nsm** | **updates** [**in** | **out**] }		Enables BGP debugging. all: all BGP debugging dampening: BGP dampening debugging events: events debugging filters: BGP filters debugging fsm: BGP finite state machine debugging keepalives: BGP deepalives debugging nsm: NSM message debugging updates in/out: inbound/outbound updates debugging

To disable BGP debugging, use the following command.

Command	Mode	Description
no debug bgp	Enable	Disables BGP debugging.
no debug bgp { **all** | **dampening** | **events** | **filters** | **fsm** | **keepalives** | **nsm** | **updates** [**in** | **out**] }		

To display the debugging information, use the following command.

Command	Mode	Description
show debugging bgp	Enable Global	Shows the debugging information of BGP.

12.1.25 BGP Monitoring and Management

12.1.25.1 Displaying BGP Information

BGP network information or configurations provided can be used to determine resource utilization and enable BGP troubleshooting functions to solve network problems.

To see the configurations involved in BGP routing protocol, use the following command.

Command	Mode	Description
show ip bgp summary	Enable	Shows the summarized network status of BGP neigh-

show ip bgp [**ipv4** {**unicast** | **multicast**}] **summary**	Global	boring routers.

12.1.25.2 BGP Neighbor

To display the detailed information on BGP neighbor router’s session, use the following command.

Command	Mode	Description
show ip bgp neighbors [*NEIGHBOR-IPv4*]	Enable Global	Shows general information on BGP neighbor connections of all neighboring routers.
show bgp ipv6 neighbors [*NEIGHBOR-IPv6*]		
show ipv6 bgp neighbors		
show ip bgp {**unicast** | **multicast**} **neighbors**		
show ip bgp [**unicast** | **multicast**] **neighbors** *NEIGHBOR-IP*		Shows information of a specified neighbor router by its IP address. NEIGHBOR-IP: neighbor router’ s IPv4/IPv6 address
show bgp neighbors *NEIGHBOR-IP*		
show ip bgp [**unicast** | **multicast**] **neighbors** *NEIGHBOR-IP* **advertised-routes**		The **advertised-routes** option displays all the routes the router has advertised to the neighbor.
show bgp ipv6 neighbors *NEIGHBOR-IPv6* **advertised-routes**		
show ip bgp [**unicast** | **multicast**] **neighbors** *NEIGHBOR-IP* **received prefix-filter**		Displays all received routes from neighbor router, both accepted and rejected.
show ip bgp [**unicast** | **multicast**] **neighbors** *NEIGHBOR-IP* **received-routes**		The **received-routes** option displays all received routes (both accepted and rejected) from the specified neighbor. To implement this feature, BGP soft reconfiguration is set.
show bgp ipv6 neighbors *NEIGHBOR-IPv6* **received-routes**		
show ipv6 bgp neighbors *NEIGHBOR-IPv6* **received-routes**		
show ip bgp [**unicast** | **multicast**] **neighbors** *NEIGHBOR-IP* **routes**		The **routes** option displays the available routes only that are received and accepted.

12.1.25.3 Logging Neighbor Changes

To enable/disable logging of status change messages without turning on BGP debugging, use the following command.

Command	Mode	Description
bgp log-neighbor-changes	Router	Enables logging of BGP neighbor status changes
no bgp log-neighbor-changes		Disables logging of BGP neighbor status changes

The LD3032 logs the following events using the above command.

- BGP notification received
- Erroneous BGP update received
- User reset request
- Peer time-out / Peer closing down the session / Member added to peer group

- Interface flap
- Router ID changed
- Neighbor deleted
- Remote AS changed
- Administrative shutdown

12.1.25.4 Checking the BGP Network Route

To check that the BGP network route is reachable through IGP, use the following command.

Command	Mode	Description
bgp network import-check	Router	Checks BGP network route exists in IGP.
no bgp network import-check		Disables the function.

12.1.25.5 Sending SNMP Trap

To enable/disable the system to send SNMP trap message of BGP routing information, use the following command.

Command	Mode	Description
bgp snmp-notification enable	Router	Configures the system to send SNMP trap of routing information while BGP is running.
bgp snmp-notification disable		Disables the system to send SNMP trap of routing information while BGP is running.

12.2 Open Shortest Path First (OSPF)

Open shortest path first (OSPF) is an interior gateway protocol developed by the OSPF working group of Internet Engineering Task Force (IETF). OSPF designed for IP network supports IP subnetting and marks on information from exterior network. Moreover, it supports packet authorization and transmits/receives routing information through IP multicast. It is most convenient to operate OSPF on layered network.

OSPF is the most compatible routing protocol in layer network environment. The first setting in OSPF network is planning network organized with router and configures border router faced with multiple section.

After that, sets up the basic configuration for OSPF router operation and assigns interface to Area. To make compatible OSPF router configuration for user environment, each router configuration must be accorded by verification.

12.2.1 Enabling OSPF

To use OSPF routing protocol, it must be activated as other routing protocols. After activation, configures network address and ID which is operated by OSPF.

The following command shows steps of activating OSPF.

Step1

Open *Router Configuration* mode from *Global Configuration* mode.

Command	Mode	Description
router ospf [<1-65535>]	Global	Opens *Router Configuration* mode with enabling OSPF.
no router ospf [<1-65535>]		Disables OSPF routing protocol.

In case that more than 2 OSPF processes are operated, a process number should be assigned. Normally, there is one OSPF which is operating in one router.

If OSPF routing protocol is disabled, all related configuration will be lost.

Step2

Configure a network ID of OSPF. Network ID decides IPv4 address of this network.

Command	Mode	Description
router-id *A.B.C.D*	Router	Assigns a router ID with enabling OSPF.
no router-id *A.B.C.D*		Deletes a configured router ID.

In case if using **router-id** command to apply new router ID on OSPF process, OSPF process must be restarted to apply. Use the **clear ip ospf process** command to restart OSPF process.

Command	Mode	Description
clear ip ospf [<0-65535>**] process**	Global	Restart the OSPF process 0-65535: process ID number

If there is changing router ID while OSPF process is operating, configuration must be processed from the first. In this case, the LD3032 can change only router ID without changing related configurations.

Command	Mode	Description
ospf router-id *A.B.C.D*	Router	Changes only a router ID without changing related configurations.
no ospf router-id *A.B.C.D*		Deletes a changed router ID.

To transfer above configuration to other routers, Use the **clear ip ospf process** command to restart OSPF process.

Step 3

Use the **network** command to specify a network to operate with OSPF.

There are two ways to show network information configurations. Firstly, shows IP address with bitmask like “10.0.0.0/8”. Secondly, shows IP address with wildcard bit information like “10.0.0.0 0.0.0.255”. The variable option after **area** must be IP address or OSPF area ID.

To configure a network, use the following command.

Command	Mode	Description
network *A.B.C.D/M* **area** {<0-4294967295> | *A.B.C.D*}	Router	Specifies a network with OSPF area ID. 0-4294967295: OSPF area ID
network *A.B.C.D A.B.C.D* **area** {<0-4294967295> | *A.B.C.D*}		

12.2.2 ABR Type Configuration

The LD3032 supports 4 types of OSPF ABR which are Cisco type ABR (RFC 3509), IBM type ABR (RFC 3509), IETF Draft type and RFC 2328 type.

To configure ABR type of OSPF, use the following command.

Command	Mode	Description
ospf abr-type {**cisco** | **ibm** | **shortcut** | **standard**}	Router	Selects an ABR type. cisco: cisco type ABR, RFC 3509 (default) ibm: IBM type ABR, RFC 3509 shortcut: IETF draft type

		standard: RFC 2328 type
no ospf abr-type {**cisco** | **ibm** | **shortcut** | **standard**}		Deletes a configured ABR type.

12.2.3 Compatibility Support

OSPF protocol in the LD3032 uses RFC 2328 which is finding shorten path. However, Compatibility configuration enables the switch to be compatible with a variety of RFCs that deal with OSPF. Perform the following task to support many different features within the OSPF protocol.

Use the following command to configure compatibility with RFC 1583.

Command	Mode	Description
compatible rfc1583	Router	Supports compatibility with RFC 1583.
no compatible rfc1583		Disables configured compatibility.

12.2.4 OSPF Interface

OSPF configuration can be changed. Users are not required to alter all of these parameters, but some interface parameters must be consistent across all routers in an attached network.

12.2.4.1 Authentication Type

Authentication encodes communications among the routers. This function is for security of information in OSPF router.

To configure authentication of OSPF router for security, use the following command.

Command	Mode	Description
ip ospf authentication [**message-digest** | **null**]	Interface	Enables authentication on OSPF interface. message-digest: MD5 encoding null: no encoding A.B.C.D: IP address for authentication
ip ospf *A.B.C.D* **authentication** [**message-digest** | **null**]		

If there is no choice of authentication type, the code communication will be based on text.

To delete comfigured authentication, use the following command.

Command	Mode	Description
no ip ospf authentication	Interface	Deletes configured authentication.
no ip ospf *A.B.C.D* **authentication**		

12.2.4.2 Authentication Key

If authentication enables on OSPF router interface, the password is needed for authentication. The authentication key works as a password. The authentication key must be consistent across all routers in an attached network.

There are two ways of authentication by user selection, one is type based on text, and another is MD5 type.

⚠ The authentication key must be consistent across all routers in an attached network.

To configure an authentication key which is based on text encoding, use the following command.

Command	Mode	Description
ip ospf authentication-key *KEY*	Interface	Configures the authentication which is based on text encoding. KEY: maximum 16 alphanumeric characters
ip ospf authentication-key *KEY* {**first** | **second**} [**active**]		
ip ospf *A.B.C.D* **authentication-key** *KEY*		
ip ospf *A.B.C.D* **authentication-key** *KEY* {**first** | **second**} [**active**]		

To configure an authentication key which is based on MD5 encoding, use the following command.

Command	Mode	Description
ip ospf message-digest-key <1-255> **md5** *KEY* [**active**]	Interface	Configures the authentication which is based on md5 type. 1-255: key ID KEY: maximum 16 alphanumeric characters
ip ospf message-digest-key <1-255> **md5** [**active**]		
ip ospf *A.B.C.D* **message-digest-key** <1-255> **md5** *KEY* [**active**]		
ip ospf *A.B.C.D* **message-digest-key** <1-255> **md5** [**active**]		

To delete a configured authentication key, use the following command.

Command	Mode	Description
no ip ospf authentication-key	Interface	Deletes a configured authentication key.
no ip ospf authentication-key {**first** | **second**}		
no ip ospf *A.B.C.D* **authentication-key**		
no ip ospf *A.B.C.D* **authentication-key** {**first** | **second**}		

no ip ospf message-digest-key <1-255>		
no ip ospf *A.B.C.D* **message-digest-key** <1-255>		

12.2.4.3 Interface Cost

OSPF protocol assigns suitable cost according to the bandwidth on the each interface to find the shortest route. Cost is used for packet routing, and routers are using the Cost to communicate.

To configure an interface cost for OSPF, use the following command.

Command	Mode	Description
ip ospf cost <1-65535>	Interface	Configures an interface cost for OSPF.
ip ospf *A.B.C.D* **cost** <1-65535>		

To delete a configured interface cost for OSPF, use the following command.

Command	Mode	Description
no ip ospf cost	Interface	Deletes a configured an interface cost for OSPF.
no ip ospf *A.B.C.D* **cost**		

12.2.4.4 Blocking Transmission of Route Information Database

OSPF routing communicates through the LAS. Each routing information is saved internal router as a datebase, but user can configure the specific interface to block the transmission of routing information saved in database to other router.

To block the transmission of routing information to other router, use the following command.

Command	Mode	Description
ip ospf database-filter all out	Interface	Blocks the transmission of routing information to other router.
ip ospf *A.B.C.D* **database-filter all out**		

To release a blocked interface, use the following command.

Command	Mode	Description
no ip ospf database-filter	Interface	Releases a blocked interface.
no ip ospf *A.B.C.D* **database-filter**		

12.2.4.5 Routing Protocol Interval

Routers on OSPF network exchange various packets, about that packet transmission, time interval can be configured in several ways

The following lists are sort of time interval which can be configured by user:

- **Hello Interval**
  OSPF router sends Hello packet to notify existence of itself. Hello interval is that packet transmission interval.
- **Retransmit Interval**
  When router transmits LSA, it is waiting for approval information come from receiver. In this time, if there is no answer from receiver for configured time, the router transmits LSA again. Retransmit-interval is configuration of the time interval between transmission and retransmission.
- **Dead Interval**
  If there is no hello packet for the configured time. The router perceives other router is stopped working. Dead interval is configuration of the time interval which perceives other router is stopped operating.
- **Transmit Delay**
  When a router transmits LSA, the traffic can be delayed by status of communications. Transmit delay is considering of the configuration for LSA transmission time.

i

The interval explained as above must be consistent across all routers in an attached network.

To configure a Hello interval, use the following command.

Command	Mode	Description
ip ospf hello-interval <1-65535>	Interface	Configures a Hello interval in the unit of second. 1-65535: interval value (default: 10)
ip ospf *A.B.C.D* **hello-interval** <1-65535>		
no ip ospf hello-interval		Sets a Hello interval to the default value.
no ip ospf *A.B.C.D* **hello-interval**		

To configure a retransmit interval, use the following command.

Command	Mode	Description
ip ospf retransmit-interval <1-65535>	Interface	Configures a retransmit interval in the unit of second. 1-65535: interval value (default: 5)
ip ospf *A.B.C.D* **retransmit-interval** <1-65535>		
no ip ospf retransmit-interval		Sets a retransmit interval to the default value.
no ip ospf *A.B.C.D* **retransmit-interval**		

To configure a dead interval, use the following command.

Command	Mode	Description
ip ospf dead-interval <1-65535>	Interface	Configures a dead interval in the unit of second. 1-65535: interval value (default: 40)
ip ospf *A.B.C.D* **dead-interval** <1-65535>		
no ip ospf dead-interval		Sets a dead interval to the default value.
no ip ospf *A.B.C.D* **dead-interval**		

To configure a transmit delay, use the following command.

Command	Mode	Description
ip ospf transmit-delay <1-65535>	Interface	Configures a transmit delay in the unit of second. 1-65535: interval value (default: 1)
ip ospf *A.B.C.D* **transmit-delay** <1-65535>		
no ip ospf transmit-delay		Sets a transmit delay to the default value.
no ip ospf *A.B.C.D* **transmit-delay**		

12.2.4.6 OSPF Maximum Transmission Unit (MTU)

Router verifies MTU when DD (Database Description) is exchanging among the routers on OSPF networks. Basically, OSPF network can not be organized if there are different sizes of MTUs between routers. Therefore MTU value must be consistent. Generally MTU value is 1500 bytes on Ethernet interface.

To configure MTU on OSPF interface, use the following command.

Command	Mode	Description
ip ospf mtu <576-65535>	Interface	Configures an MTU on OSPF interface.
no ip ospf mtu		Deletes a configured MTU on OSPF interface.

Configuration as above makes MTU consistently on same OSPF network; actual MTU value on interface itself will not be changed.

On the other hands, if there are two routers which have different MTU, it can be participated with OSPF network through the configuration that skips the verification of MTU value when there is DD exchanging.

To configure the switch to skip the MTU verification in DD process, use the following command.

Command	Mode	Description
ip ospf mtu-ignore	Interface	Configures the switch to skip the MTU verification in DD process.
ip ospf *A.B.C.D* **mtu-ignore**		

To configure the switch not to skip the MTU verification in DD process, use the following command.

Command	Mode	Description
no ip ospf mtu-ignore	Interface	Configures the switch not to skip the MTU verification in DD process.
no ip ospf *A.B.C.D* **mtu-ignore**		

12.2.4.7 OSPF Priority

Routers have each role to exchange the information on OSPF network. DR (Designated Router) is one of essential role to get and transmit the route information in the same area.

The router having the highest priority becomes DR (Designated Router). If there are routers which have same priority, the highest router ID will be DR.

Normally, router has priority 1, but it can be changed to make DR through the configuration of priority.

To configure a priority of OSPF router, use the following command.

Command	Mode	Description
ip ospf priority <0-255>	Interface	Configures a priority of OSPF router.
ip ospf *A.B.C.D* **priority** <0-255>		

To delete a configured priority of OSPF router, use the following command.

Command	Mode	Description
no ip ospf priority	Interface	Deletes a configured priority of OSPF router.
no ip ospf *A.B.C.D* **priority**		

12.2.4.8 OSPF Network Type

There are 4 types of OSPF network. Broadcast network, NBMA (Non-broadcast-multiple-access) network, Point-to-multipoint network and Point-to-point network.

User can configure OSPF network as a Broadcast network or Non-broadcast network type. For example, if the network does not support multicasing it can be configured Non-broadcast type from Broadcast type, and NBMA network as a Frame relay can be broadcast network type.

NBMA type network need virtual circuit to connect routers. But Point-to-multipoint type uses virtual circuit on part of network to save the management expenses. It does not to need to configure Neighbor router to connect routers which are not directly connected. It also saves IP resources and no need to configure the process for destination router. It supports those benefits for stable network services.

Generally, the routers and Layer 3 switches are using Broadcast type network.

To select an OSPF network type, use the following command.

Command	Mode	Description
ip ospf network {**broadcast** | **non-broadcast** | **point-to-multipoint** [**non-broadcast**] | **point-to-point**}	Interface	Selects an OSPF network type.

12.2.5 Non-Broadcast Network

To operate NBMA type network, neighbor router configuration is needed. And IP address, Priority, Poll-interval configuration as well. Priority is information for designate router selection and it configured [0] as a default. Poll-interval is the waiting time to re-get the hello packet from dead Neighbor router. It configured 120 seconds as a default.

To configure a router communicated by non-broadcast type, use the following command.

Command	Mode	Description
neighbor *A.B.C.D* [**cost** <1-65535>]	Router	Configures a neighbor router of NBMA type.
neighbor *A.B.C.D* **priority** <0-255>		
neighbor *A.B.C.D* **priority** <0-255> **poll-interval** <1-65535>		
neighbor *A.B.C.D* **poll-interval** <1-65535>		
neighbor *A.B.C.D* **poll-interval** <1-65535> **priority** <0-255>		

To delete a configured router communicated by non-broadcast type, use the following command.

Command	Mode	Description
no neighbor *A.B.C.D*	Router	Deletes a configured neighbor router of NBMA type.
no neighbor *A.B.C.D* **cost** [<1-65535>]		
no neighbor *A.B.C.D* **priority** [<0-255>]		
no neighbor *A.B.C.D* **priority poll-interval** [<1-65535>]		
no neighbor *A.B.C.D* **poll-interval** [<1-65535>]		
no neighbor *A.B.C.D* **poll-interval priority** [<0-255>]		

12.2.6 OSPF Area

Router configuration on OSPF network includes Area configuration with each interface, network. Area has various and special features. It needs to be configured pertinently to make effective management on whole of OSPF network.

OSPF network defines several router types to manage the Area. ABR (Area Border Router) is one of the router types to transmit information between Areas.

ASBR (Autonomous System Border Router) is using OSPF on oneside and using other routing protocol except for OSPF on other interface or Area. ASBR exchanges area information between different routing protocols.

Area types are various. The most principle Area types are Stub Area and NSSA (Not So Stubby Area).

12.2.6.1 Area Authentication

OSPF routers in specific Area can configure authentication for security of routing information. Encoding uses password based on text or MD5. To set password on interface assigned Area, use the **ip ospf authentication-key** and **ip ospf message-digest-key** commands in interface mode, see Section 12.2.4.1 for more information.

To configure authentication information for encoding, use the following command.

Command	Mode	Description
area {<0-4294967295> | *A.B.C.D*} **authentication**	Router	Configures authentication information which is based on text encoding in the Area.
area {<0-4294967295> | *A.B.C.D*} **authentication message-digest**		Configures authentication information which is based on MD5 encoding in the Area.

To delete configured authentication information for encoding, use the following command.

Command	Mode	Description
no area {<0-4294967295> | *A.B.C.D*} **authentication**	Router	Deletes configured authentication information.

12.2.6.2 Default Cost of Area

The default cost of Area is configured only in ABR. ABR function is for delivering the summary default route to stub area or NSSA, in that cases the default cost of area must be required. However, ABR which does not have stub area or NSSA can not use the following command.

To configure a default cost of Area, use the following command.

Command	Mode	Description
area {<0-4294967295> | *A.B.C.D*} **default-cost** <1-16777215>	Router	Configures a default cost of Area.

To delete a configured default cost of Area, use the following command.

Command	Mode	Description
area {<0-4294967295> | *A.B.C.D*} **default-cost** <1-16777215>	Router	Deletes a configured default cost of Area.

⚠ This command is only for ABR which is delivering summary default route to stub or NSSA.

12.2.6.3 Blocking the Transmission of Routing Information Between Area

ABR transmits routing information between Areas. In case of not to transmit router information to other area, the LD3032 can configure it as a blocking.

First of all, use the **access-list** or **prefix-list** command to assign LIST-NAME. And use the following command to block the routing information on LIST-NAME. This configuration only available in case of OSPF router is ABR.

To block routing information on LIST-NAME, use the following command.

Command	Mode	Description
area {<0-4294967295> | *A.B.C.D*} **filter-list access** *LIST-NAME* {**in** | **out**}	Router	Blocks routing information on LIST-NAME.
area {<0-4294967295> | *A.B.C.D*} **filter-list prefix** *LIST-NAME* {**in** | **out**}		

To delete configured blocking information, use the following command.

Command	Mode	Description
no area {<0-4294967295> | *A.B.C.D*} **filter-list access** *LIST-NAME* {**in** | **out**}	Router	Deletes configured blocking information.
no area {<0-4294967295> | *A.B.C.D*} **filter-list prefix** *LIST-NAME* {**in** | **out**}		

This command is only available for ABR.

12.2.6.4 Not So Stubby Area (NSSA)

NSSA (Not So Stubby Area) is stub Area which can transmit the routing information to Area by ASBR. On the other hand, Stub Area cannot transmit the routing information to area. To configure NSSA, use the following command.

Command	Mode	Description
area {<0-4294967295> | *A.B.C.D*} **nssa**	Router	Configures NSSA.

The following options are configurable for NSSA:

- **default-information-originate**
  This option is configuration for allowing default path of Type-7 in NSSA. It means routing path without routing information will use the interface which is allowed in default type-7 path. **metric** is for metric value, **metric-type** is for type of finding the path. **metric-type 1** uses internal path cost with external path cost as a cost, **metric type 2** always uses external cost value only.
- **no-redistribution**
  This option is configuration in NSSA for restriction to retransmit the routing information which is from outside.
- **no-summary**

This option is for restriction to exchange routing information between OSPF areas.

- **translator-role**
  NSSA-LSA (Link State Advertisement) has three types according to the way of process type. **always** changes all NSSA-LSA into Type-5 LSA. **candidate** changes NSSA-LSA into Type-5 LSA when it is translator. **never** does not change NSSA-LSA.

NSSA uses ASBR when it transmits Stub Area or other routing protocol Area into OSPF. In this case, if other routing protocol has default path, use **default-information-originate** command to configure the all of default path is using the assigned ASBR

To configure **NSSA** with various features, use command with options. **area** <0-4294967295> **NSSA** command has 4 options as **default-information-originate**, **no-redistribution**, **no-summary**, **translator-role** and it can be selected more than 2 options without order. **default-information-originate** has **metric** <0-16777214> and **metric-type** <1-2> as an option, **translator-role** must choose one of **candidate**, **never**, **always as an options**.

The following is explaining options of command:

- **default-information-originate** or
  default-information-originate metric <0-16777214> or
  default-information-originate metric-type <1-2>
- **no-redistribution**
- **no-summary**
- **translator-role** {**candidate | never | always**}

To configure NSSA with one option, use the following command.

Command	Mode	Description
area {<0-4294967295> | *A.B.C.D*} **nssa default-information-originate**	Router	Configures NSSA with one option.
area {<0-4294967295> | *A.B.C.D*} **nssa default-information-originate metric** <0-16777214>		
area {<0-4294967295> | *A.B.C.D*} **nssa default-information-originate metric-type** <1-2>		
area {<0-4294967295> | *A.B.C.D*} **nssa no-redistribution**		
area {<0-4294967295> | *A.B.C.D*} **nssa no-redistribution default-information-originate** [**metric** <0-16777214>]		
area {<0-4294967295> | *A.B.C.D*} **nssa no-redistribution default-information-originate metric-type** <1-2>		
area {<0-4294967295> | *A.B.C.D*} **nssa no-redistribution default-information-originate no-summary** [**translator-role** { **always** | **candidate** |		

never }]		
area <0-4294967295> **nssa no-redistribution default-information-originate translator-role** { **always** | **candidate** | **never** }		
area <0-4294967295> **nssa no-summary**		
area {<0-4294967295> | *A.B.C.D*} **nssa no-summary** [**no-redistribution]** **default-information-originate** [**metric** <0-16777214>]		
area {<0-4294967295> | *A.B.C.D*} **nssa no-summary** [**no-redistribution**] **default-information-originate metric-type** <1-2>		
area {<0-4294967295> | *A.B.C.D*} **nssa no-summary default-information-originate [no-redistribution]** [**translator-role** { **always** | **candidate** | **never** }]		
area {<0-4294967295> | *A.B.C.D*} **nssa no-summary no-redistribution** [**translator-role** { **always** | **candidate** | **never** }]		
area <0-4294967295> **nssa translator-role** {**candidate** | **never** | **always**}		

The following example shows how to configure NAAS with more than 2 options:

- **area** <0-4294967295> **nssa no-summary no-redistribution**
- **area** <0-4294967295> **nssa translator-role** {**candidate** | **never** | **always**} **default-information-originate metric-type** <1-2> **no-redistribution**

To delete configured NSSA, use the following command.

Command	Mode	Description
no area {<0-4294967295> | *A.B.C.D*} **nssa**	Router	Deletes configured NSSA.
no area {<0-4294967295> | *A.B.C.D*} **nssa default-information-originate**		
no area {<0-4294967295> | *A.B.C.D*} **nssa default-information-originate no-redistribution** [**no summary**]		
no area {<0-4294967295> | *A.B.C.D*} **nssa default-information-originate no-redistribution no-summary** [**translator-role** {**candidate** | **never** | **always**}]		
no area {<0-4294967295> | *A.B.C.D*} **nssa default-information-originate no-redistribution translator-role** {**candidate** | **never** | **always**}		
no area {<0-4294967295> | *A.B.C.D*} **nssa no-redistribution** [**default-information-originate**]		
no area {<0-4294967295> | *A.B.C.D*} **nssa no-redistribution default-information-originate no-summary** [**translator-role** {**candidate** | **never** | **always**}]		
no area {<0-4294967295> | *A.B.C.D*} **nssa no-redistribution**		

[**no-summary**] **default-information-originate translator-role** {**candidate** | **never** | **always**}		
no area {<0-4294967295> | *A.B.C.D*} **nssa no-redistribution no-summary** [**translator-role** {**candidate** | **never** | **always**}]		
no area {<0-4294967295> | *A.B.C.D*} **nssa no-redistribution translator-role default-information-originate** [**no-summary**]		
no area {<0-4294967295> | *A.B.C.D*} **nssa no-redistribution translator-role** [**no-summary**] [**default-information-originate**]		
no area {<0-4294967295> | *A.B.C.D*} **nssa no-summary** [**default-information-originate**]		
no area {<0-4294967295> | *A.B.C.D*} **nssa no-summary default-information-originate no-redistribution** [**translator-role** {**candidate** | **never** | **always**}]		
no area {<0-4294967295> | *A.B.C.D*} **nssa no-summary default-information-originate translator-role** [**no-redistribution**]		
no area {<0-4294967295> | *A.B.C.D*} **nssa no-summary no-redistribution** [**default-information-originate**]		
no area {<0-4294967295> | *A.B.C.D*} **nssa no-summary no-redistribution** [**default-information-originate**] [**translator-role]**		
no area {<0-4294967295> | *A.B.C.D*} **nssa no-summary translator-role** [**default-information-originate**] [**no-redistribution**]		
no area {<0-4294967295> | *A.B.C.D*} **nssa no-summary translator-role no-redistribution**		
no area {<0-4294967295> | *A.B.C.D*} **nssa translator-role** [**default-information-originate**]		
Command	**Mode**	**Description**
no area {<0-4294967295> | *A.B.C.D*} **nssa translator-role default-information-originate** [**no-redistribution**] [**no-summary**]	Router	Deletes configured NSSA.
no area {<0-4294967295> | *A.B.C.D*} **nssa translator-role no-redistribution** [**default-information-originate**] [**no-summary**]		
no area {<0-4294967295> | *A.B.C.D*} **nssa translator-role no-summary** [**no-redistribution**] [**default-information-originate**]		

12.2.6.5 Area Range

In case of OSPF belongs to several Areas, Area routing information can be shown in one routing path. Like as above, various routing information of Area can be combined and summarized to transmit to outside.

To summarize and combine the routing information, use the following command.

Command	Mode	Description
area {<0-4294967295> | *A.B.C.D*} **range** *A.B.C.D/M*	Router	Configures to use summarized information for assigned path.
area {<0-4294967295> | *A.B.C.D*} **range** *A.B.C.D/M* {**advertise** | **not-advertise**}		

Use **advertise** option to transmit summarized routing information with using summarized information. And use the **not-advertise** option to block the transmission of summarized routing information to outside.

To release the configuration, use the following command.

Command	Mode	Description
no area {<0-4294967295> | *A.B.C.D*} **range** *A.B.C.D/M*	Router	Releases the configuration to use summarized information for assigned path
no area {<0-4294967295> | *A.B.C.D*} **range** *A.B.C.D/M* {**advertise** | **not-advertise**}		

12.2.6.6 Shortcut Area

Backbone Area is the default Area among the Areas of OSPF. All traffic should pass the Backbone Area and OSPF network must be planned for that, but there is some efficiency way which is not to pass the Backbone Area. That is Shortcut, and it must be configured for efficient traffic in every ABR type, see Section 12.2.2.

To configure the shortcut option, use the following command.

Command	Mode	Description
area {<0-4294967295> | *A.B.C.D*} **shortcut** {**default** | **disable** | **enable**}	Router	Configures the shortcut option.

To releases the configured shortcut option, use the following command.

Command	Mode	Description
no area {<0-4294967295> | *A.B.C.D*} **shortcut** {**default** | **disable** | **enable**}	Router	Releases the configured shortcut option.

12.2.6.7 Stub Area

Stub Area is that ABR is connected to Backbone Area. If it is assigned as Stub Area, ABR will notify the default path to Stub Area and other routing protocol information will not transmit to Stub Area.

To create Stub Area, use the following command.

Command	Mode	Description
area {<0-4294967295> | *A.B.C.D*} **stub** [**no-summary**]	Router	Creates a Stub Area.

If **no-summary** option adds to Stub Area, other Area OSPF routing information also can not come to Stub Area, However, it only goes to default route from ABR router. That is Totally Stubby Area.

To delete a created Stub Area, use the following command.

Command	Mode	Description
no area {<0-4294967295> | *A.B.C.D*} **stub** [**no-summary**]	Router	Deletes a created Stub Area.

12.2.6.8 Maximum Area

User can set the maximum number of OSPF area that the router can belong to.

To specify the maximum number of OSPF area, use the following command.

Command	Mode	Description
maximum-area <1-4294967294>	Router	Specifies the maximum number of OSPF area.

To remove the configured maximum area value, use the following command.

Command	Mode	Description
no maximum-area	Router	Removes the configured maximum area value.

12.2.6.9 Virtual Link

In OSPF, all areas must be connected to a backbone area. If there is a break in backbone continuity, or the backbone is purposefully portioned, you can establish a virtual link. The virtual link must be configured in both routers.

OSPF network regards virtual link routers as Point-to-point router. Therefore, the Hello-interval, Retransmit-interval, Transmit-delay must be consistent across all routers in an attached network.

User can configure Authentication for security, Authentication key for password, and time period for Hello-interval, Retransmit-interval, Transmit-delay and Dead-interval to operate virtual link.

The following items describe 7 configurations for virtual link:

- **Authentication**
  This is configuration for security of routing information. **message-digest** uses MD5 to encode for authentication, **null** means not using any of authentication.

- **Authentication-key**
  Configures the authentication which is based on text encoding.

- **Message-digest-key**
  Configures the authentication which is based on md5 type.

- **Hello-interval**
  OSPF router sends Hello packet to notify existence of itself. Hello-interval is that packet transmission interval.

- **Retransmit-interval**
  When router transmits LSA, it is waiting for approval information come from receiver. In this time, if there is no answer from receiver for configured time, the router trans-

mits LSA again. Retransmit-interval is configuration of the time interval between transmission and retransmission

- **Dead-interval**
  If there is no hello packet for the configured time. The router perceives other router is stopped working. Dead-interval is configuration of the time interval which perceives other router is stopped operating.
- **Transmit-delay**
  When a router transmits LSA, the traffic can be delayed by status of communications. Transmit-delay is considering of the configuration for LSA transmission time.

Configuration for virtual link can be selected more than 2 options without order. The following is explaining options of command:

- **authentication** [**message-digest | null**]
- **authentication-key** *KEY*
- **message-digest-key** *KEY* **md5** *KEY*
- **hello-interval** <1-65535>
- **retransmit-interval** <1-65535>
- **dead-interval** <1-65535>
- **transmit-delay** <1-65535>

To configure a virtual link with one option, use the following command.

Command	Mode	Description
area {<0-4294967295> | *A.B.C.D*} **virtual-link** *A.B.C.D* **authentication** [**message-digest** | **null**]	Router	Configures a virtual link.
area {<0-4294967295> | *A.B.C.D*} **virtual-link** *A.B.C.D* **authentication-key** *KEY*		
area {<0-4294967295> | *A.B.C.D*} **virtual-link** *A.B.C.D* **message-digest-key** *KEY* **md5** *KEY*		
area {<0-4294967295> | *A.B.C.D*} **virtual-link** *A.B.C.D* **hello-interval** <1-65535>		
area {<0-4294967295> | *A.B.C.D*} **virtual-link** *A.B.C.D* **retransmit-interval** <1-65535>		
area {<0-4294967295> | *A.B.C.D*} **virtual-link** *A.B.C.D* **dead-interval** <1-65535>		
area {<0-4294967295> | *A.B.C.D*} **virtual-link** *A.B.C.D* **transmit-delay** <1-65535>		

The following example shows how to configure virtual link with more than 2 options:

- **area** <0-4294967295> **virtual-link** *A.B.C.D* **authentication-key** *KEY* **authentication** [**message-digest | null**]
- **area** <0-4294967295> **virtual-link** *A.B.C.D* **hello-interval** <1-65,535> **dead-interval** <1-65535>

To delete a configured virtual link, use the following command.

Command	Mode	Description
no area {<0-4294967295> | *A.B.C.D*} **virtual-link** *A.B.C.D* **authentication** [**message-digest** | **null**]	Router	Deletes a configured virtual link.
no area {<0-4294967295> | *A.B.C.D*} **virtual-link** *A.B.C.D* **authentication-key** *KEY*		
no area {<0-4294967295> | *A.B.C.D*} **virtual-link** *A.B.C.D* **message-digest-key** *KEY* **md5** *KEY*		
no area {<0-4294967295> | *A.B.C.D*} **virtual-link** *A.B.C.D* **hello-interval** <1-65535>		
no area {<0-4294967295> | *A.B.C.D*} **virtual-link** *A.B.C.D* **retransmit-interval** <1-65535>		
no area {<0-4294967295> | *A.B.C.D*} **virtual-link** *A.B.C.D* **dead-interval** <1-65535>		
no area {<0-4294967295> | *A.B.C.D*} **virtual-link** *A.B.C.D* **transmit-delay** <1-65535>		

12.2.7 Default Metric

OSPF finds metric based on interface bandwidth. For example, default metric of T1 link is 64, but default metric of 64K line is 1562. If there are plural lines in the bandwidth, you can view costs to use line by assigning metric to each line.

To classify costs to use line, use the following command.

Command	Mode	Description
auto-cost reference-bandwidth <1-4294967>	Router	Configures default metric in the unit of Mbps. (default: 100)

To delete the configuration, use the following command.

Command	Mode	Description
no auto-cost reference-bandwidth	Router	Deletes the configuration.

12.2.8 Graceful Restart Support

You need to restart OSPF protocol processor when there is network problem. In this case, it takes long time to restarts OSPF and there is no packet transmission. Other routers are also need to delete routing information and register it again. Graceful Restart improves those inconveniences. Although OSPF is restarting, Graceful Restart makes the transmission of a packet with routing information.

To configure the Graceful Restart, use the following command.

Command	Mode	Description
capability restart {**graceful** | **signaling | reliable-graceful**}	Router	Configures the Graceful Restart.
no capability restart		Releases the configuration.

The following items are additional options for the Graceful Restart:

- **grace-period**
  When OSPF restarts, process is keeping status in graceful for the time configured as **grace-period**. After the configured time, OSPF operates in normal.
- **helper**
  This is functions that helps other routers around the restarting router. It makes re starting router as a working and transmitting to other routers. **only-reload** is for the case of OSPF router is restarting, **only-upgrade** is for the OSPF router which is upgrading software, and **max-grace-period** works when **grace-period** from other routers has less value than it. Configuration for Helper can be selected more than 2 options without order.

To configure the additional options for Graceful Restart, use the following command.

Command	Mode	Description
ospf restart grace-period <1-1800>	Global	Configures the additional options for Graceful Restart.
ospf restart helper max-grace-period <1-1800>		
ospf restart helper max-grace-period <1-1800> **only-reload** [**only-upgrade**]		
ospf restart helper max-grace-period <1-1800> **only-upgrade** [**only-reload**]		
ospf restart helper only-reload [**only-upgrade**]		
ospf restart helper only-reload only-upgrade max-grace-period <1-1800>		
ospf restart helper only-reload max-grace-period <1-1800> [**only-upgrade**]		
ospf restart helper only-upgrade [**only-reload**]		
ospf restart helper only-upgrade only-reload max-grace-period <1-1800>		
ospf restart helper only-upgrade max-grace-period <1-1800> [**only-reload**]		

To release the configuration, use the following command.

Command	Mode	Description
no ospf restart grace-period	Global	Releases the configuration.
ospf restart helper never		
no ospf restart helper max-grace-period		

12.2.9 Opaque-LSA Support

Opaque-LSA is LSA Type-9, Type-10, Type-11. The LD3032 enables Opaque-LSA as a default but it can be released by user.

To release the enabled Opaque-LSA management, use the following command.

Command	Mode	Description
no capability opaque	Router	Releases the enabled Opaque-LSA management.

To enable Opaque-LSA management, use the following command.

Command	Mode	Description
capability opaque	Router	Enables Opaque-LSA management.

12.2.10 Default Route

You can configure ASBR (Autonomous System Boundary Router) to transmit default route to OSPF network. Autonomous System Boundary router transmits route created externally to OSPF network. However, it does not create system default route.

To have autonomous System Boundary router create system default route, use the following command.

Command	Mode	Description
default-information originate	Router	Configures the default route.

The following items are detail options for the Default Route configuration.

- **metric**
  Configures Metric value of the default route.
- **metric-type**
  metric-type is for type of finding the path. **metric-type 1** uses internal path cost with external path cost as a cost, **metric type 2** always uses external cost value only.
- **always**
  Transmits the default route to outside.
- **no-summary**
  Restricts to exchange routing information between OSPF area in NSSA.
- **route-map**
  Transmits specific routing information to assigned route which has MAP-NAME.

The detail options for default route configuration are classified in 4 as above, and those configurations can be selected more than 2 options without order.

The following is explaining options of command:

- **metric** <0-16777214>
- **metric-type** <1-2>
- **always**
- **route-map** *MAP-NAME*

To configure the default route with an option, use the following command.

Command	Mode	Description
default-information originate metric <0-16777214>	Router	Configures the default route with one option.
default-information originate metric-type <1-2>		
default-information originate always		
default-information originate route-map *MAP-NAME*		

The following example shows how to configure default route with more than 2 options:

- **default-information originate metric-type** <1-2> **always**
- **default-information originate route-map** *MAP-NAME* **metric** <0-16777214>

To delete the configuration, use the following command.

Command	Mode	Description
no default-information originate	Router	Deletes the configuration.
no default-information originate metric <0-16777214>		
no default-information originate metric-type <1-2>		
no default-information originate always		
no default-information originate route-map *MAP-NAME*		

12.2.11 ECMP Route Hashing

Equal-Cost Multi-Path (ECMP) is a forwarding mechanism that routes packets along multiple paths of equal cost. ECMP provides equally-distributed link load sharing across the paths. The hashing algorithm used is based on the source IP address (SIP) or both source and destination IP address (SIP-DIP). ECMP routes allow the switch to choose between several next hops toward a given destination.

When a dynamic route is added through Open Shortest Path First (OSPF), the switch checks the route's gateway against the ECMP static routes. If the gateway matches one of the single or ECMP static route destinations, then the OSPF route is added to the list of ECMP static routes. Traffic is load-balanced across all of the available gateways. When the OSPF dynamic route times out, it is deleted from the list of ECMP static routes.

To perform ECMP route hashing, use the following command.

Command	Mode	Description
ip ecmp-hash {**sip** | **sip-dip**}	Global	Enables ECMP hashing algorithm based on IP address. sip: source IP address (default) sip-dip: source and destination IP address

12.2.12 Finding Period

OSFP start to find the shortest path as soon as got a notification of changing the network component. You can configure the period to find the path. To configure the period of finding, use the following command.

Command	Mode	Description
timers spf *SPF-DELAY SPF-HOLD*	Router	Configures the period of finding in the unit of second. SPF-DELAY: 0-4294967295 (default: 5)

		SPF-HOLD: 0-4294967295 (default: 10)

To release the configuration, use the following command.

Command	Mode	Description
no timers spf	Router	Release the configuration.

12.2.13 External Routes to OSPF Network

If other routing protocol redistribute into OSPF network, these routes become OSPF external routes. Other routing protocols are RIP and BGP. And static route, connected route, kernel route are also external route. Those routing information can distribute into OSPF network.

There are 4 kinds of additional configuration about external routes to OSPF network. **metric** is configures Metric value of the default route, **metric-type** is for type of finding the path. **metric-type 1** uses internal path cost with external path cost as a cost, metric type 2 always uses external cost value. **route-map** is transmission of specific routing information to assigned route which has MAP-NAME, and, **tag** is using the assign tag number on the specific MAP-NAME.

Those 4 kinds of additional configuration can be selected more than 2 options without order, and it applies to consistent across all external routes in an attached network.

The following is explaining 4 options of command:

- **metric** <0-16777214>
- **metric-type** <1-2>
- **route-map** *MAP-NAME*
- **tag** <0-4294967295>

To configure the external route transmission, use the following command.

Command	Mode	Description
redistribute {**bgp** | **connected** | **kernel** | **rip** | **static**} **metric** <0-16777214>	Router	Configures the external route transmission.
redistribute {**bgp** | **connected** | **kernel** | **rip** | **static**} **metric-type** <1-2>		
redistribute {**bgp** | **connected** | **kernel** | **rip** | **static**} **route-map** *MAP-NAME*		
redistribute {**bgp** | **connected** | **kernel** | **rip** | **static**} **tag** <0-4294967295>		

The following example shows how to configure it with more than 2 options:

- **redistribute** {**bgp** | **connected** | **kernel** | **rip** | **static**} **metric** <0-16777214> **tag** <0-4294967295>
- **redistribute** {**bgp** | **connected** | **kernel** | **rip** | **static**} **tag** <0-4294967295> **metric-type** <1-2>

For efficient transmission of routing information, and to avoid non-matching between metric and OSPF routing protocol, use the **default metric** command to assign metric about redistribute route.

To configure the default metric, use the following command.

Command	Mode	Description
default-metric <0-16777214>	Router	Configures the default metric.

To delete the default metric, use the following command.

Command	Mode	Description
no default-metric [<0-16777214>]	Router	Deletes the default metric.

12.2.14 OSPF Distance

An administrative distance is a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. Numerically, an administrative distance is an integer between 0 and 255. In general, the higher the value is, the lower the trust rating is. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored.

OSPF uses three different administrative distances: intra-area, inter-area, and external. Routes learned through other domain are external, routes to another area in OSPF domain are inter-area, and routes inside an area are intra-area. The default distance for each type of route is 110. In order to change any of the OSPF distance values, use the following commands.

The following is explaining 3 options of command.

- **external** <1-255>
- **inter-area** <1-255>
- **intra-area** <1-255>

To configure the distance with 1 option, use the following command.

Command	Mode	Description
distance <1-255>	Router	Configures the distance of OSPF route. (default: 110)
distance ospf external <1-255>		
distance ospf inter-area <1-255>		
distance ospf intra-area <1-255>		

The following example shows how to configure the distance with more than 2 options:

- **distance ospf external** <1-255> **inter-area** <1-255>
- **distance ospf inter-area** <1-255> **intra-area** <1-255>

To make it as a default, use the following command.

Command	Mode	Description
no distance ospf	Router	Restores it as the default.
no distance <1-255>		Deletes a configured distance of OSPF route.

12.2.15 Host Route

OSPF regards routing information of specific host as stub link information. Routing information can be assigned to each host which is connected with one router. To configure the routing information to each host, use the following command.

Command	Mode	Description
host *A.B.C.D* **area** {*A.B.C.D* | <1-4294967295>}	Router	Configures the routing information to each host.
host *A.B.C.D* **area** {*A.B.C.D* | <1-4294967295>} **cost** <0-65535>		

To delete the routing information of specific host, use the following command.

Command	Mode	Description
no host *A.B.C.D* **area** { *A.B.C.D* | <1-4294967295>}	Router	Deletes the routing information to each host.
no host *A.B.C.D* **area** { *A.B.C.D* | <1-4294967295>} **cost** <0-65535>		

12.2.16 Passive Interface

The passive interface which is configured by OSPF network operate as stub area. Therefore passive interface can not exchange the OSPF routing information.

To configure the passive interface, use the following command.

Command	Mode	Description
passive-interface *INTERFACE* [*A.B.C.D*]	Router	Configures the passive interface.

To release the configured as passive interface, use the following command.

Command	Mode	Description
no passive-interface *INTERFACE* [*A.B.C.D*]	Router	Releases the configured as passive interface.

12.2.17 Blocking Routing Information

The LD3032 can classify and restrict the routing information. To configure this function, sort the specific routing information in **access-list** first, and block the routing information in **access-list.**

To block the routing information in access-list, use the following command.

Command	Mode	Description
distribute-list *WORD* **out** {**bgp | connected | isis | kernel | ospf** [<1-65535>] | **rip** | **static }**	Router	Blocks the routing information in access-list WORD: access-list name in/out: incoming/outgoing routing 1-65535: OSPF process ID
distribute-list *WORD* **in**		

To release the configuration, use the following command.

Command	Mode	Description
no distribute-list *WORD* **out** {**bgp** | **connected** | **isis** | **kernel** | **ospf** [<1-65535>] | **rip** | **static** }	Router	Releases the configuration.
no distribute-list *WORD* **in**		

12.2.18 Summary Routing Information

In case of external routing protocol transmits to OSPF network, more than 2 routing information can be summarized as one. For example, 192.168.1.0/24 and 192.168.2.0/24 can become 192.168.0.0/16 to transmit to OSPF network. This summary reduces the number of routing information and it improves a stability of OSPF protocol

And you can use **no-advertise** option command to block the transmission of summarized routing information to outside. Or assign the specific **tag** number to configure.

To configure the summary routing information, use the following command.

Command	Mode	Description
summary-address *A.B.C.D/M*	Router	Configures the summary routing information.
summary-address *A.B.C.D/M* **not-advertise**		Blocks the transmission of summarized routing information to outside
summary-address *A.B.C.D/M* **tag** <0-4294967295>		Configures the summary routing information with a specific tag

To delete the configured summary routing information, use the following command.

Command	Mode	Description
no summary-address *A.B.C.D/M*	Router	Deletes the summary routing information.
no summary-address *A.B.C.D/M* **not-advertise**		Blocks the transmission of summarized routing information to outside
no summary-address *A.B.C.D/M* **tag** [<0-4294967295>]		Configures the summary routing information with a specific tag

12.2.19 OSPF Monitoring and Management

You can view all kinds of statistics and database recorded in IP routing table. These information can be used to enhance system utility and solve problem in case of trouble. You can check network connection and data routes through the transmission.

12.2.19.1 Displaying OSPF Protocol Information

You can verify the information of OSPF protocol. To display the information about OSPF protocol, use the following command.

Command	Mode	Description
show ip ospf	Enable Global	Shows the information about OSPF protocol.
show ip ospf <0-65535>		Shows the information about a specific process ID in OSPF protocol.
show ip protocols ospf		Shows a current status of OSPF protocol and its information.

To display OSPF routing table to ABR and ASBR, use the following command.

Command	Mode	Description
show ip ospf [<0-65535>] **border-routers**	Enable Global	Shows OSPF routing table to ABR and ASBR.

To display the OSPF database, use the following command.

Command	Mode	Description
show ip ospf [<0-65535>] **database** {**self-originate** | **max-age** | **adv-router** *A.B.C.D* }	Enable Global	Shows the OSPF database.
show ip ospf [<0-65535>] **database** {**asbr-summary** | **external** | **network** | **router** | **summary** | **nssa-external** | **opaque-link** | **opaque-area** | **opaque-as**}		
show ip ospf [<0-65535>] **database** {**asbr-summary** | **external** | **network** | **router** | **summary** | **nssa-external** | **opaque-link** | **opaque-area** | **opaque-as**} **self-originate**		
show ip ospf [<0-65535>] **database** {**asbr-summary** | **external** | **network** | **router** | **summary** | **nssa-external** | **opaque-link** | **opaque-area** | **opaque-as**} **adv-router** *A.B.C.D*		
show ip ospf [<0-65535>] **database** {**asbr-summary** | **external** | **network** | **router** | **summary** | **nssa-external** | **opaque-link** | **opaque-area** | **opaque-as**} *A.B.C.D*		

show ip ospf [<0-65535>] **database** {**asbr-summary** | **external** | **network** | **router** | **summary** | **nssa-external** | **opaque-link** | **opaque-area** | **opaque-as**} *A.B.C.D* **self-originate**		
show ip ospf [<0-65535>] **database** {**asbr-summary** | **external** | **network** | **router** | **summary** | **nssa-external** | **opaque-link** | **opaque-area** | **opaque-as**} *A.B.C.D* **adv-router** *A.B.C.D*		

To display the interface information of OSPF, use the following command.

Command	Mode	Description
show ip ospf interface [*INTERFACE*]	Enable Global	Shows the interface information of OSPF.

To display the information of neighbor route, use the following command.

Command	Mode	Description
show ip ospf [<0-65535>] **neighbor**	Enable Global	Shows the information of neighbor router.
show ip ospf [<0-65535>] **neighbor** *A.B.C.D* [**detail**]		
show ip ospf [<0-65535>] **neighbor interface** *A.B.C.D*		
show ip ospf [<0-65535>] **neighbor detail** [**all**]		
show ip ospf [<0-65535>] **neighbor all**		

To display the routing information registered in routing table, use the following command.

Command	Mode	Description
show ip ospf [<0-65535>] **route**	Enable Global	Shows the routing information which is registered in routing table.

To display the information of virtual link, use the following command.

Command	Mode	Description
show ip ospf [<0-65535>] **virtual-links**	Enable Global	Shows the information of virtual link.

12.2.19.2 Displaying Debugging Information

To display the information about the reason of problem, use the following command.

Command	Mode	Description
debug ospf [**all**]	Enable	Shows all the debugging information.
debug ospf events [**abr** | **asbr** |		Shows information about OSPF operation such as

lsa | **nssa** | **os** | **router** | **vlink**]		OSPF neighbor router, transmitted information, deciding destination router, calculating the shortest route, and so on.
debug ospf {**ifsm** | **nfsm** | **nsm** } [**events** | **status** | **timers**]		Shows the debugging information of OSPF interface.
debug ospf lsa [**flooding** | **generate** | **refresh**]		Shows information transmitted by OSPF and calculating the shortest route.
debug ospf packet {**hello** | **dd** | **ls-ack** | **ls-request** | **ls-update** | **all**} [**send** | **recv** [**detail**]]		Shows the debugging information of each packet.
debug ospf route [**ase** | **ia** | **install** | **spf**]		Shows the debugging information of OSPF routing.

To display the debugging information, use the following command.

Command	Mode	Description
show debugging ospf	Enable Global	Shows the debugging information of OSPF.

12.2.19.3 Sending SNMP Trap

To enable/disable the system to send SNMP trap message of OSPF routing information, use the following command.

Command	Mode	Description
ospf snmp-notification enable	Router	Configures the system to send SNMP trap of routing information while OSPF is running.
ospf snmp-notification disable		Disables the system to send SNMP trap of routing information while OSPF is running.

12.2.19.4 Logging Neighbor Changes

To enable/disable the system to log changes in OSFP neighbors’ state such as system up/down and reset, use the following command.

Command	Mode	Description
ospf log-neighbor-changes	Router	Enables logging of OSPF neighbor state changes
no ospf log-neighbor-changes		Disables logging of OSPF neighbor state changes

12.2.19.5 Limiting Number of Database

The LD3032 can limit the Number of Database to process in OSPF. For example, if a router connected with many of routers, it carries overload to process the database. Therefore, Limiting the Number of Database reduces the overload on system.

To configure the limiting Number of Database, use the following command.

Command	Mode	Description

max-concurrent-dd <1-65535>	Router	Configures the limiting Number of Database.

To delete the configuration, use the following command.

Command	Mode	Description
no max-concurrent-dd <1-65535>	Router	Deletes the configuration.

12.2.19.6 Maximum Process of LSA

The LD3032 can configure maximum number of LSA to process. LSA is classified as internal route LSA and external route LSA, maximum number of LSA can configure on each class.

And also, if the process of LSA is over the configured number, you can configure it to stop the process or send the caution message. When the outer route of LSA is overflowed the assigned value, you can configure it to restart OSPF after the waiting time. If the waiting time is 0, OSPF keeps the process before the administrator reboots the system.

To assign the maximum number of LSA to process in OSPF, use the following command.

Command	Mode	Description
overflow database <1-4294967294> [**hard** | **soft**]	Router	Assigns the number of LSA for internal route.
overflow database external <0-2147483647> <0-65535>		Assigns the number of LSA for external route.

When there is an overflow, **hard** configuration will stop the process, and **soft** configuration will send a caution message.

To release the configuration, use the following command.

Command	Mode	Description
no overflow database	Router	Releases the configuration for OSPF internal route.
no overflow database external [<0-2147483647>]		Releases the configuration for OSPF external route.
no overflow database external <0-2147483647> [<0-65535>]		

12.3 Open Shortest Path First Version 3 (OSPFv3)

OSPF for IPv6 modifies the existing OSPF for IPv4 to support IPv6. The fundamentals of OSPF for IPv4 remain unchanged. Some changes have been necessary to accommodate the increased address size of IPv6 and the changes in protocol semantics between IPv4 and IPv6. OSPF for IPv6 is defined in RFC 2740, which emphasizes the differences between OSPF for IPv4 and OSPF for IPv6. It contains a large number of references to the documentation of OSPF for IPv4, which makes it hard to read. This chapter tries to concatenate the two worlds to make the reading a little bit more comfortable. It starts with an overview of OSPF, including the area structure and external routes. After the overview, it opens up the protocol to get down to the implementation details: it starts with the OSPF message format, proceeds to the neighbor relationship, and finishes with the actual link state database and the calculation of the routing table.

The followings are differences between OSPF for IPv4 and OSPF for IPv6.

- **Protocol processing per-link, not per-subnet**
  IPv6 connects interfaces to links. Multiple IP subnets can be assigned to a single link and two nodes can talk directly over a single link, even if they do not share a common IP subnet. OSPF for IPv6 runs per-link instead of per-subnet. The terms "network" and "subnet" used in OSPF for IPv4 should be replaced with the term "link"; e.g., an OSPF interface now connects to a link instead of an IP subnet.

- **Removal of addressing semantics**
  IPv6 addresses are no longer present in OSPF packet headers. They are only allowed as payload information. Router-LSA and Network-LSA (yes, they still exist) do not contain IPv6 addresses. OSPF Router ID, Area ID, and Link State ID remain at 32 bits, so they can no longer take the value of an IPv6 address. Designated Routers (DRs) and Backup Designated Routers (BDRs) are now always identified by their Router ID and no longer by their IP address.

- **Use of link-local addresses**
  OSPF assumes that each interface has been assigned a link-local unicast address. All OSPF packets use the link-local address as the source address. The routers learn the link-local addresses of all their neighbors and use these addresses as the next hop address. Packets sent on virtual links, however, must use either the global or site-local IP address as the source for OSPF packets.

12.3.1 Enabling OSPFv3

To use OSPFv3 routing protocol, it must be activated as other routing protocols. After activation, configures network address and ID which is operated by OSPFv3. The following command shows steps of activating OSPFv3.

Step1

Open *Router Configuration* mode and create an OSPFv3 routing instance.

Command	Mode	Description
router ipv6 ospf [*WORD*]	Global	Opens *Router Configuration* mode with enabling OSPFv3. WORD: OSPFv3 process tag
router ipv6 vrf ospf *WORD*		Enables IPv6 VRF routing process and opens IPv6 OSPF. WORD: VRF name to asscocicate with this instance
no router ipv6 ospf [*WORD*]		Disables OSPFv3 routing protocol.

i In case that more than two OSPFv3 processes are operated, a process number should be assigned. Normally, there is one OSPFv3 which is operating in one router.

i If OSPFv3 routing protocol is disabled, all related configuration will be lost.

Step2

Configure a network ID of OSPFv3. The network ID decides IPv4 address of this network.

Command	Mode	Description
router-id *A.B.C.D*	Router	Assigns a router ID for the OSPFv3 routing process.
no router-id		Deletes a configured router ID.

In case if using **router-id** command to apply new router ID on OSPFv3 process, OSPFv3 process must be restarted to apply. Use the **clear ipv6 ospf** [*WORD*] **process** command to restart OSPFv3 process.

Command	Mode	Description
clear ipv6 ospf [*WORD*] **process**	Enable Global IPv6 OSPF	Restarts the OSPFv3 routing process.

Step 3

Use the **ipv6 router ospf** command to specify a network to operate with OSPFv3. The variable option after **area** must be IP address or OSPFv3 area ID.

To configure an operating network with OSPFv3 on the *VLAN Interface Configuration* mode after specifying the interface to be configured, use the following command.

Command	Mode	Description
ipv6 router ospf area {<0-4294967295> | *A.B.C.D*} [**instance-id** <0-255>]	Interface [VLAN]	Specifies a network with OSPFv3 area ID. 0-4294967295: OSPFv3 area ID
ipv6 router ospf area {<0-4294967295> | *A.B.C.D*} [{**instance-id** <0-255> | **tag** WORD **instance-id** <0-255> | **tag** WORD}]		

12.3.2 ABR Type Configuration

The LD3032 supports 3 types of OSPFv3 ABR which are Cisco type ABR (RFC 3509), IBM type ABR (RFC 3509), and standard RFC 2328 type.

To configure ABR type of OSPFv3, use the following command.

Command	Mode	Description
abr-type {**cisco** | **ibm** | **standard**}	Router	Selects an ABR type. cisco: cisco type ABR, RFC 3509 (default) ibm: IBM type ABR, RFC 3509 standard: RFC 2328 type
no abr-type		Deletes a configured ABR type.

12.3.3 OSPFv3 Interface

OSPFv3 configuration can be changed. Users are not required to alter all of these parameters, but some interface parameters must be consistent across all routers in an attached network.

12.3.3.1 Interface Cost

OSPFv3 protocol assigns suitable cost according to the bandwidth on the each interface to find the shortest route. The cost is used for packet routing, and routers are using the Cost to communicate.

To set an interface cost for OSPFv3, use the following command.

Command	Mode	Description
ipv6 ospf cost <1-65535>	Interface [VLAN]	Configures an interface cost for OSPFv3
ipv6 ospf cost <1-65535> **instance-id** <0-255>		

To delete a configured interface cost for OSPFv3, use the following command.

Command	Mode	Description

no ipv6 ospf cost	Interface [VLAN]	Deletes a configured an interface cost for OSPFv3.
no ipv6 ospf cost instance-id <0-255>		

12.3.3.2 Routing Protocol Interval

The following lists are sort of time interval which can be configured by user:

- **Hello Interval**
  OSPFv3 router sends Hello packet to notify existence of itself. Hello interval is that packet transmission interval.
- **Retransmit Interval**
  When router transmits LSA, it is waiting for approval information come from receiver. In this time, if there is no answer from receiver for configured time, the router transmits LSA again. Retransmit-interval is configuration of the time interval between transmission and retransmission.
- **Dead Interval**
  If there is no hello packet for the configured time. The router perceives other router is stopped working. Dead interval is configuration of the time interval which perceives other router is stopped operating.
- **Transmit Delay**
  When a router transmits LSA, the traffic can be delayed by status of communications. Transmit delay is considering of the configuration for LSA transmission time.

i The interval explained as above must be consistent across all routers in an attached network.

To configure a Hello interval, use the following command.

Command	Mode	Description
ipv6 ospf hello-interval <1-65535> [**instance-id** <0-255>]	Interface [VLAN]	Configures a Hello interval in the unit of second. 1-65535: interval value (default: 10 seconds)
no ipv6 ospf hello-interval [**instance-id** <0-255>]		Restores a Hello interval to the default value.

To configure a dead interval, use the following command.

Command	Mode	Description
ipv6 ospf dead-interval <1-65535> [**instance-id** <0-255>]	Interface [VLAN]	Configures a dead interval in the unit of second. 1-65535: interval value (default: 40 seconds)
no ipv6 ospf dead-interval [**instance-id** <0-255>]		Sets a dead interval to the default value.

To configure a retransmit interval, use the following command.

Command	Mode	Description

ipv6 ospf retransmit-interval <1-65535> [**instance-id** <0-255>]	Interface [VLAN]	Configures a retransmit interval in the unit of second. 1-65535: interval value (default: 5 seconds)
no ipv6 ospf retransmit-interval [**instance-id** <0-255>]		Sets a retransmit interval to the default value.

To configure a transmit delay, use the following command.

Command	Mode	Description
ipv6 ospf transmit-delay <1-65535> [**instance-id** <0-255>]	Interface [VLAN]	Configures a transmit delay in the unit of second. 1-65535: interval value (default: 1 second)
no ipv6 ospf transmit-delay [**instance-id** <0-255>]		Sets a transmit delay to the default value.

12.3.3.3 OSPFv3 Priority

Routers have each role to exchange the information on OSPFv3 network. DR (Designated Router) is one of essential role to get and transmit the route information in the same area. The router having the highest priority becomes DR (Designated Router). If there are routers which have same priority, the highest router ID will be DR.

Normally, router has priority 1, but it can be changed to make DR through the configuration of priority.

To configure a priority of OSPFv3 router, use the following command.

Command	Mode	Description
ipv6 ospf priority <0-255> [**instance-id** <0-255>]	Interface [VLAN]	Configures a priority of OSPFv3 router.

To delete a configured priority of OSPFv3 router, use the following command.

Command	Mode	Description
no ipv6 ospf priority [**instance-id** <0-255>]	Interface [VLAN]	Deletes a configured priority of OSPFv3 router.

12.3.3.4 OSPFv3 Network Type

There are 4 types of OSPFv3 network. Broadcast network, NBMA (Non-broadcast-multiple-access) network, Point-to-multipoint network and Point-to-point network.

User can configure OSPFv3 network as a Broadcast network or Non-broadcast network type. For example, if the network does not support multicasting it can be configured Non-broadcast type from Broadcast type, and NBMA network as a Frame relay can be broadcast network type.

NBMA type network need virtual circuit to connect routers. But Point-to-multipoint type uses virtual circuit on part of network to save the management expenses. It does not to need to configure Neighbor router to connect routers which are not directly connected. It also saves IP resources and no need to configure the process for destination router. It supports those benefits for stable network services.

Generally, the routers and Layer 3 switches are using Broadcast type network.

To select an OSPFv3 network type, use the following command.

Command	Mode	Description
ipv6 ospf network {**broadcast** | **non-broadcast** | **point-to-multipoint** | **point-to-point**} [**instance-id** <0-255>]	Interface [VLAN]	Selects an OSPFv3 network type.
no ipv6 ospf network {**broadcast** | **non-broadcast** | **point-to-multipoint** | **point-to-point**} [**instance-id** <0-255>]		Deletes a selected network type for OSPFv3.

12.3.4 Reference Bandwidth

You can change the reference bandwidth value for the cost on OSPFv3 interfaces. Each interface on which OSPFv3 is enabled has a cost associated with it. The device advertises its interfaces and their costs to OSPFv3 neighbors.

i

By default, the reference bandwidth is 100Mbps. OSPF cost of an interface is based on the port speed and reference bandwidth value.
- Cost = reference-bandwidth/ port-speed
- 10 Mbps port's cost = 100/10 = 10
- 100 Mbps port's cost = 100/100 = 1
- 1000 Mbps port's cost = 100/1000 = 0.1, which is rounded up to 1
- 2488 Mbps port's cost = 100/2488 = 0.04, which is rounded up to 1

To set the reference bandwidth for the cost calculation on OSPFv3 interfaces, use the following command.

Command	Mode	Description
auto-cost reference-bandwidth <1-4294967>	Router	Sets the reference bandwidth for the cost on interface. 1-4294967: reference bandwidth value (default: 100Mbps)

To restore the reference bandwidth to its default value and thus restore the default costs of interface to their default value, use the following command.

Command	Mode	Description
no auto-cost reference-bandwidth	Router	Restores the reference bandwidth to its default value.

12.3.5 Non-Broadcast Network

To operate NBMA type network, neighbor router configuration is needed. And IP address, Priority, Poll-interval configuration as well. Priority is information for designate router selection and it configured [0] as a default. Poll-interval is the waiting time to re-get the hello packet from dead Neighbor router. It configured 120 seconds as a default.

To configure a router communicated by non-broadcast type, use the following command.

Command	Mode	Description
ipv6 ospf neighbor *X:X::X:X* [**instance-id** <0-255>]	Interface [VLAN]	Configures a neighbor router of NBMA type. X:X::X:X: neighbor IPv6 address

To delete a configured router communicated by non-broadcast type, use the following command.

Command	Mode	Description
no ipv6 ospf neighbor *X:X::X:X* [**instance-id** <0-255>]	Interface [VLAN]	Deletes a configured neighbor router of NBMA type.

12.3.6 OSPFv3 Area

Router configuration on OSPFv3 network includes Area configuration with each interface, network. This area has various and special features. It needs to be configured pertinently to make effective management on whole of OSPFv3 network.

OSPFv3 network defines several router types to manage the Area. ABR (Area Border Router) is one of the router types to transmit information between Areas.

ASBR (Autonomous System Border Router) is using OSPFv3 on one side and using other routing protocol except for OSPFv3 on other interface or Area. ASBR exchanges area information between different routing protocols.

Area types are various. The most principle Area types are Stub Area and NSSA (Not So Stubby Area).

12.3.6.1 Default Cost of Area

The default cost of Area is configured only in ABR. ABR function is for delivering the summary default route to stub area or NSSA, in that cases the default cost of area must be required. However, ABR which does not have stub area or NSSA can not use the following command. To configure a default cost of Area, use the following command.

Command	Mode	Description
area {A.B.C.D | <0-4294967295>} **default-cost** <1-16777215>	Router	Configures a default cost of Area.

To delete a configured default cost of Area, use the following command.

Command	Mode	Description
no area {A.B.C.D | <0-4294967295>} **default-cost**	Router	Deletes a configured default cost of Area.

This command is only for ABR which is delivering summary default route to stub or NSSA.

12.3.6.2 Not So Stubby Area (NSSA)

NSSA (Not So Stubby Area) is stub Area which can transmit the routing information to Area by ASBR. On the other hand, Stub Area cannot transmit the routing information to area. To configure NSSA, use the following command.

Command	Mode	Description
area {<0-4294967295> | *A.B.C.D*} **nssa**	Router	Configures NSSA.

The following options are configurable for NSSA:

- **default-information-originate**
  This option is configuration for allowing default path of Type-7 in NSSA. It means routing path without routing information will use the interface which is allowed in default type-7 path. **metric** is for metric value, **metric-type** is for type of finding the path. **metric-type 1** uses internal path cost with external path cost as a cost, **metric type 2** always uses external cost value only.

- **no-redistribution**
  This option is configuration in NSSA for restriction to retransmit the routing information which is from outside.

- **no-summary**
  This option is for restriction to exchange routing information between OSPF areas.

- **translator-role**
  NSSA-LSA (Link State Advertisement) has three types according to the way of process type. **always** changes all NSSA-LSA into Type-5 LSA. **candidate** changes NSSA-LSA into Type-5 LSA when it is translator. **never** does not change NSSA-LSA.

NSSA uses ASBR when it transmits Stub Area or other routing protocol Area into OSPF. In this case, if other routing protocol has default path, use **default-information-originate** command to configure the all of default path is using the assigned ASBR

To configure **NSSA** with various features, use command with options. **area** <0-4294967295> **NSSA** command has 4 options as **default-information-originate**, **no-redistribution**, **no-summary**, **translator-role** and it can be selected more than 2 options without order. **default-information-originate** has **metric** <0-16777214> and **metric-type** <1-2> as an option, **translator-role** must choose one of **candidate**, **never**, **always as an options**.

The following is explaining options of command:

- **default-information-originate** or
  default-information-originate metric <0-16777214> or

default-information-originate metric-type <1-2>

- **no-redistribution**
- **no-summary**
- **translator-role** {**candidate | never | always**}

To configure NSSA with one option, use the following command.

Command	Mode	Description
area {<0-4294967295> | *A.B.C.D*} **nssa default-information-originate**	Router	Configures NSSA with one option.
area {<0-4294967295> | *A.B.C.D*} **nssa default-information-originate metric** <0-16777214>		
area {<0-4294967295> | *A.B.C.D*} **nssa default-information-originate metric-type** <1-2>		
area {<0-4294967295> | *A.B.C.D*} **nssa no-redistribution**		
area {<0-4294967295> | *A.B.C.D*} **nssa no-redistribution default-information-originate** [**metric** <0-16777214>]		
area {<0-4294967295> | *A.B.C.D*} **nssa no-redistribution default-information-originate metric-type** <1-2>		
area {<0-4294967295> | *A.B.C.D*} **nssa no-redistribution default-information-originate no-summary** [**translator-role** { **always** | **candidate** | **never** }]		
area <0-4294967295> **nssa no-redistribution default-information-originate translator-role** { **always** | **candidate** | **never** }		
area <0-4294967295> **nssa no-summary**		
area {<0-4294967295> | *A.B.C.D*} **nssa no-summary** [**no-redistribution]** **default-information-originate** [**metric** <0-16777214>]		
area {<0-4294967295> | *A.B.C.D*} **nssa no-summary** [**no-redistribution**] **default-information-originate metric-type** <1-2>		
area {<0-4294967295> | *A.B.C.D*} **nssa no-summary default-information-originate [no-redistribution]** [**translator-role** { **always** | **candidate** | **never** }]		
area {<0-4294967295> | *A.B.C.D*} **nssa no-summary no-redistribution** [**translator-role** { **always** | **candidate** | **never** }]		
area <0-4294967295> **nssa translator-role** {**candidate** | **never** | **always**}		

The following example shows how to configure NAAS with more than 2 options:

- **area** <0-4294967295> **nssa no-summary no-redistribution**
- **area** <0-4294967295> **nssa translator-role** {**candidate** | **never** | **always**} **default-information-originate metric-type** <1-2> **no-redistribution**

To delete configured NSSA, use the following command.

Command	Mode	Description
no area {<0-4294967295> | *A.B.C.D*} **nssa**	Router	Deletes configured NSSA.
no area {<0-4294967295> | *A.B.C.D*} **nssa default-information-originate**		
no area {<0-4294967295> | *A.B.C.D*} **nssa default-information-originate no-redistribution** [**no summary**]		
no area {<0-4294967295> | *A.B.C.D*} **nssa default-information-originate no-redistribution no-summary** [**translator-role** {**candidate** | **never** | **always**}]		
no area {<0-4294967295> | *A.B.C.D*} **nssa default-information-originate no-redistribution translator-role** {**candidate** | **never** | **always**}		
no area {<0-4294967295> | *A.B.C.D*} **nssa no-redistribution** [**default-information-originate**]		
no area {<0-4294967295> | *A.B.C.D*} **nssa no-redistribution default-information-originate no-summary** [**translator-role** {**candidate** | **never** | **always**}]		
no area {<0-4294967295> | *A.B.C.D*} **nssa no-redistribution** [**no-summary**] **default-information-originate translator-role** {**candidate** | **never** | **always**}		
no area {<0-4294967295> | *A.B.C.D*} **nssa no-redistribution no-summary** [**translator-role** {**candidate** | **never** | **always**}]		
no area {<0-4294967295> | *A.B.C.D*} **nssa no-redistribution translator-role default-information-originate** [**no-summary**]		
no area {<0-4294967295> | *A.B.C.D*} **nssa no-redistribution translator-role** [**no-summary**] [**default-information-originate**]		
no area {<0-4294967295> | *A.B.C.D*} **nssa no-summary** [**default-information-originate**]		
no area {<0-4294967295> | *A.B.C.D*} **nssa no-summary default-information-originate no-redistribution** [**translator-role** {**candidate** | **never** | **always**}]		
no area {<0-4294967295> | *A.B.C.D*} **nssa no-summary default-information-originate translator-role** [**no-redistribution**]		
no area {<0-4294967295> | *A.B.C.D*} **nssa no-summary no-redistribution** [**default-information-originate**]		
no area {<0-4294967295> | *A.B.C.D*} **nssa no-summary no-redistribution** [**default-information-originate**] [**translator-role]**		
no area {<0-4294967295> | *A.B.C.D*} **nssa no-summary translator-role** [**default-information-originate**] [**no-redistribution**]		
no area {<0-4294967295> | *A.B.C.D*} **nssa no-summary trans-**		

lator-role no-redistribution		
no area {<0-4294967295> | *A.B.C.D*} **nssa translator-role** [**default-information-originate**]		

Command	Mode	Description
no area {<0-4294967295> | *A.B.C.D*} **nssa translator-role default-information-originate** [**no-redistribution**] [**no-summary**]	Router	Deletes configured NSSA.
no area {<0-4294967295> | *A.B.C.D*} **nssa translator-role no-redistribution** [**default-information-originate**] [**no-summary**]		
no area {<0-4294967295> | *A.B.C.D*} **nssa translator-role no-summary** [**no-redistribution**] [**default-information-originate**]		

12.3.6.3 Area Range

In case of OSPF belongs to several Areas, Area routing information can be shown in one routing path. Like as above, various routing information of Area can be combined and summarized to transmit to outside.

To summarize and combine the routing information, use the following command.

Command	Mode	Description
area {*A.B.C.D* | <0-4294967295>} **range** *X:X::X:X /M*	Router	Configures to use summarized information for assigned path.
area {A.B.C.D | <0-4294967295>} **range** *X:X::X:X/M* {**advertise** | **not-advertise**}		

Use **advertise** option to transmit summarized routing information with using summarized information. And use the **not-advertise** option to block the transmission of summarized routing information to outside.

To release the configuration, use the following command.

Command	Mode	Description
no area {*A.B.C.D* | <0-4294967295>} **range** *X:X::X:X/M*	Router	Releases the configuration to use summarized information for assigned path

12.3.6.4 Stub Area

Stub Area is that ABR is connected to Backbone Area. If it is assigned as Stub Area, ABR will notify the default path to Stub Area and other routing protocol information will not transmit to Stub Area.

To create Stub Area, use the following command.

Command	Mode	Description
area {*A.B.C.D* | <0-4294967295>}	Router	Creates a Stub Area.

stub [**no-summary**]		

If **no-summary** option adds to Stub Area, other Area OSPFv3 routing information also can not come to Stub Area, However, it only goes to default route from ABR router. That is Totally Stubby Area.

To delete a created Stub Area, use the following command.

Command	Mode	Description
no area {*A.B.C.D* | <0-4294967295>} **stub** [**no-summary**]	Router	Deletes a created Stub Area.

12.3.6.5 Virtual Link

In OSPFv3, all areas must be connected to a backbone area. If there is a break in backbone continuity, or the backbone is purposefully portioned, you can establish a virtual link. The virtual link must be configured in both routers.

OSPFv3 network regards virtual link routers as Point-to-point router. Therefore, the Hello-interval, Retransmit-interval, Transmit-delay must be consistent across all routers in an attached network.

User can configure time period for Hello-interval, Retransmit-interval, Transmit-delay and Dead-interval to operate virtual link.

The following items describe 4 configurations for virtual link:

- **Hello-interval**
  OSPFv3 router sends Hello packet to notify existence of itself. Hello-interval is that packet transmission interval.
- **Retransmit-interval**
  When router transmits LSA, it is waiting for approval information come from receiver. In this time, if there is no answer from receiver for configured time, the router transmits LSA again. Retransmit-interval is configuration of the time interval between transmission and retransmission
- **Dead-interval**
  If there is no hello packet for the configured time. The router perceives other router is stopped working. Dead-interval is configuration of the time interval which perceives other router is stopped operating.
- **Transmit-delay**
  When a router transmits LSA, the traffic can be delayed by status of communications. Transmit-delay is considering of the configuration for LSA transmission time.

Configuration for virtual link can be selected more than 2 options without order. The following is explaining options of command:

- **hello-interval** <1-65535>
- **retransmit-interval** <1-65535>
- **dead-interval** <1-65535>

- **transmit-delay** <1-65535>

To configure a virtual link with one option, use the following command.

Command	Mode	Description
area {*A.B.C.D* | <0-4294967295>} **virtual-link** *A.B.C.D* [**instance-id** <0-255>]	Router	Configures a virtual link.
area {*A.B.C.D* | <0-4294967295>} **virtual-link** *A.B.C.D* {**hello-interval** | **retransmit-interval** | **dead-interval** | **transmit-delay**} <1-65535>		

To delete a configured virtual link, use the following command.

Command	Mode	Description
no area {*A.B.C.D* | <0-4294967295>} **virtual-link** *A.B.C.D* [**instance-id**]	Router	Deletes a configured virtual link.
no area {*A.B.C.D* | <0-4294967295>} **virtual-link** *A.B.C.D* {**hello-interval** | **retransmit-interval** | **dead-interval** | **transmit-delay**}		

12.3.7 Default Metric

OSPFv3 finds metric based on interface bandwidth. For example, default metric of T1 link is 64, but default metric of 64K line is 1562. If there are plural lines in the bandwidth, you can view costs to use line by assigning metric to each line.

To classify costs to use line, use the following command.

Command	Mode	Description
auto-cost reference-bandwidth <1-4294967>	Router	Configures default metric in the unit of Mbps. (default: 100Mbps)

To delete the configuration, use the following command.

Command	Mode	Description
no auto-cost reference-bandwidth	Router	Deletes the configuration.

12.3.8 Graceful Restart Support

You need to restart OSPFv3 protocol processor when there is network problem. In this case, it takes long time to restarts OSPFv3 and there is no packet transmission. Other routers are also need to delete routing information and register it again. Graceful Restart improves those inconveniences. Although OSPFv3 is restarting, Graceful Restart makes the transmission of a packet with routing information.

To configure the Graceful Restart, use the following command.

Command	Mode	Description
capability restart graceful	Router	Configures the Graceful Restart.
no capability restart		Releases the configuration.

To configure the additional options for Graceful Restart, use the following command.

Command	Mode	Description
ipv6 ospf restart grace-period <1-1800>	Global	Configures the additional options for Graceful Restart. only-reload: helps only on software reloads. only-upgrade: helps only on software upgrades. max-grace-period <1-1800> : helps only if received grace-period is less than this value. router-id: router of neighbor to never to act as helper.
ipv6 ospf restart helper max-grace-period <1-1800>		
ipv6 ospf restart helper max-grace-period <1-1800> **only-reload** [**only-upgrade**]		
ipv6 ospf restart helper max-grace-period <1-1800> **only-upgrade** [**only-reload**]		
ipv6 ospf restart helper only-reload [**only-upgrade**]		
ipv6 ospf restart helper only-reload only-upgrade max-grace-period <1-1800>		
ipv6 ospf restart helper only-reload max-grace-period <1-1800> [**only-upgrade**]		
ipv6 ospf restart helper only-upgrade [**only-reload**]		
ipv6 ospf restart helper only-upgrade only-reload max-grace-period <1-1800>		
ipv6 ospf restart helper only-upgrade max-grace-period <1-1800> [**only-reload**]		

To release the configuration, use the following command.

Command	Mode	Description
no ipv6 ospf restart grace-period	Global	Releases the configuration. Never: prevent the neighbor from entering helper mode. A.B.C.D: router ID of neighbor tonever to act as helper.
ipv6 ospf restart helper never [router-id *A.B.C.D***]**		
no ipv6 ospf restart helper max-grace-period		

12.3.9 Default Route

You can configure ASBR (Autonomous System Boundary Router) to transmit default route to OSPF network. Autonomous System Boundary router transmits route created externally to OSPF network. However, it does not create system default route.

To have autonomous System Boundary router create system default route, use the following command.

Command	Mode	Description
default-information originate	Router	Configures the default route.

The following items are detail options for the Default Route configuration.

- **metric**
  Configures Metric value of the default route.
- **metric-type 1 | 2**
  is for type of finding the path. **metric-type 1** uses internal path cost with external path cost as a cost, **metric type 2** always uses external cost value only.
- **always**
  Transmits the default route to outside.
- **route-map**
  Transmits specific routing information to assigned route which has MAP-NAME.

The detail options for default route configuration are classified in 4 as above, and those configurations can be selected more than 2 options without order.

The following is explaining options of command:

- **metric** <0-16777214>
- **metric-type** <1-2>
- **always**
- **route-map** *MAP-NAME*

To configure the default route with an option, use the following command.

Command	Mode	Description
default-information originate metric <0-16777214>	Router	Configures the default route with one option.
default-information originate metric-type {**1** | **2**}		
default-information originate always		
default-information originate route-map *MAP-NAME*		

To delete the configuration, use the following command.

Command	Mode	Description
no default-information originate	Router	Deletes the configuration.
no default-information originate metric <0-16777214>		
no default-information originate metric-type {**1** | **2**}		

no default-information originate always		
no default-information originate route-map *MAP-NAME*		

12.3.10 External Routes to OSPFv3 Network

If other routing protocols redistribute into OSPFv3 network, these routes become OSPFv3 external routes. Other routing protocols are static route, connected route, kernel route that are external route. Those routing information can distribute into OSPFv3 network.

There are 3 kinds of additional configuration about external routes to OSPFv3 network. **metric** is configures Metric value of the default route, **metric-type** is for type of finding the path. **metric-type 1** uses internal path-cost with external path-cost as a cost, metric type 2 always uses external cost value. **route-map** is transmission of specific routing information to assigned route which has MAP-NAME.

Those 3 kinds of additional configuration can be selected more than 2 options without order, and it applies to consistent across all external routes in an attached network.

The following is explaining 3 options of command:

- **metric** <0-16777214>
- **metric-type** <1-2>
- **route-map** *MAP-NAME*

To configure the external route transmission, use the following command.

Command	Mode	Description
redistribute { **kernel** | **connected** | **static** | **bgp**}	Router	Advertises the external route (connected, kernel, static) into OSPFv3.
redistribute { **kernel** | **connected** | **static** | **bgp** } **metric** <0-16777214>		Specifies redistributing routes from other protocols into OSPFv3. connected: connected routes kernel: kernel routes static: IP static routes metric: specifies the external metric metric-type: specifies the external metric-type route-map: specifies name of the route-map
redistribute { **kernel** | **connected** | **static** | **bgp** } **metric-type** <1-2>		
redistribute { **kernel** | **connected** | **static** | **bgp** } **route-map** *MAP-NAME*		

To delete the configured external route transmission, use the following command.

Command	Mode	Description
no redistribute { **kernel** | **connected** | **static** | **bgp** }	Router	Deletes the configured external route transmission.

For efficient transmission of routing information, and to avoid non-matching between metric and OSPF routing protocol, use the **default-matric** command to assign metric about redistribute route.

To configure the default metric, use the following command.

Command	Mode	Description
default-metric <1-16777214>	Router	Configures the default metric.

To delete the default metric, use the following command.

Command	Mode	Description
no default-metric	Router	Deletes the default metric.

12.3.11 Passive Interface

The passive interface which is configured by OSPFv3 network accepts routing updates. Therefore a passive interface does not send the OSPFv3 routing updates. To set an interface or all interfaces as passive interface(s), use the following command.

Command	Mode	Description
passive-interface *INTERFACE*	Router	Configures an interface as passive.
passive-interface all		Sets all interfaces as passive.

To release the configured passive interface, use the following command.

Command	Mode	Description
no passive-interface *INTERFACE*	Router	Releases the configured passive interface.
no passive-interface all		

12.3.12 Summary Routing Information

You can use **not-advertise** option command to block routes that match the specified prefix/length pair. Or use the specific **tag** value that can be used a “match” value for controlling redistribution using route maps.

To create aggregate addresses for the OSPFv3 protocol, use the following command.

Command	Mode	Description
summary-address *X:X::X:X/M*	Router	Creates the aggregate addresses for OSPFv3.
summary-address *X:X::X:X/M* **not-advertise**		Blocks routes that match the specified prefix/length pair.
summary-address *X:X::X:X/M* **tag** <0-4294967295>		Configures the summary routing information with a specific tag

To delete the specified aggregate addresses for the OSPFv3, use the following command.

Command	Mode	Description
no summary-address *X:X::X:X/M*	Router	Deletes the specified aggregate addresses
no summary-address *X:X::X:X/M* {**not-advertise** | **tag** <0-4294967295>}		

12.3.13 Finding Period

OSFP start to find the shortest path as soon as got a notification of changing the network component. You can configure the period to find the path. To configure the period of finding, use the following command.

Command	Mode	Description
timers spf *SPF-DELAY SPF-HOLD*	Router	Configures the period of finding in the unit of second. SPF-DELAY: 0-2147483647 (defaut: 5000, 5 secs) SPF-HOLD: 0-2147483647
timers spf exp *SPF-MINIMUM SPF-MAXIMUM*		Configures the period using the exponential backoff delays. SPF-MINIMUM: 0-2147483647 (defaut: 5000, 5 secs) SPF-MAXIMUM: 0-2147483647

To release the configuration, use the following command.

Command	Mode	Description
no timers spf	Router	Release the configuration.

12.3.14 OSPFv3 Distance

OSPFv3 uses three different administrative distances: intra-area, inter-area, and external. Routes learned through other domain are external, routes to another area in OSPFv3 domain are inter-area, and routes inside an area are intra-area. The default distance for each type of route is 110. In order to change any of the OSPFv3 distance values, use the following commands.

The following is explaining 3 options of command.

- **external** <1-254>
- **inter-area** <1-254>
- **intra-area** <1-254>

To configure the distance with 1 option, use the following command.

Command	Mode	Description
distance <1-255>	Router	Configures the distance of OSPFv3 route. (default: 110)
distance ospfv3 external <1-254>		
distance ospfv3 inter-area <1-254>		
distance ospfv3 intra-area <1-254>		

The following example shows how to configure the distance with more than 2 options:

- **distance ospfv3 external** <1-254> **inter-area** <1-254>
- **distance ospfv3 inter-area** <1-254> **intra-area** <1-254>

To make it as a default, use the following command.

Command	Mode	Description
no distance ospfv3	Router	Restores it as the default.
no distance <1-254>		Deletes a configured distance of OSPFv3 route.

12.3.15 OSPFv3 Monitoring and Management

You can view all kinds of statistics and database recorded in IP routing table. This information can be used to enhance system utility and solve problem in case of trouble. You can check network connection and data routes through the transmission.

12.3.15.1 Displaying OSPFv3 Information

To display the information about OSPFv3 protocol, use the following command.

Command	Mode	Description
show ipv6 ospf	Enable Global	Shows the information about OSPFv3 protocol.
show ipv6 ospf *WORD*		Shows the information about a specific process ID in OSPFv3 protocol.
show ipv6 protocols ospf		Shows a current status of OSPFv3 protocol and its information.

To display the OSPFv3 database, use the following command.

Command	Mode	Description
show ipv6 ospf [*WORD*] **database**	Enable Global	Shows the OSPFv3 database.
show ipv6 ospf [*WORD*] **database** { **external** | **network** | **router** | **inter-router** | **inter-prefix** | **link** | **nssa-external** | **intra-prefix**} [**adv-router** *A.B.C.D*]		

To display the interface information of OSPFv3, use the following command.

Command	Mode	Description
show ipv6 ospf interface [{**gigabitethernet** | **tengigabitethernet** | **gpon** | **channelgroup**} *IFPORTS*]	Enable Global Router	Shows the interface information of OSPFv3

To display the information of neighbor route, use the following command.

Command	Mode	Description
show ipv6 ospf [*WORD*] **neighbor**	Enable Global	Shows the information of neighbor router.
show ipv6 ospf [*WORD*] **neighbor** *A.B.C.D*		
show ipv6 ospf [*WORD*] **neighbor** *INTERFACE* [**detail**]		
show ipv6 ospf [*WORD*] **neighbor detail**		

To display OSPFv3 paths to OSPF routers, use the following command.

Command	Mode	Description
show ipv6 ospf [*WORD*] **topology**	Enable Global	Shows the OSPFv3 paths to OSPF routers.
show ipv6 ospf [*WORD*] **topology area** {<0-4294967295 | *A.B.C.D*}		

To display the routing information which is registered in routing table, use the following command.

Command	Mode	Description
show ipv6 ospf [*WORD*] **route**	Enable Global	Shows the routing information which is registered in routing table.

To configure the format of displaying OSPFv3 routing table, use the following command.

Command	Mode	Description
ipv6 ospf display route single-line	Global	Configures the format of displaying entries in OSPFv3 routing table in single line.
no ipv6 ospf display route single-line		Deletes a configured format of displaying OSPFv3 routing table.

To display the information of virtual link, use the following command.

Command	Mode	Description
show ipv6 ospf [*WORD*] **virtual-links**	Enable Global	Shows the information of virtual link.

12.3.15.2 Logging Neighbor Changes

To enable/disable the system to log changes in OSFPv3 neighbors' state such as system up/down and reset, use the following command.

Command	Mode	Description
ospf log-neighbor-changes	Router	Enables logging of OSPFv3 neighbor state changes
no ospf log-neighbor-changes		Disables logging of OSPFv3 neighbor state changes

12.3.15.3 Limiting Number of Database

The LD3032 can limit the Number of Database to process in OSPF. For example, if a router connected with many of routers, it carries overload to process the database. Therefore, Limiting the Number of Database reduces the overload on system.

To configure the limiting Number of Database, use the following command.

Command	Mode	Description
max-concurrent-dd <1-65535>	Router	Configures the limiting number of database.
no max-concurrent-dd		Deletes the configured number of database.

12.3.15.4 Displaying Debugging Information

The LD3032 uses debug command to find the reason of problem. Use the following command.

Command	Mode	Description
debug ipv6 ospf all	Enable	Shows all the debugging information.
debug ipv6 ospf events [**abr** | **asbr** | **os** | **router** | **vlink** | **nssa**]		Shows information about OSPF operation of OSPF neighbor router, transmitted information, deciding destination router, calculating the shortest route, and so on.
debug ipv6 ospf ifs **m** [**events** | **status** | **timers**]		Shows the debugging information of OSPF interface.
debug ipv6 ospf lsa [**flooding** | **generate** | **refresh** | **install** | **maxage**]		Shows information transmitted by OSPF and calculating the shortest route.
debug ipv6 ospf nfsm [**events** | **status** | **timers**]		Shows the debugging information of OSPF Neighbor router.
debug ipv6 ospf nsm [**interface** | **redistribute**]		Shows the debugging information between OSPF process and NSM (Network Services Module).
debug ipv6 ospf packet [{**hello** | **dd** | **ls-ack** | **ls-request** | **ls-update** | **send** | **recv** | **detail**}]		Shows the debugging information of each packet.
debug ipv6 ospf route [**ase** | **ia** | **install** | **spf**]		Shows the debugging information of OSPF routing.

To turn off the debugging information according to an option, use the following command.

Command	Mode	Description
no debug ipv6 ospf all	Enable	Turns off the debugging information of OSPFv3.
no debug ipv6 ospf events [**abr** | **asbr** | **os** | **router** | **vlink | nssa**]		
no debug ipv6 ospf ifsm [**events** | **status** | **timers**]		
no debug ipv6 ospf lsa [**flooding** | **generate** | **refresh** | **install** | **maxage**]		
no debug ipv6 ospf nfsm [**events** | **status** | **timers**]		
no debug ipv6 ospf nsm [**interface** | **redistribute**]		
no debug ipv6 ospf packet [{**hello** | **dd** | **ls-ack** | **ls-request** | **ls-update** | **send** | **recv** | **detail**}]		
no debug ipv6 ospf route [**ase** | **ia** | **install** | **spf**]		

To display the debugging information, use the following command.

Command	Mode	Description
show debugging ipv6 ospf	Enable Global Bridge	Shows the debugging information of OSPFv3.

12.4 Routing Information Protocol (RIP)

Routing Information Protocol (RIP), as it is more commonly used than any other Routing Protocols, for use in small, homogeneous networks. It is a classical distance-vector routing protocol with using hop count. RIP is formally defined in documents in Request For Comments (RFC) 1058 and Internet Standard (STD) 56. As IP-based networks became both more numerous and greater in size, it became apparent to the Internet Engineeing Task Force (IETF) that RIP needed to be updated. Consequently, the IETF released RFC 1388, RFC 1723 and RFC 2453, which described RIP v2 (the second version of RIP).

RIP v2 uses broadcast User Datagram Protocol (UDP) data packets to exchange routing information. The LD3032 sends routing information and updates it every 30 seconds. This process is termed advertised. If a router does not receive an update from another router for 180 seconds or more, it marks the routes served by the non-updating router as being unusable. If there is still no update after 120 seconds, the router removes all routing table entries for the non-updating router.

The metric that RIP uses to rate the value of different routes is hop count. The hop count is the number of routers that should be traversed through the network to reach the destination. A directly connected network has a metric of zero; an unreachable network has a metric of 16. This short range of metrics makes RIP an unsuitable routing protocol for large networks.

A router that is running RIP can receive a default network via an update from another router that is running RIP, or the router can source (generate) the default network itself with RIP. In both cases, the default network is advertised through RIP to other RIP neighbors. RIP sends updates to the interfaces in the specified networks.

If an interface's network is not specified, it will not be advertised in any RIP update. The LD3032 supports RIP version 1 and 2.

12.4.1 Enabling RIP

To use RIP protocol, you should enable RIP.

Step 1 To open *Router Configuration* mode, use the following command on *Global Configuration* mode.

Command	Mode	Description
router rip	Global	Opens *Router Configuration* mode and operates RIP routing protocol.
no router rip		Restores all configurations involved in RIP to the default.

Step 2 Configure the network to operate as RIP.

Command	Mode	Description
network {*A.B.C.D/M* | *INTERFACE* }	Router	Establishes the network to operate as RIP. A.B.C.D/M: IP prefix (e.g. 35.0.0.0/8) INTERFACE: interface name
no network {*A.B.C.D/M* | *INTERFACE* }		Removes a specified network to operate as RIP.

The command **network** enables RIP interfaces between certain numbers of a special network address. For example, if the network for 10.0.0.0/24 is RIP enabled, this would result in all the addresses from 10.0.0.0 to 10.0.0.255 being enabled for RIP.

By the way, it's not possible to exchange the RIP routing information if it hasn't been established RIP network using **network** command even though interface belongs to RIP network. RIP packets with RIP routing information is transmitted to port specified with the **network** command.

12.4.2 RIP Neighbor Router

Since RIP is broadcast protocol, routers should be connected each other to transmit the routing information of RIP to non-broadcast network.

To configure neighbor router to transmit RIP information, use the following command on *Router Configuration* mode.

Command	Mode	Description
neighbor *A.B.C.D*	Router	Configures a neighbor router to exchange routing information. A.B.C.D: neighbor address
no neighbor *A.B.C.D*		Deletes the neighbor router.

i

You can block the routing information to specific interface by using the **passive-interface** command.

12.4.3 RIP Version

Basically, the LD3032 supports RIP version 1 and 2. However, you can configure to receive either RIP v1 type packets only or RIP v2 type packets only.

To configure RIP version, use the following command.

Command	Mode	Description
version {**1** | **2**}	Router	Selects one type of RIP packets to transmit either RIP v1 or RIP v2 type packet
no version {**1** | **2**}		Restores the default of specified RIP version type

The preceding task controls default RIP version settings. You can override the routers RIP version by configuring a particular interface to behave differently.

To control which RIP version an interface sends, perform one of the following tasks after opening *Interface Configuration* mode.

Command	Mode	Description
ip rip send version 1	Interface [VLAN]	Sends RIP v1 type packet only to this interface.
ip rip send version 2		Sends RIP v2 type packet only to this interface.
ip rip send version 1-compatible		Sends RIP v1-compatible type packet to this interface.
ip rip send version 1 2		Sends RIP v1 and RIP v2 type packets both.
ip rip send version 2 1		

To delete the configuration that sends RIP version packet to interface, use the following command.

Command	Mode	Description
no ip rip send version 1	Interface [VLAN]	Deletes the configuration of RIP v1 type packet for helping them to be sent to the interface.
no ip rip send version 2		Deletes the configuration of RIP v2 type packet for helping them to be sent to the interface.
no ip rip send version [**1 2**]		Deletes the configuration of both RIP v1 and v2 type packets for helping them to be sent to the interface.
no ip rip send version 1-compatible		Deletes the configuration of RIP v1-compatible type packet for helping them to be sent to the interface.

Similarly, to control how packets received from an interface are processed, perform one of the following tasks.

Command	Mode	Description
ip rip receive version 1	Interface [VLAN]	Receives RIP v1 type packet only from the interface.
ip rip receive version 2		Receives RIP v2 type packet only from the interface.
ip rip receive version 1 2		Receives both RIP v1 and RIP v2 type packets from the interface.

To delete the configuration that receives RIP version packet from the interface, use the following command.

Command	Mode	Description
no ip rip receive version 1	Interface [VLAN]	Deletes the configuration of RIP v1 type packet for helping them be received from the interface.
no ip rip receive version 2		Deletes the configuration of RIP v2 type packet for helping them to be received from interface.
no ip rip receive version 1 2		Deletes the configuration of both RIP v1 and RIP v2 type packets for helping them to be received from the interface.

12.4.4 Creating available Static Route only for RIP

This **route** command creates static route available only for RIP. If you are not familiar with RIP protocol, you would better use **redistribute static** command.

Command	Mode	Description
route *A.B.C.D/M*	Router	Creates suitable static route within RIP environment only. A.B.C.D/M: IP prefix
no route *A.B.C.D/M*		Deletes this static route established by route command.

12.4.5 Redistributing Routing Information

The LD3032 can redistribute the routing information from a source route entry into the RIP tables. For example, you can instruct the router to re-advertise connected, kernel, or static routes as well as other routes established by routing protocol. This capability applies to all the IP-based routing protocols.

To redistribute routing information from a source route entry into the RIP table, use the following command.

Command	Mode	Description
redistribute {**kernel** | **connected** | **static** | **ospf** | **bgp**}	Router	Registers transmitted routing information in another router's RIP table. 1-16: metric value WORD: pointer to route-map entries
redistribute {**kernel** | **connected** | **static** | **ospf** | **bgp** } **metric** <0-16>		
redistribute {**kernel** | **connected** | **static** | **ospf** | **bgp** } **route-map** *WORD*		

To delete the configuration for redistributing routing information in another router's RIP table, use the following command.

Command	Mode	Description
no redistribute {**kernel** | **connected** | **static** | **ospf** | **bgp**}	Router	Removes the configuration of transmitted routing information in another router's RIP table.
no redistribute {**kernel** | **connected** | **static** | **ospf** | **bgp** } **metric** <0-16>		
no redistribute {**kernel** | **connected** | **static** | **ospf** | **bgp**} **route-map** *WORD*		

As the needs of the case demand, you may also conditionally restrict the routing information between the two networks using **route-map** command.

To permit or deny the specific information, open the *Route-map Configuration* mode using the following command in *Global Configuration* mode.

Command	Mode	Description
route-map *TAG* {**deny** | **permit**} <0-65535>	Global	Creates the route map. TAG: route map tag 0-65535: sequence number
no route-map *TAG* [{**deny** | **permit**} <0-65535>]		Deletes the route map.

12.4.6 Metrics for Redistributed Routes

The metrics of one routing protocol do not necessarily translate into the metrics of another. For example, the RIP metric is a hop count and the OSPF metric is a combination of five quantities. In such situations, an artificial metric is assigned to the redistributed route. Because of this unavoidable tampering with dynamic information, carelessly exchanging routing information between different routing protocols can create routing loops, which can seriously degrade network operation. To prevent this situation, we configure metrics for this redistributed routes.

To set metrics for redistributed routes, use the following command.

Command	Mode	Description
default-metric <1-16>	Router	Configures the equal metric of all routes transmitted by routing protocol, enter the value. 1-16: default metric value
no default-metric [<1-16>		Removes the equal metric of all routes transmitted by routing protocol.

The metric of all protocol can be configured from 0 to 4294967295. It can be configured from 1 to 16 for RIP.

12.4.7 Administrative Distance

Administrative distance is a measure of the trustworthiness of the source of the routing information.

In large scaled network, Administrative distance is the feature that routers use in order to select the best path when there are two or more different routes to the same destination from two different routing protocols. Administrative distance defines the reliability of a routing protocol. Each routing protocol is prioritized in order of most to least reliable (believable) with the help of an administrative distance value.

Remember that administrative distance has only local significance, and is not advertised in routing updates. Most routing protocols have metric structures and algorithms that are not compatible with other protocols. In a network with multiple routing protocols, the exchange of route information and the capability to select the best path across the multiple protocols are critical. Administrator should set the distance value based on whole routing networks.

To configure the administrative distance value, use the following command.

Command	Mode	Description
distance <1-255> [*A.B.C.D/M* [*ACCESS-LIST*]]	Router	Sets the administrative distance value for routes. 1-255: distance value A.B.C.D/M: IP source prefix ACCESS-LIST: access list name
no distance <1-255> [*A.B.C.D/M* [*ACCESS-LIST*]]		Deletes the administrative distance value.

12.4.8 Originating Default Information

You can set an autonomous system boundary router to generate and transmit a default route into an RIP routing domain. If you specifically set to generate a default routes into an RIP network, this router becomes an autonomous system (AS) boundary router. However, an AS boundary router does not generate a default route automatically into the RIP network.

To generate a default route into RIP by the AS boundary router, use the following command on *Router Configuration* mode.

Command	Mode	Description
default-information originate	Router	Generates a default route into RIP by the AS boundary router.
no default-information originate		Disables a default route feature.

12.4.9 Routing Information Filtering

You can limit the routing protocol information by performing the following tasks.

- Block the transmission of routing information to a particular interface. This is to prevent other systems on an interface from learning about routes dynamically.
- Provides a local mechanism for increasing the value of routing metrics.

12.4.9.1 Filtering Access List and Prefix List

The LD3032 switch is able to permit and deny conditions that you can use to filter inbound or outbound routes by access-list or prefix-list. Use the **distribute-list** command to apply the access list to routes received from or forwarded to a neighbor.

User should configure the route information for a set of deny conditions based on matching each access list or prefix list. In addition, this configuration is able to be applied on the specific interface as well as the whole routes information of switch.

To block the route information based on matching access list or prefix list, use the following command.

Command	Mode	Description
distribute-list *ACCESS-LIST* {**in** | **out**} [*INTERFACE*]	Router	Apply a specific access list or prefix list to incoming or outgoing RIP route updates on interface in order to block the route. INTERFACE: interface name ACCESS-LIST: access list name PREFIX-LIST: prefix list name
distribute-list prefix *PREFIX-LIST* {**in** | **out**} [*INTERFACE*]		

To remove the filtering access list or prefix-list to incoming or outgoing RIP route

Command	Mode	Description
no distribute-list *ACCESS-LIST* {**in** | **out**} [*INTERFACE*]	Router	Removes the application of a specific access list or prefix list to incoming or outgoing RIP route updates on interface in order to block the route.
no distribute-list prefix *PREFIX-LIST* {**in** | **out**} [*INTERFACE*]		

12.4.9.2 Disabling the transmission to Interface

To prevent other routers on a local network from learning about routes dynamically, you can keep routing update messages from being sent through a router interface. This feature applies to all IP-based routing protocols except for BGP.

Disable the routing information to transmit on this interface of router, use the following command.

Command	Mode	Description
passive-interface *INTERFACE*	Router	Disables the transmission of multicast RIP messages on the interface. INTERFACE: interface name
no passive-interface *INTERFACE*		Re-enables the transmission of RIP multicast messages on the specified interface.

12.4.9.3 Offset List

An offset list is the mechanism for increasing incoming and outgoing metrics to routes learned via RIP. You can limit the offset list with an access list.

To add the value of routing metrics, use the following command.

Command	Mode	Description
offset-list *ACCESS-LIST* {**in** | **out**} <0-16> [*INTERFACE*]	Router	Add an offset to incoming or outgoing metrics to routes learned via RIP. ACCESS-LIST: access list name 0-16: type number INTERFACE: interface name

To delete the configured value of routing metrics, use the following command.

Command	Mode	Description
no offset-list *ACCESS-LIST* {**in** | **out**} <0-16> [*INTERFACE*]	Router	Removes an offset list.

12.4.10 Maximum Number of RIP Routes

You can set the maximum number of RIP routes for using on RIP protocol. To set the maximum number of routes, use the following command.

Command	Mode	Description
maximum prefix <1-65535> [1-100]	Router	Sets the maximum number of routes of RIP. 1-65535: maximum number of RIP routes 1-100: percentage of maximum routes to generate a warning (default: 75)
no maximum prefix <1-65535> [1-100]		Removes the maximum number of routes of RIP which are set before.

12.4.11 RIP Network Timer

Routing protocols use several timers that determine such variables as the frequency of routing updates, the length of time before a route becomes invalid, and other parameters. You can adjust these timers to tune routing protocol performance to better your internet needs. The default settings for the timers are as follows.

- **Update**
  The routing information is updated once every 30 seconds. This is the fundamental timing parameter of the routing protocol. Every update timer seconds, the RIP process is supposed to send the routing table to all neighboring RIP routers.
- **Timeout**
  The default is 180 seconds. It's the interval of time in seconds after which a route is declared invalid. However, this information will be still written in routing table until the neighbor routers are notified that this route is removed from the routing table.
- **Garbage**
  The invalid information of route is deleted on the routing table every 120 seconds. Once the information of route is classified as "invalid", it's eventually removed from the routing table after 120 seconds.

To adjust the timers, use the following command.

Command	Mode	Description
timers basic *UPDATE TIMEOUT GARBAGE*	Router	Adjusts RIP network timers.
no timers basic *UPDATE TIMEOUT GARBAGE*		Restores the default timers.

12.4.12 Split Horizon

Normally, routers that are connected to broadcast type IP networks and that use distance-vector routing protocols employ the split horizon mechanism to reduce the possibility of routing loops. Split horizon blocks information about routes from being advertised by a router out any interface from which that information originated. This behavior usually optimizes communications among multiple routers, particularly when links are broken. However, with non-broadcast networks, such as Frame Relay, situations can arise for which this behavior is less than ideal. For these situations, you might want to disable split horizon.

If the interface is configured with secondary IP address and split horizon is enabled, updates might not be sourced by every secondary address. One routing update is sourced per network number unless split horizon is disabled.

To enable or disable split horizon mechanism, use the following command in *Interface Configuration* mode.

Command	Mode	Description
ip rip split-horizon [**poisoned**]	Interface [VLAN]	Enables the split horizon mechanism. poisoned: performs poisoned reverse.
no rip ip split-horizon [**poisoned**]		Disables the split horizon mechanism.

12.4.13 Authentication Key

RIP v1 does not support authentication. If you are sending and receiving RIP v2 packets, you can enable RIP authentication on an interface. The key chain determines the set of keys that can be used on the interface. If a key chain is not configured, plain text authentication can be performed using string command.

The LD3032 supports two modes of authentication on an interface for which RIP authentication is enabled: plain text authentication and MD5 authentication. The default authentication in every RIP v2 packet is plain text authentication.

i

Do not use plain text authentication in RIP packets for security purposes, because the unencrypted authentication key is sent in every RIP v2 packet. Use plain text authentication when security is not an issue, for example, to ensure that misconfigured hosts do not participate in routing.

To use RIP protocol, you should enable RIP.

Step 1

To create a name for key chain for the management, use the following command on *Global Configuration* mode.

Command	Mode	Description
key chain *WORD*	Global	Creates a name for the key chain
no key chain *WORD*		Deletes a name for the key chain

Step 2

To create a name for key chain for the management, use the following command.

Command	Mode	Description
key <0-2147483647>	Keychain-Key	Configures a key identifier for key chain

Step 3

To configure RIP authentication, use the following command.

Command	Mode	Description
ip rip authentication key-chain *NAME*	Interface [VLAN]	Enables authentication for RIP v2 packets and to specify the set of keys that can be used on an interface. NAME: name of key chain
ip rip authentication mode {**text** | **md5**}		Specifies the authentication mode. text: sends a simple text password to neighbors. If a neighbor does not have the same password, request and updates from this system are rejected. md5: sends an MD5 hash to neighbors. Neighbors must share the MD5 key to decrypt the message and encrypt the response.
ip rip authentication string *STRING*		Configures RIP authentication string which will be using on interface without Key chain. The string must be shorter than 16 characters. STRING: RIP authentication string

To disable RIP authentication, use the following command.

Command	Mode	Description
no ip rip authentication key-chain *NAME*	Interface [VLAN]	Disables authentication keys that can be used on an interface.
no ip rip authentication mode {**text** | **md5**}		Disables specified authentication mode.
no ip rip authentication string *STRING*		Removes RIP authentication string which will be using on interface without Key chain.

12.4.14 Restarting RIP

Occasionally, you should restart RIP system only when the switch is still operating while you manage and configure RIP. At this time, the switch reports the neighbors that RIP system is being restarting. It keeps previous route information until the restarting is complete in timer. To restart RIP system only, use the following command.

Command	Mode	Description
rip restart grace-period <1-65535>	Global	Restarts RIP system and set the period.
no rip restart grace-period [<1-65535>]		Removes a configured period.

12.4.15 UDP Buffer Size of RIP

RIP protocol exchanges the routing information between routers using UDP packets. The LD3032 can be configured theses UDP packets buffer size, use the following command.

Command	Mode	Description
recv-buffer size <8196-2147483647>	Router	Sets the UDP Buffer size value for using RIP. 8196-2147483647: UDP buffer size value
no recv-buffer size <8196-2147483647>		Restore the default value of UDP buffer size.

12.4.16 RIP Routing Metric Update as Cisco

To enable or disable the RIP routing metric update to conform to Cisco's implementation.

Command	Mode	Description
cisco-metric-behavior enable	Router	Enables metric updation behavior as Cisco
cisco-metric-behavior disable		Disables metric updation behavior as Cisco

12.4.17 Monitoring and Managing RIP

You can display specific router information such as the contents of IP routing tables, and databases. Information provided can be used to determine resource utilization and solve network problems. You can also discover the routing path your router’s packets are taking through the network.

12.4.17.1 Displaying RIP Protocol Information

To display RIP information, use the following command.

Command	Mode	Description
show ip rip database	Enable Global	Shows RIP information being used in router.
show ip route [**database**] **rip**		Shows a routing table information involved in RIP.
show ip protocols [**rip**]		Shows a current status of RIP protocol and its information.
show ip rip interface {channel group | gpon | tengigabitethernet } *IFPORT*	Enable	Shows RIP information of specified interface. IFPORT: interface port number
show ip rip interface vlan *VLANID*		

To clear RIP information being used in router, use the following command.

Command	Mode	Description
clear ip rip route [**bgp** | **connected** | **kernel** | **ospf** | **rip** | **static** | **all** | *A.B.C.D/M*]	Enable Global	Deletes RIP information being used in router.

12.4.17.2 Displaying Debugging Information

To quickly diagnose problems, the **debug** command is useful for customers. To enable debugging of RIP routing transactions, use the following command.

Command	Mode	Description
debug rip [**all**]	Enable	Turns on all debugging options of changed RIP information.
debug rip events		Enables a debugging of RIP event such as packet transmit and sending and changed RIP information.
debug rip nsm		Enables RIP nsm debugging.
debug rip packet [**recv** | **send**]		Shows more detailed information about RIP packet. The information includes address of packet transmission and port number.
debug rip packet [**recv** | **send**] **detail**		

To disable debugging of RIP routing transactions, use the following command.

Command	Mode	Description
no debug rip [**all**]	Enable	Turns off all debugging options of changed RIP information.
no debug rip events		Disables a debugging of RIP event such as packet transmit and sending and changed RIP information.
no debug rip nsm		Disables RIP nsm debugging.
no debug rip packet [**recv** | **send**]		Disables a debugging of RIP packets.
no debug rip packet [**recv** | **send**] **detail**		

To display the debugging information, use the following command.

Command	Mode	Description
show debugging rip	Enable Global	Shows the debugging information of RIP.

12.5 Routing Information Protocol Next Generation (RIPng)

RIP (Routing Information Protocol) is the first routing protocol for IP. Because of the technical problems, new RIP, known as RIPv2 was developed. RIPng (Routing Information Protocol Next Generation), defined in RFC 2080, is an extension of RIPv2 for support of IPv6, the next generation Internet Protocol. RIPng is an entirely different protocol and does not support IPv4.

RIPng uses the same timers and message types as RIPv2. RIPng has a 30 second update timer and a 180 second hold down timer. The metric value of RIPng is also based on hop count. The RIPng metric of a network is an integer between 1 and 15, inclusive. It is set in some manner not specified in this protocol; however, given the maximum path limit of 15, a value of 1 is usually used. A directly connected network has a metric of zero; an unreachable network has a metric of 16. RIPng sends and receives the Routing Protocol messages at UDP port 521.

The multicast IPv6 address used by RIPng is FF02::9. (Remember for RIPv2, it was Class D IPv4 address 224.0.0.9).

12.5.1 Enabling RIPng

To enable RIPng, first define the RIPng routing process and then enable RIPng on each interface. To define a RIPng routing process and open *Router Configuration* mode, use the following command on *Global Configuration* mode.

Command	Mode	Description
router ipv6 rip	Global	Opens *Router Configuration* mode and defines RIPng routing protocol.
no router ipv6 rip		Restores all configurations involved in RIPng to the default.

i

If you configure the aggregation route under Router mode, the RIPng protocol must be enabled.

To enable RIPng routing on the interface, use the following command on *Interface Configuration* mode.

Command	Mode	Description
ipv6 router rip	Interface	Enables the RIPng routing on the interface.
no ipv6 router rip		Disables the RIPng routing on the interface.

To enable/disable sending RIP route information through the specified interface, use the following command.

Command	Mode	Description
ipv6 rip send-packet	Interface	Enables this interface to send the RIP route information.
no ipv6 rip send-packet		Disables this interface to send the RIP route information.

To enable/disable receiving RIP route information through the specified interface, use the following command.

Command	Mode	Description
ipv6 rip receive-packet	Interface	Enables this interface to receive the RIP route information.
no ipv6 rip receive-packet		Disables this interface to receive RIP route information.

12.5.2 Network Aggregate

Aggregation combines the characteristics of several different routes and advertises a single route. In the example of 2 routes information of 3000:1:1:1::/64 and 3000:1:1:2::/64, the **aggregate-address** command creates an aggregate entry advertising the path for a single route of 3000:1:1::/63, consisting of all elements contained in all paths being summarized. Use this feature to reduce the size of path information, even if it was included in multiple paths that were aggregated.

To summarize route's information for the transmission, use the following command.

Command	Mode	Description
aggregate-address *X:X::X:X/M*	Router	Summarizes the information of routes and transmits it to the other RIPng routers. X:X::X:X/M: network address

To delete the aggregated route's information of specific network address, use the following command.

Command	Mode	Description
no aggregate-address *X:X::X:X/M*	Router	Disables the summarization function of routes.

12.5.3 RIP Neighbor Router

Since RIP is broadcast protocol, routers should be connected each other to transmit the routing information of RIP to non-broadcast network.

To configure neighbor router to transmit RIP information, use the following command on *Router Configuration* mode.

Command	Mode	Description
neighbor *X:X::X:X INTERFACE*	Router	Configures a neighbor router to exchange routing information. X:X::X:X: neighbor IPv6 address
no neighbor *X:X::X:X INTERFACE*		Deletes the neighbor router.

You can block the routing information to specific interface by using the **passive-interface** command.

12.5.4 Adding a Static RIPng Route

This feature is provided only by FURUKAWA ELECTRIC LATAM **route** command creates static route available only for RIPng. To add a static RIPng route, use the following command.

Command	Mode	Description
route *X:X::X:X/M*	Router	Creates suitable static route within RIPng environment only. X:X::X:X/M: IPv6 address prefix
no route *X:X::X:X/M*		Deletes this static route established by route command.

12.5.5 Redistributing Routing Information

The LD3032 can redistribute the routing information from a source route entry into the RIP tables. For example, you can instruct the router to re-advertise connected, kernel, or static routes as well as other routes established by routing protocol. This capability applies to all the IP-based routing protocols.

To redistribute routing information from a source route entry into the RIP table, use the following command.

Command	Mode	Description
redistribute {**kernel** | **connected** | **static** | **ospf** | **bgp | isis | rip**}	Router	Registers transmitted routing information in another router's RIPng table. 1-16: metric value WORD: route-map name
redistribute {**kernel** | **connected** | **static** | **ospf** | **bgp | isis | rip** } **metric** <0-16>		
redistribute {**kernel** | **connected** | **static** | **ospf** | **bgp** | **isis | rip**}		

route-map *WORD*		

To delete the configuration for redistributing routing information in another router's RIP table, use the following command.

Command	Mode	Description
no redistribute {**kernel** | **connected** | **static** | **ospf** | **bgp | isis | rip**}	Router	Removes the configuration of transmitted routing information in another router's RIPng table.

i As the needs of the case demand, you may also conditionally restrict the routing information between the two networks using **route-map** command.

12.5.6 Metrics for Redistributed Routes

The metrics of one routing protocol do not necessarily translate into the metrics of another. For example, the RIP metric is a hop count and the OSPF metric is a combination of five quantities. In such situations, an artificial metric is assigned to the redistributed route. Because of this unavoidable tampering with dynamic information, carelessly exchanging routing information between different routing protocols can create routing loops, which can seriously degrade network operation. To prevent this situation, we configure metrics for redistributed routes.

To set metrics for redistributed routes, use the following command.

Command	Mode	Description
default-metric <1-16>	Router	Configures the equal metric of all routes transmitted by routing protocol, enter the value. 1-16: default metric value
no default-metric		Removes the equal metric of all routes transmitted by routing protocol.

i The metric of all protocol can be configured from 0 to 4294967295. It can be configured from 1 to 16 for RIPng.

12.5.7 Administrative Distance

Administrative distance is a measure of the trustworthiness of the source of the routing information.

In large scaled network, Administrative distance is the feature that routers use in order to select the best path when there are two or more different routes to the same destination from two different routing protocols. Administrative distance defines the reliability of a routing protocol. Each routing protocol is prioritized in order of most to least reliable (believable) with the help of an administrative distance value.

Remember that administrative distance has only local significance, and is not advertised in routing updates. Most routing protocols have metric structures and algorithms that are not compatible with other protocols. In a network with multiple routing protocols, the exchange of route information and the capability to select the best path across the multiple protocols are critical. Administrator should set the distance value based on whole routing networks.

To configure the administrative distance value, use the following command.

Command	Mode	Description
distance <1-255> [*X:X::X:X/M* [*WORD*]]	Router	Sets the administrative distance value for routes. 1-255: distance value X:X::X:X/M: IP source prefix WORD: access list name
no distance		Deletes the administrative distance value.

12.5.8 Originating Default Information

You can set an autonomous system boundary router to generate and transmit a default route into an RIP routing domain. If you specifically set to generate a default routes into an RIP network, this router becomes an autonomous system (AS) boundary router. However, an AS boundary router does not generate a default route automatically into the RIP network.

To generate a default route into RIPng by the AS boundary router, use the following command on *Router Configuration* mode.

Command	Mode	Description
default-information originate	Router	Generates a default route into RIPng by the AS boundary router.
no default-information originate		Disables a default route feature.

12.5.9 Routing Information Filtering

You can limit the routing protocol information by performing the following tasks.

- Block the transmission of routing information to a particular interface. This is to prevent other systems on an interface from learning about routes dynamically.
- Provides a local mechanism for increasing the value of routing metrics.

12.5.9.1 Filtering Access List and Prefix List

The LD3032 is able to permit and deny conditions that you can use to filter inbound or outbound routes by access-list or prefix-list. Use the **distribute-list** command to apply the access list to routes received from or forwarded to a neighbor.

User should configure the route information for a set of deny conditions based on matching each access list or prefix list. In addition, this configuration is able to be applied on the specific interface as well as the whole routes information of switch.

To block the route information based on matching access list or prefix list, use the following command.

Command	Mode	Description
distribute-list *WORD* {**in** | **out**} [*INTERFACE*]	Router	Apply a specific access list or prefix list to incoming or outgoing RIP route updates on interface in order to block the route. INTERFACE: interface name WORD: access list name PREFIX-LIST: prefix list name
distribute-list prefix *PREFIX-LIST* {**in** | **out**} [*INTERFACE*]		

To remove the filtering access list or prefix-list to incoming or outgoing RIP route

Command	Mode	Description
no distribute-list *WORD* {**in** | **out**} [*INTERFACE*]	Router	Removes the application of a specific access list or prefix list to incoming or outgoing RIP route updates on interface in order to block the route.
no distribute-list prefix *PREFIX-LIST* {**in** | **out**} [*INTERFACE*]		

12.5.9.2 Filtering Route-map

To block the RIPng route updates based on matching route-map, use the following command.

Command	Mode	Description
route-map *WORD* {**in** | **out**} *INTERFACE*	Router	Applies a specific route-map to incoming or outgoing RIP route updates on interface in order to block the route. INTERFACE: interface name WORD: route-map name

To remove the configuration based on the route-map to incoming or outgoing RIP route updates, use the following command.

Command	Mode	Description
no route-map *WORD* {**in** | **out**} *INTERFACE*	Router	Removes the configured route-map to incoming or outgoing RIP route updates on interface in order to block the route.

12.5.9.3 Passive Interface

The passive interface which is configured by RIP network accepts routing updates. Therefore a passive interface does not send the RIP routing updates. To set an interface or all interfaces as passive interface(s), use the following command.

Command	Mode	Description
passive-interface *INTERFACE*	Router	Configures an interface as passive.

To release the configured passive interface, use the following command.

Command	Mode	Description
no passive-interface *INTERFACE*	Router	Releases the configured passive interface.

12.5.9.4 Maximum Path

To set the maximum number of parallel paths for the RIPng routing table, use the following command.

Command	Mode	Description
maximum-paths <1-8>	Router	Forwards packets over multiple paths. <1-8>: the numbers of multipath supported (defualt:1)
no maximum-paths		Deletes the configured number of parallel paths.

12.5.9.5 Offset List

An offset list is the mechanism for increasing incoming and outgoing metrics to routes learned via RIP. You can limit the offset list with an access list. To add the value of routing metrics, use the following command.

Command	Mode	Description
offset-list *WORD* {**in** | **out**} <0-16> [*INTERFACE*]	Router	Add an offset to incoming or outgoing metrics to routes learned via RIP. WORD: access list name 0-16: type number
no offset-list *WORD* {**in** | **out**} <0-16> [*INTERFACE*]		Removes an offset list.

12.5.10 Maximum Number of RIP Routes

You can set the maximum number of RIP routes for using on RIP protocol. To set the maximum number of routes, use the following command.

Command	Mode	Description
maximum prefix <1-65535> [1-100]	Router	Sets the maximum number of routes of RIP. 1-65535: maximum number of RIP routes 1-100: percentage of maximum routes to generate a warning (default: 75)
no maximum prefix		Removes the maximum number of routes of RIP which are set before.

12.5.11 RIP Network Timer

Routing protocols use several timers that determine such variables as the frequency of routing updates, the length of time before a route becomes invalid, and other parameters. You can adjust these timers to tune routing protocol performance to better your internet needs. The default settings for the timers are as follows.

- **Update**
  The routing information is updated once every 30 seconds. This is the fundamental timing parameter of the routing protocol. Every update timer seconds, the RIP process is supposed to send the routing table to all neighboring RIP routers.
- **Timeout**
  The default is 180 seconds. It’s the interval of time in seconds after which a route is declared invalid. However, this information will be still written in routing table until the neighbor routers are notified that this route is removed from the routing table.
- **Garbage**
  The invalid information of route is deleted on the routing table every 120 seconds. Once the information of route is classified as “invalid”, it’s eventually removed from the routing table after 120 seconds.

To adjust the timers, use the following command.

Command	Mode	Description
timers basic *UPDATE TIMEOUT GARBAGE*	Router	Adjusts RIP network timers. UPDATE: routing table update timer value in second (5-2147483647, default: 30 seconds) TIMEOUT: routing information timeout timer value in second (5-2147483647, default: 180 seconds) GARBAGE: garbage collection timer value in second (5-2147483647, default: 120 seconds)
no timers basic		Restores the default timers.

12.5.12 Split Horizon

Normally, routers that are connected to broadcast type IP networks and that use distance-vector routing protocols employ the split horizon mechanism to reduce the possibility of routing loops. Split horizon blocks information about routes from being advertised by a router out any interface from which that information originated. This behavior usually optimizes communications among multiple routers, particularly when links are broken. However, with non-broadcast networks, such as Frame Relay, situations can arise for which this behavior is less than ideal. For these situations, you might want to disable split horizon. If the interface is configured with secondary IP address and split horizon is enabled, updates might not be sourced by every secondary address. One routing update is sourced per network number unless split horizon is disabled.

To enable or disable split horizon mechanism, use the following command in *Interface Configuration* mode.

Command	Mode	Description
ipv6 rip split-horizon [**poisoned**]	Interface	Enables the split horizon mechanism. poisoned: performs poisoned reverse.
no rip ipv6 split-horizon [**poisoned**]		Disables the split horizon mechanism.

12.5.13 UDP Buffer Size of RIP

RIP protocol exchanges the routing information between routers using UDP packets. The LD3032 can be configured theses UDP packets buffer size, use the following command.

Command	Mode	Description
recv-buffer-size <32768-2147483647>	Router	Sets the UDP Buffer size value for using RIP. 32768-2147483647: UDP buffer size value
no recv-buffer-size		Restore the default value of UDP buffer size.

12.5.14 Metric Calculation Method

RIPng uses hop count as its metric value. Hop count is the number of routers (number of hops) from the source router through which data must pass to reach the destination network. RIPng selects the best path to a destination network based only on the number of hops to the destination network. If you have multiple paths with different bandwidth to the destination network, then RIP’s best path calculation may become wrong.

The hop count (metric value) of zebos method is increased as soon as it receives the routing updates. However, zebra (cisco) method increases the hop count (metric) after it sends the routing updates to the destination network.

To apply the sum of metric in the RIB, use the following command.

Command	Mode	Description
metric-sum rib apply	Router	Selects the metric calculation method of zebos.
no metric-sum rib apply		Selects the metric calculation method of zebra. (default)

12.5.15 Monitoring and Managing RIPng

You can display specific router information such as the contents of IP routing tables, and databases. Information provided can be used to determine resource utilization and solve network problems. You can also discover the routing path your router’s packets are taking through the network.

12.5.15.1 Displaying RIPng Protocol Information

To display RIPng information, use the following command.

Command	Mode	Description
show ipv6 rip [**database**]	Enable Global Bridge	Shows RIP information being used in router.
show ipv6 route [**database**] **rip**		Shows a routing table information involved in RIP.
show ipv6 protocols rip		Shows a current status of RIP protocol and its information.
show ipv6 rip interface [*INTERFACE*]	Enable Global	Shows RIP information of specified interface.

To clear RIPng information being used in router, use the following command.

Command	Mode	Description
clear ipv6 rip route [**bgp** | **connected** | **kernel** | **ospf** | **rip** | **static** | **all** | *X:X::X:X/M*]	Enable Global	Deletes a specific route from the RIPng route table.

12.5.15.2 Displaying Debugging Information

To quickly diagnose problems, the **debug** command is useful for customers. To enable debugging of RIP routing transactions, use the following command.

Command	Mode	Description
debug ipv6 rip [**all**]	Enable	Turns on all debugging options of changed RIP information.
debug ipv6 rip events		Enables a debugging of RIP event such as packet transmission and RIP information change.
debug ipv6 rip nsm		Enables RIP NSM debugging.
debug ipv6 rip packet [**recv** | **send**]		Shows more detailed information about RIP packet. The information includes address of packet transmission and port number.
debug ipv6 rip packet [**recv** | **send**] **detail**		

To disable debugging of RIP routing transactions, use the following command.

Command	Mode	Description
no debug ipv6 rip [**all**]	Enable	Turns off all debugging options of changed RIP information.
no debug ipv6 rip events		Disables a debugging of RIP event such as packet transmission and RIP information change.
no debug ipv6 rip nsm		Disables RIP NSM debugging.
no debug ipv6 rip packet [**recv** | **send**]		Disables a debugging of RIP packets.
no debug ipv6 rip packet [**recv** | **send**] **detail**		

To display the debugging information, use the following command.

Command	Mode	Description
show debugging ipv6 rip	Enable Global Bridge	Shows the debugging information of RIP.

12.6 Route Map for IP Routing Protocol

Route maps are used to redistribute routes between processes or for route health injection. The commands of route map are valid for RIP, BGP and OSPF. To define a route map for use with supported feature, perform the following steps:

Step1

Open *Route-Map Configuration* mode from *Global Configuration* mode to create a route map entry.

Command	Mode	Description
route-map *WORD* {**permit** | **deny**} <1-65535>	Global	Defines a route map to control filtering. WORD: route-map name
no route-map *WORD* [{**permit** | **deny**} <1-65535>]		Deletes the configured route map.

Step2

Match any routes that have a specified metric or destination network using match command.

Command	Mode	Description
match as-path *WORD*	Route-map	Matches a BGP autonomous system path access list. WORD: BGP AS path access list name
match community {<1-99> | <100-199> | *WORD* } [**exact-match**]		Specifies the BGP community list to be matched. 1-99: standard community-list number 100-199: expanded community-list number WORD: community-list name
match interface *INTERFACE*		Matches any routes with the specified next hop interface.
match ip address {<1-199> | <1300-2699> | *WORD* | **prefix-list** *WORD*}		Matches any routes that have a destination network that matches a standard or extended ACL or prefix-list. 1-199: IP access-list number 1300-2699: IP access-list number (extended range) WORD: IPv4/IPv6 ACL name or prefix-list name
match ipv6 address *WORD*		
match ipv6 address prefix-list *WORD*		
match ip next-hop {<1-199> | <1300-2699> | *WORD* | **prefix-list** *WORD* }		Matches any routes that have a next hop router address that matches a standard or extended ACL or prefix-list. 1-199: IP access-list number 1300-2699: IP access-list number (extended range) WORD: IPv4/IPv6 access-list name or prefix-list name X:X::X:X: IPv6 address of next hop
match ipv6 next-hop {*X:X::X:X* | *WORD*}		
match {**metric** | **tag**} <0-4294967295>		Matches any routes that a specified metric or tag.

Command	Mode	Description
match origin {**egp** | **igp** | **incomplete**}	Route-map	Matches BGP origin code. egp: learned via Exterior Gateway Protocol igp: local IGP incomplete: the origin of the path information is unknown or learned through other means
match route-type external {**type-1** | **type-2**}		Matches the route type.

To delete the specified match criteria, use the following command.

Command	Mode	Description
no match as-path [*WORD*]	Route-map	Removes the specified match criteria.
no match community {<1-99> | <100-199> | *WORD* } [**exact-match**]		
no match interface [*INTERFACE*]		
no match ip address [{<1-199> | <1300-2699> | *WORD*}]		
no match ip address prefix-list [*WORD*]		
no match ip next-hop {<1-199> | <1300-2699> | *WORD* | **prefix-list** [*WORD*] }		
no match ip next-hop *WORD*		
no match {**metric** | **tag**} <0-4294967295>		
no match origin {**egp** | **igp** | **incomplete**}		
no match route-type external {**type-1** | **type-2**}		

Step 3

Use the **set** command that specifies the set redistribution actions to be performed, if the match criteria are met.

Command	Mode	Description
set aggregator as <1-65535> *A.B.C.D*	Route-map	Sets the AS number for the route map and router ID.
set as-path prepend <1-65535>		Modifies an AS path for a route.
set atomic-aggregate		Sets an atomic aggregate attribute.
set community {*AA:NN* | **internet** | **local-AS** | **no-advertise** | **no-export**} [**additive**]		Sets the communities attribute. AA:NN : AA= AS number, NN = number assigned to community internet: specifies the internet local-AS: specifies no sending outside the local AS no-advertise: specifies no advertisement of this route to eBGP peers no-export: specifies no advertisement of this route to any peer
set community [**none**]		

		additive: adds to the existing communities

Command	Mode	Description
set comm-list {<1-99> | <100-199> | *WORD* } **delete**	Route-map	Deletes the matched communities from the community attribute of an inbound/outbound update when applying route-map.
set dampening [<1-45>]		Sets the route-flap dampening parameters.
set dampening <1-45> <1-20000> <1-20000> <1-255> [<1-45>]		
set extcommunity rt *AA:NN*		Sets the extended community attribute. rt: specifies the route tatget of the extended community soo: specifies the site-of-origin of the extended community
set extcommunity soo *AA:NN*		
set ip next-hop [*A.B.C.D*]		Indicates where to output packets that pass a match clause of a route map.
set ipv6 next-hop [X*:X::X:X*]		Sets an IPv6 next hop to which matching packets will be forwarded. X:X::X:X: global address of next hop
set ipv6 next-hop local *X:X::X:X*		Sets an IPv6 local address to which matching packets will be forwarded. X:X::X:X: IPv6 address of next hop
set local-preference <0-4294967295>		Sets the BGP local preference path attribute. 0-4294967295: preference value
set metric {<0-4294967295> | <+/-**metric**>}		Sets the metric value.
set metric-type {**type-1** | **type-2**}		Sets the metric type.
set origin {**egp** | **igp** | **incomplete**}		Sets the BGP origin code.
set originator-id *A.B.C.D*		Sets the originator ID attribute.
set tag <0-4294967295>		Sets a tag value of the destination routing protocol.
set vpnv4 next-hop *A.B.C.D*		Sets a VPNv4 next-hop address.
set weight <0-4294967295>		Sets the weight for the routing table.

Use the **no set** command to disable the specified set redistribution action.

Command	Mode	Description
no set aggregator as [<1-65535> *A.B.C.D*]	Route-map	Removes the specified action criteria.
no set as-path prepend [<1-65535>]		
no set atomic-aggregate		
no set community {*AA:NN* | **internet** | **local-AS** | **no-advertise** | **no-export**} [**additive**]		
no set community [**none**]		
no set comm-list {<1-99> | <100-199> | *WORD* } **delete**		

no set dampening [<1-45>]		
no set dampening <1-45> <1-20000> <1-20000> <1-255> [<1-45>]		
no set extcommunity rt [*AA:NN*]		
no set extcommunity soo [*AA:NN*]		
Command	**Mode**	**Description**
no set ip next-hop [*A.B.C.D*]	Route-map	Removes the specified action criteria.
no set local-preference [<0-4294967295>]		
no set metric {<0-4294967295> | <+/-**metric**>}		
no set metric-type {**type-1** | **type-2**}		
no set origin {**egp** | **igp** | **incomplete**}		
no set originator-id [*A.B.C.D*]		
no set tag [<0-4294967295>]		
no set vpnv4 next-hop [*A.B.C.D*]		
no set weight [<0-4294967295>]		

To display the current route map information, use the following command.

Command	Mode	Description
show route-map	Enable Global	Shows the current route map information.

12.7 Virtual Routing and Forwarding (VRF)

Virtual Routing and Forwarding (VRF) is a feature that enables multiple instances of routing table within the single router at the same time. Since the routing tables are independent, the private IP address can be used without the confliction. In general it is utilized for VPN service to provide separate routing table for each customer's network.

Virtual Private Networks (VPN) provides a secure way for customers to share the bandwidth over a common backbone network. Each VPN requires its own routing table called VRF table. Supporting multiple VRF tables allow a switch to support multiple VPNs, where IP addresses can be overlapped among the VPNs. VRF forms virtual packet forwarding/routing tables by associating one or more Layer 3 interfaces with a given VRF table. Based on the input L3 interface, a VRF ID is obtained, which is used to access the VRF table.

Provider Equipment (PE) routers maintain virtual routing tables which are per-site forwarding tables. Every site to which the PE router is attached is associated with one of these tables. A particular packet's IP destination address is looked up in a particular virtual routing table only if that packet has arrived directly from a site that is associated with that table. The PE router maintains a separate forwarding environment and a separate forwarding table for each VPN in a PE-based VPN approach.

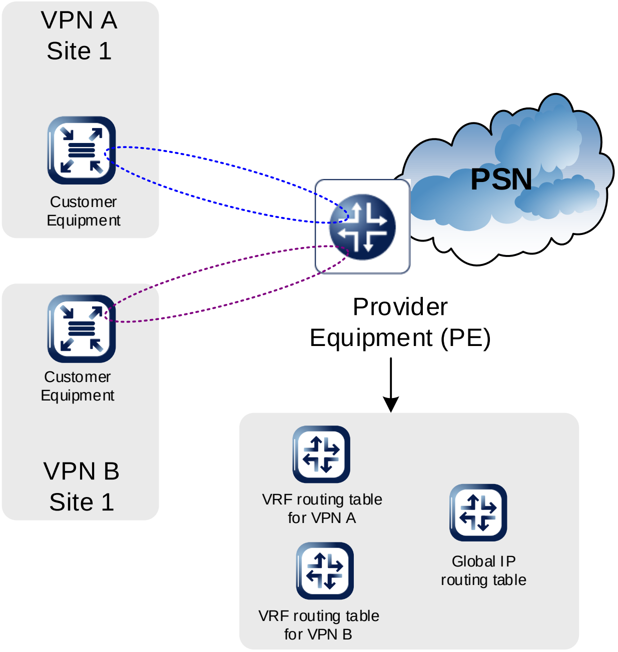


Fig. 12.1 Virtual Routing Concept

12.7.1 Creating a VRF Routing Table

VRF can be created and deleted like VLAN management. Once a VRF table is created, it can be bound with L3 interfaces which are called as VRF interfaces. The incoming packets from a VRF interface is forwarded based on the corresponding (bound) VRF table.

The static route can be added to or deleted from a VRF table, and routing protocols can also run on it.

To create a VRF table, use the following command.

Command	Mode	Description
ip vrf *WORD*	Global	Creates a VRF table. WORD: VPN routing/forwarding instance name

To delete the specified VRF table, use the following command.

Command	Mode	Description
no ip vrf *WORD*	Global	Deletes the specified VRF table. WORD: VPN routing/forwarding instance name

12.7.2 VRF Selection based on Source IP Address

The VPN Routing and Forwarding (VRF) Selection feature allows a specified interface on a provider edge (PE) router to route packets to different Virtual Private Networks (VPNs) based on the source IP address of the packet. This feature is an improvement over using a policy-based router to route packets to different VPNs.

To add a source IPv4/IPv6 address to a VRF selection table, use the following command.

Command	Mode	Description
ip vrf selection source *A.B.C.D/M* **vrf** *WORD*	Global	Adds a source IPv4 address to a VRF selection table. source: VRF selection by source IPv4 address A.B.C.D/M: source IPv4 address prefix with mask WORD: VPN routing/forwarding instance name
ipv6 vrf selection source *X:X::X:X/M* **vrf** *WORD*		Adds a source IPv6 address to a VRF selection table. source: VRF selection by source IPv6 address X:X::X:X/M: source IPv6 address prefix with mask WORD: VPN routing/forwarding instance name
no ip vrf selection source *A.B.C.D/M* **vrf** *WORD*		Removes the configured source IPv4/IPv6 address from a VRF selection table.
no ipv6 vrf selection source *X:X::X:X/M* **vrf** *WORD*		

12.7.3 Configuring VRF Routing Table

12.7.3.1 VRF Description

To add a description tag of VRF routing table, use the following command.

Command	Mode	Description
description *LINE*	VRF	Adds a description tag to a virtual routing table.

		LINE: the description for the virtual router
no description		Removes the description of virtual routing table.

12.7.3.2 Router ID

To create a router id, use the following command.

Command	Mode	Description
router-id *A.B.C.D*	VRF	Creates a router ID. A.B.C.D: router identifier in IP address format
no router-id [*A.B.C.D*]		Removes a router ID.

12.7.3.3 VRF Designated Port

To specify a designated port of a virtual router, use the following command.

Command	Mode	Description
designated-port *PORTS*	VRF	Specifies a designated port and binds this physical port to a VRF.
no designated-port *PORTS*		Deletes a specified designated port.

12.7.4 Binding an Interface to VRF

To associate an interface with a VRF, use the following command.

Command	Mode	Description
ip vrf forwarding *WORD*	Interface	Binds a specific interface to the virtual router. WORD: VPN routing/forwarding instance name
no ip vrf forwarding *WORD*		Removes the association between an interface and a VRF.

12.7.5 Enabling the Lookup

To enable/disable the lookup into a global routing table when the VRF routing table lookup fails, use the following command.

Command	Mode	Description
ip vrf onfail-use-vrf0	Interface	Enables the lookup into a global routing table.
no ip vrf onfail-use-vrf0		Disables the lookup into a global routing table.

12.7.6 VRF in the Dynamic Routing Daemons

12.7.6.1 OSPF

The OSPF process that created by this command updates the virtual routing table configured in the command line. The OSPF VRF feature is used to advertise the routing information between the CE and the PE.

The OSPF process sends the routing information that was advertised into the NSM. This is sent to the NSM server by the NSM-Protocol messaging protocol. Because the NSM message that is sent to the NSM server includes VRF-ID value, the routing information that is sent from the dynamic routing protocol to the NSM daemon makes an appropriate VRF routing table updated.

To specify the existing VRF instance in running OSPF, use the following command.

Command	Mode	Description
router ospf *WORD NAME*	Global	Specifies the VRF instance in running OSPF/OSPFv3 process. A specified OSPF/OSPFv3 process implements routing with the interfaces connected to this VRF. WORD: 1-65535, OSPF/OSPFv3 process ID NAME: VRF name to associate with this instance
router ipv6 ospf *WORD NAME*		
no router ospf *WORD NAME*		Removes the configured VRF from OSPF process
no router ipv6 ospf *WORD NAME*		

You can run a specific OSPF/OSPFv3 process with same network and neighbor per VRF instance, which was created with VPN Routing/Forwarding instance name using **ip vrf** *WORD* command.

12.7.6.2 BGP

The BGP supports the feature to advertise the routing information between CE and PE, and between PE and PE. Use the following command in order to enable address family routing process, which open you in *Address-Family Configuration* mode.

Command	Mode	Description
address-family ipv4 vrf *NAME*	Router	Opens the *Address-Family-VRF Configuration* mode to enable the exchanging of IPv4/IPv6 VRF routing information between PE and CE. NAME: VRF name
address-family ipv6 vrf *NAME*		
address-family vpnv4 [**unicast**]		Opens the *Address-Family-VPN Configuration* mode to exchange VPN routing information among ISP PE-routers.
exit-address-family	Address-Family	Exits to *AF Configuration* mode.

12.7.7 Establishing IP Static Routes for a VRF

To add a new static route entry for the specified interface, use the following command.

Command	Mode	Description
ip route vrf *WORD A.B.C.D/M GATEWAY INTERFACE* [<1-255>]	Global	Adds a new static entry to the VRF routing table. WORD: VPN Routing/Forwarding instance name A.B.C.D/M: IP destination prefix with mask GATEWAY: IP gateway address INTERFACE: IP gateway interface name 1-255: distance value for this route A.B.C.D: source IP address
ip route vrf *WORD A.B.C.D/M INTERFACE*		
ip route vrf *WORD A.B.C.D/M* **null** [<1-255>]		
ip route vrf *WORD A.B.C.D/M* { *GATEWAY* | **null** } **src** *A.B.C.D*		
ipv6 route vrf *WORD X:X::X:X/M* {*X:X::X:X* | *INTERFACE*} [<1-255>]		Adds a new static entry to the VRF routing table. WORD: VPN Routing/Forwarding instance name X:X::X:X/M: IPv6 destination prefix with mask X:X::X:X: IPv6 gateway address INTERFACE: IPv6 gateway interface name
ipv6 route vrf *WORD X:X::X:X/M X:X::X:X INTERFACE* [<1-255>]		

To remove the static route entry from VRF, use the following command.

Command	Mode	Description
no ip route vrf *WORD A.B.C.D/M*	Global	Deletes the static route entry.
no ip route vrf *WORD A.B.C.D/M GATEWAY INTERFACE* [<1-255>]		
no ip route vrf *WORD A.B.C.D/M INTERFACE*		
no ip route vrf *WORD A.B.C.D/M* **null** [<1-255>]		
no ipv6 route vrf *WORD X:X::X:X/M* [*X:X::X:X* | *INTERFACE*]		
no ipv6 route vrf *WORD X:X::X:X/M X:X::X:X* [*INTERFACE*]		

To display the routing information of the VRF, use the following command.

Command	Mode	Description
show {**ip** | **ipv6**} **route vrf** *WORD* [**database**]	Enable Global Bridge	Shows all IPv4/IPv6 routes of the virtual routing table. database: display IPv4/IPv6 routes learned by NSM
show {**ip** | **ipv6**} **route vrf** *WORD* **summary**		Shows summary counters for all routes in the IP routing table associated with a VRF.
show ip route vrf *WORD* [**database**] {**bgp** | **connected** | **kernel** | **ospf** | **static**}		Shows all IPv4/IPv6 routes of the virtual routing table for a protocol from a particular table. bgp: display selected BGP routes connected: display selected directly connected routes kernel: display selected kernel routes ospf: display selected OSPF routes static: display selected static routes
show ipv6 route vrf *WORD* [**database** **e**] { **bgp** | **connected** | **kernel** | **ospf** | **static**}		

show ip route vrf *WORD* { *A.B.C.D* | *A.B.C.D/M* }		Shows the specified IPv4/IPv6 address and IPv4/IPv6 prefix entries in the VRF routing table.
show ipv6 route vrf *WORD* { *X:X::X:X* | *X:X::X:X/M* }		

To display the FIB table that stores IPv4/IPv6 routes used for the specified VPN routing and forwarding, use the following command.

Command	Mode	Description
show ip route vrf *WORD* **fib**	Enable Global Bridge	Displays the FIB table that stores IPv4 routes actually used for the specified VPN Routing/ Forwarding. VRF-NAME: a existing VPN routing/forwarding instance name
show ipv6 route vrf *WORD* **fib**		Displays the FIB table that stores IPv6 routes actually used for the specified VPN Routing/ Forwarding. WORD: the existing VPN routing/forwarding instance name

12.7.8 Tracing Packet Route

You can discover the routes that packets will actually take when traveling to their destinations. To do this, the **traceroute** command sends probe datagrams and displays the round-trip time for each node. If the timer goes off before a response comes in, an asterisk (*) is printed on the screen.

Command	Mode	Description
traceroute *WORD* **vrf** *NAME*	Enable	Traces packet routes through the network. WORD: destination IPv4/IPv6 address or host name NAME: VPN routing/forwarding instance name
traceroute ipv6 *WORD* **vrf** *NAME*		

12.7.9 Telnet Access

To connect to a remote host via telnet, use the following command.

Command	Mode	Description
telnet {*A.B.C.D* | **ipv6** *X:X::X:X*} [**vrf** *NAME*]	Enable	Connects to a remote host via telnet. A.B.C.D | X:X::X:X: IPv4/IPv6 address or host name of a remote system TCP-PORT: TCP port number NAME: VPN routing/forwarding instance
telnet {*A.B.C.D* | **ipv6** *X:X::X:X*} *TCP-PORT* [**vrf** *NAME*]		
telnet ipv6 *X:X::X:X* **interface** *INTERFACE* [{*TCP-PORT* [**vrf** *NAME*] | **vrf** *NAME*}]		

12.7.10 VRF Network Connection (PING)

To check if your system is correctly connected to the network, use the **ping** command. For IP network, this command transmits a message to internet control message protocol (ICMP). ICMP is an internet protocol that notifies fault situation and provides information on the location where IP packet is received. When the ICMP echo message is received at the location, its replying message is returned to the place where it came from.

To perform a ping test to display network status, use the following command.

Command	Mode	Description
ping *WORD* **vrf** *NAME*	Enable	Performs a ping test to verify network status. WORD: destination IPv4 address or hostname NAME: VPN routing/forwarding instance name
ping ipv6 *WORD* [*INTERFACE*] **vrf** *NAME*		Performs a ping test to verify network status. WORD: destination IPv6 address or hostname INTERFACE: VRF interface name NAME: VPN routing/forwarding instance name

12.7.11 Displaying VRF Information

To display a list of all virtual routers and their descriptions, use the following command.

Command	Mode	Description
show ip vrf [*WORD*]	Enable Global Bridge	Shows a list of all virtual routers and their descriptions. WORD: VPN routing/forwarding instance name

To display the contents of the running configuration on a virtual router, use the following command.

Command	Mode	Description
show running-config vrf *WORD*	All	Shows the running configuration for a specific virtual router. WORD: VPN routing/forwarding instance name

13 GPON Configuration

Gigabit Passive Optical (GPON) technology has the active network elements OLT (Optical Line Termination) at the central office and ONU/ONT (Optical Network Unit / Termination) at the subscriber site.

Typical GPON configuration consists of a single PON port at the OLT and a number of ONUs connected to it over a single fiber feeder.

Generally, a Time Division Multiplexing (TDM) is used in the downstream data transmission. OLT broadcasts data to every ONUs using TDM approach. Every ONU receives each downstream frame and pinks up only that data addressed to it by the OLT. Optionally, FEC coding and AES encryption are applied to the user data.

To deliver data to OLT in upstream direction, the OLT implements a Time Division Multiple Access (TDMA) approach. ONU (ONT) receives data from the user ports and combines them into bursts. Each ONU (ONT) transmits its data in a strict accordance with the Bandwidth Map generated by OLT for the synchronization. Using DBA mechanism OLT can rearrange upstream bandwidth to provide more resources to those ONU tightly loaded with traffic.

The ONU provides network termination for a Passive Optical Network (PON) in the home or business. The ONU connects via a high speed interface to the PON network and provides subscriber access to data (Ethernet), voice (POTS) and video services. GPON gives edge networks an unparalleled bandwidth advantage in their ability to offer truly high speed triple play service (i.e. voice, video and data) especially when compared with existing cable or DSL services.

The following figure is the example of the GPON network set up.

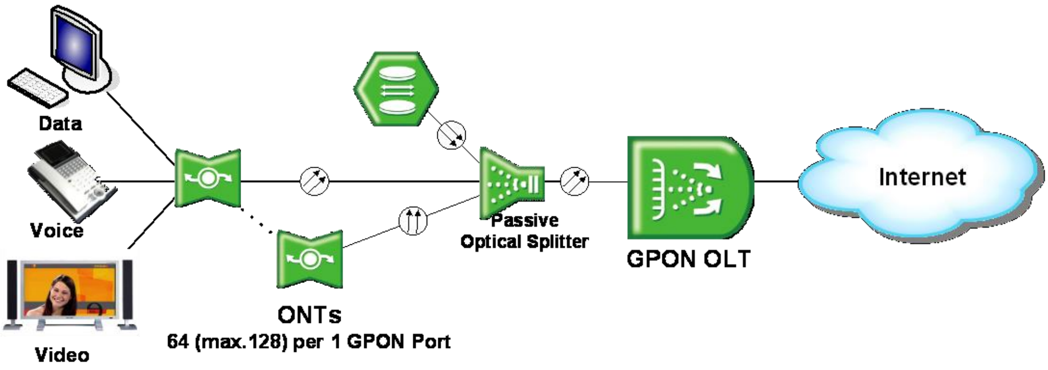


Fig. 12.2 Example of GPON Network

Basic Operation

- Configure OLT and ONU (ONT) in *GPON Interface Configuration* mode.
- For common ONU (ONT) configuration, create a profile in *ONU Profile Configuration* mode.
- If the created profile is modified, the profile will be applied to the ONUs (ONTs) automatically.

Specifying OLT ID and ONU ID

When specifying an OLT ID in the CLI, you can simply put the number in the form of *SLOT*/*PORT* such as **1/1**, **1/2**, **1/3**, **1/4, 1/5,** …**2/15**, **2/16**. Multiple input is also possible, e.g. **2/1, 2/2, 2/3** or **2/1-2/4**.

When specifying an ONU ID, just remember that the ONU ID is always between 0 and 127 or ONU serial number. Multiple input for the ONU ID is the same as the ONU ID, e.g. **1-3**, **8-22, DSNWcb00282d**.

CLI Structure

To configure GPON functionalities, enter the **interface gpon** *OLT-ID* command in *Global Configuration* mode. The *GPON Interface Configuration* mode is a stage of preparation for the detail PON configuration.

To open *GPON Interface* mode, use the following command.

Command	Mode	Description
interface gpon *OLT-ID*	Global	Opens *GPON Interface* mode.

13.1 OLT Management

This section describes how to manage an OLT. The OLT is managed in *GPON Interface Configuration* mode.

13.1.1 OLT Description

To specify or modify a description of an OLT, use the following command.

Command	Mode	Description
olt description *DESCRIPTION*	Interface [GPON]	Registers the OLT's description.
no olt description		Deletes the description of OLT.

To display a description of an OLT, use the following command.

Command	Mode	Description
show olt description [**gpon** *OLT-ID*]	Enable/Global	Shows the OLT's description.
show olt description	Interface [GPON]	

13.1.2 Activating OLT

To activate/deactivate an OLT, use the following command.

Command	Mode	Description
olt activate	Interface [GPON]	Activates a specified OLT.
olt deactivate		Deactivates a specified OLT.

13.1.3 Downstream Encryption

Encryption of downstream data is automatic process performed by OLT for specified ONU-IDs configured as encrypted. GPON OLT uses encryption key of the ONU (ONT) associated with encrypted OLT-ID. To synchronize encryption and decryption keys between OLT and ONU (ONT), you have to activate the key exchange process. For security reasons, GPON standard requires periodic key exchange for all active ONUs (ONTs) that use downstream data traffic.

Encryption of downstream data uses AES algorithm with a key generated by each ONU (ONT) and configured by GPON OLT. To enable/disable the encryption mode of downstream traffic, use the following command.

Command	Mode	Description
onu encryption *ONU-ID* **enable**	Interface [GPON]	Enables the encryption mode. ONU-ID: ONU ID (1 to 128) or ONU serial number
onu encryption *ONU-ID* **disable**		Disables the encryption mode.

To start/stop an encryption key exchange process between OLT and ONU (ONT) and specify an interval of key exchange, use the following command.

Command	Mode	Description
olt key-exchange start <10-86400>	Interface [GPON]	Starts an encryption key exchange process between OLT and ONU and specifies an exchange interval. 10-86400: interval for encryption key switchover
olt key-exchange stop		Stops periodic process of encryption key exchange.

To display the status of encryption mode or information of the encryption key exchange process, use the following command.

Command	Mode	Description
show onu encryption gpon *OLT-ID*	Enable Global	Shows the status of encryption mode. ONU-ID: ONU ID (1 to 128) or ONU serial number
show onu encryption [*ONU-ID*]	Interface [GPON]	
show olt key-exchange [**gpon** *OLT-ID*]	Enable Global	Shows the configured interval and the encryption key exchange process information.
show olt key-exchange	Interface [GPON]	

13.1.4 OLT Bandwidth

13.1.4.1 Upstream Bandwidth

To set the total amount of bandwidth in use for upstream traffic, use the following command.

Command	Mode	Description
olt total upstream-bw <1031616-1244160>	Interface [GPON]	Sets the total amount of bandwidth in use for upstream traffic. 1031616-1244160: total upstream bandwidth (default: 1120000kbps)
no olt total upstream-bw		Deleted the configured total amount of bandwidth in use for upstream traffic.

To display the information of OLT's total upstream bandwidth, use the following command.

Command	Mode	Description
show olt total upstream-bw gpon *OLT-ID*	Enable Global	Shows the total upstream bandwidth of OLT
show olt total upstream-bw	Interface [GPON]	

13.1.4.2 Bandwidth Scheduler

To allocate the bandwidth of the best effort traffic according to the fairness criterion, use the following command.

Command	Mode	Description
olt bw-scheduler be-fairness-method {**guaranteed** | **maximum**}	Interface [GPON]	Configures the bandwidth scheduler. be-fairness-method: best effort fairness method configuration guaranteed: according to guaranteed bw maximum: according to maximum bw

To display the status of OLT's bandwidth scheduler, use the following command.

Command	Mode	Description
show olt bw-scheduler [**gpon** *OLT-ID*]	Enable/Global	Shows the status of OLT's bandwidth scheduler.
show olt bw-scheduler	Interface [GPON]	

13.1.5 Auto ONU Fault Detection

If a certain ONU's laser is enabled consistently by an optical module's fault, all other normal ONUs connected to the same OLT will be deregistered; a single ONU fault may cause a whole network disruption.

Preventing such a problem, the LD3032 provides the auto ONU (ONT) fault detection feature. Normally, if an ONU (ONT) fault occurs, a specific error signal is followed by the fault. Thus, the LD3032 validates whether an ONU (ONT) fault occurs by detecting the specific error signal. The auto ONU fault detecting mechanism is as follows:

When detecting an error signal (an ONU fault) in a certain OLT, the LD3032 generates a corresponding syslog message, and then disables the laser of each ONU currently connected to the OLT one by one for 60 seconds. At the moment that the faulty ONU's laser is disabled, the error signal also disappears, then the system realizes that which the faulty ONU is and memorizes its serial number. After 60 seconds, when the disconnected ONUs (ONTs) start to enable their laser, if the ONU having the same serial number memorized before tries to enable its laser, the LD3032 disables the laser permanently. To resume the laser, the ONU needs a power reset.

To enable/disable the auto ONU fault detection, use the following command.

Command	Mode	Description
olt signal-check {**enable** | **disable**}	Interface [GPON]	Enables/disables the auto ONU (ONT) fault detection. (When an ONU fault occurs, the system will only generate the syslog message.)
olt signal-check auto-onu-block		Enables/disables the auto ONU (ONT) fault detection.

{**enable** | **disable**}		(When an ONU fault occurs, the system will disable the ONU's laser permanently.)

To display a current configuration of the auto ONU fault detection, use the following command.

Command	Mode	Description
show olt signal-check [**gpon** *OLT-ID*]	Enable/Global	Shows a current configuration of the auto ONU (ONT) fault detection.
show olt signal-check	Interface [GPON]	

To guarantee a right operation of this feature, the SIU_GPON16 and an ONU (ONT) loaded with the newest firmware are needed.

13.1.6 Maximal Distance between OLT and ONU (ONT)

PON systems distribute the bandwidth of each fiber core among up to 64 (max.128) line termination points using splitters. The actual maximum distance between OLT and ONU (ONT) is typically 20 km. The logical handling of GPON data streams however allows a distance of up to 60 km.

To determine maximal GPON distance between OLT and ONU (ONT), use the following command.

Command	Mode	Description
olt max-distance default	Interface [GPON]	Determine maximal distance between OLT and ONU. default: 0-20km 20-60: maximal distance (km)
olt max-distance <20-60>		

13.1.7 Forward Error Correction (FEC) Mode

Forward Error Correction (FEC) feature can improve the quality and reach of an optical link. FEC is implemented according to G984.3 standard, which defines the use of the code which is able to protect 239 bytes of the payload with 16 redundant bytes, allowing the receiver to detect and correct transmission errors.

To enable/disable downstream FEC mode, use the following command.

Command	Mode	Description
olt fec-mode ds enable	Interface [GPON]	Enables downstream FEC mode per OLT ID.
olt fec-mode ds disable		Disables downstream FEC mode per OLT ID.

To enable/disable upstream FEC mode, use the following command.

Command	Mode	Description
olt fec-mode us enable	Interface [GPON]	Enables upstream FEC mode per OLT ID. (Available max. bandwidth: 918912 Kbps)

olt fec-mode us disable		Disables upstream FEC mode per OLT ID.

13.1.8 MAC Aging Time

To manage a MAC table in the OLT system, use the following command.

Command	Mode	Description
olt mac aging-time <30-86400>	Interface [GPON]	Specifies MAC aging time. 30-86400: aging time (default: 300s)

13.1.9 OLT Link Down Detection

If the power of ONU is turned off by user, this ONU is supposed to send the alarm message of dying-gasp to OLT. When the last ONU is deregistered from the LD3032 after it generates an alarm by ONU dying-gasp event, we can regard that the link of this GPON port is down and it's not the cable connection problem.

To enable/disable GPON link down detection, use the following command.

Command	Mode	Description
olt cable-down enable	Global	Enables GPON link down detection
olt cable-down disable		Disables GPON link down detection

To set a number of ONUs that are deregistered without dying-gasp alarm message for detecting the PON link of OLT, use the following command.

Command	Mode	Description
olt cable-down reference-count <1-8>	Global	Sets the number of deregistered ONUs without sending dying-gasp alarms. The numbers indicate the abnormal behavior that the link of GPON port is down. 1-8: count of inactive ONU (default: 3)
no olt cable-down reference-count		Deletes a configured number of deregistered ONUs and returns to the default value.

i

To use this feature, the dying-gasp alarms should be enabled for each GPON-OLT node.

To display the state of GPON link down detection, use the following command.

Command	Mode	Description
show olt cable-down	Enable/Global	Shows the configuration of GPON link down detection.

13.1.10 OLT Transceiver

To change active GPON port of OLT manually, use the following command.

Command	Mode	Description
olt transceiver port { **a** | **b** }	Interface [GPON]	Specifies active GPON port. (default: A)

To enable/disable GPON port redundancy, use the following command.

Command	Mode	Description
olt transceiver redundancy {**enable** | **disable**}	Interface [GPON]	Enables/disables GPON port type A redundancy. (default: enable)

To display GPON port information, use the following command.

Command	Mode	Description
show olt transceiver	Interface [GPON]	Shows GPON TX port information.
show olt transceiver-type		
show olt transceiver-type gpon *IFPORT*		

13.1.11 GPON Redundancy

The LD3032 provides up to 36 GPON OLT ports, and supports the redundancy of OLT port for the stable network service. Through this function, the system can group the specific GPON ports in order to make a standby OLT port operate instead of a working one when this does not operate normally. This redundancy prevents the service from halting, and guarantees reliability of communication service.

13.1.11.1 Redundancy Type B with SIU_GPON16

The redundancy type B allows GPON redundancy by either port or card basis. Therefore, it can be configured between port #A and port #B within the same line card or different line card, or between slot 1 and 2 within the same chassis.

The following table shows OLT redundancy components.

Item	Description
Master OLT	Primary port in redundancy group. DB of this port is to be synchronized with Slave OLT.
Slave OLT	Secondary (= redundant) port in redundancy group. It copies DB from Master OLT and its own DB is initialized.
Working OLT	Active port in service in redundancy group.
Standby OLT	Standby port in redundancy group.

Tab. 12.1 OLT Redundancy Components

You can configure the OLT port redundancy by grouping two OLT ports and specifying each one to Master and Slave. Master OLT is the primary port which plays the role of criterion for DB synchronization and the configuration commands. Slave OLT is the additional port for port redundancy, whose DB is initialized and synchronized with the Master OLT's when it is configured as a redundancy group's entry.

Basically, Master OLT operates as Working OLT. If the Working OLT fails or does not receive a signal for a certain reason, a switchover to Standby OLT occurs to keep the service on.

13.1.11.2 Redundancy Group

OLT redundancy is configured based on a group ID. To configure the OLT redundancy group, use the following command.

Command	Mode	Description
olt redundancy group *GROUP-ID* **gpon** *MASTER-ID SLAVE-ID*	Global	Configures the OLT redundancy group. GROUP-ID: redundancy group ID MASTER-ID: master OLT ID SLAVE-ID: slave OLT ID
no olt redundancy group *GROUP-ID*		Deletes the configuration of the OLT redundancy group.

13.1.11.3 OLT Switchover

OLT switchover is the capability to change the role of GPON port between a standby OLT and working OLT upon the failure or abnormal operation of the previously active (working) GPON port. You can specify the criteria for OLT switchover operation by using the commands.

To configure the switchover criteria to convert working OLT into standby OLT, use the following command.

Command	Mode	Description
olt redundancy trigger los {**on** | **off**} **group** *GROUP-ID*	Global	Configures whether to perform a switchover when detecting LOS event from working OLT. GROUP-ID: redundancy group ID
olt redundancy trigger slot {**on** | **off**} **group** *GROUP-ID*		Configures whether to perform a switchover when detecting the status change on the slot that working OLT belongs to.
olt redundancy trigger gpon-mac {**on** | **off**} **group** *GROUP-ID*		Configures whether to perform a switchover when detecting abnormal status (no response, not controllable) from GPON MAC chip of working OLT.
olt redundancy trigger manual {**on** | **off**} **group** *GROUP-ID*		Configures whether to perform a switchover when a user forces a redundancy group to switch over.

When a switchover is executed, the process is pended for about two seconds for DB synchronization between working OLT and standby OLT. During this time, additional switchover is not executed even if the other condition of switchover occurs.

To automatically perform a switchover under the certain condition except for manual switchover, the RX link status of standby OLT should be "RX Detect".

The status change of the slot includes the following condition:
- The status of a slot with the working OLT is changed by the commands such as **slot restart**, **slot lock**, **slot power down**, etc.

All of the switchover conditions are enabled (on) by default.

To force a switchover from the Master OLT to the Slave OLT in a redundancy group manually, use the following command.

Command	Mode	Description
olt redundancy switchover force group *GROUP-ID*	Global	Performs a manual switchover from the master OLT to slave OLT. GROUP-ID: redundancy group ID
olt redundancy switchover group *GROUP-ID*		Performs a manual switchover from the master OLT to slave OLT. This command operates only if the RX link status of standby OLT is "RX Detect". GROUP-ID: redundancy group ID

13.1.11.4 Slave OLT Activation

To activate or deactivate a slave OLT in an OLT redundancy group, use the following command.

Command	Mode	Description
olt redundancy slave {**activate** | **deactivate**} **group** *GROUP-ID*	Global	Activates/deactivates a slave OLT in an OLT redundancy group GROUP-ID: redundancy group ID

13.1.11.5 Standby OLT Optic Status Configuration

The system checks the RX power of standby OLT every 2 seconds in order to ascertain whether to be connected to ONU normally by its optic fiber. (However, in case that any activated ONUs are not connected to working OLT, the system can not check whether the standby OLT is linked to ONU normally or not, because a standby OLT cannot detect the RX power.) When the RX power of standby OLT is detected, it reports the information to SFU in order to notify the system.

⚠ To perform a switchover automatically under the certain condition except for a manual switchover, the link status of standby OLT should be under "RX Detect" condition.

Basically, TX power of standby OLT is disabled in order not to affect working OLT. But you can enable the TX power temporarily to check whether the standby OLT operates normally or not, for the reason of replacing the board or SFP module, etc.

⚠ Be cautious when you enable the TX power of standby OLT, because it may cause problems for ONUs in service.

To configure the TX power of standby OLT, use the following command.

Command	Mode	Description
olt redundancy standby-optic enable group *GROUP-ID* <1-600>	Global	Enables TX power of standby OLT in specified redundancy group for the specified time. After the specified time period, TX power is automatically disabled. GROUP-ID: redundancy group ID 1-600: time period (unit: second)
olt redundancy standby-optic enable group *GROUP-ID* **permanent**		Enables TX power of standby OLT in specified redundancy group continuously.
olt redundancy standby-optic disable group *GROUP-ID*		Disables TX power of standby OLT.

⚠ If the system is in detecting the RX power of the standby OLT normally, the user-input command for enabling TX power does not execute.

13.1.11.6 DB Synchronization

To display the synchronization status of the active OLT and standby OLT DB, use the following command.

Command	Mode	Description
olt redundancy db-sync check group *GROUP-ID*	Global	Shows the synchronization status of the active OLT and standby OLT DB. GROUP-ID: redundancy group ID

To resynchronize the active OLT and standby OLT DB, use the following command.

Command	Mode	Description
olt redundancy db-sync resync group *GROUP-ID*	Global	Resynchronizes the active OLT and standby OLT DB. (This is executed only when two DBs are different each other.) GROUP-ID: redundancy group ID

13.1.11.7 Displaying Redundancy Information

To display the OLT redundancy configuration, use the following command.

Command	Mode	Description
show olt redundancy status	Enable Global Interface [GPON]	Shows the role of each OLT and the reason for switchover.
show olt redundancy detail-status [*GROUP-ID*]		Shows all of the detail information on all or specified redundancy group(s). GROUP-ID: redundancy group ID

i

You can check the status of RX power by using **show olt redundancy detail-status** command that shows the status information as "RX Detect".

13.1.12 Maximum Number of ONU

You can set the maximum number of ONUs (ONTs) connected to a specified OLT. To set the maximum number of ONUs, use the following command.

Command	Mode	Description
olt max-onu-count <1-128>	Interface [GPON]	Sets the maximum number of ONU connections. 1-128: maximum number of ONUs connected to a specified OLT (default: 128)
no olt max-onu-count		Removes the maximum number of ONU.

To display the configured maximum number of ONUs, use the following command.

Command	Mode	Description
show olt max-onu-count [**gpon** *OLT-ID*]	Enable/Global	Shows the configured maximum number of ONUs.
show olt max-onu-count	Interface [GPON]	

13.1.13 OLT Anti-Spoofing

When the LD3032 learns the same MAC address from the two (or more) different ONUs on the same GPON, the system regards the latest ONU(s) as the fault operation, and make the ONU(s) block the inflow of sub-level MAC by MAC filtering. Through this anti-spoofing, the LD3032 can prevent the malicious spoofing attack.

To enable/disable the OLT anti-spoofing, use the following command.

Command	Mode	Description
olt anti-spoofing enable [**expire-timeout** <60-65535>]	Interface [GPON]	Enables the OLT anti-spoofing. 60-65535: expire timeout (= MAC filtering operation time). After the configured expiration, the OLT system can learn again the MAC regarded as a fault.
olt anti-spoofing disable		Disables the OLT anti-spoofing.

To clear MAC filtering due to the anti-spoofing operation, use the following command.

Command	Mode	Description
clear olt anti-spoofing	Interface [GPON]	Clears MAC filtering being operated currently occurred by anti-spoofing function. ONU-ID: ONU ID (1-128) or serial number MAC: MAC address VID: VID
clear olt anti-spoofing *ONU-ID* [*MAC VID*]		

To display the user configuration of the OLT anti-spoofing, use the following command.

Command	Mode	Description
show olt anti-spoofing [**gpon** *OLT-ID*]	Enable/Global	Shows the user configuration of the OLT anti-spoofing.
show olt anti-spoofing	Interface [GPON]	

To display the current OLT anti-spoofing status, use the following command.

Command	Mode	Description
show olt anti-spoofing status gpon *OLT-ID*	Enable Global	Shows the current anti-spoofing MAC filtering status per ONU, MAC and VID.
show olt anti-spoofing status	Interface [GPON]	

13.1.14 ONU RX-Power Update

To configure the interval of ONU rx-power update, use the following command.

Command	Mode	Description
onu rx-power update {<1-1440> | **disable**}	Global	Configures the interval of ONU rx-power update. 1-1440: interval (unit: minute) disable: do not update

To display the configuration of ONU rx-power update, use the following command.

Command	Mode	Description
show onu rx-power update	Enable Global Interface [GPON]	Shows the configuration of ONU rx-power update.

To display the received signal power information from an ONU, use the following command.

Command	Mode	Description
show olt rx-power gpon *OLT-ID* [*ONU-ID*]	Enable Global	Shows OLT RX signal power from all ONUs.
show olt rx-power	Enable Global	Shows the configuration of OLT rx-power update.
show olt rx-power [*ONU-ID*]	Interface [GPON]	Shows OLT RX signal power from an ONU.

13.1.15 Configurations for RF Return Packet Forwarding

In case the ONUs are connected with the set-top-boxes supporting Ethernet return path capabilities, GPON OLT can use Ethernet for the return path to head-end infrastructure. Deploying an ONU/MDU with an RF to Ethernet converter enables RF-digital-RF conversion. At the ONU, the upstream return path packet is carried in GPON OLT. The GPON OLT aggregates the packets from the ONUs and sends them to the Ethernet to RF converter as the head-end node. This RF converter converts the Ethernet signals to back to RF signal.

To specify the destination MAC address, ethertype, and VLAN ID for the head-end node on the connection to send RF return path traffic, use the following command.

Command	Mode	Description
onu rf-pw dst-mac *MACADDR*	Global	Sets the destination MAC address of RF return path modulator’s FPGA.
onu rf-pw ethtype *TYPE-NUM*		Sets the ethernet type and VLAN ID for RF return path traffic forwarding. TYPE-NUM: ethernet type (e.g. 0x8864 - PPPoE)
onu rf-pw vid <1-4094>		

To delete the configured parameters for the head-end node on the connection, use the following command.

Command	Mode	Description
no onu rf-pw dst-mac	Global	Deletes the configured destination MAC address, ethernet type or VLAN ID for the head-end node connection.
no onu rf-pw ethtype		
no onu rf-pw vid		

i This feature is available for RF return modulator (V5800) only. The LD3032 is not provide compatibility with other RF return modulators.

To display the configured parameters for the head-end node, use the following command.

Command	Mode	Description
show onu rf-pw	Enable/Global Interface [GPON]	Shows the configured parameters for the head-end node to send the RF return path traffic.

13.1.16 Downstream Traffic Control

The LD3032 provides the function to control the downstream traffic based on MAC address and VLAN ID by each OLT. Basically, the OLT system creates MAC table through MAC learning with the incoming traffic from ONU, and transmits the downstream traffic to GEM port with the MAC table information. However, LD3032 can control this downstream traffic with MAC address and VLAN ID by user configuration.

To configure the downstream traffic control, use the following command.

Command	Mode	Description
olt ds-gem-mapping {**mac** | **mac-vid** | **vid** | **per-flow** [**key-mac**| **key-mac-vid**]}	Interface [GPON]	Configures the GEM port mapping mode. mac, mac-vid: GEM port mapping with destination MAC address or destination MAC address and VLAN ID vid: GEM port mapping with VLAN ID (default: mac)
onu vlan-gem-mapping *ONU-ID* **vid** *RANGE* **mapper** *MAPPER-ID*		Maps GEM port of ONU and VLAN ID. (This configuration is valid only when the GEM port mapping mode is specified as ‘vid’ and the GEM port is assigned through ONU profile configuration.) ONU-ID: ONU ID or serial number RANGE: VLAN ID range (This value should be unique by each OLT port.) MAPPER-ID: mapper number configured on Traffic Profile
onu vlan-gem-mapping all vid *RANGE* {**multicast-gem** | **broadcast-gem**}		Maps the multicast or broadcast GEM port used by all ONUs and the specified VLAN ID. RANGE: VLAN ID range

no onu vlan-gem-mapping [*ONU-ID* [**vid** *RANGE*] | **all** [**vid** *RANGE*]]		Deletes the GEM port mapping configuration above.

The traffic is not transmitted while the GEM port mapping mode is being changed due to user configuration.

To configure the downstream GEM port mode per flow, use the following command.

Command	Mode	Description
olt per-flow vid *RANGE* **mapping-method** {**mac** | **mac-vid** | **vid**}	Interface [GPON]	Configures a downstream GEM port mapping based on flow.
no olt per-flow [**vid** *RANGE*]		Deletes the configured downstream GEM port mapping per flow.

To display the configuration of downstream traffic control, use the following command.

Command	Mode	Description
show onu vlan-gem-mapping [**gpon** *OLT-ID*]	Enable Global	Shows VLAN ID mapped to GEM port of ONU.
show olt ds-gem-mapping [**gpon** *OLT-ID*]		Shows the GEM port mapping mode configured on the OLT.
show olt per-flow [**gpon** *OLT-ID*] [*VLANS*]		Shows the downstream GEM Port mode per flow.
show onu vlan-gem-mapping [*ONU-ID*]	Interface [GPON]	Shows VLAN ID mapped to GEM port of ONU.
show olt ds-gem-mapping		Shows the GEM port mapping mode configured on the OLT.
show olt per-flow [*VLANS*]		Shows the downstream GEM Port mode per flow.

If the LD3032 is configured in the downstream GEM mapping mode per flow, you can configure downstream QoS mapping mode based on MAC address / VLAN ID and the mapping between queue and CoS value. To configure the downstream traffic control by QoS mapping, use the following command.

Command	Mode	Description
olt ds-qos-mapping mode {**mac** | **vid** }	Interface [GPON]	Configures the downstream QoS mapping mode. (This configuration is valid only when the downstream GEM port mapping mode is specified as 'flow'.) mac: QoS mapping mode based on destination MAC address vid: QoS mapping mode based on VLAN ID mac vid: QoS mapping mode based on MAC + VLAN ID
olt ds-qos-mapping queue-		Configures the queue count and priority value accord-

count {**2** | **4** | **8**} [**cos-map** <0-7> <0-7> <0-7> <0-7> <0-7> <0-7> <0-7> <0-7>]		ing to CoS value. 2 | 4 | 8 : queue count 0-7 : queue number per each CoS value (CoS 0 to CoS 7)
no olt ds-qos-mapping mode		Deletes the QoS mapping configuration mode.
no olt ds-qos-mapping		Deletes the queue count and CoS-Queue mapping table.

The traffic is not transmitted while the GEM port mapping mode is being changed due to user configuration.

To display the configuration of downstream QoS mapping, use the following command.

Command	Mode	Description
show olt ds-qos-mapping [**gpon** *OLT-ID*]	Enable Global	Shows the queue count and CoS-Queue mapping table of the GPON OLT.
show olt ds-qos-mapping mode [**gpon** *OLT-ID*]		Shows the QoS mapping mode configured on the OLT.
show olt ds-qos-mapping	Interface [GPON]	Shows the queue count and CoS-Queue mapping table status.
show olt ds-qos-mapping mode		Shows the downstream QoS mapping mode.

To configure the traffic control by selecting the method of upstream flow mapping, use the following command.

Command	Mode	Description
olt us-flow-mapping per-mapper	Interface [GPON]	Selects the upstream flow mapping based on mapper. This method learns MAC addresses of incoming traffic from the several GEM port IDs associated with different ONUs to a MAPPER-defined GEM port ID.
olt us-flow-mapping per-gem		Selects the upstream flow mapping based on GEM port. This method learns MAC addresses of incoming traffic from the GEM port IDs associated with different ONUs to each GEM port ID, respectively.

To display the configured upstream flow mapping, use the following command.

Command	Mode	Description
show olt us-flow-mapping [**gpon** *OLT-ID*]	Enable/Global	Shows the upstream flow mapping status.
show olt us-flow-mapping	Interface [GPON]	

13.1.17 Multicast/Broadcast GEM Port Separation

All the downstream multicast and broadcast flows from the LD3032 are transmitted through a single GEM port ID. The multicast and broadcast flows need to be separated from each other to properly forward all broadcast/multicast traffic for multiple ONTs.

To configure a multicast GEM port ID, use the following command.

Command	Mode	Description
olt multicast-gem <4094-4095>	Global	Adds a specific GEM port ID to the multicast stream. 4094-4095: multicast GEM port ID
show olt multicast-gem	Enable Global Interface [GPON]	Shows the specified GEM port ID for multicast stream.

To enable/disable the interworking with IGMP snooping table, use the following command.

Command	Mode	Description
olt interwork igmp-snooping {**enable** | **disable**}	Global	Enables/disables the interworking with IGMP snooping table.

To add a static MAC address into the MAC table, use the following command.

Command	Mode	Description
olt static-mac *MACADDR* {**mcast** | **bcast**} [**vid** <1-4094>]	Interface [GPON]	Adds a static MAC address for multicast/broadcast stream.
olt static-mac start *MACADDR* **end** *MACADDR* {**mcast** | **bcast**} [**vid** <1-4094>]		Adds a static range of MAC addresses for multicast/broadcast stream.
no olt static-mac *MACADDR* {**mcast** | **bcast**} [**vid** <1-4094>]		Deletes the configured static MAC address.
no olt static-mac start *MACADDR* **end** *MACADDR* {**mcast** | **bcast**} [**vid** <1-4094>]		Deletes the configured static MAC address range.

To display the configured static MAC address table, use the following command.

Command	Mode	Description
show olt static-mac gpon *OLT-ID*	Enabl/Global	Shows the static MAC table.
show olt static-mac	Interface [GPON]	

13.1.18 Configuring Port/TCONT Threshold

When one GPON port is connected to a lot of ONTs with T-CONTs and GEM ports, you can specify the maximum numbers (threshold) of T-CONTs and GEM port count. So that an alarm is generated if a given threshold is exceeded.

To configure the threshold of GEM port count, use the following command.

Command	Mode	Description
olt threshold port <1-3966>	Interface [GPON]	Sets the threshold of GEM port count for ONT. 1-3966 : threshold value
no olt threshold port		Deletes the configured threshold of GEM port.

To configure the threshold of dynamic / fixed T-CONT count for ONT, use the following command.

Command	Mode	Description
olt threshold tcont dynamic *DYNAMIC_VALUE* [**fixed** *FIXED_VALUE*]	Interface [GPON]	Sets the threshold of Dynamic/Fixed T-CONT count for ONT. DYNAMIC_VALUE: 1 to 384 FIXED_VALUE: 1 to 384
olt threshold tcont fixed *FIXED_VALUE* [**dynamic** *DYNAMIC_VALUE*]		
no olt threshold tcont {**dynamic** | **fixed**}		Deletes the configured threshold of T-CONT count.

To display the configuration of GEM-port/ T-CONT threshold, use the following command.

Command	Mode	Description
show olt threshold port [**gpon** *OLT-ID*]	Enable Global	Shows the configured GEM-port/ T-CONT count threshold of ONTs.
show olt threshold tcont [**gpon** *OLT-ID*]		
show olt threshold port	Interface [GPON]	
show olt threshold tcont		

13.1.19 ONU Deactivation Monitoring

ONU deactivation monitoring function generates alarms based on ONU (ONT)'s deactivation. The system calculates the current percentage by the number change of active ONUs every hour. If the number of active ONU is reduced and the current percent is lower than a given alarm-raise percent, the deactive monitor alarm is on. If the current percent exceeds the configured alarm-clear percent, the deactive monitor alarm changes to off.

To enable/disable ONU deactivation monitoring, use the following command.

Command	Mode	Description
olt deactive-monitor {**enable** |	Interface	Enables/disables ONU deactivation monitoring func-

disable}	[GPON]	tion.

To configure ONU deactivation monitoring, use the following command.

Command	Mode	Description
olt deactive-monitor alarm-raise <1-99>	Interface [GPON]	Sets the deactive ONU-raise percent. 1-99: (default: 30%)
olt deactive-monitor alarm-clear<1-99>		Sets the deactive ONU-clear percent. If the current percent becomes higher than this value, the alarm status changes to off. 1-99: (default: 70%)
olt deactive-monitor period <10-86400>		Sets the deactive ONU monitoring period. If the current percent is higher than a alarm-raise percent, the alarm is off and the current percent changes to 100% after a period. 10-86400: deactive ONU monitoring period (default: 10 seconds)
no olt deactive-monitor alarm-raise		Deletes the configured value of deactive ONU monitoring parameters.
no olt deactive-monitor alarm-clear		
no olt deactive-monitor period		

To display the configuration of ONU deactivation monitoring, use the following command.

Command	Mode	Description
show olt deactive-monitor [**gpon** *OLT-ID*]	Enable Global	Shows the configuration of ONU deactivation monitoring.
show olt deactive-monitor	Interface [GPON]	

To clear the alarms of ONU deactivation monitoring, use the following command.

Command	Mode	Description
clear olt deactive-monitor alarm	Interface [GPON]	Clears the collected alarms by ONU deactivation monitoring.

13.1.20 OLT Bit Error Ratio (BER)

You can configure the monitor direction and the alarm threshold of the bit error ratio. The system generates a bit error ratio (BER) alarm when the total number of error bits or bit error rate of the data transferred between the OLT and ONUs exceeds the alarm threshold. Both uplink and downlink data between OLT and ONU can be monitored.

To configure the OLT Bit Error Ratio (BER), use the following command.

Command	Mode	Description
olt ber ds-interval <1000-10000> [**olt ber sd-threshold** <4-9>] [**olt ber sf-threshold** <3-8>] [**olt ber us-interval** <1000-10000>]	Interface [GPON]	Specifies the monitor direction and interval of the bit error ratio. ds-interval: Downstream BER interval from OLT to ONU us-interval: Upstream BER interval from ONU to OLT 1000-10000: downstream BER interval value (default: 5000ms) 1000-10000: upstream BER interval value (default: 2000ms)
olt ber us-interval <1000-10000> [**olt ber ds-interval** <1000-10000>] [**olt ber sd-threshold** <4-9>] [**olt ber sf-threshold** <3-8>]		
olt ber sd-threshold <4-9> [**olt ber ds-interval** <1000-10000>] [**olt ber us-interval** <1000-10000>] [**olt ber sf-threshold** <3-8>]		Sets the threshold for reporting of signal degrade (SD) BER or signal fail (SF) BER alarms. 4-9: SD threshold value (default: 8) 3-8: SF threshold value (default: 7)
olt ber sf-threshold <3-8> [**olt ber ds-interval** <1000-10000>] [**olt ber us-interval** <1000-10000>] [**olt ber sd-threshold** <4-9>]		

To display the information of OLT Bit Error Ratio (BER), use the following command.

Command	Mode	Description
show olt ber [**gpon** *OLT-ID*]	Enable/Global	Shows OLT's Bit Error Ratio (BER) configuration (including upstream/downstream BER interval and threshold).
show olt ber	Interface [GPON]	

13.1.21 OMCC Monitoring

If an error occurs on the ONT Management and Control Channel (OMCC), the OLT attemps to recover from an error and the ONUs are deactivated by the OLT until the OMCC is recovered.

To enable/disable the OMCC recovery monitoring function with ONU deactivation process, use the following command.

Command	Mode	Description
olt omcc-recovery enable	Interface [GPON]	Enables the OMCC recovery monitoring function with ONU deactivation process.
olt omcc-recovery threshold <5-720>		Sets the threshold limit for OMCC recovery attempts. 5-720: the number of times OLT can atttemp to retry OMCC recovery (default: 5)
olt omcc-recovery mode deactivation		Sends the deactivation PLOAM when OLT detects the OMCC problem.
olt omcc-recovery mode reset		Sends the specific (ONT reset) PLOAM when OLT detects the OMCC problem.

Command	Mode	Description
olt omcc-recovery disable		Disables the OMCC recovery monitoring function with ONU deactivation process.

i

Disabling OMCC recovery monitoring with **olt omcc-recovery disable** command provides the data transmission service between OLT and ONU without ONU deactivation process even if an error occurs on the OMCC.

To display the information of OMCC recovery monitoring, use the following command.

Command	Mode	Description
show olt omcc-recovery [**gpon** *OLT-ID*]	Enable Global	Shows the status of OMCC recovery monitoring.
show olt omcc-recovery	Interface [GPON]	

To configure the force MIB upload option to resolve the ONU deactivation issue because of OMCC error, use the following command.

Command	Mode	Description
onu mib-upload *ONU-ID*	Interface [GPON]	Configures the force MIB upload of ONU to resolve the ONU deactivation caused by OMCC error.

13.1.22 OMCI-DB Validation Check

To check whether information about OMCI ME uploaded from ONU is normal or abnormal, use the following command.

Command	Mode	Description
olt omci-db-check enable	Interface [GPON]	Enables the OMCI DB check function.
olt omci-db-check disable		Disables the OMCI DB check function.
olt omci-db-check invalid-action base-db {mib-reset | none | notify | onu-reset} <1-100**>**		Configures action for invalid OMCI detection base-db: action for base DB fail invalid-db: action for invalid DB ref-db: action for referece DB fail
olt omci-db-check invalid-action invalid-db {mib-reset | none | notify | onu-reset} <1-100**>**		
olt omci-db-check invalid-action ref-db {mib-reset | none | notify | onu-reset} <1-100**>**		1-100: retry count

13.1.23 OMCI MIB Upload Suppression

To reduce the number of OMCI MIB upload by using the Reference DB, use the following command.

Command	Mode	Description
olt omci-mib-upload-sup enable	Interface [GPON]	Enables the OMCI DB check function.
olt omci-mib-upload-sup disable		Disables the OMCI DB check function.

13.1.24 PLOAM Message

To send a physical layer OAM (PLOAM) message to a specific ONU ID for debugging, use the following command.

Command	Mode	Description
olt specific-ploam *ONU-ID MSG_ID DATA*	Interface [GPON]	Sends the PLOAM message to a specific ONU ID for ONU-ID: ONU ID number used in PLOAM messages (1-255) MSG_ID: Downstream PLOAM message ID value or private PLOAM ID defined by the G.984.3 (1-255) DATA: 10 bytes HEX

13.1.25 Flow Control Configuration

To configure the flow control on GPON port, use the following command.

Command	Mode	Description
olt flow-control ds enable	Interface [GPON]	Enables the flow-control on the gpon interface.
olt flow-control ds disable		Disables the flow-control on the gpon interface.

13.1.26 Displaying OLT Information

To display GPON OLT information, use the following command.

Command	Mode	Description
show olt status [**gpon** *OLT-ID*]	Enable Global Interface [GPON]	Shows the information of active/inactive GPON OLT IDs.

The following is an example of displaying active/inactive OLT IDs of the LD3032.

```
SWITCH(gpon)# show olt status
--------------------------------------------------------------
 OLT_ID |  Status   |  Protect  | Distance | FEC mode(DS/US)
--------------------------------------------------------------
   1    |    Active |          |    20 Km |  enable/disable
```

```
  2   |    Active |         |    20 Km |  enable/disable
  3   |    Active |         |    20 Km |  enable/disable
  4   |    Active |         |    20 Km |  enable/disable
SWITCH(gpon)# show olt status 2
---------------------------------------------------------
 OLT_ID |  Status   |  Protect  | Distance | FEC mode(DS/US)
---------------------------------------------------------
  2    |   Active |         |    20 Km |  enable/disable
SWITCH(gpon)#
```

The Received Signal Strength Indication (RSSI) is a measurement of the power present in a received radio signal. The RSSI functionality in a newly released GPON OLT transceiver helps the operators monitor the received optical signal strength from each ONU (ONT).

To display the received signal power information from an ONU, use the following command.

Command	Mode	Description
show olt rx-power gpon *IFPORT* [*ONU-ID*]	Enable Global	Shows OLT Rx signal power from an ONU.
show olt rx-power [*ONU-ID*]	Interface [GPON]	

The following is an example of displaying the OLT RX power information of ONU ID 3.

```
SWITCH(config-gpon-olt[1])# show olt rx-power 3

----------------------------
  ONU  |     Rx Power
 ----------------------------
 3    | -16.0033 dBm
SWITCH(config-gpon-olt[1])#
```

13.1.26.1 OLT Traffic Statistics

To display traffic statistics of an OLT, use the following command.

Command	Mode	Description
show olt statistics gpon *OLT-ID*	Enable/Global	Shows traffic statistics of an OLT.
show olt statistics	Interface [GPON]	
show olt statistics onu gpon *OLT-ID ONU-ID*	Enable/Global	Shows traffic statistics of a specified ONU (ONT) collected by an OLT.
show olt statistics onu *ONU-IDs*	Interface [GPON]	

show olt statistics activation gpon *OLT-ID*	Enable/Global	Shows traffic statistics of GPON activation data.
show olt statistics activation	Interface [GPON]	
show olt statistics alarm gpon *OLT-ID* [*ONU-IDs*]	Enable/Global	Shows the ONU alarm counter data. ONU-ID: ONU ID (1-128) or ONU serial number
show olt statistics alarm [*ONU-IDs*]	Interface [GPON]	

To clear collected statistics, use the following command.

Command	Mode	Description
clear olt statistics	Interface [GPON]	Clears collected traffic statistics of an OLT.
clear olt statistics activation		Clears the collected traffic statistics of GPON activation data.
clear olt statistics alarm *ONU_IDs*		Clear the collected ONU alarm counter data. ONU-ID: ONU ID (1-128) or ONU serial number
clear olt statistics onu *ONU_IFPORT*		Clear the collected traffic statistics of a specified ONU. ONU-IFPORT: physical Interface port number
clear olt statistics gpon *IFPORT*	Global	Clear the collected statistics of a specified GPON interface.

13.1.26.2 MAC Address

To display the MAC addresses and a total MAC entry counts of the ONUs (ONTs) connected to a current OLT, use the following command.

Command	Mode	Description
show olt mac	Enable Global	Shows the MAC addresses of ONUs (ONTs) connected to OLT
show olt mac gpon *OLT-ID* [*ONU-IDs*]		
show olt mac count		Shows the number of MAC entries of ONUs (ONTs) connected to a specified OLT.
show olt mac count gpon *OLT-ID* [*ONU-IDs*]		

To add a MAC address of the ONUs (ONTs) connected to a current OLT, use the following command.

Command	Mode	Description
olt add-mac *ONU-ID MACADDR VLAN GEM-PORT*	Interface [GPON]	Adds the static MAC addresses of ONU. ONU-ID: ONU ID (1-128) or serial number GEM-PORT: GEM port ID

To display a MAC address of the ONUs (ONTs) connected to a current OLT, use the following command.

Command	Mode	Description
show olt mac [*ONU-ID* [*VLANS*]]	Interface [GPON]	Shows the MAC addresses currently learned on ONU. ONU-ID: ONU ID (1-128) or serial number
show olt mac count [*ONU-IDs*]		Shows the number of MAC addresses currently learned on a specified ONT.

To clear MAC addresses learned on a current OLT, use the following command.

Command	Mode	Description
clear olt mac [*ONU-ID*]	Interface [GPON]	Clears MAC addresses learned on a current OLT.
clear olt mac *ONU-ID* [*MAC-ADDR VLAN*]		Clears MAC addresses of specified ONU (ONT). MACADDR: MAC address VLAN: vlan ID

13.1.26.3 OLT Slot Information

To display the slot information of running SIUs as GPON OLT, use the following command.

Command	Mode	Description
show gpon slot-status	Global	Shows GPON slot information in a chassis

13.1.26.4 GPON Daemon Memory Usage

To display the memory usage of GPON, use the following command.

Command	Mode	Description
show memory gpon	Enable Global	Shows the memory usage of GPON daemon.

13.1.26.5 GPON Profile Count

To display the total number of GPON-based profiles, use the following command.

Command	Mode	Description
show profile count	Enable Global	Shows the profile list and the sum of saved GPON-based profiles.

13.2 ONU Management

This section describes how to manage an ONU (ONT). The LD3032 provides the centralized remote ONU (ONT) management concept, so you can manage every remote ONU (ONT) connected to the LD3032 without any local configuration for the ONUs (ONTs).

13.2.1 ONU Registration

The default ONU (ONT) registration mode is the auto mode in which an OLT registers ONUs automatically, when receiving the serial number from the ONU. For an optimized ONU configuration, however, the manual mode is recommended. Some options are only available in the manual mode.

The LD3032 is able to register ONU (ONT) automatically and manually.

- By default, the LD3032 registers ONUs automatically when the ONU is connected through its serial number registration. In this case, ONU ID is also given.
- Administrator can register specific ONUs (ONTs) manually with MAC address or serial number.

13.2.1.1 Activating/deactivating ONU

To activate/deactivate the ONU(ONT), use the following command.

Command	Mode	Description
onu activate *ONU-ID*	Interface [GPON]	Activates the specified ONU ID.
onu deactivate *ONU-ID*		Deactivates the specified ONU ID.

13.2.1.2 ONU Registration Method

There are several methods to register an ONU. You use a different method to recognize an existing ONU during subsequent activations. For example, authenticating a newly activated ONU by serial number allows for increased security during normal operation, whereas authenticating an ONU by registration ID (PLOAM password) allows for flexibility during installation and repair.

To specify the ONU registration method, use the following command.

Command	Mode	Description
onu activation-mode serial-number	Global	Configures the ONU’s serial-number based registration mode. (default)
onu activation-mode registration-id		Configures the ONU’s registration ID based registration mode.

i

You should remove all ONU database before changing the ONU registration method.

Serial Number-based ONU Registration

For ONU (ONT) registration, OLT requests a serial number of the connected ONUs (ONTs) periodically. OLT registers a specific ONU which replies to OLT with its serial number. The LD3032 can allocate ONU-ID to an ONU which sends a valid serial number to OLT. When ONU with the specific serial number is activated, it is assigned the allocated ONU-ID.

To register/delete ONU (ONT) automatically by ONU's serial number acquisition, use the following command.

Command	Mode	Description
discover-serial-number start <1-1200>	Interface [GPON]	Starts to register ONT by its serial number and specifies an interval for ONU's serial number acquisition. 1-1200: serial number acquisition interval
discover-serial-number stop		Stops discovering ONT using its serial number.
show discover-serial-number interval		Shows the configured interval for requesting ONU's serial number.
show discover-serial-number interval [**gpon** *OLT-ID*]	Enable/Global	

To remove the serial number of ONU, use the following command.

Command	Mode	Description
onu remove serial-number *ONU-ID*	Interface [GPON]	Removes the ONU serial number. ONU-ID: ONU ID (1-128) or ONU serial number

Registration ID-based ONU Registration

A registration ID is assigned to a subscriber at the management level, and provisioned both into the OLT and communicated to installation or repair personnel or even to the subscriber directly. The registration ID populates the ONU's PLOAM password, which is used by the OLT to recognize the ONU. The OLT may learn the value of the ONU's serial number for possible subsequent use in serial number based authentication.

To enter the registration ID into the ONU in the field, use the following command.

Command	Mode	Description
onu add *ONU-ID* **registration-id** *ID*	Interface [GPON]	Adds ONU (ONT) with a specified resgistration ID. ID: registration ID (PLOAM password)

13.2.1.3 Manual ONU (ONT) Registration Mode

To register/delete ONU (ONT) manually, use the following command.

Command	Mode	Description
onu add *ONU-ID SERIAL_NUM* {**auto-learning** | *PASSWD* [**enable** | **disable**]}	Interface [GPON]	Registers ONU (ONT) with specified ONU-ID, serial number and password. Enables/disables the password auto-learning mode of the ONU (ONT) ONU-ID:ONU ID (1 to 128) or ONU serial number SERIAL_NUM: ONU's serial number PASSWD: ONU password
no onu *ONU-ID*		Deletes the registered ONU with ONU ID.

13.2.1.4 ONU Registration Mode

The default ONU registration mode is the auto mode in which an OLT registers ONUs automatically, when recognizing the optical signal from the ONUs. For an optimized ONU configuration, however, the manual mode is recommended. Some options are only available in the manual mode.

Upon registering an ONU automatically, the registration mode of the ONU will be changed to the manual mode. Note that when you use this command, the registration mode of the ONUs that are already registered in the auto mode will be changed to the manual mode as well.

To change the ONU registration mode from auto to manual mode, use the following command.

Command	Mode	Description
olt auto-to-manual gpon *OLT-ID* **enable**	Global	Sets the current ONU registration mode to the manual mode. OLT-ID: GPON port number
olt auto-to-manual enable	Interface [GPON]	

To change the ONU registration mode from manual to auto mode, use the following command.

Command	Mode	Description
olt auto-to-manual gpon *OLT-ID* **disable**	Global	Sets the current ONU registration mode to the auto mode.
olt auto-to-manual disable	Interface [GPON]	

To display the ONU registration mode, use the following command.

Command	Mode	Description
show olt auto-to-manual [**gpon** *OLT-ID*]	Enable/Global	Shows the current ONU registration mode.

Command	Mode	Description
show olt auto-to-manual	Interface [GPON]	

13.2.1.5 Changing ONU Registration Mode

If user wants to change automatically the states of ONU (ONT) to manage manually at a time, use the following command.

Command	Mode	Description
onu fix {**all** | *ONU-ID*}	Interface [GPON]	Changes automatically registered ONUs (ONTs) to manage manually. ONU-ID: ONU ID (1 to 128) or ONU serial number

13.2.1.6 ONU Service Mode

Depending on the individual FTTH subscriber network deployment, the GPON link can be terminated with different client-side equipment options like Single Family Unit (SFU) and Home Gateway Unit (HGU). To select the ONU network service mode, use the following command.

Command	Mode	Description
onu service-mode *ONU-ID* {**hgu** | **sfu**}	Interface [GPON]	Specifies the network service mode of ONU. ONU-ID: ONU ID (1 to 128) or ONU serial number hgu: home gateway unit sfu: single family unit
no onu service-mode [*ONU-ID*]		Deletes the configure network service mode of ONU.

To display the configured ONU service mode, use the following command.

Command	Mode	Description
show onu service-mode [**gpon** *OLT-ID*]	Enable Global	Shows the configured ONU service mode. OLT-ID: OLT ID (PON port number) ONU-ID: ONU ID (1 to 128) or ONU serial number
show onu service-mode [*ONU-ID*]	Interface [GPON]	

13.2.1.7 ONU Description

To specify or modify a description of an ONU, use the following command.

Command	Mode	Description
onu description *ONU-ID DESCRIPTION*	Interface [GPON]	Registers the ONU's description. ONU ID (1 to 128) or ONU serial number
no onu description *ONU-ID*		Deletes the description of ONU.

To display a description of an ONU, use the following command.

Command	Mode	Description
show onu description gpon *OLT-ID*	Enable/Global	Shows the ONU’s description.
show onu description [*ONU-ID*]	Interface [GPON]	

13.2.1.8 ONU Connectivity via Ping Test

To verify the network connectivity with the ONU, use the following command.

Command	Mode	Description
omci ping *ONU-ID*	Interface [GPON]	Shows the network connectivity between OLT ID and ONU ID. ONU ID (1 to 128) or ONU serial number

13.2.2 Assigning IP address

To configure the IP host service ID, IP address and gateway address for an ONU, use the following command.

Command	Mode	Description
onu static-ip *ONU-ID* **ip-host** *SERVICE-ID A.B.C.D/M* **gw** *A.B.C.D*	Interface [GPON]	Configures the IP host service ID, IP address and gateway address for an ONU. ONU-ID: ONU ID (1 to 128) or ONU serial number SERVICE-ID: IP host service ID A.B.C.D/M: IP address A.B.C.D: IP gateway address
no onu static-ip *ONU-ID* **ip-host** *SERVICE-ID*		Deletes the configured IP host service ID, IP address and gateway address for the ONU.

To assign a static IPv6 address for IPv6 host of ONU, use the following command.

Command	Mode	Description
onu static-ip *ONU-ID* **ipv6-host** *SERVICE-ID X:X::X:X/M* **default-router** *X:X::X:X*	Interface [GPON]	Configures the IPv6 host service ID, IPv6 address and IPv6 gateway address for an ONU. ONU-ID: ONU ID (1 to 128) or ONU serial number SERVICE-ID: IPv6 host service ID X:X::X:X/M: IPv6 address X:X::X:X: IPv6 address of default router
no onu static-ip *ONU-ID* **ipv6-host** *SERVICE-ID*		Deletes the configured static IPv6 address of IPv6 host.

i

For the details of how to create and configure the IP host service, see 13.4.5 IP Host Service Configuration. The IP assignment on IP host service configuration has to be specified as “**static**” when assigning IP address to ONU.

To display the configured IP host service ID on ONU, use the following command.

Command	Mode	Description
show onu ip-host gpon *OLT-ID ONU-ID*	Enable Global	Shows the configured IP host service ID on ONU.
show onu ip-host *ONU-ID*	Interface [GPON]	

13.2.3 Activating Administration for UNI

To enable/disable the administration of the ONU (ONT) UNI port, use the following command.

Command	Mode	Description
onu port-admin *ONU-IDs* **uni** {**eth** | **pots** | **ces** | **virtual-eth** | **video** | **wifi**} *UNI-PORTs* {**enable** | **disable**}	Interface [GPON]	Enables/disables the administration of UNI port on the specified ONU. ONU-ID: ONU ID (1 to 128) or ONU serial number eth/pots/ces/virtual-eth/Video/wifi: Ethernet / POTS / CES / virtual Ethernet/Video / Wi-Fi UNI-PORT: UNI port number

i

To see the admin status of the ONU (ONT) UNI, use **show onu uni-status** command. (See 13.2.21 Displaying ONU Information)

13.2.4 Forward Error Correction (FEC) Mode

To enable/disable FEC mode for ONU ID, use the following command.

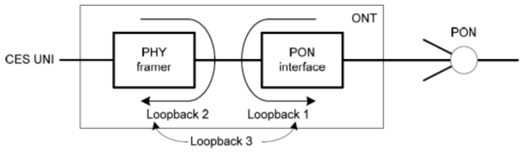
Command	Mode	Description
onu us-fec-mode *ONU-IDs* **enable**	Interface [GPON]	Enables upstream FEC mode for ONU ID.
onu us-fec-mode *ONU-IDs* **disable**		Disables upstream FEC mode for ONU ID.

i

If you want to enable the upstream FEC mode for ONU, you should enable upstream FEC mode for OLT first. For the detail of how to enable the upstream FEC mode for OLT, see 13.1.7 Forward Error Correction (FEC) Mode.

13.2.5 Loopback

To enable/disable the loopback for UNI of ONU, use the following command.

Command	Mode	Description
onu loopback *ONU-IDs* **uni eth** *UNI-PORTs* {**enable type 3** | **disable**}	Interface [GPON]	Enables/disables the loopback for the specified Ethernet (type 3) UNI port of ONU. ONU-IDs: ONU ID (1 to 128) or ONU serial number UNI-PORTs: UNI port number
onu loopback *ONU-IDs* **uni ces** *UNI-PORTs* {**enable type** <1-5> | **disable**}		Enables/disables the loopback for the specified CES/TDM UNI port of ONU. ONU-IDs: ONU ID (1 to 128) or ONU serial number UNI-PORTs: UNI port number 1: payload loopback 2: line loopback 3: OpS-directed loopback 1 (loopback from/to PON side) 4: OpS-directed loopback 2 (loopback from/to CES UNI side) 5: OpS-directed loopback 3 (loopback of both PON side and CES UNI side)  ONT PON CES UNI PHY framer PON interface Loopback 2 Loopback 1 Loopback 3

i

To see the status of the ONU (ONT) UNI, use **show onu uni-status** command. (See 13.2.21 Displaying ONU Information)

13.2.6 ONU Laser Down

If a certain ONU's laser is enabled consistently by an optical transceiver's fault, all other normal ONUs connected to the same OLT will be deregistered; a single ONU fault may cause a whole network disruption.

To prevent such a problem, you can manually disable the laser (TX power of transceiver) of the faulty ONU considered as the cause of the problem. By the way, if you disable the laser without specifying laser-off time, the ONU needs a power reset to resume the laser.

To disable an ONU's laser, use the following command.

Command	Mode	Description
onu tx-off-optic *ONU-ID* [<1-65525>]	Interface [GPON]	Disables an ONU's laser for specified time. After the time, the laser will be enabled. ONU-ID: 1-128 or ONU serial number 1-65525: disable transceiver during input times (unit:sec)

To guarantee a right operation of this feature, an ONU should be loaded with the newest firmware.

13.2.7 Source MAC address Monitoring

The LD3032 can monitor its source MAC table to find a defective ONUs (ONTs). Auto ONU (ONT) blocking function can be used to manage and troubleshoot the defective ONU-related problems.

To enable/disable OLT for source MAC address monitoring, use the following command.

Command	Mode	Description
olt srcmac-monitor enable	Interface [GPON]	Enables the source MAC address monitoring.
olt srcmac-monitor enable auto-onu-block [**expire-timeout** <60-65535>]		Enables the source MAC address monitoring with auto ONU blocking feature auto-onu-block: When an ONU fault occurs, the system will disable the ONU's laser permanently. 60-65535: expire time (second)
olt srcmac-monitor disable		Disables the source MAC address monitoring.

To display the information of source MAC monitoring, use the following command.

Command	Mode	Description
show olt srcmac-monitor [**gpon** *OLT-ID*]	Enable Global	Shows the configured source MAC address monitoring for OLT.
show olt srcmac-monitor	Interface [GPON]	

To force the state of a blocked ONU ID to change to unblocked state, use the following command.

Command	Mode	Description
onu unblock *ONU-ID*	Interface [GPON]	Forces the state of a blocked ONU ID to change to unblocked state.

To force the state of a unblocked ONU ID to change to blocked state, use the following command.

Command	Mode	Description
onu block *ONU-ID*	Interface [GPON]	Forces the state of a unblocked ONU ID to change to blocked state.

To display the link status of ONUs, use the following command.

Command	Mode	Description
show onu block status gpon *OLT-ID* [*ONU-ID*]	Enable/Global	Shows the link status of ONUs OLT-ID: GPON port number ONU-ID: ONU ID (1 to 128) or ONU serial number
show onu block status [*ONU-ID*]	Interface [GPON]	

13.2.8 ONU MAC address Filtering

The MAC filter table lists MAC destination addresses associated with the bridge port, each with an allow/disallow forwarding indicator for traffic flowing out of the bridge port. In this way, the upstream traffic is filtered on the ANI-side bridge ports, and the downstream traffic is filtered on the UNI-side bridge ports.

To enable/disable the MAC filtering function for UNI-side bridge port, use the following command.

Command	Mode	Description
onu mac-filter *ONU-ID* **uni** { **eth** | **ip-host** | **ces** | **virtual-eth** } *PORT* { **filter** | **forward** } *MACADDR*	Interface [GPON]	Enables the MAC filtering function for UNI-side bridge port. eth: Ethernet port ip-host: IP host service virtual-eth: virtual Ethernet ces: circuit emulation service PORT: port number forward: forwards a specific MAC address of UNI-side port filter: blocks a specific MAC address of UNI-side port MACADDR: MAC address
no onu mac-filter *ONU-ID* **uni** { **eth** | **ip-host** | **ces** | **virtual-eth** } *PORT* { **filter** | **forward** } *MACADDR*		Disables the MAC filtering function for UNI-side bridge port.

To enable/disable the MAC filtering function for ANI-side bridge port, use the following command.

Command	Mode	Description
onu mac-filter *ONU-ID* **ani** { **mapper** | **gem** } *PORT* { **filter** | **forward** } *MACADDR*	Interface [GPON]	Enables the MAC filtering function per ANI-side mapper ID or GEM port ID.
no onu mac-filter *ONU-ID* **ani** { **mapper** | **gem** } *PORT* [{ **filter** | **forward** } *MACADDR*]		Disables the MAC filtering function per ANI-side mapper ID or GEM port ID.

To display the information of MAC filtering and MAC table data, use the following command.

Command	Mode	Description
show onu mac-filter gpon *OLT-ID*	Enable/Global	Shows the MAC filtering function.
show onu mac-filter [*ONU-ID*]	Interface [GPON]	
show onu mac gpon *OLT-ID ONU-ID* **uni** {**eth** | **virtual-eth**} *UNI-PORT*	Enable/Global	Shows the MAC table data of ONU's UNI ports.
show onu mac *ONU-ID* **uni** {**eth** | **virtual-eth**} *UNI-PORT*	Interface [GPON]	

13.2.9 POTS Interface Configuration

To configure the parameters of POTS interface in an ONT, use the following command.

Command	Mode	Description
onu voip-sip *ONU-ID* **phone-number pots** *POTS-NUMBER NUMBER* [**display** *DISPLAY*]	Interface [GPON]	Saves a phone number and a display information of a specified phone device connected to POTS interface at an ONU managed by OMCI protocol. ONU-ID: 1-128 or ONU serial number POTS-NUMBER: POTS port number NUMBER: phone number DISPLAY: display information
no onu voip-sip *ONU-ID* **phone-number pots** *POTS-NUMBER*		Deletes the configured data parameters of VoIP user.

For the enhanced system security, the LD3032 can use authentication for a VoIP user to have access to the softswitch.

To configure the authentication user name and password for VoIP user to have access to softswitch, use the following command.

Command	Mode	Description
onu voip-sip *ONU-ID* **auth pots** *POTS-NUMBER NAME* [*PASSWD*]	Interface [GPON]	Configures an user ID and password for a specified VoIP device connected to an ONU to have access to softswitch. ONU-ID: 1-128 or ONU serial number POTS-NUMBER: POTS port number NAME: user name used for authentication PASSWD: password used for authentication
no onu voip-sip *ONU-ID* **auth pots** *POTS-NUMBER*		Deletes the configured authentication information for VoIP user.

The user display name, phone number, authentication user name and password is limited to a maximum of 25 characters (bytes).

To display VoIP service and VoIP line status information, use the following command.

Command	Mode	Description
show onu voip line gpon *OLT-ID ONU-ID*	Enable Global	Shows the information of VoIP service and line status. ONU-ID: 1-128 or ONU serial number
show onu voip line *ONU-ID*	Interface [GPON]	

13.2.10 VoIP MGC Configuration

13.2.10.1 Message ID Configuration

To configure the message ID according to the specific VoIP service, use the following command.

Command	Mode	Description
onu voip-mgc *ONU-ID* **message-id service** *VOIP_SERVICE MESSAGE_ID*	Interface [GPON]	Configures the message ID according to the specific VoIP service. ONU-ID: ONU ID or serial number VOIP_SERVICE: VoIP service number MESSAGE_ID: message ID
no onu voip-mgc *ONU-ID* **message-id service** *VOIP_SERVICE*		Deletes the configured message ID.

For the details of how to create and configure the VoIP service, see 13.4.6 VoIP Service Configuration (POTS UNI).

13.2.10.2 ONT Termination ID Configuration

The attribute specifies the base string for the MGC (H.248) physical termination ID(s) for the ONT. This string is intended to uniquely identify an ONT. Vendor-specific termination identifiers (i.e., port IDs) are optionally added to this string to uniquely identify a termination on a specific ONT.

To configure the termination ID on POTS interface of ONT, use the following command.

Command	Mode	Description
onu voip-mgc *ONU-ID* **termination-id pots** *POTS_NUMBER TERMINATION_ID*	Interface [GPON]	Specifies the termination ID on POTS interface of ONT. ONU-ID: ONU ID or serial number POTS_NUMBER: POTS port number TERMINATION_ID: termination ID
no onu voip-mgc *ONU-ID* **termination-id pots** *POTS_NUMBER*		Deletes the configured termination ID.

13.2.11 ONU Port Configuration

13.2.11.1 UNI Ethernet Port Configuration

To configure the UNI Ethernet port of ONU, use the following command.

Command	Mode	Description
onu port-config *ONU-IDs* **uni eth** *UNI-PORTs* **medium-mode** {**mdi** | **mdi-x** | **auto**}	Interface [GPON]	Configures the medium mode of ONU UNI Ethernet port. ONU-ID: 1-128 or ONU serial number UNI-PORT: ONU UNI port number mdi: MDI mode mdi-x: MDIX mode auto: automatically
onu port-config *ONU-IDs* **uni eth** *UNI-PORTs* **speed** {**auto** | **1000** | **100** | **10**} **duplex** {**auto** | **full** | **half**}		Configures the speed and duplex mode of ONU UNI Ethernet port.
onu port-config *ONU-IDs* **uni eth** *UNI-PORTs* **power-control** {**enable** | **disable**}		Enables/disables the Power over Ethernet (PoE) port on the specified ONU.
onu uni-description *ONU-ID* **eth** *UNI-PORT DESCRIPTION*		Adds the description on the specified ONU UNI Ethernet port.
no onu uni-description *ONU-ID* **eth** *UNI-PORT*		Deletes the description of the specified ONU UNI Ethernet port.

To display the status of ONU UNI Ethernet port, use the following command.

Command	Mode	Description
show onu uni-status eth gpon *OLT-ID*	Enable/Global	Shows the status of ONU UNI Ethernet port.
show onu uni-status eth [*ONU-IDs*]	Interface [GPON]	

To display the configured description on ONU UNI port, use the following command.

Command	Mode	Description
show onu uni-description gpon *OLT-ID*	Enable Global	Shows the configured description on ONU UNI port.
show onu uni-description [*ONU-ID*]	Interface [GPON]	

13.2.11.2 ANI RF Video Port Configuration

To configure the ANI RF video port of ONU, use the following command.

Command	Mode	Description
onu port-config *ONU-IDs* **ani video** *ANI-PORTs* **agc** *AGC_VALUE*	Interface [GPON]	Configures the AGC value of ONU ANI RF video port. ONU-ID: 1-128 or ONU serial number ANI-PORT: ANI port number AGC_VALUE: Automatic Gain Control value (-12.7~12.7 dB)
no onu port-config *ONU-IDs* **ani video** *ANI-PORTs* **agc**		Deletes the AGC value of the specified ONU ANI video port.

13.2.11.3 Displaying Multicast Counter Information

To display the multicast counter information per UNI Ethernet port of ONU, use the following command.

Command	Mode	Description
show onu igmp-pm-data gpon *OLT-ID ONU-ID* **uni** {**eth** | **virtual-eth**} *UNI-PORT*	Enable Global	Shows the IGMP message counters per UNI port of ONU. The counters are a total number of successful/unsuccessful joins, leave messages, general queries, specific queries and invalid IGMP messages. ONU-ID: 1-128 or ONU serial number UNI-PORT: UNI port number
show onu igmp-pm-data *ONU-ID* **uni** {**eth** | **virtual-eth**} *UNI-PORT*	Interface [GPON]	
clear onu igmp-pm-data *ONU-ID* **uni** {**eth** | **virtual-eth**} *UNI-PORT*		Clears the collected IGMP message counters.

13.2.11.4 PPPoE Configuration

To configure the Point - to -Point Protocol over Ethernet (PPPoE) of ONU, use the following command.

Command	Mode	Description
onu pppoe *ONU_ID* **host** *HOST_NUM* **user-account** *USER PASSWORD*	Interface [GPON]	Configures the PPPoE of ONU and sets the user and password for PPPoE configuration server. ONU-ID: 1 - 128 or ONU serial number *HOST_NUM:* host number *USER :*user name used for authentication *PASSWORD:* password used for authentication
no onu pppoe *ONU_ID* **host** *HOST_NUM*		Deletes the configured PPPoE host number.
show onu pppoe account [*ONU_ID*]		Shows the PPPoE account of ONU.
show onu pppoe status *ONU_ID*		Shows the ONU status information for PPPoE.

13.2.12 ONU Loop Detect Configuration

A loop may occur when double paths are used for the link redundancy between switches and one sends unknown unicast or multicast packet that causes endless packet floating on the LAN. That superfluous traffic eventually can result in network fault.

The ONU periodically sends the loop-detecting packet to all the ports with a certain interval, and then if the loop-detecting packet is received, the switch performs a pre-defined behavior such as “blocked”. The user may need to change this state to “unblocked (normal)” via OLT.

To change the “blocked” state of ONU due to the loop detection into “unblocked”, use the following command.

Command	Mode	Description
onu loop-detect unblock *ONU-IDs*	Interface [GPON]	Changes the “blocked” state due to loop detect into “unblocked (normal)”.

To display whether the specific ONU is in the state of “blocked” or “unblocked” due to the loop detect, use the following command.

Command	Mode	Description
show onu loop-detect [**gpon** *OLT-ID*]	Enable Global	Shows whether the ONU is in the state of “blocked” or “unblocked”.
show onu loop-detect [*ONU-IDs*]	Interface [GPON]	

13.2.13 ONU Inactive Aging-time

The ONU inactive aging-time can be used while the registration mode of the ONU is configured in the manual mode. If a number of days for an OLT to check the ONU’s registration status pass without the ONU’s activation, the ONU will be automatically deregistered.

To specify the registration aging time for the ONUs that are manually registered, use the following command.

Command	Mode	Description
onu inactive aging-time <1-30>	Interface [GPON]	Specifies the maximum number of days that an ONU is inactive. If the ONU has been inactive during that number of days, the ONU will be automatically deregistered by OLT. 1-30: aging time measured in days
onu inactive aging-time disable		Sets the ONU aging time to be unlimited (default)

To display the configured aging time for the inactive ONUs, use the following command.

Command	Mode	Description
show onu inactive aging-time	Enable	Shows the configured aging time for the inactive

[**gpon** *OLT-ID*]	Global	ONUs.
show onu inactive aging-time	Interface [GPON]	

You can monitor how long the ONU has been inactive status displayed in the Inactive Time field using **show onu detail-info** command. If the ONU's activation status is active, the inactive time value remains unchanged at 0:00:00:00.

13.2.14 ONU Reset

For various reasons such as HW or SW error, you may need to reset an ONU (ONT). To reset an ONU, use the following command.

Command	Mode	Description
onu reset *ONU-IDs*	Interface [GPON]	Resets a specified ONU. ONU-ID: ONU ID (1 to128) or ONU serial number
onu re-config *ONU-ID*		Resets the ONU MIB.
onu restore-factory reset *ONU-IDs*		Restores the factory default settings of ONU. ONU-ID: ONU ID (1 to128) or ONU serial number

After restoring a default configuration, you need to restart ONU to initiate.

13.2.15 ONU Password Type Configuration

To configure ONU password type, use the following command.

Command	Mode	Description
onu password-type {**hex** | **ascii**}	Global	Configures ONU password type.

13.2.16 Diagnostic Monitoring for ONU's Optical Transceiver

The Digital Diagnostic Monitoring Interface (DDMI) feature provides diagnostic information about the module's present operating conditions. The transceiver generates this diagnostic data by digitization of internal analog signals.

To display the operating parameters of ONU's GPON module, use the following command.

Command	Mode	Description
show onu ani optic-module-info gpon *OLT-ID ONU-ID*	Enable/Global	Shows the operating parameters of the GPON module, including the optical characteristics.
show onu ani optic-module-info *ONU_ID*	Interface [GPON]	
show onu uni optic-module-info gpon *OLT-ID ONU-ID PORT*	Enable/Global	Shows the operating parameters of the module of UNI port including the optical characteristics.
show onu uni optic-module-	Interface	

info *ONU-ID PORT*	[GPON]	

To use the above command, ONU (ONT) should support DDMI feature and provide diagnostic information about the module's present operating conditions to OLT.

13.2.17 ONU System Account

To add system-account information for ONUs, use the following command.

Command	Mode	Description
onu system-account *ONU-ID USER* [*PASSWD*]	Interface [GPON]	Creates the login account ID and password for ONU ID. ONU-ID: ONU ID (1 to128) or ONU serial number USER: user name PASSWD: password

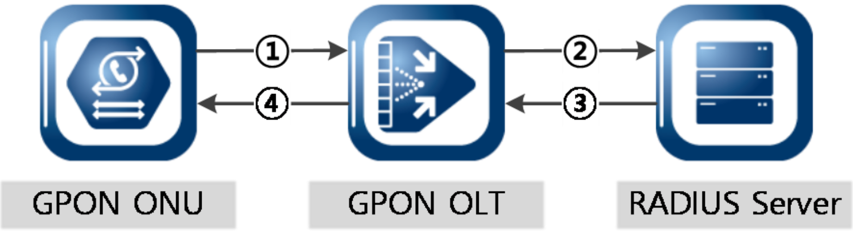
To display the system-account information of ONU ID, use the following command.

Command	Mode	Description
show onu system-account gpon *OLT-ID ONU-ID*	Enable/Global	Shows the system-account information of ONU.
show onu system-account *ONU-ID*	Interface [GPON]	

13.2.18 ONU Authentication from RADIUS server

You can use the RADIUS authentication process when an ONU (ONT) is activated and it attempts to access an OLT. The RADIUS Access-Request message is sent from the OLT to the RADIUS server. If the ONU is valid, the RADIUS server consults a database of ONUs to find the ONU which matches the authentication attributes in the connection request. If the RADIUS server has the valid ONU-related information, it sends the configuration settings placed into a RADIUS Access-Accept message to the OLT for the ONU registration. The OLT receives the service profile settings from the RADIUS server and it assigns a new service profile to ONU.

RADIUS Authentication Process



① **Upload MIB Info**: During the initial connection between OLT and ONU, the ONU uploads the MIB information. On the OLT side, the OLT checks the ONU validation using ONU model name, firmware version and serial number.

② **Sends RADIUS message**: If the RADIUS authentication is required when the OLT and ONU are connected each other, the OLT sends Access-Request message with the authentication attributes (user name, user password, OLT-ID, ONU-ID, ONT model name, serial number, firmware version) to the RADIUS server.

③ **Receive Response message**: If the RADIUS message is sent by a valid ONU, and if the authentication attributes contain the correct values, the Access-Accept message of ONU configuration settings is sent by the RADIUS server.

④ **Set the configuration**: The OLT receives the service profile information from the RADIUS server. The new service profile settings are assigned to ONU.

The RADIUS server sends Disconnect messages (DM) request in order to terminate a user session on a network access server, whereas it sends Change-of-Authorization (CoA) request messages to modify session authorization attributes of ONU.

The OLT checks that the key of DM message from the RADIUS server is valid. If the key value is invalid, the packets are silently discarded.

The following table shows the RADIUS message format and types.

Message Type	Authentication Attributes (RADIUS Code Field)
Access-Request (OLT → server)	(a) Service-Type: “Authenticate Only (8)”. (b) User-Name & User-Password: ONU Model Name (c) Vendor-Specific Vendor ID: IANA registered FURUKAWA ELECTRIC LATAM (6296) (d) Vendor-Specific Attribute: OLT_ID, ONT_ID, Model Name, Serial Number, Firmware Version info. (e) Message-Authenticator: KEY and MD5
Access-Accept (server → OLT)	(a) Furukawa-Gpon-Onu-Profile (b) Furukawa -Gpon-Onu-Static-Ip (c) Furukawa-Gpon-Onu-Voip-Sip-Number (d) Furukawa-Gpon-Onu-Voip-Sip-Auth (e) Furukawa-Gpon-Onu-Uni-Port-Admin (f) Furukawa-Gpon-Onu-VoIP-Mgc-Msg-Id (g) Furukawa-Gpon-Onu-VoIP-Mgc-Term-Id (h) Furukawa-Gpon-Onu-Description (i) Furukawa-Gpon-Onu-Uni-Eth-Port-Medium (j) Furukawa-Gpon-Onu-Uni-Eth-Auto-Detect (k) Furukawa-Gpon-Onu-Mac-Filter (l) Furukawa-Gpon-Onu-Mgmt-Mode-Ip-Path-Ftp (m) Furukawa-Gpon-Onu-Mgmt-Mode-Ip-Path-Tftp (n) Furukawa-Gpon-Onu-Mgmt-Mode-Ip-Path-Uri
CoA-Request (server → OLT)	(a) User-Name (b) User-Password (c) Furukawa-Gpon-Olt-Id (d) Furukawa-Gpon-Onu-Id

	(e) Furukawa-Gpon-Onu-Model-Name (f) Furukawa-Gpon-Onu-Serial-Num (g) Furukawa-Gpon-Onu-Firmware-Version (h) Furukawa-Gpon-Onu-Profile (i) Furukawa-Gpon-Onu-Static-Ip (j) Furukawa-Gpon-Onu-Voip-Sip-Number (k) Furukawa -Gpon-Onu-Voip-Sip-Auth (l) Furukawa-Gpon-Onu-Uni-Port-Admin (m) Furukawa-Gpon-Onu-VoIP-Mgc-Msg-Id (n) Furukawa-Gpon-Onu-VoIP-Mgc-Term-Id (o) Furukawa-Gpon-Onu-Description (p) Furukawa-Gpon-Onu-Uni-Eth-Port-Medium (Not support yet) (q) Furukawa-Gpon-Onu-Uni-Eth-Auto-Detect (Not support yet) (r) Furukawa-Gpon-Onu-Mac-Filter
DM-Request (server → OLT)	(a) User-Name (b) User-Password (c) Furukawa-Gpon-Olt-Id (d) Furukawa-Gpon-Onu-Id (e) Furukawa-Gpon-Onu-Model-Name (f) Furukawa-Gpon-Onu-Serial-Num (g) Furukawa-Gpon-Onu-Firmware-Version

Tab. 12.2 RADIUS Authentication Message Type

To configure IP address and key value of RADIUS server for ONU authentication, use the following command.

Command	Mode	Description
onu auth radius-server host *A.B.C.D* **key** *WORD* [**auth-port** <0-65535>]	Global	Specifies an IP address with key value and UDP port of RADIUS server. A.B.C.D: RADIUS server IP address WORD: RADIUS authorization key value 0-65535: UDP port (default: 1812)
onu auth radius-username { **serial-number** | **model-name**}		Sends the ONU's serial number-based or its model name-based ID key value on the authentication message to RADIUS server. serial-number: uses GPON serial number of ONU (default) model-name: uses model name of ONU
onu auth radius-password { **serial-number** | **model-name**}		Sends the ONU's serial number-based or its model name-based password on the authentication message to RADIUS server.
no onu auth radius-server host *A.B.C.D*		Deletes the configured RADIUS server address.

To display the information of RADIUS server for ONU authentication, use the following command.

Command	Mode	Description
show onu auth radius-server	Global	Shows the information of RADIUS server for ONU authentication

i You can see the status of ONU authentication via RADIUS server by the **debug gpon rauth** command.

To enable/disable the ONU authentication for ONU profile, use the following command.

Command	Mode	Description
onu auth-control {**enable** | **disable** }	Interface [GPON]	Enables/disables the authentication control function for the specified OLT port.
onu auth-control reauthenticate		Performs re-authentication processing for ONU.

To display the information of ONU authentication status and profile, use the following command.

Command	Mode	Description
show onu auth-status [**gpon** *OLT-ID*]	Global	Shows the current authentication status of ONU.
show onu auth-status [*ONU-ID*]	Interface [GPON]	

13.2.19 CFM OAM for ONU Management

CFM OAM is now standardized as IEEE 802.1ag. CFM contains the concepts of maintenance domains and supports autonomy for customers, providers, operators, etc. It enables end-to-end management of connectivity and services, each domain can run its own OAM. By CFM OAM feature, the service providers who own the network end-to-end may be able to guarantee services over networks they own.

CFM OAM Elements

You need to know conceptual information of CFM OAM. CFM OAM consists of the following management elements.

- **Maintenance Entity (ME)**
  An OAM entity that requires management. An MD is owned by a ME. It is a relationship between two Maintenance association end points (MEPs) within a single MA.
- **Maintenance Domain (MD)**
  In Ethernet CFM, an MD is a management space for monitoring and administering of a network. A network controlled by an operator that supports connectivity between MEPs.
- **Maintenance Association (MA)**
  A set of MEPs that belong to the same MA identifier and MD level within one service

instance to verify the integrity of the service.

- **Maintenance Association End Point (MEP)**
  A provisioned reference point that can initiate/terminate proactive OAM frames. Each MEP has a unique MEP ID within its MA.
- **Maintenance Association Intermediate Point (MIP)**
  A provisioned reference point that can respond to diagnostic OAM frames initiated by a MEP.
- **Service Instance**
  CFM OAM defines that a service instance is one entity within MD.

CFM Messages

There are different types of CFM messages:

- **Continuity Check Message (CCM)**
  Each MEP sends periodic CCMs to other MEPs with a multicast destination address. The loss of CCMs that ride along the data path would indicate a connectivity failure.
- **Loopback Message/Response (LBM/LBR)**
  A LBM is sent to a unicast destination MAC address. MEP at the destination MAC address responds to the LBM with an LBR. These messages are useful for verifying connectivity with a specific L2 destination.
- **LinkTrace Message/Response (LTM/LTR)**
  A LTM is sent to a multicast MAC address. Each MIP at the same MD level responds with a LTR. LTM is then forwarded to the next hop until it reaches the destination MAC address. These messages are used for tracing the L2 path to a specific L2 destination.

CFM OAM Features

The important features provided by 802.1ag CFM OAM are:

- Supports Connectivity Check Message (CCM), LinkTrace (LTM) and LoopBack messages (LBM)
- Helps service providers assign selected subscribers restricted access to manage all functions for their own domains
- Fault detection, notification and verification
- Traces the path to another MEP or MIP in the same domain

A CFM maintenance domain (MD) is a management space on a network that is owned and operated by a single entity and defined by a set of ports internal to it, but at its boundary. To use CFM OAM, you should create MD. MD is defined by a given MD name and level that are configured by user. MD level determines the MEPs/MIPs that are interested in the contents of the CFM frame and through which the CFM frame is allowed to pass.

To create a CFM Maintenance Domain (MD) and configure its name and level, use the following command.

Command	Mode	Description
onu cfm md *DOMAIN* **level** <0-7>	Global	Creates a MD name and specifies a MD's level DOMAIN: Maintenance Domain's name 0-7: MD's level to use (default: 0)
no onu cfm md *DOMAIN*		Deletes the configured MD with a unique name.

i Each MD has an index, an unique name and MD level. Several MDs can have same level. But one single MD cannot have several levels.

MEPs periodically exchange Continuity Check OAM messages to detect loss of continuity or incorrect network connections. To create a Maintenance Association (MA) with its name as a service instance for a specific MD and specify the interval of Continuity Check Messages (CCMs) that are sent by MEPs in the specified MA, use the following command.

Command	Mode	Description
onu cfm ma <1-65535> *MA_NAME* **md** *MD_NAME* **ccm interval** { **100ms** | **1s** | **10s** | **1m** | **10m** | **disable** }	Global	Specifies a MA for MD and the interval of sending continuity check messages (CCMs). 1-65535: MA index MA_NAME: name of MA MD_NAME: Maintenance Domain's name
no onu cfm ma <1-65535>		Deletes the configured MA.

i There is at least one MA within a signle MD.

To configure a MIP and its level on the VLAN ID, use the following command.

Command	Mode	Description
onu cfm *ONU_ID* **mip level** *LEVEL* **vlan** *VLANS*	Interface [GPON]	Specifies a MIP and its level on the VLAN ID. ONU_ID: ONU ID (1 to128) or ONU serial number LEVEL: MIP's level (0 to 7) VLAN: VLAN list (maximum 12)
no onu cfm *ONU_ID* **mip** [**level** *LEVEL*]		Removes the configured MIP.

To specify the ONU ID and bridge's UNI Ethernet port or ANI mapper to which the MEP is attached, use the following command.

Command	Mode	Description
onu cfm *ONU_ID* **mep** { **uni eth** *PORT* | **ani mapper** *PORT* } **mep-id** *MEP_ID* **ccm** { **enable** | **disable** }	Interface [GPON]	Enables/disables the continuity check messages (CCMs) exchange and specifies an ONU ID and MEP ID. ONU-ID: ONU ID (1 to128) or ONU serial number PORT: ONU's UNI Ethernet port number or ANI mapper port number MEP_ID: MEP ID (1 to 8191)

onu cfm *ONU_ID* **mep** { **uni eth** *PORT* | **ani mapper** *PORT* } **mep-id** *MEP_ID* **primary-vlan** *VLANS* **peer-mep-id** *ID* **ma** <1-65535>		Configures a MEP on the ONU ID and assigns a remote MEP ID and primary VLAN ID. MEP_ID: MEP ID (1 to 8191) VLANS: primary VLAN ID ID: remote MEP ID (1 to 8191) 1-65535: MA index
no onu cfm *ONU_ID* **mep** [{**uni eth** *PORT* | **ani mapper** *PORT*} [**mep-id** *MEP_ID*]]		Removes the configured MEP ID from ONU.

Ethernet Loopback function supports fault verification through Loopback Messages (LBM) and Loopback Reply (LBR). These messages are used during initial set-up or after a fault has been detected to verify that the fault has occurred between two end points. CFM OAM allows both unicast and multicast loopback. Ethernet Traceroute function is used to retrieve adjacency relationship between a MEP and a remote MEP or MIP. And it is also used for fault localization. The LD3032 sends LinkTrace Message (LTM) frames to discover a path for a link trace.

To configure the source / destination MEP to send the LoopBack Message (LBM) or Link-Trace message (LTM), use the following command.

Command	Mode	Description
onu cfm test loopback *ONU_ID* **mep** { **uni eth** *PORT* | **ani mapper** *PORT* } **mep-id** *MEP_ID* {**rmep-id** <1-8191> | **rmac** *MACADDR*} [**count** *NUMBER*]	Interface [GPON]	Performs the Loopback/Traceroute test for ONU and specifies MEP ID and remote MEP ID/ MAC address to send LBM/LTM from the ONU. ONU_ID: ONU ID (1 to128) or ONU serial number PORT: ONU's UNI Ethernet port number or ANI mapper port number MEP_ID: MEP ID 1-8191: destination MEP ID MACADDR: destination MAC address to send LBMs/LTMs NUMBER: the number of attempts for sending LBMs (default:1) 1-64: LBM/LTM's TTL value (default: 64)
onu cfm test traceroute *ONU_ID* **mep** { **uni eth** *PORT* | **ani mapper** *PORT* } **mep-id** *MEP_ID* {**rmep-id** <1-8191> | **rmac** *MACADDR*} [**ttl** <1-64>]		

To display the information of CFM OAM, use the following command.

Command	Mode	Description
show onu cfm mep [**gpon** *OLT_ID*]	Enable Global	Shows the information of MEP configured on an OLT.
show onu cfm mip [**gpon** *OLT_ID*]		Shows the information of MIP configured on an OLT.
show onu cfm ma [<1-65535>]	Global	Shows the information of MA.
show onu cfm md [*DOMAIN*]		Shows the configured MD and level.
show onu cfm mep [*ONU_ID*]	Interface	Shows the status of MEP configured on an ONU.

show onu cfm mep ccm-db *ONU_ID* {**uni eth** *PORT* | **ani mapper** *NUMBER*} **mep-id** *MEP_ID*	[GPON]	Shows the information of a MEP in the CCM database.
show onu cfm mip [*ONU_ID*]		Shows the status of MIP configured on an ONU.

13.2.20 ONU Firmware Upgrade

The LD3032 provides the remote ONU (ONT) upgradeability. This feature allows the system administrators not to offer the local service for a single ONU (ONT) upgrade at the customer premise. To upgrade an ONU (ONT) successfully, you need to download a new ONU (ONT) firmware in the system.

13.2.20.1 Manual Upgrade (1)

(1) Downloading Firmware to OLT

To download ONU (ONT) firmware in the system, use the following command.

Command	Mode	Description
copy {**ftp** | **tftp**} **onu firmware download**	Enable	Downloads ONU firmware via FTP or TFTP.
copy onu firmware *source-file-name destication-file-name*		Save the file name of the existing firmware with a new firmware filename (destination-file-name).

The following is an example of downloading ONU (ONT) firmware in the system.

```
SWITCH# copy ftp onu firmware download
 To exit : press Ctrl+D
--------------------------------------
IP address or name of remote host (FTP): xxx.xxx.xxx.xxx
Download File Name : XXXXXX.x
User Name : user
Password:
```

To remove the downloaded ONU (ONT) firmware in OLT, use the following command.

Command	Mode	Description
remove onu firmware {**all** |*FILE-NAME*}	Enable	Removes the downloaded ONU (ONT) firmware in OLT.

To display the list of the downloaded ONU (ONT) firmware in OLT, use the following command.

Command	Mode	Description
show onu firmware-list	Enable Global	Shows the downloaded ONU (ONT) firmware list in OLT.

	Interface [GPON]	

(2) Downloading Firmware to ONU (Upgrading)

To download the specified ONU (ONT) firmware in the ONU (ONT), use the following command.

Command	Mode	Description
onu firmware download *ONU-ID FILE_NAME* {**os1** | **os2**}	Interface [GPON]	Downloads ONU (ONT) firmware in the ONU (ONT). ONU-ID: ONU ID (1-128) or ONU serial number FILE_NAME: ONU firmware name

You can see the status of ONU firmware by the **show onu firmware version** command as follows:

To display the status of ONU firmware, use the following command.

Command	Mode	Description
show onu firmware version gpon *OLT-ID* [*ONU-IDs*]	Enable Global	Shows the status of ONU firmware. OLT-ID: GPON port number ONU-ID: ONU ID (1-128) or ONU serial number
show onu firmware version [*ONU-IDs*]	Interface [GPON]	Shows the status of ONU firmware. ONU-ID: ONU ID (1-128) or ONU serial number

(3) Specifying Default OS of ONU

To specify the default OS of ONU (ONT), use the following command.

Command	Mode	Description
onu firmware commit *ONU-ID* {**os1** | **os2**}	Interface [GPON]	Specifies the default OS of ONU (ONT).

(4) Restarting ONU

In order to use the new upgraded firmware, you should restart the ONU (ONT). At this time, the upgraded OS should be specified as a default OS by using **onu firmware commit** command.

Before restarting the ONU (ONT), you should check the service status of ONU, whether to save the other configuration, or else.

To restart an ONU (ONT), use the following command.

Command	Mode	Description
onu reset *ONU-ID*	Interface [GPON]	Resets a specified ONU. ONU-ID: ONU ID (1 to128) or ONU serial number

- **Changing Active Firmware**

If an ONU supports the dual OS, you can change the active firmware using the following command. To change the active firmware, use the following command.

Command	Mode	Description
onu firmware active-change *ONU-ID*	Interface [GPON]	Changes the active OS of ONU (with ONU reboot). ONU-ID: ONU ID (1 to 128) or ONU serial number

13.2.20.2 Manual Upgrade (2)

(1) Downloading Firmware to OLT

To download ONU (ONT) firmware in the system, use the following command.

Command	Mode	Description
copy {**ftp** | **tftp**} **onu firmware download**	Enable	Downloads ONU firmware via FTP or TFTP.

The following is an example of downloading ONU (ONT) firmware in the system.

```
SWITCH# copy ftp onu firmware download
 To exit : press Ctrl+D
--------------------------------------
IP address or name of remote host (FTP): xxx.xxx.xxx.xxx
Download File Name : XXXXXX.x
User Name : user
Password:
```

To remove the downloaded ONU (ONT) firmware in OLT, use the following command.

Command	Mode	Description
remove onu firmware {**all** |*FILE-NAME*}	Enable	Removes the downloaded ONU (ONT) firmware in OLT.

To display the list of the downloaded ONU (ONT) firmware in OLT, use the following command.

Command	Mode	Description
show onu firmware-list	Enable Global Interface [GPON]	Shows the downloaded ONU (ONT) firmware list in OLT.

(2) Upgrading Firmware

To upgrade an ONU (ONT) with the downloaded ONU (ONT) firmware, use the following command.

Command	Mode	Description
onu upgrade *ONU-ID FILENAME* {**ftp** *A.B.C.D USER PASSWD* | **tftp** *A.B.C.D*}	Interface [GPON]	Upgrades an ONU (ONT) with a specified firmware. ONU-ID: ONU ID (1-128) or ONU serial number FILENAME: firmware file name A.B.C.D: FTP/TFTP server IP address USER: FTP server user name PASSWD: FTP server password
onu upgrade bootloader *ONU-ID FILENAME*		Upgrades the bootloader image of ONU (ONT) ONU-ID: ONU ID (1-128) or ONU serial number FILENAME: bootloader image file name

If you execute the **onu upgrade** command, the firmware stored in OLT is downloaded to the standby (not running) OS of the specified ONU (ONT), and the standby OS is specified as default one. For example, if OS1 is running, the firmware is downloaded to OS2, and the OS2 is specified as the default.

When completing the firmware upgrade, the related Syslog message is reported.

(3) Restarting ONU

In order to use the new upgraded firmware, you should restart the ONU (ONT).

Before restarting the ONU (ONT), you should check the service status of ONU, whether to save the other configuration, or else.

To restart an ONU (ONT), use the following command.

Command	Mode	Description
onu reset *ONU-ID*	Interface [GPON]	Resets a specified ONU. ONU-ID: ONU ID (1 to128) or ONU serial number

To display the status of ONU firmware, use the following command.

Command	Mode	Description
show onu firmware version gpon *OLT-ID* [*ONU-IDs*]	Enable Global	Shows the status of ONU firmware. OLT-ID: GPON port number ONU-ID: ONU ID (1-128) or ONU serial number
show onu firmware version [*ONU-IDs*]	Interface [GPON]	Shows the status of ONU firmware. ONU-ID: ONU ID (1-128) or ONU serial number
show onu bootloader version gpon *OLT-ID* [*ONU-IDs*]	Enable Global	Shows the ONU bootloader version information. OLT-ID: GPON port number ONU-ID: ONU ID (1-128) or ONU serial number
show onu bootloader version [*ONU-IDs*]	Interface [GPON]	

- **Changing Active Firmware**

If an ONU supports the dual OS, you can change the active firmware using the following command. To change the active firmware, use the following command.

Command	Mode	Description
onu firmware active-change *ONU-ID*	Interface [GPON]	Changes the active OS of ONU (with ONU reboot). ONU-ID: ONU ID (1 to 128) or ONU serial number

13.2.20.3 Auto Upgrade

For efficient system maintenance, the LD3032 provides the auto upgrade functionality for ONU firmware in the operational environment. You can simply upgrade the ONU firmware without an effort for every single ONU.

(1) Downloading Firmware to OLT

To download ONU (ONT) firmware in the system, use the following command.

Command	Mode	Description
copy {**ftp** | **tftp**} **onu firmware download**	Enable	Downloads ONU firmware via FTP or TFTP.

To remove the downloaded ONU (ONT) firmware in OLT, use the following command.

Command	Mode	Description
remove onu firmware {**all** |*FILE-NAME*}	Enable	Removes the downloaded ONU (ONT) firmware in OLT.

To display the list of the downloaded ONU (ONT) firmware in OLT, use the following command.

Command	Mode	Description
show onu firmware-list	Enable Global Interface [GPON]	Shows the downloaded ONU (ONT) firmware list in OLT.

(2) Auto Upgrade Configuration

Download GPON ONU firmware using the following command.

Command	Mode	Description
onu auto-upgrade firmware *NAME FW_NAME*	Global	Configures to be auto-upgraded with the specified firmware for the ONU. NAME: ONU model name FW_NAME: ONU firmware name

onu auto-upgrade firmware *NAME FW_NAME* {**ftp** *A.B.C.D USER PASSWD* | **tftp** *A.B.C.D*}		Configures to be auto-upgraded with the specified firmware for the ONU through the TFTP/FTP server. NAME: ONU model name FW_NAME: ONU firmware name A.B.C.D: FTP/TFTP server IP address USER: FTP server user name PASSWD: FTP server password
no onu auto-upgrade firmware *NAME*		Deletes the auto-upgrade configured for the specified ONU. NAME: ONU model name

The firmware downloaded by **copy** {**ftp** | **tftp**} **onu download** command is deleted when the OLT system restarts. If you want to perform auto-upgrade even when the firmware does not exist in the OLT, you should specify the TFTP/FTP server from which the firmware can be downloaded.

To display the information of TFTP/FTP server specified for auto-upgrade, use the following command.

Command	Mode	Description
show onu auto-upgrade firmware [**info**]	Enable Global	Shows the information of TFTP/FTP server specified for auto-upgrade.

The following is an example of displaying the information of the specified TFTP/FTP server.

```
SWITCH(config)# show onu auto-upgrade firmware info
 -------------------------------------------------------------------------------
        Firmware Name        | T/FTP |       IP       |    User    |  Password
 -------------------------------------------------------------------------------
   G_ONU_DALLAS_22_0_8_33.bin |  TFTP |      10.55.2.4 |       XXX |   XXXX
```

To specify the execution condition of ONU auto upgrade configuration above, you should specify a target version of ONU firmware with (or without) **exclude** option. Through the target version and the option, auto upgrade execution condition is determined.

To set the target version for ONU, use the following command.

Command	Mode	Description
onu auto-upgrade target-version *NAME VERSION* [**exclude**]	Global	Sets the target version for ONU. NAME: ONU model name VERSION: target version
no onu auto-upgrade target-version *NAME*		Deletes the configured target version for ONU.

If **exclude** option is used, the auto-upgrade is performed only when the ONU's existing firmware version is *different from* the specified target version. Otherwise, if **exclude** option is not used, the auto-upgrade is performed only when the ONU’s existing firmware version is *same as* the specified target version.

To display the target version configuration for ONU auto upgrade, use the following command.

Command	Mode	Description
show onu auto-upgrade target-version	Enable Global	Shows the target version configuration for ONU auto upgrade.

(3) Specifying Time and Retry Count

- **Specifying Time for Auto Upgrade**

You should set the clock of switch to start auto upgrade of ONU (download to ONU) at specified time. To specify the time to start auto upgrade of ONU, use the following command.

Command	Mode	Description
onu auto-upgrade model-name *NAME* **start-time** <0-23> **end-time** <0-23>	Global	Specifies the time to start auto upgrade of ONU. NAME: ONU model name 0-23: start/end time (unit: o’clock)
onu auto-upgrade model-name *NAME* **start-time disable**		Deletes the specified time.
no onu auto-upgrade model-name *NAME* **start-time**		

To see the ONU model name, use **show onu model-name** command. (See 13.2.21 Displaying ONU Information)

- **Retry Count for Auto Upgrade**

The retry count argument specifies how many times to retry the auto upgrading of ONU if the first attempt fails. To specify the retry count of auto upgrade, use the following command.

Command	Mode	Description
onu auto-upgrade retry-count <3-10>	Global	Specifies the retry count of auto upgrade. 3-10 : retry count (default: 3)
no onu auto-upgrade retry-count		Deletes the configured retry count.

(4) Configuration of ONU Restart

To use the upgraded ONU firmware, the ONU must restart.

You can configure the upgrade-completed ONU to restart at specified time. To specify the time that the upgrade-completed ONU restarts, use the following command.

Command	Mode	Description
onu auto-upgrade reboot-time [*NAME*] {<0-23> | **immediately**}	Global	Specifies the time that the upgrade-completed ONU restarts. NAME: ONU model name 0-23: restart time (unit: o'clock)
onu auto-upgrade reboot-time [*NAME*] **disable**		Deletes the specified time.

(5) Enabling Auto Upgrade (on *GPON Interface Configuration* mode)

To enable/disable ONU auto upgrade on the specific OLT port, use the following command.

Command	Mode	Description
onu auto-upgrade {**enable** | **disable**} [*ONU_IDs*]	Interface [GPON]	Enables/disables ONU auto upgrade configuration on the OLT port.

In order to apply the auto upgrade for ONU, you should enable the configured auto upgrade on the specific OLT port by **onu auto-upgrade enable** command on *GPON Interface Configuration* mode.

To perform the auto upgrade of OLT firmware when the version of two firmware is different, regardless of the lastest firmware version, use the following command.

Command	Mode	Description
onu auto-upgrade version-match all { **enable** | **disable**}	Interface [GPON]	Enables/disables the ONU auto upgrade function without verification of the firmware version.

(6) Displaying Auto-upgrade Configuration

To display the ONU auto upgrade configuration, use the following command.

Command	Mode	Description
show onu auto-upgrade info	Enable Global	Shows a progress of ONU auto-upgrade.
show onu auto-upgrade model-list gpon *OLT-ID* [*NAME*]		Shows a list of ONU model names configured to be auto-upgraded. NAME: ONU model name
show onu auto-upgrade model-list [*NAME*]	Interface [GPON]	

To display the firmware for ONU auto-upgrade, use the following command.

Command	Mode	Description
show onu auto-upgrade firm-	Enable	Shows the firmware information of auto-upgraded

ware [**info**]	Global	ONU.

The following is an example of displaying the firmware for ONU auto-upgrade.

```
SWITCH(config-if[GPON1/1])# show onu auto-upgrade current-fw
Current Firmware : G_ONU_DALLAS_22_0_8_33.bin
```

```
SWITCH(config)# show onu auto-upgrade firmware
 -----------------------------------------------------------------------------
      Model    |         Firmware Name        |    Version    |      Status
 -----------------------------------------------------------------------------
         H645 |    G_ONU_DALLAS_22_0_8_33.bin |     22.1.8.33  | Download Complete
```

To display the status of ONU firmware, use the following command.

Command	Mode	Description
show onu firmware version gpon *OLT-ID* [*ONU-IDs*]	Enable Global	Shows the status of ONU firmware. OLT-ID: GPON port number ONU-ID: ONU ID (1-128) or ONU serial number
show onu firmware version [*ONU-IDs*]	Interface [GPON]	Shows the status of ONU firmware. ONU-ID: ONU ID (1-128) or ONU serial number

- **Changing Active Firmware**

If an ONU supports the dual OS, you can change the active firmware using the following command. To change the active firmware, use the following command.

Command	Mode	Description
onu firmware active-change *ONU-ID*	Interface [GPON]	Changes the active OS of ONU (with ONU reboot). ONU-ID: ONU ID (1 to 128) or ONU serial number

13.2.21 Displaying ONU Information

To display the ONU (ONT) information, use the following command.

Command	Mode	Description
show onu info [**gpon** *OLT-ID*]	Enable Global	Shows the information of ONU (ONT) per OLT ID. OLT-ID: GPON port number
show onu detail-info [**gpon** *OLT-ID*]		Shows the ONU (ONT) information in detail. OLT-ID: GPON OLT port number ONU-ID: ONU ID (1 to 128) or ONU serial number
show onu detail-info [*ONU-ID*]	Interface [GPON]	
show onu info [*ONU-ID*]		Shows the ONU (ONT) information.
show onu feature-list [**gpon** *OLT-ID*]	Enable/Global	Shows the ONU feature list.
show onu feature-list [*ONU-ID*]	Interface [GPON]	

show onu alarm-status [**gpon** *OLT-ID*]	Enable/Global	Shows the alarm status of ONUs.
show onu alarm-status [*ONU-ID*]	Interface [GPON]	

To display the registered ONU (ONT) information, use the following command.

Command	Mode	Description
show onu active [**gpon** *OLT-ID*]	Enable Global	Shows the registered ONU (ONT) information. OLT-ID: GPON port number
show onu active count [**gpon** *OLT-ID*]		Shows the number of active ONUs connected to a specified GPON port.
show onu active [*ONU-ID*]	Interface [GPON]	Shows the registered ONU (ONT) information. ONU-ID: ONU ID (1 to 128) or ONU serial number
show onu active count		Show the number of active ONUs.

To display a reason of ONU deactivation, use the following command.

Command	Mode	Description
show onu deactive-reason gpon *OLT-ID*	Enable/Global	Shows the reason of inactive ONUs.
show onu deactive-reason	Interface [GPON]	

To display the model names of the ONUs connected to a specified OLT, use the following command.

Command	Mode	Description
show onu model-name gpon *OLT-ID*	Enable/Global	Shows the model names of the ONUs. ONU-ID: ONU ID (1 to 128) or ONU serial number
show onu model-name [*ONU-ID*]	Interface [GPON]	

To display the number of MAC addresses currently learned in an ONU, use the following command.

Command	Mode	Description
show onu mac-address gpon *OLT-ID*	Enable/Global	Shows the number of MAC addresses currently learned in ONUs connected to a current OLT.
show onu mac-address [*ONU-ID*]	Interface [GPON]	

To display a host name of the specified ONU, use the following command.

Command	Mode	Description
show onu hostname gpon *OLT-*	Enable/Global	Shows a host name of the specified ONU.

ID		
show onu hostname [*ONU-IDs*]	Interface [GPON]	

To display the IGMP group list of ONU (ONT), use the following command.

Command	Mode	Description
show onu igmp-group-list gpon *OLT-ID ONU-ID*	Enable Global	Shows the current IGMP group list of the ONU. ONU-ID: ONU ID (1 to 128) or ONU serial number
show onu igmp-group-list *ONU-ID*	Interface [GPON]	

To display the status of the ONU (ONT) UNI, use the following command.

Command	Mode	Description
show onu uni-status [**gpon** *OLT-ID*]	Enable Global	Shows the status of the ONU UNI. ONU-ID: ONU ID (1 to 128) or ONU serial number
show onu uni-status [*ONU-IDs*]	Interface [GPON]	
show onu uni-status eth gpon *OLT-ID*	Enable Global	Shows the status of ONU UNI Ethernet port.
show onu uni-status eth [*ONU-IDs*]	Interface [GPON]	

To display the configured description on ONU UNI port, use the following command.

Command	Mode	Description
show onu uni-description gpon *OLT-ID*	Enable Global	Shows the configured description on ONU UNI port.
show onu uni-description [*ONU-ID*]	Interface [GPON]	

To display the configured IP host service ID on ONU, use the following command.

Command	Mode	Description
show onu ip-host gpon *OLT-ID ONU-ID*	Enable Global	Shows the configured IP host service ID on ONU.
show onu ip-host *ONU-ID*	Interface [GPON]	

To display the system or RF video status of ONU, use the following command.

Command	Mode	Description
show onu system-status gpon	Enable	Shows the status of ONU system.

OLT-ID ONU-ID	Global	
show onu system-status *ONU-ID*	Interface [GPON]	
show onu video status gpon *OLT-ID ONU-ID*	Enable Global	Shows the ONU's RF video status.
show onu video status *ONU-ID*	Interface [GPON]	

To display the status of ONU supporting Power over Ethernet (PoE) feature, use the following command.

Command	Mode	Description
show onu poe status gpon *OLT-ID ONU-ID*	Enable Global	Shows the status of PoE ONU system.
show onu poe status *ONU-ID*	Interface [GPON]	

To display the Point-to-Point Protocol over Ethernet (PPPoE)-related authentication information of ONU, use the following command.

Command	Mode	Description
show onu pppoe status gpon *OLT-ID ONU-ID*	Enable Global	Shows the PPPoE authentication information of ONU.
show onu pppoe status *ONU-ID*	Interface [GPON]	

To display information about specified port ID, use the following command.

Command	Mode	Description
show onu port-id gpon *IFPORT*	Enable Global	Shows information about ONU port.

13.2.22 Generic Status Portal (GSP)

The generic status portal managed entity provides a way for the OLT to discover the status and configuration information of a non-OMCI management domain within an ONU. The non-OMCI management domain is indicated by the virtual Ethernet interface point associated with this generic status portal.

The generic status portal ME uses two attributes which are **status** and **config** to convey status and configuration from a non-OMCI managed domain to the OMCI. Each of these attributes uses an XML document to present this information.

Whenever the information in this table changes, and after a soak interval, the ONU issues an AVC to the OLT. The rate at which AVCs are issued is controlled by the **avc-report** attribute.

To configure GSP, follow these steps.

Step 1 You need to open *ONU Profile Configuration* mode to configure an ONU profile. To create an ONU profile, use the following command.

Command	Mode	Description
onu-profile *NAME* **create**	Global	Creates an ONU profile. NAME: ONU profile name

Step 2 To enable GSP function, use the following command.

Command	Mode	Description
gsp {**disable** | **enable**}	ONU-Profile	Enables generic status portal. (default: disable)
gsp avc-report {**enable** {|**10min**|**sec**}|**disable**}		Configures the rate of AVC report. 10min: ONU issues one AVC report to the OLT per 10 minutes sec: ONU issues one AVC report to the OLT per seconds enable: Whenever the information changes, ONU generates AVC report. (Not recommended.) disable: Not generating the report to the OLT

Step 3 To apply the ONU profile to connected ONUs use the following command.

Command	Mode	Description
onu-profile *ONU-IDs NAME*	Interface [GPON]	Applies an ONU profile to specified ONUs. ONU-IDs: ONU ID (1 to 128) or ONU serial number NAME: ONU profile name

Step 4 To update GSP information, use the following command.

Command	Mode	Description
onu gsp update {**status | config**} *ONU_ID*	Interface [GPON]	Updates GSP. ONU_ID: ONU ID (1 to128) or ONU serial number

i

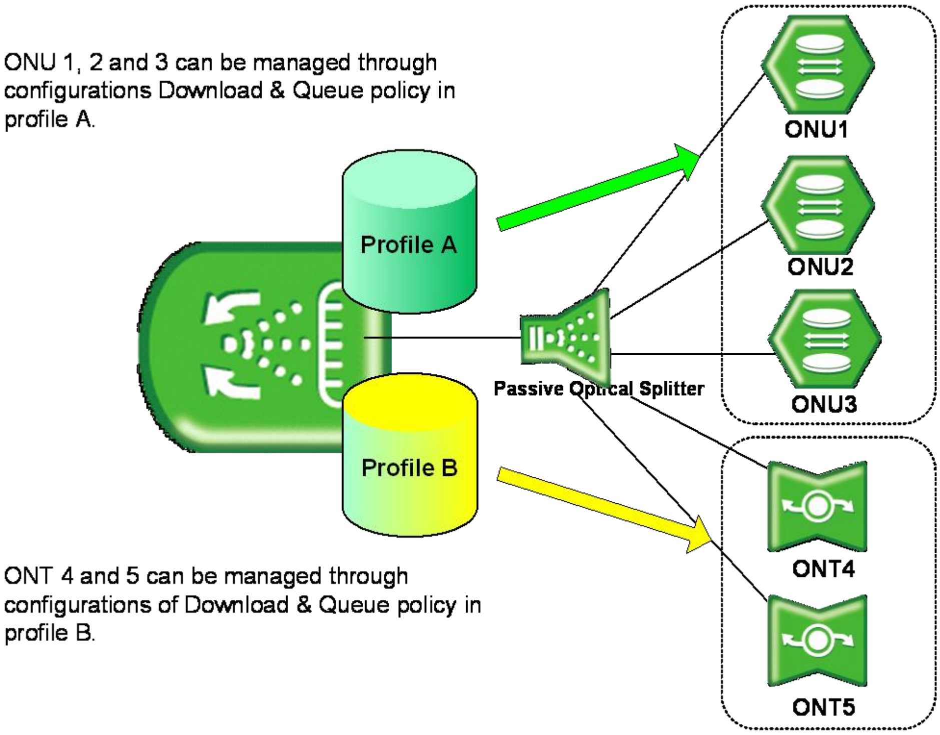
In case of **enable** status, whenever the information in the table changes, GSP will be automatically updated according to ***Step 2*** avc-report rate settings.

Step 5 To display a current configured GSP information, use the following command.

Command	Mode	Description
show onu gsp {**config | status**}	Interface	Shows the configured GSP information.

ONU_ID	[GPON]	config: configuration document table status: status document table ONU_ID: ONU ID (1 to128) or ONU serial number TAG_NAME: tag name
show onu gsp {**status | config**} *ONU_ID* **tag** *TAG_NAME*		
show onu gsp {status | config} *ONU_ID* **tag-list**		

13.3 ONU Profile


ONU 1, 2 and 3 can be managed through configurations Download & Queue policy in profile A.

ONT 4 and 5 can be managed through configurations of Download & Queue policy in profile B.

Fig. 12.3 ONU Profile

The LD3032 provides the easy and efficient management solution for various service environments with the ONU profile.

The ONU profile is a collection of configurations for the operation of an ONU (ONT). You can manage all ONUs connected to an OLT by simply applying the configured profile to ONUs without any local configuration. In case of a modification of a profile, the modified configurations will be automatically applied to ONUs, which are managed by the profile.

This will prevent unnecessary resources to configure every single ONU (ONT), allowing the maintenance efficiency to dramatically increase.

One ONU profile can be applied to several ONUs (ONTs), but one ONU cannot be managed by several ONU profiles.

13.3.1 Creating ONU Profile

You need to open *ONU Profile Configuration* mode to configure an ONU profile. To create an ONU profile, use the following command.

Command	Mode	Description
onu-profile *NAME* **create**	Global	Creates an ONU profile. NAME: ONU profile name

To modify an existing ONU profile, use the following command.

Command	Mode	Description
onu-profile *NAME* **modify**	Global	Modifies an ONU profile. NAME: ONU profile name

To delete a created ONU profile, use the following command.

Command	Mode	Description
no onu-profile {*NAME* | **all**}	Global	Deletes an ONU profile. NAME: ONU profile name

13.3.2 Configuring ONU Profile

13.3.2.1 RX Optical Power Threshold

The ONUs periodically monitor the RX optical power and send the alarm message to their OLT when the RX optical power exceeds the user-defined threshold. To set the transmit rate of an UNI port, use the following command.

Command	Mode	Description
rx-power threshold {**low** *VALUE* [**high** *VALUE*] | **high** *VALUE* [**low** *VALUE*] }	ONU-Profile	Sets the RX optical power threshold and sends RX power high/low alarm to OLT when the RX power exceeds the threshold or it is below the threshold. VALUE: -127 to 0 dBm
no rx-power threshold [**low** | **high**]		Deletes the configured RX optical power threshold.

13.3.2.2 Rogue ONU

The first method is that after detecting the existence of a rogue ONT, the rouge ONT is identified and isolated from the service by the OLT.

GPON OLT allocates the time slot for each ONU to transmit upstream traffic similarly to the TDM method. The allocated time is announced by the bandwidth map that is contained in the downstream GEM frame and the ONT only transmits the traffic based on the allocated bandwidth map. Due to this nature of GPON technology, the wrong transmit time of the ONT makes collision in upstream direction. This can be resulted from continuous transmitting data of the malfunctioned ONT which is called “Rogue ONT”.

The polling interval attribute represents the interval of polling optical transceiver at the ONT. And the polling count for rogue ONT attribute represents the number of consecutive polling, which results in abnormality, for declaring the optical transceiver as abnormal.

To configure a polling interval and count for rogue ONT, use the following command.

Command	Mode	Description
rogue onu polling [<10-60000> <1-250>]	ONU-Profile	Specifies a polling interval and count for rogue ONT. 10-60000: polling interval value (unit: millisecond) 1-250: polling count
rogue onu polling disable		Deletes the specified polling interval and count.

To enable/disable the alarm for rogue ONU and specify the alarm count that is the maximum number of retransmission of alarms in case of no response from OLT, use the following command.

Command	Mode	Description
rogue onu alarm enable <1-5>	ONU-Profile	Enables the alarm after detecting a rogue ONU. 1-5: alarming count
rogue onu alarm disable		Disables the alarm after detecting a rogue ONU.

To set the waiting time for OLT’s response, use the following command.

Command	Mode	Description
rogue onu waiting-time <100-50000>	ONU-Profile	Sets the waiting time for OLT’s response 100-50000: waiting time (unit: millisecond)
rogue onu waiting-time disable		Deletes the specified waiting time for OLT’s response.

13.3.2.3 Card Type Configuration

You need to select a card type in case that ONT is provided with the configurable circuit pack (e.g., T1/E1). To set a card type on the configurable circuit pack, use the following command.

Command	Mode	Description
circuit-pack card-config c-ds1-e1 {**ds1** | **e1**}	ONU-Profile	Selects a card type on the configurable circuit pack. c-ds1-e1: Configurable DS1/E1 module c-ds1-e1-j1: Configurable DS1/E1/J1 module
circuit-pack card-config c-ds1-e1-j1 {**ds1** | **e1** | **j1**}		
no circuit-pack card-config {**c-ds1-e1** | **c-ds1-e1-j1**}		Deletes the configuration of card type on the configurable circuit pack.

13.3.2.4 Loop Detect Configuration

A loop may occur when double paths are used for the link redundancy between switches and one sends unknown unicast or multicast packet that causes endless packet floating on the LAN. That superfluous traffic eventually can result in network fault.

The LD3032 provides the function to configure the ONU’s loop detecting. The loop detecting mechanism is as follows:

The ONU periodically sends the loop-detecting packet to all the ports with a certain interval, and then if the loop-detecting packet is received, the switch performs a pre-defined behavior.

To enable/disable the loop detection, use the following command.

Command	Mode	Description
loop-detect {**enable** | **disable**}	ONU-Profile	Enables/disables the loop detection.

To define the behavior when a loop is occurred, use the following command.

Command	Mode	Description
loop-detect block	ONU-Profile	Enables the blocking option. This configures to automatically change the state to BLOCKED when a loop is detected. (default: disable)
loop-detect block block-timer {<1-65535> | **unlimited**}		Sets the interval of changing the state of BLOCKED to NORMAL. 1-65535: interval (unit: second, default: 600) unlimited: do not change the state
no loop-detect block		Disables the blocking option.

To set the interval of sending the loop-detecting packet, use the following command.

Command	Mode	Description
loop-detect send-period <1-65535>	ONU-Profile	Sets the interval of sending the loop-detecting packet. 1-65535: interval (unit: second)

13.3.2.5 ONU Threshold

To set the threshold of ONU CPU load, use the following command.

Command	Mode	Description
cpu-load threshold <0-100>	ONU-Profile	Sets the threshold of CPU load in the unit of percent (%). 0-100: ONU CPU load threshold value
no cpu-load threshold		Deletes the configured threshold of CPU load.

To set the threshold of ONU temperature, use the following command.

Command	Mode	Description
temperature high-threshold <-40-100>	ONU-Profile	Sets the threshold of ONU temperature in the unit of centigrade (°C). -40-100: ONU temperature
temperature low-threshold <-40-100>		
no temperature { **high-threshold** | **low-threshold** }		Deletes a configured threshold of ONU temperature.

To set the threshold of ONU memory in use, use the following command.

Command	Mode	Description
memory-usage threshold <0-100>	ONU-Profile	Sets the threshold of ONU memory in the unit of percent (%). 0-100: ONU memory in use
no memory-usage threshold		Deletes the configured threshold of ONU memory.

13.3.2.6 Uplink MAC learning

To enable/disable the MAC learning of ONT's internal switch, use the following command.

Command	Mode	Description
switch-control uplink-mac-learning enable	ONU-Profile	Enables the MAC learning of ONU's uplink port
switch-control uplink-mac-learning disable		Disables the MAC learning of ONU's uplink port

i

This feature is available for the H645B, H645, H645A only.

To display the uplink MAC learning status of ONU, use the following command.

Command	Mode	Description
show onu switch-control gpon *OLT-ID ONU-ID*	Enable/Global	Shows the uplink MAC learning status of ONU's uplink port.
show onu switch-control *ONU-ID*	Interface [GPON]	

13.3.2.7 GPON Optic Module Threshold of ONU

The ONU's GPON optic module can operate depending on monitoring type of temperature, RX/TX power, voltage or Txbias. To set the threshold of GPON optical transceiver of ONU, use the following command.

Command	Mode	Description
ani-rx-power threshold {**low** *VALUE* [**high** *VALUE*] | **high** *VALUE* [**low** *VALUE*] }	ONU-Profile	Configures the RX optical power threshold and sends the configured threshold value to ONUs. The ONUs monitors the change of values and sends RX power high/low alarm to OLT when the RX power exceeds the threshold or it is below the threshold. VALUE: RX power threshold value (-127 to 0 dBm)
ani-tx-power threshold {**low** *VALUE* [**high** *VALUE*] | **high** *VALUE* [**low** *VALUE*] }		Configures the TX optical power threshold and sends the configured threshold value to ONUs. The ONUs monitors the change of values and sends TX power high/low alarm to OLT when the TX power exceeds the threshold or it is below the threshold. VALUE: TX power threshold value (-127 to 0 dBm)

ani-temperature threshold {**low** *VALUE* [**high** *VALUE*] | **high** *VALUE* [**low** *VALUE*] }		Configures the temperature threshold and sends the configured threshold value to ONUs. The ONUs monitors the change of values and sends temperature high/low alarm to OLT when the temperature exceeds the threshold or it is below the threshold. VALUE: temperature threshold value (-128～127℃）
ani-tx-bias threshold {**low** *VALUE* [**high** *VALUE*] | **high** *VALUE* [**low** *VALUE*] }		Configures the txbias threshold and sends the configured threshold value to ONUs. The ONUs monitors the change of values and sends txbias high/low alarm to OLT when the txbias exceeds the threshold or it is below the threshold. VALUE: tx-bias threshold value (0～ 131 mA）
ani-voltage threshold {**low** *VALUE* [**high** *VALUE*] | **high** *VALUE* [**low** *VALUE*] }		Configures the voltage threshold and sends the configured threshold value to ONUs. The ONUs monitors the change of values and sends voltage high/low alarm to OLT when the voltage exceeds the threshold or it is below the threshold. VALUE: voltage threshold value (0～ 10.0 V)

To delete the threshold of module operation depending on specified monitoring type, use the following command.

Command	Mode	Description
no {**ani-rx-power** | **ani-voltage** | **ani-tx-bias** | **ani-tx-power** | **ani-temperature**} **threshold** [{**low** | **high**}]	ONU-Profile	Deletes the configured threshold.

13.3.2.8 CPU Packet Limit

ONU CPU packet limitation is one of important protecting mechanism from traffic attacking. For example, the ONU CPU packet forwarding is configured with 1000 PPS for broadcast packet, 1000 broadcast packet per second will be forwarded by ONU CPU.

To configure maximum PPS of ONU for Broadcast / Unknown-multicast / L2 DLF type of packet, use the following command.

Command	Mode	Description
cpu-packet-limit {**broadcast** | **multicast** | **dlf**} *RATE*	ONU-Profile	Limits the broadcast / unknown-multicast / L2 DLF packets per second forwarded by ONU CPU. RATE: 100 to 40000 PPS (Unit: packet per second)
no cpu-packet-limit {**broadcast** | **multicast** | **dlf**}		Deletes the configured CPU packet limit.

13.3.2.9 DLF Trap to CPU

To enable/disable the upstream Destination Lookup Failure (DLF) packet forwarding to a CPU, use the following command.

Command	Mode	Description
trap-to-cpu dlf enable	ONU-Profile	Forwards the upstream DLF packets to a CPU.
trap-to-cpu dlf disable		Forwards the upstream DLF packets according to the VLAN rules.

13.3.2.10 MAC Full Policy

By default, ONT will block new source MAC address frame when ONT MAC table is full. The protecting mechanism can be configurable by 'block or forwarding', thus you can configure the basic policy of ONT when MAC table is full.

To block/forward new source MAC address frame when MAC table is full, use the following command.

Command	Mode	Description
mac-full policy forward	ONU-Profile	Forwards new source MAC address frame when ONU MAC table is full.
mac-full policy drop		Blocks new source MAC address frame when ONU MAC table is full.

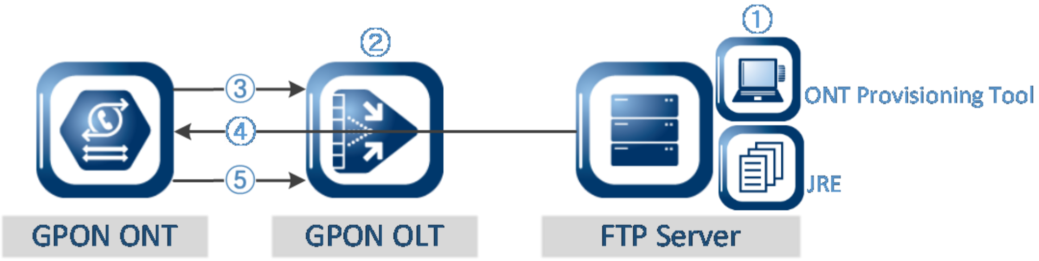
13.3.2.11 ONT Auto-configuration and Service Provisioning

Automated provisioning and remote management of ONTs are vital service delivery activities of ISPs and operators - helping to reduce costs, lead times and complexity as well as to deploy new subscriber services.

ONT provisioning method simplifies network operations by eliminating the need to configure every network element interface between the OLT ingress and subscriber ports of our ONTs (H64x series) for diverse GPON service applications.

If the ONT service provisioning settings in XML file are saved in a FTP server prior to installation/activation of ONTs, the OLT can relay the configured XML file from the FTP server to the activated ONTs using the commands.

ONT Provisioning Process



① **ONT Provisioning Tool & JRE Installation**: Install JRE (version 1.6) and provisioning tool (ONTProvisionTool.exe) to FTP server. Create a new XML configuration file and modify the ONT settings for ONT provisioning. The ONT configuration parameters can be changed or saved in XML.

② **File Transfer from FTP server to ONT**: For the ONT configuration file (XML file) transfer, the ONT provisioning-related commands should be executed on the OLT. The OLT is capable to relay the user-defined XML file from the FTP server to the activated ONTs.

③ **ONT Activation**

④ **Receive XML configuration file from FTP server**: The ONT receives the ONT service configuration file in XML from FTP server. The new service settings are assigned to this ONT.

⑤ **Send File Transfer Message**: On the OLT side, the OLT can monitor a file transfer status by receiving the messages (“File transfer in progress”, “File transfer complete”, “Remote failure”, “Local failure”) from ONT.

IP-Path Management

To configure the ONT provisioning feature and specify a FTP server and GPON provisioning file, use the following command.

Command	Mode	Description
onu mgmt-mode ip-path *ONU_ID* **ftp id** *ID* **password** [*PASSWORD*]	Interface [GPON]	Sets an user name and password to access FTP server for GPON ONT provisioning. ONU-ID: 1-128 or ONU serial number ID: user name PASSWD: password
onu mgmt-mode ip-path *ONU_ID* **uri** *URI* **file** {*FILE_NAME* | **none**}		Specifies a FTP server and ONT provisioning file (XML file) name. URI: FTP server address FILE_NAME: ONT provisioning file name **none**: The file name is named after GPON serial number of each ONT. The ONT is supposed to ask .xml provisioning file named after its own GPON serial number. If selecing this option, it is necessary that the FTP server has each .xml provisioning file corresponding to each ONT.

no onu mgmt-mode ip-path *ONU_ID*		Deletes the configurations of GPON provisioning.

To configure the ONT provisioning feature in *ONU-Profile Configuration* mode and specify a FTP server and GPON provisioning file, use the following command.

Command	Mode	Description
mgmt-mode mode ip-path	ONU-Profile	Selects the MGMT IP-Path mode for ONT provisioning.
mgmt-mode ip-path ftp id *ID* **password** [*PASSWORD*]		Sets an user name and password to access FTP server for GPON ONT provisioning. ID: user name PASSWD: password
mgmt-mode ip-path uri *URI* **file** {*FILE_NAME* | **none**}		Specifies a FTP server and ONT provisioning file (XML file) name. URI: FTP server address FILE_NAME: ONT provisioning file name **none**: The file name is named after GPON serial number of each ONT. The ONT is supposed to ask .xml provisioning file named after its own GPON serial number. If selecing this option, it is necessary that the FTP server has each .xml provisioning file corresponding to each ONT.
no mgmt-mode mode		Deletes the configured GPON provisioning mode.
no mgmt-mode ip-path		Deletes the configurations of GPON provisioning per ONT.

i

You can configure ONT provisioning in both *ONU-Profile* and *GPON Interface* Configuration modes. The configuration in *GPON Interface* mode has higher priority in the system.

To display the GPON provisioning configuration for each ONT, use the following command.

Command	Mode	Description
show onu mgmt ip-path gpon *OLT-ID*	Enable Global	Shows the information of ONT provisioning configuration.
show onu mgmt ip-path *ONU-ID*	Interface [GPON]	

TR-069 Management

One of the provisioning methods is the standard open protocol TR-069. The TR-069 protocol is HTTP-based and provides communication between the ONT and an ACS (Auto Configuration Server). TR-069 protocol simplifies ONT management by specifying the use of an ACS to perform remote, centralized management of ONTs. The LD3032 supports TR-069 to provision and manage ONTs.

To enable/disable the TR-069 management, use the following command.

Command	Mode	Description
mgmt-mode mode tr-069	ONU-Profile	Enables the TR-069 management mode.
no mgmt-mode mode		Disables the TR-069 management mode.

To configure the TR-069 management mode, use the following command.

Command	Mode	Description
mgmt-mode tr-069 uri *URI*	ONU-Profile	Configures TR-069 management server address. URI: URI address of the TR-069 management server
mgmt-mode tr-069 access id *ID* **password** *PASSWD*		Specifies the user name and password to access management server. ID: user name PASSWD: password
mgmt-mode tr-069 associated-tag *VLAN*		Specifies a VLAN ID for TR-069 traffic.
no mgmt-mode tr-069 uri		Deletes the configured server address.
no mgmt-mode tr-069 access		Deletes the defined user name and password.
no mgmt-mode tr-069 associated-tag		Deletes the VLAN ID for TR-069 management.

13.3.2.12 Applying Traffic & PM Profile

To add/delete the user-defined Traffic profile to a specified ONU profile, use the following command.

Command	Mode	Description
traffic-profile *NAME*	ONU-Profile	Adds the existing Traffic profile to ONU profile. NAME: Traffic profile name
no traffic-profile		Removes the Traffic profile from ONU profile.

i For the details of how to create and configure the traffic profile, see 13.4 Traffic Profile.

To add/delete the user-defined PM profile to a specified ONU profile, use the following command.

Command	Mode	Description
pm-profile *NAME*	ONU-Profile	Adds the existing PM profile to ONU profile. NAME: Traffic profile name
no pm-profile		Removes the PM profile from ONU profile.

i For the details of how to create and configure the PM profile, see 13.10 Performance Monitoring (PM) Profile.

13.3.3 Overwriting Traffic Profile Configuration

Basically, one traffic profile can be applied to the ONU profile. So, if a number of cases for traffic profile configuration are required on the ONU profile, the user should create the corresponding traffic profiles and apply them to the ONU profile.

The overwriting traffic profile configuration can help reducing the count of creating and applying the traffic profile. This configuration overwrites the corresponding setting of the applied traffic profile.

13.3.3.1 VLAN Configurations

To configure a VLAN tagging operation for a specific UNI port, use the following command.

Command	Mode	Description
uni eth *UNI-PORT* **vlan-operation us-oper keep**	ONU-Profile	Sets the policy of VLAN tagging for upstream frame. keep: keeps forwarding the existing tagged/untagged frame
uni eth *UNI-PORT* **vlan-operation us-oper** {**add** | **overwrite**} <1-4094> <0-7>		Sets the policy of VLAN tagging for upstream frame. add: adds a specified VID (double tagging) with tag in case of tagged frame overwrite: replaces an existing tagged/untagged frame to a specified VID with tag. 1-4094: VLAN ID 0-7: CoS value
uni eth *UNI-PORT* **vlan-operation ds-oper** {**keep** | **remove**}		Sets the policy of VLAN tagging for downstream frame. keep: keeps forwarding the incoming tagged frame from OLT to UNI. remove: removes a tag from the incoming tagged packet and forwards it to UNI.
no uni eth *UNI-PORT* **vlan-operation us-oper**		Deletes the configured policy of VLAN tagging operation.
no uni eth *UNI-PORT* **vlan-operation ds-oper**		

13.3.3.2 Max Host

To configure the maximum number of hosts for a MAC bridge ID, use the following command.

Command	Mode	Description
bridge *BRIDGE-ID* **max-hosts** <0-255>	ONU-Profile	Sets the maximum number of hosts that can connect to the specified MAC bridge ID. BRIDGE-ID: MAC bridge ID 0-255: the maximum number of hosts (0: unlimited)

13.3.3.3 Rate Limit

To configure the rate limit for downstream traffic of an ONU, use the following command.

Command	Mode	Description
uni eth *UNI-PORT* **rate-limit downstream** *PIR_BANDWIDTH* [*SIR_BANDWIDTH*]	ONU-Profile	Sets the downstream traffic bandwidth for UNI port. SIR_BANDWIDTH: 0 to 2147483584 (in steps of 64Kbps) PIR_BANDWIDTH: 0 to 2147483584
no uni eth *UNI-PORT* **rate-limit**		Deletes the configured rate limit

To configure the rate limit for downstream traffic of ONU profile, use the following command.

Command	Mode	Description
rate-limit downstream {*RATE* | **unlimited**}	ONU-Profile	Sets the downstream traffic bandwidth for ONU. RATE: 0 to 2147483584 (in steps of 64Kbps)
no rate-limit downstream		Deletes the configured rate limit.

To limit the maximum rate of upstream IGMP traffic, use the following command.

Command	Mode	Description
igmp us-rate-limit <1-65535>	ONU-Profile	Limits the maximum rate of upstream IGMP traffic. 1-65535: maximum IGMP packets per second
no igmp us-rate-limit		Deletes the configured IGMP packet limit.

13.3.3.4 IGMP Group List

You can configure the maximum number of multicast groups that a host on a port can join. To specify the maximum number of IGMP groups per UNI-side port, use the following command.

Command	Mode	Description
uni eth *UNI-PORT* **igmp max-groups** <0-255>	ONU-Profile	Specifies the maximum number of IGMP groups for a port. UNI-PORT: UNI port number 0-255: number of IGMP groups (default: 16)

You can configure the maximum number of multicast groups that a host on a port can join. To specify the maximum number of IGMP groups, use the following command.

Command	Mode	Description
igmp max-groups <0-255>	ONU-Profile	Specifies the maximum number of IGMP groups. 0-255: maximum number of IGMP groups (default: 16)
no igmp max-groups		Deletes a specified maximum number of IGMP groups.

13.3.3.5 Activating Administration for Ethernet UNI

To enable/disable the administration of the Ethernet UNI port, use the following command.

Command	Mode	Description
uni eth *UNI-PORT* **port-admin** {**enable** | **disable**}	ONU-Profile	Enables/disables the administration of Ethernet UNI port on the specified ONU.

i To see the admin status of the ONU (ONT) UNI, use **show onu uni-status** command. (See 13.2.21 Displaying ONU Information)

13.3.3.6 Mapping between T-CONT ID and DBA profile

To specify the GEM ports (priority queue) per T-CONT and the bandwidth of GEM port by mapping between T-CONT ID and DBA profile, use the following command.

Command	Mode	Description
tcont *TCONT-ID* **dba-profile** *DBA-PROFILE*	ONU-Profile	Specifies the priority queues of T-CONT by mapping between the DBA profile and T-CONT ID. Sets T-CONT's bandwidth by specifying the DBA profile DBA-PROFILE: DBA profile name
no tcont *TCONT-ID* **dba-profile**		Disables the mapping between T-CONT ID and DBA profile.

13.3.4 Saving Profile

After configuring an ONU profile, you need to save the profile with the following command.

Command	Mode	Description
apply	ONU-Profile	Saves an ONU profile configuration.

i Even if you modify a running profile, you also need to use the **apply** command to apply the changes to ONUs (ONTs).

13.3.5 Applying ONU Profile

To apply/release an ONU profile to/from connected ONUs (ONTs), use the following command.

Command	Mode	Description
onu-profile *ONU-IDs NAME*	Interface [GPON]	Applies an ONU profile to specified ONUs. ONU-IDs: ONU ID (1 to 128) or ONU serial number NAME: ONU profile name
no onu-profile *ONU-IDs*		Releases an ONU profile from connected ONUs. ONU-ID: ONU ID (1 to 128) or ONU serial number

13.3.6 Checking ONU Profile Configuration

To display the status of ONU profile configuration, use the following command.

Command	Mode	Description
show onu status [**gpon** *OLT-ID*]	Enable Global	Shows the status of ONU profile configuration.
show onu status [*ONU-ID*]	Interface [GPON]	

You should check the status of ONU profile configuration by using the **show onu status** command. If the configuration is normal, the system shows “success”. Otherwise, if the configuration fails, it shows the reason of failure.

13.3.7 Displaying ONU profile

To display a configured ONU profile, use the following command.

Command	Mode	Description
show onu-profile [*NAME*]	Enable Global Interface [GPON]	Shows a configured ONU profile. NAME: ONU profile name

To display the list of ONUs (ONTs) where an ONU profile is applied, use the following command.

Command	Mode	Description
show onu-profile onu-list *NAME*	Enable Global	Shows the list of ONUs (ONTs) where an ONU profile is applied. NAME: ONU profile name

To display the information of current profile, use the following command.

Command	Mode	Description
show current-profile	Current-Profile	Shows the information currently configured for the profile.

13.4 Traffic Profile

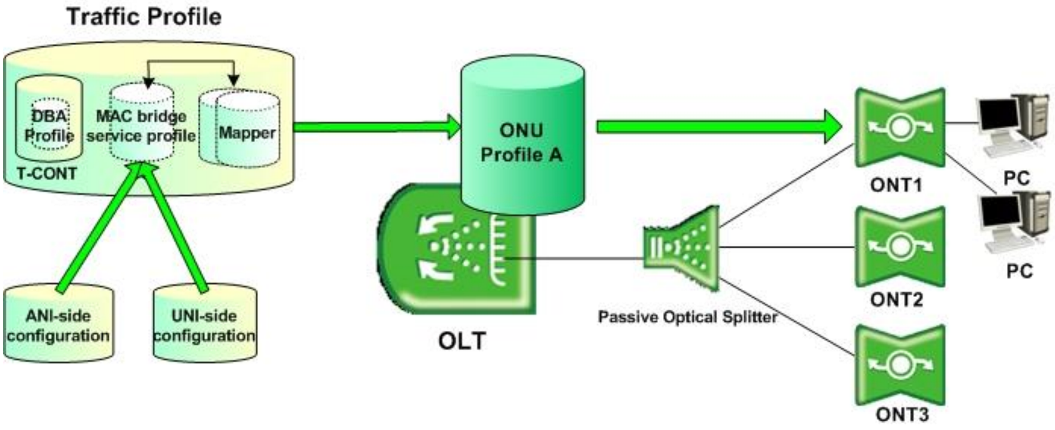


Fig. 12.4 Traffic Profile

The LD3032 provides the easy and efficient management solution for various service models that are comprised of MAC bridging and 802.1p mapping functionality using the traffic profile.

There are two major layer 2 functions available: MAC bridging and 802.1p mapping. MAC bridging is described in IEEE 802.1D. The bridge has many features, and can be used to direct traffic based on MAC address or on VLAN characteristics (using the VLAN filter feature). The mapping function describes the steering of traffic from one UNI-side entity to ANI-side port-IDs. The mapper is equivalent to a MAC bridge with VLAN filters that only operate on the priority bits of the VLAN tags.

i The LD3032 is supported by all G.984.4 compliant vender system based on the 1:N, N:M, 1:MP, and N:MP model. Only a single 802.1p mapper is need for 1:N, N:M model deployments. However, multiple 802.1p mappers can be used for 1:MP, N:MP model deployments.

13.4.1 Creating Traffic Profile

To create a traffic profile and open *Traffic Profile Configuration* mode, use the following command.

Command	Mode	Description
traffic-profile *NAME* **create**	Global	Creates a traffic profile. NAME: traffic profile name

After opening *Traffic Profile Configuration* mode, the prompt changes from SWITCH(config)# to SWITCH(config-traffic-pf[*NAME*])#.

To delete a created traffic profile, use the following command.

Command	Mode	Description
no traffic-profile {*NAME* | **all**}	Global	Deletes the traffic profile with its all configurations.

To modify an existing traffic profile, use the following command.

Command	Mode	Description
traffic-profile *NAME* **modify**	Global	Modifies the existing traffic profile. NAME: traffic profile name

i

The OMCI and service model of MAC bridging and 802.1p mapping functionality must be supported by the ONUs (ONTs).

13.4.2 Creating a Mapper

A mapper provides support for upstream flow routing based on 802.1p priority bits. The LD3032 supports the DSCP to IEEE802.1p mapping to allow the OLT to prioritize all traffic based on the incoming DSCP value according to the DiffServ to IEEE802.1p mapping table.

To create an IEEE802.1p mapper for a specified traffic profile, use the following command.

Command	Mode	Description
mapper *MAPPER_ID*	Traffic-Profile	Creates a 802.1p mapper for a specified traffic profile. MAPPER_ID: 1 to 32, 802.1p mapper ID
no mapper *MAPPER_ID*		Removes the created mapper from the traffic profile

i

The LD3032 is supported by all G.984.4 compliant vender system based on the 1:N, N:M, 1:MP, and N:MP model. Only a single 802.1p mapper is need for 1:N, N:M model deployments. However, multiple 802.1p mappers can be used for 1:MP, N:MP model deployments.

To configure a mapper for upstream transmission, use the following command.

Command	Mode	Description
gemport count {**1** | **2** | **4** | **8**}	Traffic-Mapper	Sets the GEM port count of mapper. The GEM port count corresponds to a total number of priority queues.
dscp-to-pbit {**enable** | **disable**}		Enables/disables the DSCP to P-bit marking for untagged frame forwarding.
default-cos <0-7>		Specifies CoS value for untagged frame forwarding.
cos-mapping cos *RANGE* **gemport** *GEM-PORT-VALUE*		Specifies the range of CoS values for mapping with GEM port. RANGE: CoS range GEM-PORT-VALUE: corresponds to the gemport count

i If a mapper is associated with ports of a bridge, the 802.1ag entities should be associated with the bridge and its port, rather than with the mapper.

To configure the rate limit for an GEM port ID, use the following command.

Command	Mode	Description
gemport *GEM-PORT-RANGE* **rate-limit** { **upstream** | **downstream**} *PIR_VALUE* [*SIR_VALUE*]	Traffic-Mapper	Sets the downstream/upstream traffic bandwidth for GEM port ID. RANGE: GEM port range SIR_VALUE: SIR bandwidth range of 0 to 2147483584 (in steps of 64Kbps) PIR_VALUE: PIR bandwidth range of 0 to 2147483584
no gemport *GEM-PORT-RANGE* **rate-limit** { **upstream** | **downstream** }		Deletes the configured rate limit of GEM port ID.

i You should configure GEM port count for mapper before setting the rate limit for GEM port.

To apply the configured Rate-limit profile for GEM ports, use the following command.

Command	Mode	Description
gemport *RANGE* **rate-limit profile** *NAME*	Traffic-Mapper	Applies the configured Rate-limit profile to specified GEM port. NAME: Rate-limit profile name
no gemport *RANGE* **rate-limit profile**		Removes the Rate-limit profile from the GEM port.

i For the details of how to create and configure the Rate-limit profile, see 13.12 Rate-limit Profile.

13.4.3 MAC Bridge Service Profile

A MAC bridge service profile can be configured per each UNI-side port or it can be configured for the multiple UNI-side ports.

The MAC bridge service profile is comprised of ANI-side port for the upstream traffic management and UNI-side port for the downstream traffic management. The system creates both ANI-side and UNI-side MAC bridge port config data ME.

To create a bridge ID and open a *MAC Bridge Service Profile Configuration* mode, use the following command.

Command	Mode	Description

bridge *BRIDGE_ID*	Traffic-Profile	Creates a bridge ID in traffic profile. BRIDGE_ID: 1 to 32, MAC Bridge ID

After opening *MAC Bridge Service Profile Configuration* mode, the prompt changes from SWITCH(config)# to SWITCH(config-traffic-pf[*NAME*]-bridge[*BRIDGE_ID*])#.

To remove the configured bridge ID from a traffic profile, use the following command.

Command	Mode	Description
no bridge *BRIDGE_ID*	Traffic-Profile	Removes the configured bridge ID from a traffic profile

13.4.3.1 Max Host

To configure the max host for a MAC bridge service profile, use the following command.

Command	Mode	Description
max-hosts <0-255>	Traffic-Bridge Traffic Bridge-UNI	Sets the maximum number of hosts. 0-255: maximum MAC number (0: unlimited)
no max-hosts		Deletes the configured max host.

13.4.3.2 MAC Learning

To enable/disable the ONU’s MAC learning, use the following command.

Command	Mode	Description
mac-learning {**enable** | **disable**}	Traffic-Bridge	Enables/disables the MAC learning for this bridge service profile. (default: enable)

13.4.3.3 UNI Port Bridge

To enable/disable the bridging feature between UNI ports, use the following command.

Command	Mode	Description
port-bridge enable	Traffic-Bridge	Enables the UNI port bridging feature.
port-bridge disable		Disables the UNI port bridging feature.

13.4.3.4 Multicast Interworking Termination Point

The multicast GEM port is represented by a GEM network Connection Termination Point Managed Entity (CTP ME) and a multicast GEM interworking TP ME. The multicast GEM interworking TP is then connected into the ONU through a MAC Bridge Config Data ME.

To enable/disable the MAC bridge port configuration of MAC bridge service profile for multicast Interworking Termination Point (IW TP), use the following command.

Command	Mode	Description

multicast link-mac-bridge enable	Traffic-Bridge	Connects the multicast GEM port network CTP ME to a MAC bridge service profile ME. (default)
multicast link-mac-bridge disable		Disables the connections between the multicast GEM port network CTP ME to the MAC bridge service profile.

13.4.3.5 ANI Port Configuration

To enable/disable a connection between MAC bridge service profile and a mapper ID, use the following command.

Command	Mode	Description
ani mapper *MAPPER_ID*	Traffic-Bridge	Connects a MAC bridge service profile with a mapper ID. MAPPER_ID: IEEE802.1p mapper ID (1 to 32)
no ani mapper *MAPPER_ID*		Disconnects a mapper ID from the MAC bridge service profile.

To enable/disable a connection between MAC bridge service profile and the GEM Port ID Network TCP, use the following command.

Command	Mode	Description
ani gem *GEM_NUM*	Traffic-Bridge	Connects a MAC bridge service profile with a GEM Port ID. GEM_NUM: GEM port ID (1 to 32)
no ani gem *GEM_NUM*		Disconnects a GEM Port ID from the MAC bridge service profile.

If there are more than one mapper connected to a MAC bridge service profile, you need to configure a VLAN tagging filtering for VLAN ID-based traffic forwarding. To enable/disable VLAN tagging filtering function on ANI interface, use the following command.

Command	Mode	Description
vlan-filter [**vid** <1-4094>] **untagged** {**allow** | **discard**}	Traffic Bridge-ANI	Enables a VLAN tagging filtering function of ANI-side port. allow: forwards the untagged frames to the ANI-side port discard: blocks the untagged frames to the ANI-side port 1-4094: VLAN ID(s)
vlan-filter vid {**add** | **del**} *VID*		Adds or deletes the VLAN ID on the VLAN list configured by **vlan-filter vid** command above.
no vlan-filter		Disables the VLAN tagging filtering function.

The LD3032 provides an alternate approach to address filtering from that supported through MAC bridge port filter table data. This alternate approach is useful when all groups of addresses are stored beforehand in the ONU, and it designates which groups are valid or invalid for filtering. On a circuit pack in which all groups of addresses are pre-assigned and stored locally, the ONU creates or deletes an instance of this managed entity automatically upon creation or deletion of a MAC bridge port configuration data ME.

To enable/disable MAC filtering function on ANI interface, use the following command.

Command	Mode	Description
mac-filter {**ip4-mcast** | **ip6-mcast**| **ip4-bcast** | **rarp** | **ipx** | **net-beui** | **apple-talk** | **bridge-manage** | **arp** | **pppoe**}	Traffic Bridge-ANI	Enables the MAC filtering function according to the protocol type for ANI-side bridge port.
no mac-filter {**ip4-mcast** | **ip6-mcast**| **ip4-bcast** | **rarp** | **ipx** | **net-beui** | **apple-talk** | **bridge-manage** | **arp** | **pppoe**}		Disables the MAC filtering function according to the protocol type for ANI-side bridge port.

The following table shows ten attributes that permit the OLT to specify whether MAC address or Ethertypes of the given type are forwarded or filtered. In each case, the initial value of the attribute is 0.

Protocol	MAC Address	Ethertype
IPv4 multicast	01.00.5E.00.00.00 – 01.00.5E.7F.FF.FF	–
IPv6 multicast	33.33.00.00.00.00 –33.33.FF.FF.FF.FF	–
IPv4 broadcast	FF.FF.FF.FF.FF.FF	0x0800
RARP	FF.FF.FF.FF.FF.FF	0x8035
IPX	FF.FF.FF.FF.FF.FF	0x8137
	09.00.1B.FF.FF.FF, 09.00.4E.00.00.02	–
NetBEUI	03.00.00.00.00.01	–
AppleTalk	FF.FF.FF.FF.FF.FF	0x809B, 0x80F3
	09.00.07.00.00.00 – 09.00.07.00.00.FC, 09.00.07.FF.FF.FF	–
Bridge management information	01.80.C2.00.00.00 – 01.80.C2.00.00.FF	–
ARP	FF.FF.FF.FF.FF.FF	0x0806
PPPoE broadcast	FF.FF.FF.FF.FF.FF	0x8863

Tab. 12.3 Protocol Types for MAC Filtering

13.4.3.6 UNI Port Configuration

A UNI-side port is an ONU device port connected to a subscriber. To enable/disable a connection between a MAC bridge service profile and UNI-side port for the downstream traffic, use the following command.

Command	Mode	Description
uni {**eth** | **virtual-eth**} *UNI-PORT*	Traffic	Connects an UNI port of ONT to a specified MAC bridge service profile.

	Bridge	UNI-PORT: UNI port number
no uni {**eth** | **virtual-eth**} *UNI-PORT*		Removes the UNI port of ONT from the MAC bridge service profile.

To specify an Inter-domain name attribute on the virtual Ethernet interface, use the following command.

Command	Mode	Description
inter-domain-name *NAME*	Traffic Bridge-Virtual-ETH-UNI	Specifies the inter-domain name attribute of virtual Ethernet interface. NAME: Inter-domain name (maximum 24 bytes character string)
no inter-domain-name		Deletes the specified inter-domain name of the virtual Ethernet interface.

VLAN Tagging Filtering

To enable/disable VLAN tagging filtering function on the UNI-side port, use the following command.

Command	Mode	Description
vlan-filter [**vid** <1-4094>] **untagged** {**allow** | **discard**}	Traffic Bridge-UNI	Enables a VLAN tagging filtering function of UNI-side port. allow: forwards the untagged frames to UNI-side port discard: blocks the untagged frames to UNI-side port 1-4094: VLAN ID(s)
vlan-filter vid {**add** | **del**} *VID*		Adds or deletes the VLAN ID on the VLAN list configured by **vlan-filter vid** command above.
no vlan-filter		Disables the VLAN tagging filtering function.

VLAN Tagging Operating

To configure a VLAN tagging operation, use the following command.

Command	Mode	Description
vlan-operation us-oper keep	Traffic Bri dge-UNI	Sets the policy of VLAN tagging for upstream frame. keep: keeps forwarding the existing tagged/untagged frame
vlan-operation us-oper {**add** | **overwrite**} <1-4094> <0-7>		Sets the policy of VLAN tagging for upstream frame. add: adds a specified VID (double tagging) with tag in case of tagged frame overwrite: replaces an existing tagged/untagged frame to a specified VID with tag. 1-4094: VLAN ID 0-7: CoS value
vlan-operation ds-oper {**keep** | **remove**}		Sets the policy of VLAN tagging for downstream frame. keep: keeps forwarding the incoming tagged frame from OLT to UNI.

		remove: removes a tag from the incoming tagged packet and forwards it to UNI.
no vlan-operation		Deletes the configured policy for VLAN tagging operation.

Rate Limit

To configure the rate limit for an UNI-side port of ONU, use the following command.

Command	Mode	Description
rate-limit {**upstream** | **downstream**} *PIR_BANDWIDTH* [*SIR_BANDWIDTH*]	Traffic Bridge-UNI	Sets the downstream/upstream traffic bandwidth for UNI port. SIR_BANDWIDTH: 0 to 2147483584 (in steps of 64Kbps) PIR_BANDWIDTH: 0 to 2147483584
no rate-limit {**upstream** | **downstream**}		Deletes the configured rate limit.

To apply the configured Rate-limit profile for an UNI-side port of ONU, use the following command.

Command	Mode	Description
rate-limit profile *NAME*	Traffic Bridge-UNI	Applies the configured Rate-limit profile to specified UNI port. NAME: Rate-limit profile name
no rate-limit profile		Removes the Rate-limit profile from connected UNI port.

i

For the details of how to create and configure the Rate-limit profile, see 13.12 Rate-limit Profile.

To configure the rate limit for the multicast traffic, use the following command.

Command	Mode	Description
multicast rate-limit <0-1031616>	Traffic Bridge-UNI	Sets the maximum bandwidth of multicast traffic. 0-1031616: maximum bandwidth (in steps of 8kbps, 0 is disable)

Maximum Frame Size

To specify the maximum frame size to be handled by an UNI-side port, use the following command.

Command	Mode	Description
max-frame <64-2036>	Traffic Bridge-UNI	Sets the maximum frame size for an UNI port.
no max-frame		Deletes the configured maximum frame size.

IGMP Group

To specify the maximum number of IGMP groups, which are correspond to IGMP join message from the UNI-side port, use the following command.

Command	Mode	Description
igmp max-group <0-255>	Traffic Bridge-UNI	Sets the maximum number of IGMP groups for an UNI port.

Mapping between Multicast Profile and UNI port

To apply the configured multicast profile to a specified UNI-side port, use the following command.

Command	Mode	Description
multicast-profile *PROFILE*	Traffic Bridge-UNI	Applies the existing multicast profile to a specified UNI port. PROFILE: Multicast profile name
no multicast-profile		Deletes the mapping between a multicast profile and this UNI port.

Activating Administration for UNI

To enable/disable the administration of the ONU (ONT) UNI port, use the following command.

Command	Mode	Description
port-admin {**enable** | **disable**}	Traffic Bridge-UNI	Enables/disables the administration of UNI port.

To see the admin status of the ONU (ONT) UNI, use **show onu uni-status** command. (See 13.2.21 Displaying ONU Information)

Extended VLAN Tagging Operation Profile Association

To associate the extended VLAN tagging operation profile to the current mode, use the following command.

Command	Mode	Description
extended-vlan-tagging-operation *NAME*	Traffic Bridge-UNI	Associates the extended VLAN tagging operation profile. NAME: profile name
no extended-vlan-tagging-operation		Disassociates the extended VLAN tagging operation profile.

For the details of how to create and configure the extended VLAN tagging operation profile, see 13.6 Extended VLAN Tagging Operation Profile.

MAC Filtering Function

To configure the MAC filtering function for an UNI-side port of ONU, use the following command.

Command	Mode	Description
mac-filter { **ip4-mcast** | **ip6-mcast** | **ip4-bcast** | **rarp** | **ipx** | **net-beui** | **apple-talk** | **bridge-managed** | **arp** | **pppoe** }	Traffic Bridge-UNI	Enables the MAC filtering function according to the protocol type for UNI-side bridge port.
no mac-filter { **ip4-mcast** | **ip6-mcast** | **ip4-bcast** | **rarp** | **ipx** | **net-beui** | **apple-talk** | **bridge-managed** | **arp** | **pppoe** }		Disables the MAC filtering function according to the protocol type for UNI-side bridge port.

For the details of how to configure the MAC filtering operation, see 13.4.3.5 ANI Port Configuration.

13.4.3.7 IP-host Service Link

To link an IP-host service to MAC bridge service profile, use the following command.

Command	Mode	Description
link ip-host-config *SERVICE-ID*	Traffic-Bridge	Links an IP-host service to MAC bridge service profile. SERVICE-ID: IP-host service ID (1 to 32)
no link ip-host-config *SERVICE-ID*		Disconnects the linked IP-host service.

For the details of how to create and configure the IP-host service, see 13.4.5 IP Host Service Configuration.

13.4.3.8 TDM Service Link

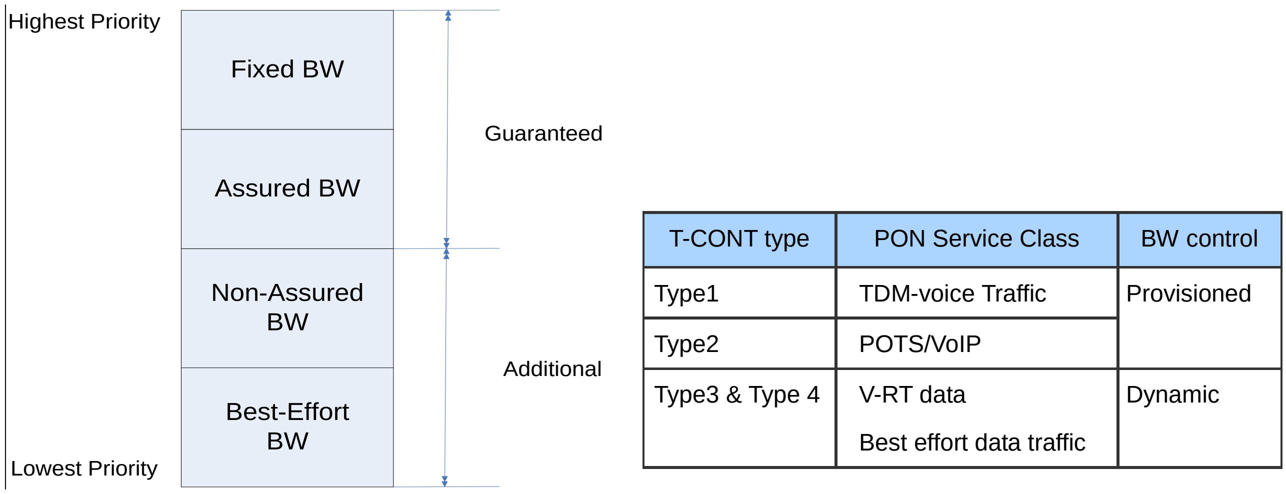
To link a TDM service to MAC bridge service profile, use the following command.

Command	Mode	Description
link tdm-service *SERVICE_ID*	Traffic-Bridge	Links a TDM service to MAC bridge service profile. SERVICE_ID: TDM service ID (1 to 8)
no link tdm-service *SERVICE_ID*		Disconnects the linked TDM service.

For the details of how to create and configure the TDM service, see 13.4.7 TDM Service Configuration (CES UNI).

13.4.4 T-CONT Mode

Transmission containers (T-CONTs) are used for the management of upstream bandwidth in PON section of the TC layer. T-CONTs dynamically receive grants, identified by Alloc-ID, from the OLT. A single T-CONT can carry GEM traffic with various service classes. It also accommodates one or more physical queues and aggregates them into a single logical buffer so that this feature can be used for enhanced QoS implementation in upstream direction. The mechanism of T-CONT is shown in Fig. 12.5.



T-CONT type	PON Service Class	BW control
Type1	TDM-voice Traffic	Provisioned
Type2	POTS/VoIP	
Type3 & Type 4	V-RT data Best effort data traffic	Dynamic

Fig. 12.5 Priority of T-CONT types

The LD3032 provides the easy and efficient management solution using T-CONT concept with the Traffic profile.

A GPON port is connected with multiple ONUs/ONTs via splitter. The GPON encapsulation mode (GEM) frames are transmitted between the OLT and the ONUs (ONTs). A GEM frame is identified by a GEM port ID. In the upstream direction, the T-CONTs carry the data stream.

The Traffic profile is a collection of configurations about dynamic bandwidth allocation and GEM port according to the service priority levels. You can configure each T-CONT to have a priority value using GEM port number.

You need to open *Traffic Profile Configuration* mode to configure a T-CONT. A T-CONT ID can include multiple T-CONTs and supports up to 8 priority queues per T-CONT.

To create a T-CONT ID in *Traffic Profile Configuration* mode, use the following command.

Command	Mode	Description
tcont *TCONT-ID*	Traffic-Profile	Creates a T-CONT ID. TCONT-ID: T-CONT ID, 1 to 32

After opening *T-CONT Configuration* mode, the prompt changes from SWITCH(config-traffic-pf[*NAME*])# to SWITCH(config-traffic-pf[*NAME*]-tcont[*TCONT-ID*])#.

To delete the T-CONT ID, use the following command.

Command	Mode	Description
no tcont *TCONT_ID*	Traffic-Profile	Deletes the configured T-CONT ID.

13.4.4.1 GEM Port Configuration

To specify the GEM ports (priority queue) per T-CONT by mapping between T-CONT and GEM port, use the following command.

Command	Mode	Description
gemport *GEM-PORTS* [**queue** <0-7>]	Traffic-TCONT	Specifies the priority queues of a GEM port. GEM-PORTS: mapper ID/GEM port ID (ex: 1/1= mapper #1:gem port 1, 1/2= mapper#1:gem port 2, 2/1-4=mapper #2:all gem ports)
no gemport *GEM-PORTS*		Deletes the configured mapping between T-CONT and the list of GEM ports.

13.4.4.2 Configuration of Weight on WRR Scheduling

To specify the weight value to queue number on WRR scheduling mode, use the following command.

Command	Mode	Description
queue <1-8> **weight** <1-255>	Traffic-TCONT	Specifies the weight value to queue number on WRR scheduling mode. 1-8: queue number (a lower number indicates a higher priority.) 1-255: weight value

13.4.4.3 DBA Profile Association

You can associate a configured DBA profile with T-CONT by using the following command.

Command	Mode	Description
dba-profile *NAME*	Traffic-TCONT	Associates a configured DBA profile with T-CONT. NAME: DBA profile name

i

For the details of how to create and configure a DBA profile, see 13.5 DBA Profile.

13.4.4.4 Displaying T-CONT Information

To display the information of T-CONT, use the following command.

Command	Mode	Description
show tcont-id gpon *OLT-ID* [*ONU-ID*]	Enable Global	Shows the information of T-CONT ID of OLT.
show onu tcont gpon *OLT-ID*		
show tcont [*ONU-ID*]	Interface [GPON]	Shows the information of T-CONT allocation for ONU.
show onu detail-info [*ONU-ID*]		Shows the detailed information (status, serial number, T-CONT number, T-CONT queue number) of ONU.
show current-profile	All modes of Traffic-profile	Shows the information currently configured for the profile.

13.4.5 IP Host Service Configuration

In order to configure an IP host, you need to create an IP host service ID. To create the IP host service ID and enter the configuration mode for the host, use the following command.

Command	Mode	Description
ip-host-config *HOST_NUMBER*	Traffic-Profile	Creates the IP host service ID and enters the configuration mode for the host. HOST_NUMBER : IP host number (1-32)
no ip-host-config *HOST_NUMBER*		Deletes the created IP host service ID.

After opening *IP-host Configuration* mode, the prompt changes from SWITCH(config-traffic-pf[*NAME*])# to SWITCH(config-traffic-pf[*NAME*]-iphost[*ID*])#.

13.4.5.1 IP Address

To specify the IP address assignment on the host, use the following command.

Command	Mode	Description
ip address {**static** | **dhcp**}	Traffic-IP-host	Specifies the IP address assignment on the host.

13.4.5.2 DNS

To specify the DNS address assignment on the host, use the following command.

Command	Mode	Description
dns primary *A.B.C.D* [**secondary** *A.B.C.D*]	Traffic-IP-host	Specifies the primary/secondary DNS IP address on the host.

ipv6 dns primary *X:X::X:X* [**secondary** *X:X::X:X*]		Specifies the primary/secondary DNS IPv6 address on the host.
no dns		Deletes the configured DNS IP address.
no ipv6 dns		Deletes the configured DNS IPv6 address.

13.4.5.3 VLAN Tagging Operating

To configure a VLAN tagging operation on the host, use the following command.

Command	Mode	Description
vlan-operation us-oper keep	Traffic-IP-host	Sets the policy of VLAN tagging for upstream frame. keep: keeps forwarding the existing tagged/untagged frame
vlan-operation us-oper {**add** | **overwrite**} *VLAN* <0-7>		Sets the policy of VLAN tagging for upstream frame. add: adds a specified VID (double tagging) with tag in case of tagged frame overwrite: replaces an existing tagged/untagged frame to a specified VID with tag. VLAN: VLAN ID (1-4094) 0-7: CoS value
vlan-operation ds-oper {**keep** | **remove**}		Sets the policy of VLAN tagging for downstream frame. keep: keeps forwarding the incoming tagged frame from OLT to UNI. remove: removes a tag from the incoming tagged packet and forwards it to UNI.
no vlan-operation		Deletes the configured policy for VLAN tagging operation.

13.4.5.4 VLAN Tagging Filtering

If there are more than one mapper connected to VLAN tagging, you need to configure a VLAN tagging filtering for VLAN ID-based traffic forwarding. To enable/disable VLAN tagging filtering function on ANI interface, use the following command.

Command	Mode	Description
vlan-filter [**vid** <1-4094>] **untagged** {**allow** | **discard**}	Traffic-IP-host	Enables a VLAN tagging filtering function of ANI-side port. allow: forwards the untagged frames to the ANI-side port discard: blocks the untagged frames to the ANI-side port 1-4094: VLAN ID(s)
vlan-filter vid {**add** | **del**} *VID*		Adds or deletes the VLAN ID on the VLAN list configured by **vlan-filter vid** command above.
no vlan-filter		Disables the VLAN tagging filtering function.

13.4.5.5 IPv6 Configuration

To configure the IPv6 DHCP client mode, use the following command.

Command	Mode	Description
ipv6 dhcp client na	Traffic-IP-host	Sets the DHCPv6 client mode using non-temporary address.
ipv6 dhcp client stateless		Sets the DHCPv6 client mode using the stateless address.

To display the DHCPv6 client information, use the following command.

Command	Mode	Description
ipv6 dhcp client information refresh minimum <600-315360000>	Interface [br] Traffic-IP-host	Sets the DHCPv6 client mode using non-temporary address. minimum: minimum time **600-315360000: information refresh time (unit: second, default: 86400**
ipv6 dhcp client stateless		Sets the DHCPv6 client mode using the stateless address.

To control transmission of IPv6 Router Solicitation(RS) messages on the host, use the following command.

Command	Mode	Description
ipv6 suppress-rs	Traffic-IP-host	Disables the sending of RS messages on the IP host.
no ipv6 suppress-rs		Sends RS messages on the IP host.

13.4.5.6 Extended VLAN Tagging Operation Profile Association

To associate the extended VLAN tagging operation profile to the host, use the following command.

Command	Mode	Description
extended-vlan-tagging-operation *NAME*	Traffic-IP-host	Associates the extended VLAN tagging operation profile. NAME: profile name
no extended-vlan-tagging-operation		Disassociates the extended VLAN tagging operation profile.

i

For the details of how to create and configure the extended VLAN tagging operation profile, see 13.6 Extended VLAN Tagging Operation Profile.

13.4.5.7 VoIP Service Link

To link the VoIP service to the host, use the following command.

Command	Mode	Description
link voip-service *SERVICE_ID*	Traffic-IP-host	Links the VoIP service to the host. SERVICE_ID: VoIP service ID (1-32)
no link voip-service *SERVICE_ID*		Disconnects the linked VoIP service.

i For the details of how to create and configure the VoIP service, see 13.4.6 VoIP Service Configuration (POTS UNI).

13.4.5.8 TDM Service Link

To link the TDM service to the host, use the following command.

Command	Mode	Description
link tdm-service *SERVICE_ID*	Traffic-IP-host	Links the TDM service to the host. SERVICE_ID: TDM service ID (1 to 8)
no link tdm-service *SERVICE_ID*		Disconnects the linked TDM service.

i For the details of how to create and configure the TDM service, see 13.4.7 TDM Service Configuration (CES UNI).

13.4.6 VoIP Service Configuration (POTS UNI)

In order to configure VoIP service, you need to create an VoIP service ID.

To create the VoIP service ID and enter the configuration mode for the service, use the following command.

Command	Mode	Description
voip-service *SERVICE_ID*	Traffic-Profile	Creates the VoIP service ID and enters the configuration mode for the service. SERVICE_ID: 1 to 32, VoIP service number
no voip-service *SERVICE_ID*		Deletes the created VoIP service ID.

After opening *VoIP Service Configuration* mode, the prompt changes from SWITCH(config-traffic-pf[*NAME*])# to SWITCH(config-traffic-pf[*NAME*]-voip[*ID*])#.

13.4.6.1 VoIP Service Management Mode

The LD3032 provides VoIP management function for the subtended ONUs. There are two VoIP management models: IP-path managed model and OMCI (ONT Management and Control Interface) managed model.

OMCI Managed Model

The full OMCI is used to control the VoIP configurations and OLT can handle these configurations for VoIP clients integrated in the ONT.

IP-path Managed Model

OMCI might still be used either to communicate the URI (FTP/HTTP server) of a configuration file to VoIP client integrated in the ONT, or to configure the VoIP client itself.

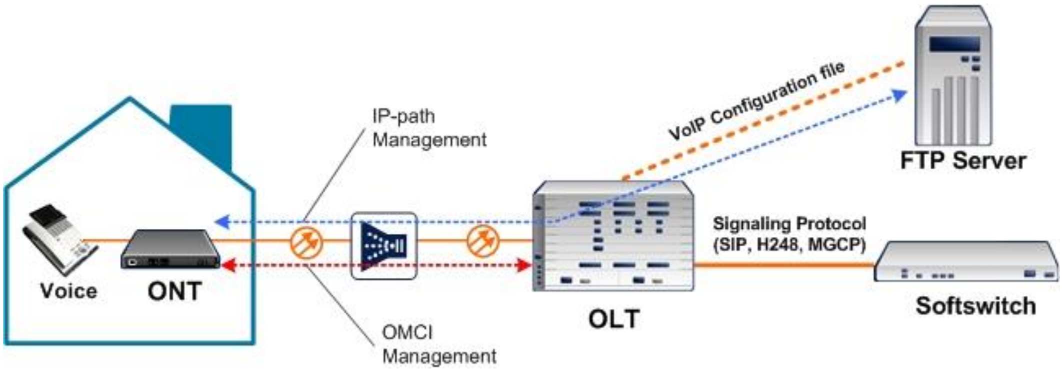


Fig. 12.6 VoIP Service Architecture

The LD3032 supports the VoIP service management with two modes based on the managed models above.

To configure VoIP service management mode, use the following command.

Command	Mode	Description
manage-method {**omci** | **ip-path**}	Traffic-VoIP	Sets VoIP service management mode. omci: ONT Management and Control Interface ip-path: IP-path managed
no manage-method		Deletes the configured VoIP service management mode.

13.4.6.2 OMCI Managed VoIP

If you configure the VoIP service management mode as OMCI managed by using **voip-profile omci** command, you need to connect VoIP profile with which OLT can handle the configurations for VoIP clients. To connect VoIP profile to the current VoIP service, use the following command.

Command	Mode	Description
voip-profile *NAME*	Traffic-VoIP	Connects VoIP profile to the current VoIP service. NAME: VoIP profile name
no voip-profile		Disconnects the specified VoIP profile.

i You need to create a VoIP profile first to connect the existing VoIP profile to the current VoIP service. For the details of how to create and configure the VoIP profile, see 13.7 VoIP Profile.

13.4.6.3 IP-path Managed VoIP

If you configure the VoIP service management mode as IP-path managed by using **voip-profile ip-path** command, you need to set IP-path configuration in *VoIP IP-path Configuration* mode.

When you use the **voip-profile ip-path** command, you enter automatically *VoIP IP-path Configuration* mode.

Whenever an ONU is deployed with the IP-path managed VoIP service, the OLT should assign the URL of a VoIP configuration file to communicate with the ONU VoIP client. The LD3032 provides an authentication method for ONUs to have access to the VoIP configuration server.

To configure IP-path managed VoIP mode, use the following command.

Command	Mode	Description
ip-path uri *URI*	Traffic VoIP-IP-path	Configures a VoIP configuration server. URI: IP-path URI
ip-path auth *NAME* [*PASSWD*]		Sets the user ID and password for IP-path managed model to have access to VoIP configuration server. NAME: user name used for authentication PASSWD: password used for authentication
no ip-path { **uri** | **auth** }		Deletes the configured VoIP configuration server or authentication information.

To specify the protocol on the current VoIP service, use the following command.

Command	Mode	Description
protocol { **h248** | **sip** | **mgcp**}	Traffic VoIP-IP-path	Specifies the protocol on the current VoIP service. sip: Session Initiation Protocol h248, mgcp: Media Gateway Control protocol (= MEGACO)

13.4.6.4 POTS UNI Configuration

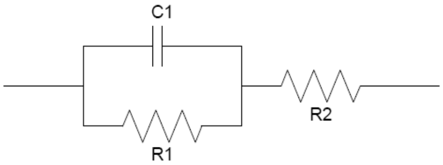
To configure the user network interface, use the following command.

Command	Mode	Description
uni {**pots** | **isdn**} *POTS_NUMBER*	Traffic-VoIP	Configures the VoIP user network interface. pots: POTS (Plain Old Telephone Service) isdn: ISDN (Integrated Services Digital Network) (future release) POTS_NUMBER: POTS port number
no uni {**pots** | **isdn**} *POTS_NUMBER*		Deletes the configuration of UNI.

If you specify UNI as the POTS by using **uni pots** command, you need to perform the configuration for the interface in *VoIP-UNI Configuration* mode as follows:

i When you use the **uni pots** command, you enter automatically *VoIP-UNI Configuration* mode, where you can configure the specified POTS interface.

To specify the impedance for the POTS UNI, use the following command.

Command	Mode	Description
impedance {**600** | **900** | **750** | **820** | **1050**}	Traffic VoIP-UNI	Specifies the impedance for the specified POTS UNI. 600: 600 Ohm (default) 900: 900 Ohm 750: C1=150 nF, R1=750 Ohm, R2=270 Ohm 820: C1=115 nF, R1=820 Ohm, R2=220 Ohm 1050: C1=230 nF, R1=1050 Ohm, R2=320 Ohm 
no impedance		Deletes the configured impedance for the POTS UNI.

To specify the on-hook transmission type, use the following command.

Command	Mode	Description
transmission-path {**full-time** | **part-time**}	Traffic VoIP-UNI	Allows setting the POTS UNI either to full-time on-hook transmission or part-time on-hook transmission. (default: full-time)
no transmission-path		Deletes the configured on-hook transmission type.

To specify Rx/Tx gain value for the receive/transmit signal, use the following command.

Command	Mode	Description
gain rx *VALUE* **tx** *VALUE*	Traffic VoIP-UNI	Specifies Rx/Tx gain value for the receive/transmit signal. VALUE: −120 (–12.0 dB) to 60 (+6.0 dB) (form: two's complement number, default: 0)

To specify POTS holdover time, use the following command.

Command	Mode	Description
pots-holdover-time <0-65535>	Traffic VoIP-UNI	Determines the time during which POTS loop voltage is held up when the ONT is not ranged on the PON. After the specified time elapses, the ONT drops loop voltage, and may thereby cause premises intrusion alarm circuits to go active. When the ONT ranges successfully on the PON, it restores POTS loop voltage immediately and resets the timer to zero. 0-65535: POTS holdover time (unit: second, default:

		0(= ONT vendor's factory policy))

13.4.6.5 Protocol Type Configuration

To perform the configuration for protocol type-based service that is offered from an IP host, use the following command.

Command	Mode	Description
udp port *PORT* **tos** *TOS*	Traffic-VoIP	Specifies the port number that offers the UDP/TCP/TLSP/protocol-type service and the value of the TOS field of the IPv4 header. PORT: port number TOS: type of service per IETF RFC 1349 or a differentiated services code point (DSCP) defined by IANA (default: 0)
protocol { **udp** | **tcp** | **tlsp** | *TYPE*} **port** *PORT* **tos** *TOS*		

13.4.7 TDM Service Configuration (CES UNI)

This section describes the configuration of CES UNI in the ONT where the physical path terminates and physical level functions are performed.

In order to configure CES UNI and TDM service, you need to specify the CES port first.
To specify the CES port, use the following command.

Command	Mode	Description
ces *PORT*	Traffic-Profile	Specifies the CES port. PORT: CES port number (1 to 8)
no ces *PORT*		Deletes the CES port configuration.

After opening *CES Configuration* mode, the prompt changes from SWITCH(config-traffic-pf[*NAME*])# to SWITCH(config-traffic-pf[*NAME*]-ces[*PORT*])#.

13.4.7.1 Expected Circuit Pack Type

To specify the expected circuit pack type, use the following command.

Command	Mode	Description
expected-type { **auto** | **ds1** | **e1** | **c-ds1-e1** | *VALUE* }	Traffic-CES	Specifies the expected circuit pack type. auto: Autosense ds1: DS1 e1: E1 c-ds1-e1: Configurable DS1/E1 VALUE: 1 to 254 (according to "Table 9.1.5-1 – Circuit pack types" in "ITU-T G.984.4")

13.4.7.2 Framing Structure

To specify the framing structure, use the following command.

Command	Mode	Description
framing { **extend-superframe** | **superframe** | **unframed** | **g-704** | **jt-g-704** | **basic-g-704** | **basic-crc4** | **basic-ts16** | **basic-crc4-ts16** }	Traffic-CES	Specifies the framing structure. (mandatory for DS1 interfaces)

13.4.7.3 Encoding

To specify the line coding scheme, use the following command.

Command	Mode	Description
encoding { **b8zs** | **ami** | **hdb3** | **b3zs** }	Traffic-CES	Specifies the line coding scheme. (mandatory for DS1 and DS3 interfaces) b8zs: B8ZS , ami: AMI hdb3: HDB3 b3zs: B3ZS

13.4.7.4 Line Length

To specify the cable line length with power feed, use the following command.

Command	Mode	Description
line-length power-feed ds1-non-power line-length { **110** | **220** | **330** | **440** | **550** | **660** }	Traffic-CES	Specifies the length of the twisted pair cable from a DS1 physical UNI to the DSX-1 cross-connect point. ds1-non-power: non-power feed type DS1 110~660: line length (unit: ft) (110: 0 to 110, 660: 550 to 660) ds1-power-short: power feed type DS1 (Wet T1), short haul 133~655: line length (unit: ft) (133: 0 to 133, 655: 533 to 655) ds1-power-long: power feed type DS1 (Wet T1), long haul 0/7_5/15/22_5: line length (unit: db) (7_5: 7.5, 22_5: 22.5)
line-length power-feed ds1-power-short line-length { **133** | **266** | **399** | **533** | **655** }		
line-length power-feed ds1-power-long line-length { **0** | **7_5** | **15** | **22_5** }		
line-length power-feed ds3-power line-length { **225** | **450** }		Specifies the length of coaxial cable from a DS3 physical UNI to the DSX-3 cross-connect point. ds3-power: DS3 power feed 225/450: line length (unit: ft) (225: 0 to 225, 450: 226 to 450)
no line-length		Deletes the configured line length.

13.4.7.5 DS1 Mode

To specify the mode of DS1, use the following command.

Command	Mode	Description
ds1-mode connect ds1-cpe line-length { **short** | **long** }	Traffic-CES	Specifies the mode of DS1. ds1-cpe: DS1 CPE (loopback: smart jack) ds1-niu-cpe: DS1 NIU CPE (loopback: intelligent office repeater) short: line length - short haul long: line length - long haul no-power: no power feed with-power: with power feed
ds1-mode connect ds1-niu-cpe power { **no-power** | **with-power** }		
no ds1-mode		Deletes the configured DS1 mode.

13.4.7.6 Line Type

To specify the line type used in DS3 or E3 application, use the following command.

Command	Mode	Description
line-type { **other** | **ds3-m23** | **ds3-syntran** | **ds3-cbit-parity** | **ds3-clear-channel** | **e3-framed** | **e3-plcp** }	Traffic-CES	Specifies the line type used in a DS3 or E3 application. (mandatory for DS3 and E3 interfaces, not applicable to other interfaces)

13.4.7.7 TDM Service Configuration

In order to configure TDM service, you need to create an TDM service ID.

To create the TDM service ID and enter the configuration mode for the service, use the following command.

Command	Mode	Description
tdm-service *SERVICE_ID* **mode** { **pw-ip** | **pw-mef8** | **pw-mpls** }	Traffic-CES	Creates a TDM service ID and enters the configuration mode for the service. pw-ip: pseudowire IP transport (UDP/IP) pw-mef8: pseudowire MEF8 pw-mpls: pseudowire MPLS
no tdm-service *SERVICE_ID*		Deletes the created TDM service ID.

After creating a TDM service ID with **pw-ip** option, the prompt changes from SWITCH(config-traffic-pf[*NAME*]-ces[*PORT*])# to SWITCH(config-traffic-pf[*NAME*]-ces[*PORT*]-svc[*ID*]-pw-ip)#. In this mode, you can perform the following configuration.

Applying TDM Pseudowire Profile

In order to configure the TDM service, you need to connect TDM pseudowire profile.
To connect TDM pseudowire profile to the current TDM service, use the following command.

Command	Mode	Description

tdm-pw-profile *NAME*	Traffic CES-PW-IP	Connects TDM pseudowire profile. NAME: TDM pseudowire profile name
no tdm-pw-profile		Disconnects the specified TDM pseudowire profile.

For the details of how to create and configure the TDM pseudowire profile, see 13.8 TDM Pseudowire Profile.

Far-End URI

To specify the URI of the far-end, use the following command.

Command	Mode	Description
far-end-ip *URI*	Traffic CES-PW-IP	Specifies the URI of the far-end, when the pseudowire service is transported via IP. URI: far-end URI (Both target address and port number should be specified.)
no far-end-ip		Deletes the specified far-end URI.

UDP/TOS Configuration

To perform the configuration for protocol type-based service that is offered from an IP host, use the following command.

Command	Mode	Description
udp port *PORT* **tos** *TOS*	Traffic CES-PW-IP	Specifies the port number that offers the UDP/TCP/TLSP/protocol type service and the value of the TOS field of the IPv4 header. PORT: port number TOS: type of service per IETF RFC 1349 or a differentiated services code point (DSCP) defined by IANA (default: 0)
protocol { **udp** | **tcp** | **tlsp** | *TYPE*} **port** *PORT* **tos** *TOS*		

13.4.7.8 Displaying TDM Pseudowire Information

To display the information of TDM pseudowire profiles, use the following command.

Command	Mode	Description
show tdm-pw-profile [*NAME*]	Global Interface [GPON]	Shows the information of TDM pseudowire profiles. NAME: TDM pseudowire profile name

To display the list information of source MAC addresses for TDM pseudowire of ONU, use the following command.

Command	Mode	Description
show onu tdm-pw source-mac gpon *OLT-ID ONU-ID*	Enable/Global	Shows the list of source MAC addresses for TDM pseudowire of the specified ONU.

show onu tdm-pw source-mac *ONU-ID*	Interface [GPON]	

13.4.8 Management Mode

The OLT manages the ONU through an ONU management and control interface (OMCI) path. An OMCI is a configuration transmission path defined in the GPON standard. If the OLT manages the ONU through a non-OMCI path, this ONU's UNI port is connected as a Virtual Eth and is controlled by its web/TR-69/SNMP management system.

To specify the management mode of ONU's UNI port, use the following command.

Command	Mode	Description
mgmt-mode uni { **eth** | **pots** | **ces** | **video** } *UNI_PORT* { **omci** | **non-omci link virtual-eth** *NUMBER*}	Traffic-Profile	Specifies the management mode of ONU's UNI port using OMCI or non-OMCI path. UNI_PORT: UNI port number (1-32)
no mgmt-mode uni { **eth** | **pots** | **ces** | **video** } *UNI_PORT*		Deletes the specified UNI port's management mode.

To display the configured management mode of ONU, use the following command.

Command	Mode	Description
show onu uni-mgmt gpon *OLT-ID ONU-ID*	Enable Global	Shows the management mode of ONU ID.
show onu uni-mgmt *ONU-ID*	Interface [GPON]	

13.4.9 Video Return Path Mode

RF return path technology enables the pay-per-view and video-on-demand services that are simply offered over traditional MSO (Multiservice Operator) infrastructure. In order to configure video RF return path service, you need to create a Video return service ID.

A single traffic profile can be used to serve one single video return path service ID.

To create the VoIP service ID and enter the configuration mode for the service, use the following command.

Command	Mode	Description
video-return-path-service *SERVICE_ID*	Traffic-Profile	Creates the VoIP service ID and enters the configuration mode for the service. SERVICE_ID: 1, Video return service number
no video-return-path-service *SERVICE_ID*		Deletes the created VoIP service ID.

After opening *Video Return Path Service Configuration* mode, the prompt changes from SWITCH(config-traffic-pf[*NAME*])# to SWITCH(config-traffic-pf[*NAME*]-vrp[*ID*])#.

To configure the video return path service-related parameters, use the following command.

Command	Mode	Description
frequency *HERTZ*	Traffic-VRP	Specifies the VRP tunner frequency to use. (unit: Hertz)
vrp { **mode1** | **mode2-256k** | **mode2-1m** | **mode2-3m** }		Specifies the format to be used for the VRP service. mode1: SCTE 55-1 (256 kbit/s data rate, 62 byte PDUs, preceded by the unique word 0xCC CC CC 00) mode2-1m: SCTE 55-1 (1.544 Mbit/s data rate, 59 byte PDUs, preceded by the unique word 0xCC CC CC 0D) mode2-256k: SCTE 55-1 (256 kbit/s data rate, 59 byte PDUs, preceded by the unique word 0xCC CC CC 0D) mode2-3m: SCTE 55-1 (3.088 Mbit/s data rate, 59 byte PDUs, preceded by the unique word 0xCC CC CC 0D)
mode1-physical {**default** | **alternate**} { **stage-6** | **stage-7** | **stage-8** | **stage-9** | **stage-10** | **stage-11** | **stage-12** | **stage-13** }		Controls the physical layer configuration to be used in mode 1. default: DQPSK default mode alternate: DQPSK alternate mode stage-6: Randomizer stage 6 preload (Bit 7) stage-7: Randomizer stage 7 preload (Bit 6) stage-8: Randomizer stage 8 preload (Bit 5) stage-9: Randomizer stage 9 preload (Bit 4) stage-10: Randomizer stage 10 preload (Bit 3) stage-11: Randomizer stage 11 preload (Bit 2) stage-12: Randomizer stage 12 preload (Bit 1) stage-13: Randomizer stage 13 preload (Bit 0)

13.4.10 Creating a GEM Port Network CTP

The GEM port Network CTP profile manages the upstream traffic identified by the GEM Port-ID. Each GEM port is identified by a port ID uniquely. The port ID ranges from 0 to 32. A GEM port ID is unique per GPON interface and represents a specific traffic or group of flows between the OLT and the ONT. When each GEM port carries the traffic flows, traffic control is performed according to the specific service profile.

To create a GEM port network CTP for a specified traffic profile, use the following command.

Command	Mode	Description
gemport-nctp *GEM_PORT_ID*	Traffic-Profile	Creates a GEM port network CTP profile associated with GEM port ID. GEM_PORT_ID: 1 to 32, GEM port number
no gemport-nctp *GEM_PORT_ID*		Removes the created GEM port Network CTP from the traffic profile

After opening *GEM Port Network CTP Service Configuration* mode, the prompt changes from SWITCH(config-traffic-pf[*NAME*])# to SWITCH(config-traffic-pf[*NAME*]-gem[*ID*])#.

To connect a service profile (MAC bridge, IP Host config, video return path service) with a GEM Port ID, use the following command.

Command	Mode	Description
service {**bridge** | **ip-host** | **video-return-path**} *SVC_ID*	Traffic-GEM	Specifies a service profile to be mapped to the GEM port network CTP for traffic management. bridge: MAC bridge ip-host: IP Host config video-return-path: video return path service SVC_ID: service ID

13.4.11 Saving Traffic Profile

To save the traffic profile after configuring a traffic profile, use the following command.

Command	Mode	Description
apply	Traffic-Profile	Saves a traffic profile configuration.

i Whenever you modify a traffic profile, you should apply the changes again using the **apply** command. If you do not, it will not be applied.

13.4.12 Adding/Applying Traffic Profile

If you want to apply a created traffic profile to an ONU profile, open *ONU Profile Configuration* mode, where you can add the traffic profile.

```
SWITCH(config-traffic-pf[AAA])# apply
SWITCH(config-traffic-pf[AAA])# exit
SWITCH(config)# onu-profile BB create
SWITCH(config-onu-profile[BB])# traffic-profile AAA
SWITCH(config-onu-profile[BB])# apply
```

To add/delete the configured traffic profile to a specified ONU profile, use the following command.

Command	Mode	Description
traffic-profile *NAME*	ONU-Profile	Adds the configured traffic profile to ONU profile. NAME: traffic profile name
no traffic-profile		Removes the traffic profile from ONU profile.

i You should modify a traffic profile, you should apply the changes again using the **apply** command. If you do not, it will not be applied.

13.4.13 Displaying Traffic Profile Information

To display the information of traffic profiles, use the following command.

Command	Mode	Description
show traffic-profile [*NAME*]	Enable Global Interface [GPON] Traffic-profile	Shows the currently applied configuration information of traffic profile. NAME: traffic profile name
show current-profile	Current-Profile	Shows the information currently configured for the profile.

To display the information of GEM port ID, use the following command.

Command	Mode	Description
show port-id [*ONU-ID*]	Interface [GPON]	Shows the GEM port ID information. ONU-ID: ONU ID (1 to 128)

To display the DBA profile associated with the specific Traffic profile, use the following command.

Command	Mode	Description
show traffic-profile *NAME* **dba-profile**	Enable Global Interface [GPON]	Shows the DBA profile associated with the specified Traffic profile. NAME: Traffic profile name

To display the VLAN filter configured on the specific Traffic profile, use the following command.

Command	Mode	Description
show traffic-profile *NAME* **vlan-filter**	Enable Global Interface [GPON]	Shows the VLAN filter configured on the specified Traffic profile. NAME: Traffic profile name

13.4.14 Sample Configuration

For the sample configuration, see “Configuration Example 1” in 13.15 Sample Configuration.

13.5 DBA Profile

You need to open *DBA Profile Configuration* mode to set the bandwidth allocation and ONU status reporting mode.

13.5.1 Creating DBA Profile

To create/delete/modify a DBA profile, use the following command.

Command	Mode	Description
dba-profile *PROFILE* **create**	Global	Creates a DBA profile. PROFILE: DBA profile name
no dba-profile {*PROFILE* | **all**}		Deletes a DBA profile.
dba-profile *PROFILE* **modify**		Modifies the configured DBA profile.

13.5.2 Configuring DBA Profile

If the LD3032 bandwidth allocation method for ONU upstream transmission is dynamic (DBA), there are two methods of DBA are defined for GPON: status-reporting (SR) DBA, which is based on ONU reports via the dynamic bandwidth report upstream (DBRu) field, and non-status-reporting (NSR) DBA, which is based on OLT monitoring per T-CONT utilization.

To set the bandwidth allocation and ONU status reporting mode of DBA profile, use the following command.

Command	Mode	Description
mode fixed [**cbr**]	DBA Profile	Configure a fixed-UBR bandwidth allocation mode. fixed: fixed-ubr bandwidth (fixed-ubr BW: minimum 512 kbps) cbr: fixed-cbr bandwidth
mode { **nsr** | **sr** }		Configure an ONU status reporting mode of DBA profile. nsr: non status reporting dynamic bandwidth allocation sr: status reporting dynamic bandwidth allocation (fixed-cbr BW: minimum 512 kbps)
sla fixed <0-1031616>		Sets a bandwidth. 0-1031616: fixed bandwidth (unit: 64Kbps) 0-1031616: assured bandwidth (unit: 64Kbps) 128-1031616: maximum bandwidth (unit: 64Kbps) (default option: best-effort (=do not use **non-assured** option))
sla assured <0-1031616>		
sla maximum <128-1031616> [**non-assured**]		

! The maximum bandwidth value should be same or more than the sum of a fixed bandwidth and assured bandwidth value.

Maximum B/W ≥ fixed B/W + assured B/W

If there are a “non-assured” T-CONT and “best-effort” T-CONT, the “non-assured” T-CONT takes precedence over the other one to be allocated the remained bandwidth by OLT.

To delete the configured bandwidth allocation policy of DBA profile, use the following command.

Command	Mode	Description
no sla { **fixed** | **assured** | **maximum**}	DBA-Profile	Deletes the configured bandwidth allocation policy.

13.5.3 Saving DBA Profile

After configuring a DBA profile, you need to save the profile using the following command.

Command	Mode	Description
apply	DBA-Profile	Saves a DBA profile configuration.

Whenever you modify a DBA profile, you should apply the changes again using the **apply** command. If you do not, it will not be saved with new changes.

You can apply the flexible bandwidth allocation per T-CONT according to the priority of traffic. After saving the DBA profile and creating T-CONT profile, you should apply the DBA profile on a specified GEM port of T-CONT profile to specify the bandwidth of GEM port by mapping between T-CONT and DBA profile.

13.5.4 Displaying DBA Profile

To display DBA profile information, use the following command.

Command	Mode	Description
show dba-profile [*NAME*]	Global Interface [GPON] DBA-profile Traffic-TCONT	Shows the information of DBA profiles.

13.6 Extended VLAN Tagging Operation Profile

You can configure the ONU’s extended VLAN tagging operation. In order to configure the operation, you need to create an extended VLAN tagging operation profile. To create the profile, use the following command.

Command	Mode	Description
extended-vlan-tagging-operation *NAME* **create**	Global	Creates an extended VLAN tagging operation profile. NAME: profile name
no extended-vlan-tagging-operation {*NAME* | **all**}		Deletes an extended VLAN tagging operation profile.
extended-vlan-tagging-operation *NAME* **modify**		Modifies the configured extended VLAN tagging operation profile.

After opening (creating) *GPON Extended VLAN Operation Configuration* mode, the prompt changes from SWITCH(config)# to SWITCH(config-ext-vlan-oper[*NAME*])#.

13.6.1 Received Frame VLAN Tagging Operation Table Configuration

This configuration specifies a table that filters and tags upstream frames. Each entry represents a tagging rule, comprising a filtering part and a treatment part. Each incoming upstream packet is matched against each rule in list order. The first rule that matches the packet is selected as the active rule, and the packet is then treated according to that rule. There are three categories of rules: untag, single-tag, and double-tag rules.

Logically, these categories are separate, and apply to their respective incoming frame types. In other words, a single-tag rule should not apply to a double-tagged frame, even though the single-tag rule might match the outer tag of the double-tagged frame.

Single-tag rules have a filter outer priority field = 15 (indicating no external tag), untag rules have both filter priority fields = 15 (indicating no tags), and double-tag rules have both filter priority fields set to a value that is different from 15 (indicating two tags).

Each tagging rule is based on 'remove' and 'add' operation, where up to two tags can be removed or added. A modify operation is applied by the combination of 'remove' and 'add'.

Note that when a single tag is added, the treatments use the 'inner tag' data-fields for definiteness – this is true even for treatments where a single tag is added to a frame that already has a tag, i.e., added as a second tag. The 'outer tag' data-fields are used only when two tags are added by the same rule.

The terms 'inner' and 'outer' only have meaning with respect to the tags that are being filtered or added.

One set operation can add, modify or delete one entry. The first 8 bytes of each entry are guaranteed to be unique, and are used to identify table entries. The OLT deletes a table entry by setting its last eight bytes to all 0xFF.

When the table is created, the ONT should predefine three entries that list the default treatment (of normal forwarding) for untagged, single-tagged, and double-tagged frames. As an exception to the rule on ordered processing, these default rules are always considered as a last resort for frames that do not match any other applicable rule. Best practice dictates that these entries not be deleted; however, they can be modified to produce the desired default behaviour.

15, x, x, 15, x, x, x, (0, 15, x, x, 15, x, x)
15, x, x, 14, x, x, x, (0, 15, x, x, 15, x, x)
14, x, x, 14, x, x, x, (0, 15, x, x, 15, x, x)

The ‘x’ is a "do not care" field and should be set to zero.

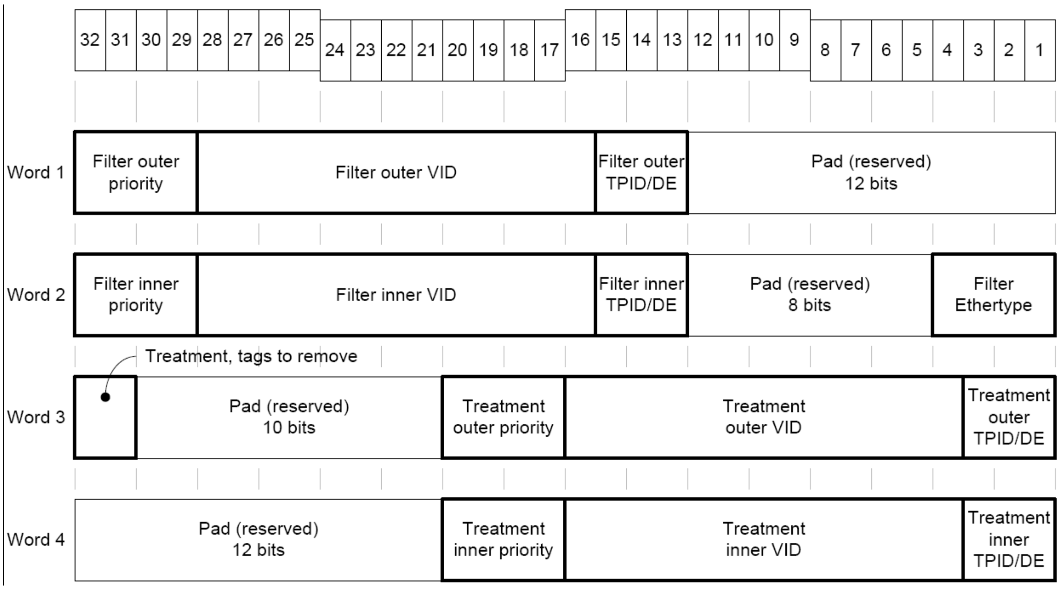


Fig. 12.7 Received Frame Layout

13.6.1.1 Configuration for Single-tagged Frame Treatment

To create the mapping table to configure the single-tagged frame treatment, use the following command.

Command	Mode	Description
single-tagged-frame *TABLE*	GPON-ext-vlan-oper	Creates the mapping table to configure the single-tagged frame treatment. TABLE: table number
no single-tagged-frame *TABLE*		Deletes the specified table.

After opening (creating) the mapping table to configure the single-tagged frame treatment, the prompt changes from SWITCH(config-ext-vlan-oper[*NAME*])# to SWITCH(config-ext-vlan-oper[*NAME*]-single-tagged-frame[*TABLE*])#.

To configure the filtering for single-tagged frames, use the following command.

Command	Mode	Description
filter inner vid {**any** | <0-4094>} **cos** {**any** | <0-7>} **tpid** {**any** | **0x8100** | **input** [**dei** {**0** | **1**}]}	Single-Tagged-Frame	Configures the received single-tagged frames to be filtered by the provided values concerning inner tag. vid any: do not filter on the inner VID. vid 0-4094: filters received frames on this value. cos any: do not filter on the inner priority. cos 0-7: filters received frames on this value. tpid any: do not filter on the inner TPID field. tpid 0x8100: filters received frames on this value. tpid input: input TPID attribute value, don't care about DE bit. tpid input dei 0: input TPID, DE=0 tpid input dei 1: input TPID, DE=1
no filter inner		Deletes the filtering configuration above.

To configure the treatment of filtered single-tagged frames, use the following command.

Command	Mode	Description
treat {**remove** {**single** | **double**} | **discard-frame**}	Single-Tagged-Frame	Configures the treatment of filtered single-tagged frames. remove single: removes one tag (the outer tag is stripped from double-tagged frames.) remove double: removes all of outer and inner tags. discard-frame: drops the frames.
treat inner vid {<0-4094> | **copy-inner** } **cos** {<0-7> | **copy-inner** | **dscp-to-pbit**} **tpid** {**output dei** {**0** | **1** | **copy-inner** } | **copy-inner** | **0x8100**}		Configures the inner tag treatment for filtered single-tagged frames. 0-4094: uses this value as the VID in the inner VLAN tag. copy-inner: copies value from inner tag of received frame. 0-7: uses this value as the priority in the inner VLAN tag.
treat outer vid {<0-4094> | **copy-inner** } **cos** {<0-7> | **copy-inner** | **dscp-to-pbit**} **tpid** {**output dei** {**0** | **1** | **copy-inner** } | **copy-inner** | **0x8100**}		Configures the outer tag treatment for filtered single-tagged frames.
no treat {**remove-discard** | **outer** | **inner**}		Deletes the treatment-related configuration above.

13.6.1.2 Configuration for Double-tagged Frame Treatment

To create the mapping table to configure the double-tagged frame treatment, use the following command.

Command	Mode	Description
double-tagged-frame *TABLE*	GPON-ext-vlan-oper	Creates the mapping table to configure the double-tagged frame treatment. TABLE: table number
no double-tagged-frame *TABLE*		Deletes the specified table.

After opening (creating) the mapping table to configure the double-tagged frame treatment, the prompt changes from SWITCH(config-ext-vlan-oper[*NAME*])# to SWITCH(config-ext-vlan-oper[*NAME*]-double-tagged-frame[*TABLE*])#.

To configure the filtering for double-tagged frames, use the following command.

Command	Mode	Description
filter inner vid {**any** | <0-4094>} **cos** {**any** | <0-7>} **tpid** {**any** | **0x8100** | **input** [**dei** {**0** | **1**}]}	Double-Tagged-Frame	Configures the received double-tagged frames to be filtered by the provided values concerning inner tag. vid any: do not filter on the inner VID. vid 0-4094: filters received frames on this value. cos any: do not filter on the inner priority. cos 0-7: filters received frames on this value. tpid any: do not filter on the inner TPID field. tpid 0x8100: filters received frames on this value. tpid input: input TPID attribute value, don't care about DE bit. tpid input dei 0: input TPID, DE=0 tpid input dei 1: input TPID, DE=1
filter outer vid {**any** | <0-4094>} **cos** {**any** | <0-7>} **tpid** {**any** | **0x8100** | **input** [**dei** {**0** | **1**}]}		Configures the received double-tagged frames to be filtered by the provided values concerning outer tag.
no filter {**inner** | **outer**}		Deletes the filtering configuration above.

To configure the treatment of filtered double-tagged frames, use the following command.

Command	Mode	Description
treat {**remove** {**single** | **double**} | **discard-frame**}	Double-Tagged-Frame	Configures the treatment of filtered double-tagged frames. remove single: removes one tag (the outer tag is stripped from double-tagged frames.) remove double: removes all of outer and inner tags. discard-frame: drops the frames.
treat inner vid {<0-4094> | **copy-inner** | **copy-outer**} **cos** {<0-7> | **copy-inner** | **copy-outer** | **dscp-to-pbit**} **tpid** {**output dei** {**0** | **1** | **copy-inner** | **copy-outer**} | **copy-inner** | **copy-outer** | **0x8100**}		Configures the inner tag treatment for filtered double-tagged frames. 0-4094: uses this value as the VID in the inner VLAN tag. copy-inner: copies value from inner tag of received frame. copy-outer: copies value from outer tag of received frame. 0-7: uses this value as the priority in the inner VLAN tag.
treat outer vid {<0-4094> | **copy-inner** | **copy-outer**} **cos** {<0-7> | **copy-inner** | **copy-outer** | **dscp-to-pbit**} **tpid** {**output dei** {**0** | **1** | **copy-inner** | **copy-outer**} | **copy-inner** | **copy-outer** | **0x8100**}		Configures the outer tag treatment for filtered double-tagged frames.
no treat {**remove-discard** | **outer** | **inner**}		Deletes the treatment-related configuration above.

13.6.1.3 Configuration for Untagged Frame Treatment

To create the mapping table to configure the untagged frame treatment, use the following command.

Command	Mode	Description
untagged-frame *TABLE*	GPON-ext-vlan-oper	Creates the mapping table to configure the untagged frame treatment. TABLE: table number
no untagged-frame *TABLE*		Deletes the specified table.

After opening (creating) the mapping table to configure the untagged frame treatment, the prompt changes from SWITCH(config-ext-vlan-oper[*NAME*])# to SWITCH(config-ext-vlan-oper[*NAME*]-untagged-frame[*TABLE*])#.

To configure the filtering for untagged frames, use the following command.

Command	Mode	Description
filter ether-type {**ipoe** | **pppoe** | **arp** | **ipv6-ipoe**}	Untagged-Frame	Configures the received untagged frames to be filtered by the provided option.
no filter ether-type		Deletes the filtering configuration above.

To configure the treatment of filtered untagged frames, use the following command.

Command	Mode	Description
treat inner vid <0-4094 **cos** {<0-7> | **dscp-to-pbit**} **tpid** {**output dei** {**0** | **1** } | **0x8100**}	Untagged-Frame	Configures the inner tag treatment for filtered untagged frames. 0-4094: uses this value as the VID in the inner VLAN tag. 0-7: uses this value as the priority in the inner VLAN tag.
treat outer vid <0-4094> **cos** {<0-7> | | **dscp-to-pbit**} **tpid** {**output dei** {**0** | **1** } | **0x8100**}		Configures the outer tag treatment for filtered untagged frames.
treat discard-frame		Drops the filtered untagged frames.
no treat {**remove-discard** | **outer** | **inner**}		Deletes the treatment-related configuration above.

For untagged frames, queue information need to be specified. You can configure whether they use a default DSCP to CoS mapping table as specifying the queue (assuming that the untagged frames can use the DSCP to CoS mapping table). Unless you configure the table to be used, the untagged frames use default queue information.

To configure to use a default DSCP to CoS mapping table as specifying queue for untagged frames, use the following command.

Command	Mode	Description
dscp-to-cos-map default-map	GPON-ext-vlan-oper	Configures to use a default DSCP to CoS mapping table as specifying queue for untagged frames.
no dscp-to-cos-map		Deletes the configuration above. (= Configures to use default queue information as specifying queue for untagged frames.)

13.6.2 TPID Configuration

To configure the specific TPID value for operations on the input (filtering) side and output (tagging) side of the table, use the following command.

Command	Mode	Description
tpid { **input** *VALUE* | **output** *VALUE* }	GPON-ext-vlan-oper	Configures the specific TPID value for operations on the input (filtering) side and output (tagging) side of the table. VALUE: TPID
no tpid { **input** | **output** }		Deletes the configured TPID value.

13.6.3 Downstream Mode Configuration

Although the extended VLAN tagging operation pertains to upstream traffic, this configuration specifies the mode for downstreaming mapping.

The operation performed in the downstream direction is the inverse of that performed in the upstream direction. For one-to-one VLAN mappings, the inverse is trivially defined. Many-to-one mappings are possible, however, and these are treated as follows. If the many-to-one mapping results from multiple operation rules producing the same ANI-side tag configuration, then the first rule in the list defines the inverse operation. If the many-to-one mapping results from “do not care” fields in the filter being replaced with provisioned fields in the ANI-side tags, then the inverse is defined to set the corresponding fields on the ANI-side with their lowest value.

To enable/disable the extended VLAN tagging operation for the downstream mode, use the following command.

Command	Mode	Description
downstream-mode {**enable** | **disable**}	GPON-ext-vlan-oper	Enables/disables the extended VLAN tagging operation for the downstream mode.

13.6.4 Saving and Applying Profile

After configuring an profile, you need to save the profile with the following command.

Command	Mode	Description
apply	GPON-ext-vlan-oper	Saves an profile configuration.

i

Whenever you modify the profile, you should apply the changes again using the **apply** command. If you do not, it will not be applied.

To apply the configured Extended VLAN Tagging Operation profile per UNI port or IP host, use the following command.

Command	Mode	Description
extended-vlan-tagging-operation *NAME*	Traffic-Bridge-UNI Traffic-IP-host	Applies the configured extended VLAN tagging operation profile to specified UNI port or host. NAME: Extended VLAN Tagging Operation profile name
no extended-vlan-tagging-operation		Removes the Extended VLAN Tagging Operation profile from UNI port or host.

i For the details of how to apply the Extended VLAN Tagging Operation profile per UNI port or IP host, see 13.4.3.6 UNI Port Configuration or 13.4.5.6 Extended VLAN Tagging Operation Profile Association.

13.6.5 Overwriting ONU Extended VLAN Tagging Operation

Basically, one Extended VLAN Tagging Operation profile should be applied to the UNI port or IP host after creating a Traffic profile. So, if a number of cases for VLAN tagging operation configuration for ONU are required, the user should create the Traffic profiles and the corresponding UNI port/IP host and apply the configured extended VLAN tagging operation profile to an UNI/host one by one.

The overwriting ONU Extended VLAN Tagging Operation profile configuration can help reducing the count of creating and applying the traffic profile/ONU profile per ONU ID.

This feature can overwrite the inner VLAN tag treatment of filtered frames based on the filtering rules of the associated Extended VLAN operation profile to apply to a particular ONU.

To associate the extended VLAN tagging operation profile to the specified ONU ID and overwrite the inner tag treatment, use the following command.

Command	Mode	Description
onu extended-vlan *ONU-ID NAME* **double-tagged-frame** *TABLE* **treat inner vid** {<0-4094> | **copy-inner** | **copy-outer**} **cos** {<0-7> | **copy-inner** | **copy-outer** | **dscp-to-pbit**}	Interface [GPON]	Associates the extended VLAN tagging operation profile to ONU ID and configures the inner tag treatment for filtered double-tagged frames. ONU-ID: ONU ID (1 to128) or ONU serial number NAME: Extended VLAN tagging operation profile name TABLE: rule table number (1 to 32) 0-4094: uses this value as the VID in the inner VLAN tag. copy-inner: copies value from inner tag of received frame. copy-outer: copies value from outer tag of received frame. 0-7: uses this value as the priority in the inner VLAN tag.

onu extended-vlan *ONU-ID NAME* **single-tagged-frame** *TABLE* **treat inner vid** {<0-4094> | **copy-inner** } **cos** {<0-7> | **copy-inner** | **dscp-to-pbit**}		Associates the extended VLAN tagging operation profile to ONU ID and configures the inner tag treatment for filtered single-tagged frames.
onu extended-vlan *ONU-ID NAME* **untagged-frame** *TABLE* **treat inner vid** <0-4094> **cos** {<0-7> | **dscp-to-pbit**}		Associates the extended VLAN tagging operation profile to ONU ID and configures the inner tag treatment for filtered untagged frames.
no onu extended-vlan *ONU-ID NAME* { **double-tagged-frame** | **single-tagged-frame** | **untagged-tagged-frame** } *TABLE*		Removed the extended VLAN tagging operation profile association from ONU ID and the configured inner tag treatment.

13.6.6 Displaying Extended VLAN Tagging Operation Profile

To display a configured Extended VLAN tagging operation profile, use the following command.

Command	Mode	Description
show running-config extended-vlan-tagging-operation [*NAME*]	All	Shows the configured extended vlan tagging operation profile. NAME: Extended VLAN tagging operation profile name

To display the information of current profile, use the following command.

Command	Mode	Description
show current-profile	Current-Profile	Shows the information currently configured for the profile.

13.7 VoIP Profile

13.7.1 OMCI Management Configuration

The GPON system enables multi-vendor interoperability between OLT and ONT. The OMCI specification addresses the ONT configuration management, fault management and performance management for GPON system operation and for several services including voice services. The OMCI and the configuration server based architecture are the standard alternatives to convey the operation of the ONT for VoIP. In addition, the VoIP user agent at the ONT needs to work in conjunction with a softswitch for voice service features.

You need to open *VoIP Profile Configuration* mode to configure VoIP based on OMCI management. To implement the configurations of VoIP between OLT and ONU, an ONU profile should be included by the configured VoIP profile. You can easily manage the VoIP network parameters of ONUs using the VoIP profile.

i The ONT must be applied by VoIP profile defined in LD3032 if the ONT has POTS terminations and if OLT is to be used to remotely manage and provide the VoIP service.

13.7.1.1 Creating VoIP Profile

To create a VoIP profile, use the following command.

Command	Mode	Description
voip-profile *NAME* **create**	Global	Creates a VoIP profile. NAME: VoIP profile name

After opening *VoIP Profile Configuration* mode, the prompt changes from SWITCH(config)# to SWITCH(config-voip-profile[*NAME*])#.

To delete an existing VoIP profile, use the following command.

Command	Mode	Description
no voip-profile *NAME*	Global	Deletes n VoIP profile. NAME: VoIP profile name

To modify an existing VoIP profile, use the following command.

Command	Mode	Description
voip-profile *NAME* **modify**	Global	Modifies the exisitng VoIP profile. NAME: VoIP profile name

13.7.1.2 VoIP Media Configuration

To specify fax mode, use the following command.

Command	Mode	Description
fax-mode {**passthru** | **t-38**}	VoIP-Profile	Specifies fax mode.

To configure codec negotiation with codec type, packet period and silence suppression, use the following command.

Command	Mode	Description
codec-nego <1-4> **codec** {**pcmu** | **gsm** | **g723** | **dvi4-8k** | **dvi4-16k** | **lpc** | **pcma** | **g722** | **l16-2ch** | **l16-1ch** | **qcelp** | **cn** | **mpa** | **g728** | **dvi4-11k** | **dvi4-22k** | **g729**} **packet-period** *VALUE* **silence-suppression** *VALUE*	VoIP-Profile	Configures codec negotiation by specifying codec, packet period and silence suppression. 1-4: codec negotiation number pcmu ~ g729: codecs as defined by IETF RFC 3551 (default: pcmu) VALUE: 10~30, packet period (unit: ms, default: 10) VALUE: 0~1, whether silence suppression is on or off (0 = off, 1 = on)

To specify out-of-band DTMF carriage, use the following command.

Command	Mode	Description
oob-dtmf {**enable** | **disable**}	VoIP-Profile	Specifies out-of-band DTMF carriage. When enabled, DTMF signals are carried out of band via RTP or the associated signalling protocol. When disabled, DTMF tones are carried in the PCM stream.

13.7.1.3 Voice Service Configuration

To configure the announcement type, use the following command.

Command	Mode	Description
announcement-type { **silence** | **reorder-tone** | **fast-busy** | **voice-announcement** }	VoIP-Profile	Specifies the treatment when a subscriber goes off hook but does not attempt a call.

To configure the target value of jitter buffer, use the following command.

Command	Mode	Description
jitter-target *VALUE*	VoIP-Profile	Specifies the target value of jitter buffer. The system tries to maintain the jitter buffer at the target value. VALUE: 0-65535, target value of jitter buffer, the value 0 specifies dynamic jitter buffer sizing. (unit: ms)
no jitter-target		Deletes the configured target value of jitter buffer.

To configure the maximum depth of the jitter buffer, use the following command.

Command	Mode	Description
jitter-buffer-max *VALUE*	VoIP-Profile	Specifies the maximum depth of the jitter buffer associated with this service. VALUE: 0-65535, maximum depth of jitter buffer (unit: ms)
no jitter-buffer-max		Deletes the configured maximum depth of the jitter buffer.

To configure echo cancellation, use the following command.

Command	Mode	Description
echo-cancel {**true** | **false**}	VoIP-Profile	Specifies whether echo cancellation is on or off. (true = on, false = off)

To configure the variant of POTS signalling used on the associated UNIs, use the following command.

Command	Mode	Description
pstn-protocol-variant *E164_COUNTRY_CODE*	VoIP-Profile	Controls which variant of POTS signalling is used on the associated UNIs. Its value is equal to the E.164 country code. E164_COUNTRY_CODE: 0-65535
no pstn-protocol-variant		Deletes the configured E.164 country code.

13.7.1.4 RTP Configuration

To configure the RTP port used for voice traffic, use the following command.

Command	Mode	Description
rtp-local-port min *VALUE* {**max** *VALUE* }	VoIP-Profile	Defines the base and highest RTP port that should be used for voice traffic. VALUE: 0-65535, the base RTP port (default: 50000) VALUE: 0-65535, the highest RTP port

To configure Diffserv code point to be used for outgoing RTP packets, use the following command.

Command	Mode	Description
rtp-dscp-mark *VALUE*	VoIP-Profile	Specifies Diffserv code point to be used for outgoing RTP packets for this profile. VALUE: 0-255, Diffserv code point for outgoing RTP packets

To enable/disable RTP piggyback events, use the following command.

Command	Mode	Description
rtp-piggyback-event {**enable** | **disable**}	VoIP-Profile	Enables/disables RTP piggyback events. (default: disable)

To enable/disable handling of tones via RTP tone events, use the following command.

Command	Mode	Description
rtp-tone-event {**enable** | **disable**}	VoIP-Profile	Enables/disables handling of tones via RTP tone events per IETF RFC4733 and IETF RFC4734. (default: disable)

To enable/disable handling of DTMF via RTP DTMF events, use the following command.

Command	Mode	Description
rtp-dtmf-event {**enable** | **disable**}	VoIP-Profile	Enables/disables handling of DTMF via RTP DTMF events per IETF RFC4733 and IETF RFC 4734. (default: disable) This configuration is ignored unless out-of-band DTMF in the VoIP media configuration is enabled. (For out-of-band DTMF, see **oob-dtmf** command in 13.7.1.2 VoIP Media Configuration.)

To enable/disable handling of CAS via RTP CAS events, use the following command.

Command	Mode	Description
rtp-cas-event {**enable** | **disable**}	VoIP-Profile	Enables/disables handling of CAS via RTP CAS events per IETF RFC4733 and IETF RFC4734. (default: disable)

13.7.1.5 Signaling Code

To specify the POTS-side signaling, use the following command.

Command	Mode	Description
signaling-code {**loop-start** | **ground-start** | **loop-reverse-battery** | **coin-first** | **dial-tone-first** | **multi-party** }	VoIP-Profile	Specifies the POTS-side signaling.

13.7.1.6 DTMF Digit Configuration

To configure DTMF digit power levels, use the following command.

Command	Mode	Description
dtmf-digit levels *VALUE*	VoIP-Profile	Specifies the power level of DTMF digits that may be generated by the ONT toward the subscriber set. It is a 2s complement value referred to 1mW at the 0TLP (dBm0), with resolution 1dB. VALUE: DTMF digit power level
no dtmf-digit levels		Deletes the configured DTMF digit power levels.

To configure DTMF digit duration, use the following command.

Command	Mode	Description
dtmf-digit duration *VALUE*	VoIP-Profile	Specifies the duration of DTMF digits that may be generated by the ONT toward the subscriber set. VALUE: DTMF digit duration (unit: ms)
no dtmf-digit duration		Deletes the configured DTMF digit duration.

13.7.1.7 Hook Flash Time Configuration

To configure hook flash time, use the following command.

Command	Mode	Description
hook-flash-time {**max** | **min**} *VALUE*	VoIP-Profile	Defines the maximum or minimum duration recognized by the ONT as a switchhook flash. VALUE: maximum or minimum hook flash time (unit: ms)
no hook-flash-time {**max** | **min**}		Deletes the configured hook flash time.

13.7.1.8 VoIP Extended Operation Configuration

To configure the special line service, use the following command.

Command	Mode	Description
special-line-service disable	VoIP-Profile	Disables the special line service.
special-line-service hot-line *NUMBER*		Enables the hot-line feature that it immediately dials a pre-configured number as soon as the handset goes off hook.
special-line-service warm-line timeout <1-30> *NUMBER*		Enables the warm-line feature that it dials a pre-configured number if no digits were entered before the specified timer value expired when the handset went off hook. 1-30: warm-line timeout value (unit: seconds)

When a three-way call is established, the audio mixing can be perfomed by media server or client (ONT). With the media server, audio mixing is performed for all active calls at the server and it sends the audio stream using one audio channel to the client. In case of client, it mixes audio locally and thus achieves three-way calling without assistance from the media server.

To handle the three-way call audio mixing by server or client, use the following command.

Command	Mode	Description
three-way-ssw-mixing server	VoIP-Profile	Enables the server to control the transfer and perform audio mixing for the three-way call conferencing.
three-way-ssw-mixing client		Enables the client (ONT) to control the transfer and perform audio mixing for the three-way call conferencing.

To display the configure paramters for VoIP extended opration, use the following command.

Command	Mode	Description
show onu voip voip-ext-oper gpon *OLT-ID ONU-ID*	Enable/Global	Shows the VoIP extended operation parameters. ONU-ID: 1-128 or ONU serial number
show onu voip voip-ext-oper *ONU-ID*	Interface [GPON]	

13.7.2 OMCI-based SIP Configuration

If the ONUs are fully provisioned and managed from the LD3032 using OMCI, you can configure POTS interface, call features and SIP agents of these ONUs.

You need to enter SIP mode to perform the SIP-related detail configuration such as VoIP application service, SIP agent, etc. To enter the SIP mode, use the following command.

Command	Mode	Description
protocol sip	VoIP-Profile	Enters the SIP mode.

13.7.2.1 SIP Agent Configuration

This defines the configuration necessary to establish communication for signalling between the SIP user agent and SIP servers. To specify an SIP proxy server, use the following command.

Command	Mode	Description
proxy-server *ADDRESS*	VoIP-SIP	Configures IP address or URI of SIP proxy server for SIP signalling messages. ADDRESS: SIP proxy server IP address or URI
no proxy-server		Deletes the configured address of SIP proxy server.

To specify an outbound SIP proxy server, use the following command.

Command	Mode	Description
outbound-proxy-server *ADDRESS*	VoIP-SIP	Configures IP address or URI of outbound SIP proxy server for SIP signalling messages. ADDRESS: outbound SIP proxy server IP address or URI
no outbound-proxy-server		Deletes the configured address of outbound SIP proxy server.

To specify an SIP DNS, use the following command.

Command	Mode	Description
dns primary *A.B.C.D* [**secondary** *A.B.C.D*]	VoIP-SIP	Specifies the primary/secondary SIP DNS IP address. A.B.C.D: primary/secondary DNS server address (default: 0 (= no primary/secondary SIP DNS is defined))
no dns		Deletes the configured address of SIP DNS server.

To specify a register server, use the following command.

Command	Mode	Description
register-server *ADDRESS*	VoIP-SIP	Specifies the register server IP address or resolved name. ADDRESS: register server address
no register-server		Deletes the configured address of register server.

To identify an SIP gateway softswitch vendor, use the following command.

Command	Mode	Description
soft-switch *NAME*	VoIP-SIP	Identifies the SIP gateway softswitch vendor. NAME: vendor name
no soft-switch		Deletes the configured SIP gateway softswitch vendor name.

The format of vendor name is four ASCII coded alphabetic characters (A..Z) as defined in ATIS-0322000. A value of four null characters indicates no particular vendor.

To configure the SIP registration expiration time, use the following command.

Command	Mode	Description
reg-exp-time <0-65535>	VoIP-SIP	Specifies the SIP registration expiration time. If the value is 0, the SIP agent does not add an expiration time to the registration requests and does not perform re-registration. 0-65535: SIP registration expiration time (unit: second, default: 3600)

To configure the SIP re-registration head start time, use the following command.

Command	Mode	Description
rereg-head-start-time <0-65535>	VoIP-SIP	Specifies the time prior to timeout that causes the SIP agent to start the re-registration process. (unit: second, default: 360)

To specify a host part , use the following command.

Command	Mode	Description
host-part-server *URI*	VoIP-SIP	Specifies the host or domain part of the SIP address of record for users connected to the ONT. URI: host part URI
no host-part-server		Deletes the configured host part URI.

To enable/disable ONT to transmit SIP options, use the following command.

Command	Mode	Description
sip-option-transmit-control {**enable** | **disable**}	VoIP-SIP	Enables/disables ONT to transmit SIP options. (default: disable)
no sip-option-transmit-control		Sets no transmit-control value.

To configure the URI format in outgoing SIP messages, use the following command.

Command	Mode	Description
sip-uri-format {**tel-uri** | **sip-uri**}	VoIP-SIP	Specifies the format of the URI in outgoing SIP messages. (default: TEL URI)
no sip-uri-format		Deletes the configured format of URI in outgoing SIP messages.

13.7.2.2 SIP Detailed Feature Operation

If you specify the SIP server doamin, SIP server supports DNS for resolving the IP address of a proxy required to send a SIP message. This information is stored in DNS cache to prevent sending every DNS Query packets.

To set a SIP stack DNS cache update policy, use the following command.

Command	Mode	Description
dns-cache-policy ttl	VoIP-SIP	Specifies the expired time of DNS cache by TTL value in DNS response message. ttl: SIP stack DNS Cache is updated by TTL value
dns-cache-policy permanent		Retains the DNS resolved IP address without the expired time of DNS cache. permanent: SIP Stack DNS Cache is updated when VoIP configurations are changed

SIP timers define the transaction expiration timers, retransmission intervals when UDP is used as a transport, and the lifetime of dynamic TCP connection. The retransmission and expiration timers correspond to the timers defined in RFC 3261.

To specify various timers that SIP uses, use the following command.

Command	Mode	Description
sip-timer t1 <0-2500> **t2** <0-5000> **td** <5000-65535>	VoIP-SIP	Specifies the SIP timers. t1: Round-trip time (RTT) estimate (default: 500 ms) t2: maximum retransmission interval for non-INVITE requests and INVITE responses td: wait time for response retransmissions

The LD3032 supports SIP session timer which allows a periodic refreshing of SIP sessions using the register message to prevent the termination of SIP session. When using NAT with SIP service, NAT terminates the SIP session in case there is no SIP message transmission for a certain time period. To specify a session timeout to maintain the connection of SIP session, use the following command.

Command	Mode	Description
session-timer timeout <1-65535>	VoIP-SIP	Defines the time for waiting to maintain the connection of SIP session by force.
no session-timer		Deletes the configured SIP session timer.

When the user dials digits that do not match the digit map, it’s possible to keep dialing by pressing “#” button. It is called the end-of-digit. To enable/disable the use of an end-of-digit, use the following command.

Command	Mode	Description
end-of-digit {**enable** | **disable**}	VoIP-SIP	Enables/disables the use of an end-of-digit.
end-sharp-token {**hex** | **ascii**}		Translates the characters to the hexadecimal value or ASCII character code and sends them. For example, the hash (#) symbol has a hexadecimal value of 0x23, so it is encoded as %23.

To display the parameters of SIP detailed feature operation, use the following command.

Command	Mode	Description
show onu voip sip-detail-oper gpon *OLT-ID ONU-ID*	Enable Global	Shows the configured parameters of SIP detailed feature operation. ONU-ID: 1-128 or ONU serial number
show onu voip sip-detail-oper *ONU-ID*	Interface [GPON]	

13.7.2.3 VoIP Application Service

The configuration of VoIP application service defines the attributes of calling features used in conjunction with a VoIP line service, such as CID, call waiting, call transfer, call presentation, direct connect, and etc.

To configure the CID features, use the following command.

Command	Mode	Description
caller-id {**call-number** | **call-name** | **cid-blocking** | **cid-number** | **cid-name** | **acr**}	VoIP-SIP	Enables each feature for caller ID. (default: disabled) call-number: calling number call-name: calling name cid-blocking: CID blocking (both number and name) cid-number: permanent presentation status for number cid-name: permanent presentation status for name acr: anonymous CID blocking. It may not be possible to support this feature in the ONT.
no caller-id		Disables all the features for caller ID.

To configure the call waiting features, use the following command.

Command	Mode	Description
call-waiting {**call-wait** | **cid-announce**}	VoIP-SIP	Enables each feature for call waiting. (default: disabled) call-wait: call waiting cid-announce: caller ID announcement
no call-waiting		Disables the call waiting feature.

To configure the call processing (transfer) features, use the following command.

Command	Mode	Description
call-progress-transfer {**3way** | **call-transfer** | **call-hold** | **call-park** | **not-disturb** | **flash-emerg-call** | **emerg-originating-hold** | **6way**}	VoIP-SIP	Enables each feature for call processing. (default: disabled) 3way: 3way call call-transfer: call transfer call-hold: call hold call-park: call park not-disturb: do not disturb flash-emerg-call: flash on emergency service call (flash is to be processed during an emergency service call) emerg-originating-hold: emergency service originating hold (determines whether call clearing is to be performed on on-hook during an emergency service call) 6way: 6way call
no call-progress-transfer		Disables all the features for call processing.

To configure the call presentation features, use the following command.

Command	Mode	Description
call-present {**splash-ring** | **dial-tone** | **visual-indicate** | **call-forward**}	VoIP-SIP	Enables each feature for call presentation. (default: disabled) splash-ring: message waiting indication splash ring dial-tone: message waiting indication special dial tone visual-indicate: message waiting indication visual indication call-forward: call forwarding indication
no call-present		Disables all the features for call presentation.

To configure the direct connect feature, use the following command.

Command	Mode	Description
direct-connect enable	VoIP-SIP	Enables the direct connect feature. (default: disabled)
direct-connect delay-option		Enables the dial tone feature delay option.
direct-connect disable		Disables the direct connect feature.

To specify a direct connect target, use the following command.

Command	Mode	Description
direct-connect-uri *URI*	VoIP-SIP	Configures the URI of direct connect. URI: direct connect URI
no direct-connect-uri		Deletes the configured URI of direct connect.

To specify a bridged line agent, use the following command.

Command	Mode	Description
bridged-line-agent-uri *URI*	VoIP-SIP	Configures the URI of bridged line agent. URI: bridged line agent URI
no bridged-line-agent-uri		Deletes the configured URI of bridged line agent.

To specify a conference factory, use the following command.

Command	Mode	Description
conference-factory-uri *URI*	VoIP-SIP	Configures the URI of conference factory. URI: conference factory URI
no conference-factory-uri		Deletes the configured URI of conference factory.

13.7.2.4 VoIP Feature Access Codes

The configuration of VoIP feature access codes defines administrable feature access codes for the VoIP subscriber.

To configure VoIP feature access codes, use the following command.

Command	Mode	Description
feature cancel-call-wait *VALUE*	VoIP-SIP	Specifies the access code for each feature. VALUE: a string of characters from the set (0..9, *, #) with trailing nulls in any unused bytes
feature call-hold *VALUE*		
feature call-park *VALUE*		
feature caller-id-act *VALUE*		
feature caller-id-deact *VALUE*		
feature do-not-disturb-act *VALUE*		
feature do-not-disturb-deact *VALUE*		
feature do-not-disturb-pin-change *VALUE*		
feature emerg-service-number *VALUE*		
feature intercom-service *VALUE*		
no feature cancel-call-wait		Deletes the specified access code for each feature.
no feature call-hold		
no feature call-park		
no feature caller-id-act		
no feature caller-id-deact		
no feature do-not-disturb-act		
no feature do-not-disturb-deact		
no feature do-not-disturb-pin-change		
no feature emerg-service-number		
no feature intercom-service		

13.7.2.5 SIP User Data

The configuration of SIP user data defines the user-specific attributes associated with a specific VoIP CTP.

To specify an SIP voicemail server, use the following command.

Command	Mode	Description
voicemail-server-uri *ADDRESS*	VoIP-SIP	Configures IP address or URI of SIP voicemail server. ADDRESS: voicemail server IP address or URI

To specify the voicemail subscription expiration time, use the following command.

Command	Mode	Description
voicemail-subscript-expire-time *VALUE*	VoIP-SIP	Defines the voicemail subscription expiration time. If this value is 0, the SIP agent uses an implementation-specific value. (unit: second, default: 3600)

To configure a release timer, use the following command.

Command	Mode	Description
release-timer <0-255>	VoIP-SIP	Configures a release timer. The value 0 specifies that the ONT is to use its internal default. (unit: second, default: 10)

To configure a ROH timer, use the following command.

Command	Mode	Description
roh-timer <0-255>	VoIP-SIP	Defines the time for the receiver off hook condition before ROH tone is applied. The value 0 disables ROH timing. (unit: second, default: 15)

13.7.2.6 Network Dial Plan

To configure the critical dial timeout, use the following command.

Command	Mode	Description
dial-plan crit-timeout *TIMEOUT*	VoIP-SIP	Defines the critical dial timeout for digit map processing. TIMEOUT: critical dial timeout (unit: ms, default: 4000)

To configure the partial dial timeout, use the following command.

Command	Mode	Description
dial-plan part-timeout *TIMEOUT*	VoIP-SIP	Defines the partial dial timeout for digit map processing. TIMEOUT: partial dial timeout (unit: ms, default: 16000)

To configure the dial plan format, use the following command.

Command	Mode	Description
dial-plan format {**h248** | **nsc** | **vendor**}	VoIP-SIP	Defines the dial plan format standard that is supported in the ONT for VoIP. h248: H.248 format with specific plan (table entries define the dialling plan) nsc: NSC format vendor: vendor-specific format

To configure the dial plan table, use the following command.

Command	Mode	Description
dial-plan table *TABLE_ID TABLE_TOKEN*	VoIP-SIP	Adds a dial plan with the configured token. TABLE_ID: A unique identifier of a dial plan within the dial plan table TABLE_TOKEN: the token used by the VoIP service to process dial plans (This ASCII string is typically delimited by ":".)
no dial-plan table *TABLE_ID*		Deletes the created dial plan table.

i The dial plan created by **dial-plan table** command can be applied only if you configure the dial plan format as H.248 by using **dial-plan format h248** command.

i In order to see the configured dial plan, use **show voip-profile** command.

13.7.3 OMCI-based MGC Configuration

MGCP (Media Gateway Control Protocol) is a signalling and call control protocol used within VoIP systems that typically interoperate with the public switched telephone network (PSTN).

If the ONUs are fully provisioned and managed from the LD3032 using OMCI, you can configure the MGC-related settings of these ONUs. The MGC entity defines the media gateway controller configuration associated with an MG subscriber. It is conditionally required for ONUs (ONTs) that support MGCP (H.248, Megaco) VoIP service.

You need to enter MGC mode to perform the MGC-related detail configuration. To enter the MGC mode, use the following command.

Command	Mode	Description
protocol {**mgcp** | **h248**}	VoIP-Profile	Enters the MGC mode.

To configure the IP address of primary and secondary MGC server that controls the signalling messages, use the following command.

Command	Mode	Description
mgc {**primary** | **secondary**} *A.B.C.D*	VoIP-MGC	Configures the IP address of primary and secondary MGC server.
no mgc {**primary** | **secondary**}		Deletes the configured IP address.

To configure the version of MGCP to be used, use the following command.

Command	Mode	Description
mgc version *VALUE*	VoIP-MGC	Configures the version of MGCP.

To define the message format, use the following command.

Command	Mode	Description
mgc msg-format {**text-long** | **text-short** | **binary**}	VoIP-MGC	Configures the message format. (default: text-long)

To specify the maximum retry time for MGC transactions, use the following command.

Command	Mode	Description
mgc max-retry-time <0-65534>	VoIP-MGC	Configures the maximum retry time for MGC transactions. 0-65534: maximum retry time (unit: second)
no mgc max-retry-time		Deletes the configured maximum retry time.

To specify the maximum number of times that a message is retransmitted to the MGC, use the following command.

Command	Mode	Description
mgc max-retry-attempts <0-65534>	VoIP-MGC	Configures the maximum number of times that a message is retransmitted to the MGC. 0-65534: maximum number of times
no mgc max-retry-attempts		Deletes the configured maximum number of times.

To specify the service status delay time for changes in line service status, use the following command.

Command	Mode	Description
mgc service-change-delay <0-65534>	VoIP-MGC	Configures the service status delay time for changes in line service status. 0-65534: service status delay time
no mgc service-change-delay		Deletes the configured delay time.

To specify the gateway softswitch name, use the following command.

Command	Mode	Description
mgc soft-switch *NAME*	VoIP-MGC	Specifies the gateway softswitch name. NAME: gateway softswitch (format: four ASCII coded alphabetic characters [A-Z])
no mgc soft-switch		Deletes the gateway softswitch name configuration.

13.7.4 Saving VoIP Profile

After configuring a VoIP profile, you need to save the profile with the following command.

Command	Mode	Description
apply	VoIP-Profile	Saves a VoIP profile configuration.

i

Whenever you modify a VoIP profile, you should apply the changes again using the **apply** command. If not, the changes will not be applied.

13.7.5 Displaying VoIP Information

To display the information of VoIP profiles, use the following command.

Command	Mode	Description
show voip-profile [*NAME*]	Global Interface [GPON] VoIP-profile	Shows the information of VoIP profiles. NAME: VoIP profile name

To display VoIP service and VoIP line status information, use the following command.

Command	Mode	Description
show onu voip line gpon *OLT-ID ONU-ID*	Enable Global	Shows the information of VoIP service and line status. ONU-ID: 1-128 or ONU serial number
show onu voip line *ONU-ID*	Interface [GPON]	

To display the information of current profile, use the following command.

Command	Mode	Description
show current-profile	Current-Profile	Shows the information currently configured for the profile.

13.7.6 Sample Configuration

For the sample configuration, see “Configuration Example 1” in 13.15 Sample Configuration.

13.8 TDM Pseudowire Profile

Pseudowire emulation is a method for transmitting any Layer 2 protocol over PSNs (Packet Switched Networks). It allows a seamless connection between two network elements by creating logical links, or virtual tunnels, across the packet network. In TDM pseudowires, the transmitted E1, T1, E3, or T3 streams are encapsulated in packets upon entering the network and then reconstructed at the pseudowire egress, where clocking information is also regenerated. As a result, real-time traffic is delivered transparently without distortion, avoiding the complexities of translating signaling data, while ensuring that synchronization criteria are met.

In order to perform the TDM pseudowire related configuration, you should create/enter the TDM pseudowire profile. For the creation and configuration of the profile, see the following sections.

13.8.1 Creating TDM Pseudowire Profile

To create a TDM pseudowire profile, use the following command.

Command	Mode	Description
tdm-pw-profile *NAME* **create**	Global	Creates a TDM pseudowire profile. NAME: TDM pseudowire profile name

After opening *TDM Pseudowire Profile Configuration* mode, the prompt changes from SWITCH(config)# to SWITCH(config-tdm-pw-profile[*NAME*])#.

To delete an existing TDM pseudowire profile, use the following command.

Command	Mode	Description
no tdm-pw-profile {*NAME* | **all**}	Global	Deletes the TDM pseudowire profile. NAME: TDM pseudowire profile name

To modify an existing TDM pseudowire profile, use the following command.

Command	Mode	Description
tdm-pw-profile *NAME* **modify**	Global	Modifies the exisitng TDM pseudowire profile. NAME: TDM pseudowire profile name

13.8.2 Basic Service Type

To specify the basic service type, use the following command.

Command	Mode	Description
service-type {**unstructured** | **octet-aligned-unstructured** | **structured**}	TDM-PW-Profile	Specifies the basic service type, either a transparent bit pipe or an encapsulation that recognizes the underlying structure of the payload. unstructured: Basic unstructured (also known as structure agnostic) octet-aligned-unstructured: Octet-aligned unstructured, structure agnostic. Applicable only to DS1, a mode in which each frame of 193 bits is encapsulated in 25 bytes with 7 padding bits structured: Structured (structure-locked)

13.8.3 Signalling

To configure the signalling, use the following command.

Command	Mode	Description
signalling { **no-signalling** | **cas-carry-packet** | **cas-carry-channel** }	TDM-PW-Profile	Specifies the signalling attribute. no-signalling: No signalling visible at this layer cas-carry-packet: CAS, to be carried in the same packet stream as the payload cas-carry-channel: CAS, to be carried in a separate signalling channel

13.8.4 Payload Size

To specify the payload size per packet, use the following command.

Command	Mode	Description
payload-size {**192** | **200** | **256** | **1024**}	TDM-PW-Profile	Defines the number of payload bytes per packet. Valid only if service type = unstructured or unstructured octet-aligned. Valid choices depend on the TDM service as follows. 192: DS1 200: DS1, required only if unstructured octet-aligned service is supported 256: E1 1024: DS3 / E3
no payload-size		Deletes the configured payload size.

13.8.5 Payload Encapsulation Delay

To configure the payload encapsulation delay (only for structured service), use the following command.

Command	Mode	Description
payload-encapsulation-delay { **1** | **2** | **3** | **4** | **5** | **8** }	TDM-PW-Profile	Defines the delay time (which corresponds to number of 125 microsecond frames) to be encapsulated in each pseudowire packet. Valid only if service type = structured. The minimum set of choices for various TDM services is listed below, and is affected by the possible presence of in-band signalling. 8: 8 ms (that corresponds to 64 frames), no signalling, N = 1, required 5: 5 ms (that corresponds to 40 frames), no signalling, N = 1, desired 4: 4 ms (that corresponds to 32 frames), no signalling, N = 2~4 3: 3 ms (that corresponds to 24 frames), with DS1 CAS 2: 2 ms (that corresponds to 16 frames), with E1 CAS 1: 1 ms (that corresponds to 8 frames), no signalling, N > 4
no payload-encapsulation-delay		Deletes the configured payload encapsulation delay time.

13.8.6 Timing Mode

To configure the timing mode of the TDM service, use the following command.

Command	Mode	Description
timing-mode {**network** | **differential** | **adaptive** | **loop**}	TDM-PW-Profile	Selects the timing mode of the TDM service. If RTP is used, this configuration must be set to be consistent with the value of the RTP time stamp mode configuration in the RTP parameters setting at the far end. network: Network timing (default) differential: Differential timing adaptive: Adaptive timing loop: Loop timing. local TDM transmit clock derived from local TDM receive stream

13.8.7 RTP Pseudowire Parameter

If a pseudowire service uses RTP, the RTP pseudowire parameters provide configuration for the RTP layer. You can configure the RTP pseudowire parameters by referring to the following sections.

13.8.7.1 Clock Reference

To specify the frequency of the common timing reference, use the following command.

Command	Mode	Description
rtp-clock-reference *VALUE*	TDM-PW-Profile	Specifies the frequency of the common timing reference. VALUE: in multiples of 8 kHz (for example, input 1 means 8 kHz) (default: 1)

13.8.7.2 RTP Time Stamp Mode

To specify the RTP time stamp mode, use the following command.

Command	Mode	Description
rtp-time-stamp-mode {**unknown** | **absolute** | **differential**}	TDM-PW-Profile	Determines the mode in which RTP timestamps are generated in the TDM to PSN direction. unknown: Unknown or not applicable (default) absolute: Absolute. Timestamps are based on the timing of the incoming TDM signal differential: Differential. Timestamps are based on the ONT's reference clock, which is understood to be stratum-traceable along with the reference clock at the far end

13.8.7.3 RTP Payload Type

To configure the RTP payload type, use the following command.

Command	Mode	Description
rtp-payload-type payload *VALUE* **signalling** *VALUE*	TDM-PW-Profile	Specifies the RTP payload type in the TDM to PSN direction. payload VALUE: for the payload channel signalling VALUE: 96 to 127, for the optional separate signalling channel. If signalling is not transported in its own channel, this value should be set to 0.
rtp-expect-payload-type payload *VALUE* **signalling** *VALUE*		Specifies the RTP payload type in the PSN to TDM direction. The received payload type may be used to detect malformed packets. payload VALUE: for the payload channel signalling VALUE: for the optional separate signalling channel
no rtp-expect-payload-type		Deletes the configured RTP payload type in the PSN to TDM direction.

13.8.7.4 RTP Synchronization Source

To configure the RTP synchronization source, use the following command.

Command	Mode	Description
rtp-sync-source payload *VALUE* **signalling** *VALUE*	TDM-PW-Profile	Specifies the RTP synchronization source in the TDM to PSN direction. payload VALUE: for the payload channel signalling VALUE: for the optional separate signalling channel. If signalling is not transported in its own channel, this value should be set to 0.
rtp-expect-sync-source payload *VALUE* **signalling** *VALUE*		Specifies the RTP synchronization source in the PSN to TDM direction. The received synchronization source may be used to detect misconnection (stray packets). payload VALUE: for the payload channel signalling VALUE: for the optional separate signalling channel
no rtp-expect-sync-source		Deletes the configured RTP synchronization source in the PSN to TDM direction.

13.8.8 Pseudowire Maintenance Configuration

If you need the configuration for pseudowire service exception handling, you should connect a pseudowire maintenance profile to the current profile.

To connect the pseudowire maintenance profile to the current profile, use the following command.

Command	Mode	Description
pw-maintenance-profile *NAME*	TDM-PW-Profile	Connects a pseudowire maintenance profile to the current TDM pseudowire profile.
no pw-maintenance-profile		Disconnects the specified pseudowire maintenance profile.

i For the details of how to create and configure the pseudowire maintenance profile, see 13.9 Pseudowire Maintenance Profile.

13.8.9 Saving TDM Pseudowire Profile

After configuring a TDM pseudowire profile, you need to save the profile with the following command.

Command	Mode	Description
apply	TDM-PW-Profile	Saves a TDM pseudowire profile configuration.

i Whenever you modify a TDM pseudowire profile, you should apply the changes again using the **apply** command. If not, the changes will not be applied.

13.8.10 Displaying TDM Pseudowire Information

To display the information of TDM pseudowire profiles, use the following command.

Command	Mode	Description
show tdm-pw-profile [*NAME*]	Enable Global Interface [GPON] TDM-PW-Profile	Shows the information of TDM pseudowire profiles. NAME: TDM pseudowire profile name

To display the list information of source MAC addresses for TDM pseudowire of ONU, use the following command.

Command	Mode	Description
show onu tdm-pw source-mac gpon *OLT-ID ONU-ID*	Enable Global	Shows the list of source MAC addresses for TDM pseudowire of the specified ONU.
show onu tdm-pw source-mac *ONU-ID*	Interface [GPON]	

13.9 Pseudowire Maintenance Profile

The pseudowire maintenance profile permits the configuration of pseudowire service exception handling. The pseudowire maintenance profile primarily affects the alarms declared by the subscribing pseudowire termination. And also, the settings of a pseudowire maintenance profile affect the pseudowire performance monitoring history.

13.9.1 Creating Pseudowire Maintenance Profile

To create a pseudowire maintenance profile, use the following command.

Command	Mode	Description
pw-maintenance-profile *NAME* **create**	Global	Creates a pseudowire maintenance profile. NAME: pseudowire maintenance profile name

After opening *PW Maintenance Profile Configuration* mode, the prompt changes from SWITCH(config)# to SWITCH(config-pw-maintenance-profile[*NAME*])#.

To delete an existing pseudowire maintenance profile, use the following command.

Command	Mode	Description
no pw-maintenance-profile {*NAME* | **all**}	Global	Deletes the pseudowire maintenance profile. NAME: pseudowire maintenance profile name

To modify an existing pseudowire maintenance profile, use the following command.

Command	Mode	Description
pw-maintenance-profile *NAME* **modify**	Global	Modifies the exisitng pseudowire maintenance profile. NAME: pseudowire maintenance profile name

13.9.2 Jitter Buffer Maximum Depth

To specify the maximum depth of the playout buffer in the PSN to TDM direction, use the following command.

Command	Mode	Description
jitter-buffer-max-depth *VALUE*	PW-Maintenance-Profile	Specifies the desired maximum depth of the playout buffer in the PSN to TDM direction. VALUE: expressed as a multiple of the 125 μs frame rate
no jitter-buffer-max-depth		Deletes the configured maximum depth of the playout buffer.

13.9.3 Jitter Buffer Desired Depth

To specify the desired nominal fill depth of the playout buffer in the PSN to TDM direction, use the following command.

Command	Mode	Description
jitter-buffer-desired-depth *VALUE*	PW-Maintenance-Profile	Specifies the desired nominal fill depth of the playout buffer in the PSN to TDM direction. VALUE: expressed as a multiple of the 125 μs frame rate
no jitter-buffer-desired-depth		Deletes the configured nominal fill depth of the playout buffer.

13.9.4 Fill Policy

To specify the payload bit pattern to be applied toward the TDM service, if no payload packet is available to play out, use the following command.

Command	Mode	Description
fill-policy {**vendor-specific** | **play-out-ais** | **play-out-all-1s** | **play-out-all-0s** | **repeat-prev-data** | **play-out-ds1-idle**}	PW-Maintenance-Profile	Defines the payload bit pattern to be applied toward the TDM service if no payload packet is available to play out. vendor-specific: ONT default, vendor-specific (recommended: AIS for unstructured service, all 1s for structured service) play-out-ais: Play out AIS according to the service definition (for example, DS3 AIS) play-out-all-1s: Play out all 1s play-out-all-0s: Play out all 0s repeat-prev-data: Repeat the previous data play-out-ds1-idle: Play out DS1 idle (Appendix C of "b-ATIS T1.403")
no fill-policy		Deletes the configured payload bit pattern.

13.9.5 Alarm-related Policy

The LD3032 supports four pairs of alarm-related policies configuration which causes the corresponding alarm to be declared or cleared. To configure the policy (anomaly rate) that causes the alarm to be declared or cleared, use the following command.

Command	Mode	Description
buffer-over-underrun-declaration-policy <1-100>	PW-Maintenance-Profile	Defines the anomaly rate that causes the corresponding alarm to be declared. If this density of anomalies occurs during the alarm onset soak interval, the alarm is declared. buffer-over-underrun: buffer overrun/underrun loss-packet: loss packet malformed-packet: malformed packet misconnect-packet: misconnect packet
loss-packet-declaration-policy <1-100>		
malformed-packet-declaration-policy <1-100>		
misconnect-packet-declaration-		

Command	Mode	Description
policy <1-100>		1-100: anomaly rate (unit: integer percentage)
buffer-over-underrun-clear-policy <0-99>		Defines the anomaly rate that causes the corresponding alarm to be cleared. If no more than this density of anomalies occurs during the alarm clear soak interval, the alarm is cleared. buffer-over-underrun: buffer overrun/underrun loss-packet: loss packet malformed-packet: malformed packet misconnect-packet: misconnect packet 1-99: anomaly rate (unit: integer percentage)
loss-packet-clear-policy <0-99>		
malformed-packet-clear-policy <0-99>		
misconnect-packet-clear-policy <0-99>		

To delete the configured anomaly rate, use the following command.

Command	Mode	Description
no buffer-over-underrun-declaration-policy	PW-Maintenance-Profile	Deletes the configured anomaly rate that causes the corresponding alarm to be declared or cleared.
no loss-packet-declaration-policy		
no malformed-packet-declaration-policy		
no misconnect-packet-declaration-policy		
no buffer-over-underrun-clear-policy		
no loss-packet-clear-policy		
no malformed-packet-clear-policy		
no misconnect-packet-clear-policy		

13.9.6 L-bit/R-bit Receive/Transmit Policy

To configure the L-bit receive policy, use the following command.

Command	Mode	Description
l-bit-receive-policy {**play-out** | **repeat-last-packet** | **send-idle**}	PW-Maintenance-Profile	Defines the action toward the TDM interface when far end TDM failure is indicated on packets received from the PSN (L-bit set). play-out: Play out service-specific AIS (default) repeat-last-packet: Repeat last received packet send-idle: Send channel idle signalling and idle channel payload to all DS0s comprising the service
no l-bit-receive-policy		Deletes the configured L-bit receive policy.

To configure the R-bit transmit set policy, use the following command.

Command	Mode	Description
r-bit-transmit-set-policy *VALUE*	PW-Maintenance-Profile	Defines the number of consecutive lost packets that causes the transmitted R-bit to be set in the TDM to PSN direction, indicating lost packets to the far end. VALUE: number of consecutive lost packets

Command	Mode	Description
no r-bit-transmit-set-policy		Deletes the configured R-bit transmit set policy.

To configure the R-bit receive policy, use the following command.

Command	Mode	Description
r-bit-receive-policy {**none** | **play-out** | **send-idle**}	PW-Maintenance-Profile	Defines the action toward the N x 64 TDM interface when remote failure is indicated on packets received from the PSN (R-bit set = 0b10 while the L-bit is cleared). none: Do nothing (default) play-out: Play out service-specific RAI/REI/RDI code send-idle: Send channel idle signalling and idle channel payload to all DS0s comprising the service

13.9.7 SES Threshold

To configure the SES threshold, use the following command.

Command	Mode	Description
ses-threshold *VALUE*	PW-Maintenance-Profile	Defines the number of lost, malformed or otherwise unusable packets expected in the PSN to TDM direction within a one-second interval that causes a severely errored second to be counted. Stray packets do not count toward a severely errored second, nor do packets whose L-bit is set at the far end. VALUE: Number of lost, malformed or otherwise unusable packets (default: 3)
no ses-threshold		Deletes the configured SES threshold.

13.9.8 Saving Pseudowire Maintenance Profile

After configuring a pseudowire maintenance profile, you need to save the profile with the following command.

Command	Mode	Description
apply	PW-Maintenance-Profile	Saves a pseudowire maintenance profile configuration.

i

Whenever you modify a pseudowire maintenance profile, you should apply the changes again using the **apply** command. If not, the changes will not be applied.

13.9.9 Displaying Pseudowire Maintenance Information

To display the information of pseudowire maintenance profiles, use the following command.

Command	Mode	Description
show pw-maintenance-profile [*NAME*]	Enable Global Interface [GPON] PW-Maintenance-Profile	Shows the information of pseudowire maintenance profiles. NAME: pseudowire maintenance profile name

To display the information of current profile, use the following command.

Command	Mode	Description
show current-profile	Current-Profile	Shows the information currently configured for the profile.

13.10 Performance Monitoring (PM) Profile

Performance Monitoring (PM) profile is used for the traffic statistics of all ONUs (ONTs) collected by an OLT. The ONT conceptually has only two storage bins: a current accumulator and a history bin. The current accumulator is used to store data collected for the current 15-minute interval. The history bin is used to store data for the previous 15-minute interval. At the end of the current 15-minute interval, they switch roles: the previous accumulator bin becomes the new history bin, while the content of the history bin is discarded and the bin itself is initialized as the new accumulator.The ONT performs no calculations upon the collected data nor does it keep an archive of collected data beyond the previous 15-minute interval. All calculations based on collected data and archiving of past intervals is performed by the OLT.

13.10.1 Creating PM Profile

To create a PM profile, use the following command.

Command	Mode	Description
pm-profile *NAME* **create**	Global	Creates a PM profile. NAME: PM profile name

To delete a created PM profile, use the following command.

Command	Mode	Description
no pm-profile {*NAME* | **all**}	Global	Deletes a created PM profile. NAME: PM profile name

To modify an existing PM profile, use the following command.

Command	Mode	Description
pm-profile *NAME* **modify**	Global	Modifies the existing PM profile. NAME: PM profile name

i

To collect the traffic statistics of ONUs via PM profile, the ONU must be applied with a Traffic Profile.

13.10.2 Collecting ONU Traffic Statistics

To enable/disable the performance monitoring (PM) function to collect the traffic statistics of the configured GEM port, use the following command.

Command	Mode	Description
pm gemport	PM-Profile	Enables the PM function to collect the GEM port-related counters.
no pm gemport		Disables the PM function to collect the GEM port-related counters.

To enable/disable the performance monitoring (PM) function to collect the traffic statistics of the configured ANI port, use the following command.

Command	Mode	Description
pm aniport	PM-Profile	Enables PM function to collect the data of ANI port's counters that are FCS error and the downstream GEM frame discarded due to buffer overflow or etc.
no pm aniport		Disables PM function to collect the data of ANI port's counters.

To enable/disable the performance monitoring (PM) function to collect the traffic statistics of the configured pseudowire, use the following command.

Command	Mode	Description
pm pseudowire	PM-Profile	Enables the PM function to collect the pseudowire-related counters.
no pm pseudowire		Disables the PM function to collect the pseudowire-related counters.

To enable/disable the performance monitoring (PM) function to collect the traffic statistics of the configured UNI port as Ethernet type 3, use the following command.

Command	Mode	Description
pm uni-eth3	PM-Profile	Enables the PM function to collect the counters of the configured UNI port as Ethernet type 3.
no pm uni-eth3		Disables the PM function to collect the counters of the configured UNI port as Ethernet type 3.

To enable/disable the performance monitoring (PM) function to collect the traffic statistics of the Ethernet frame over the configured UNI port, use the following command.

Command	Mode	Description
pm uni-eth-frame { **us** | **ds** }	PM-Profile	Enables the PM function to collect the Ethernet frame related conuters of UNI port. us: upstream ds: downstream
no pm uni-eth-frame		Disables the PM function to collect the Ethernet frame related conuters of UNI port.

To enable/disable the performance monitoring (PM) function to collect the traffic statistics of the configured CES UNI port, use the following command.

Command	Mode	Description
pm uni-ces	PM-Profile	Enables the PM function to collect the counters of the configured CES UNI port.
no pm uni-ces		Disables the PM function to collect the counters of the configured CES UNI port.

To enable/disable the performance monitoring (PM) function to collect the traffic statistics of the configured GEM NCTP ports, use the following command.

Command	Mode	Description
pm gem-nctp	PM-Profile	Enables the PM function to collect the counters of the configured GEM port network CTP for a specified traffic profile.
no pm gem-nctp		Disables the PM function to collect the counters of the configured GEM port network CTP.

13.10.3 Saving PM Profile

After configuring a PM profile, you need to save the profile with the following command.

Command	Mode	Description
apply	PM-Profile	Saves a PM profile configuration.

i

Even if you modify a running profile, you also need to use the **apply** command to apply the changes to ONUs (ONTs).

13.10.4 Displaying PM Profile Information

To display the information of PM profiles, use the following command.

Command	Mode	Description
show pm-profile [*NAME*]	Global Interface [GPON] PM-Profile	Shows the information of PM profiles. NAME: PM profile name

To display the information of current profile, use the following command.

Command	Mode	Description
show current-profile	Current-Profile	Shows the information currently configured for the profile.

13.10.5 Displaying ONU Traffic Statistics

To display the traffic statistics of an ONU applied by PM profile, use the following command.

Command	Mode	Description
show onu statistics gpon *OLT-ID* [*ONU-ID*]	Enable Global	Shows the information of ONU counters collected via PM profile. (15 Min, Prev_15 Min, total)
show onu statistics [*ONU-ID*]	Interface	

	[GPON]	
show onu statistics detail gpon *OLT-ID*	Enable Global	Shows the information of GEM port counters collected via PM profile. (15 Min, Prev_15 Min, total)
show onu statistics detail [*ONU-ID*]	Interface [GPON]	
show onu statistics {**current** | **current-detail**} **gpon** *OLT-ID ONU-ID*	Enable Global	Shows the information of current ONU counters collected via PM profile. (current counter, total + current counter)
show onu statistics {**current** | **current-detail**} *ONU-ID*	Interface [GPON]	
show onu statistics avg-pkt gpon *OLT-ID ONU-ID* [**uni-eth-frame** *UNI_ID*]	Enable Global	Shows the information of ONU counter (average packets) collected via PM profile.
show onu statistics avg-pkt *ONU-ID* [**uni-eth-frame** *UNI_ID*]	Interface [GPON]	
show onu statistics {**pre_15** | **hour** | **day** | **total**} **gpon** *OLT-ID ONU-ID* {**eth** *PORT* {**us** | **ds**} | **pots** *PORT* | **tdm** *PORT* | **pw** *NUMBER* | **gem** *PORT* | **gem-nctp** *PORT* | **ani** *PORT* }	Enable Global	Shows the information of ONU counters collected via PM profile based on Ethernet, POTS, TDM, GEM, ANI port or pseudowire number. pre_15/hour/day/total: time duration (previous 15min / hour / day / total) us/ds: upstream/downstream PORT: port number NUMBER: pseudowire number
show onu statistics {**pre_15** | **hour** | **day** | **total**} *ONU-ID* {**eth** *PORT* {**us** | **ds**} | **pots** *PORT* | **tdm** *PORT* | **pw** *NUMBER* | **gem** *PORT* **gem-nctp** *PORT* | **ani** *PORT* }	Interface [GPON]	

To clear the collected traffic statistics, use the following command.

Command	Mode	Description
clear onu statistics	Global	Clears collected traffic statistics of an ONU.
clear onu statistics gpon *OLT-ID* [*ONU-ID*]		
clear onu statistics [*ONU-ID*]	Interface [GPON]	Clears collected traffic statistics of an ONU.

13.10.6 Sample Configuration

For the sample configuration, see “Configuration Example 2” in 13.15 Sample Configuration.

13.11 Multicast Profile

The multicast profile is used for ONU (ONT) to handle the multicast traffic using a IGMP-related commands. Multicast profile managed entity organizes data associated with multicast management at subscriber ports of 802.1 bridges, including 802.1p mappers when the provisioning model is mapper-based rather than bridge-based. Instances of this managed entity are created and deleted by the OLT. It is the responsibility of the OLT to manage the members of a multicast group and control the multicast connection in ONTs

13.11.1 Creating Multicast Profile

To create a multicast profile, use the following command.

Command	Mode	Description
multicast-profile *NAME* **create**	Global	Creates a multicast profile. NAME: multicast profile name

After opening *Multicast Profile Configuration* mode, the prompt changes from SWITCH(config)# to SWITCH(config-mcast-profile[*NAME*])#.

To delete a created multicast profile, use the following command.

Command	Mode	Description
no multicast-profile {*NAME* | **all**}	Global	Deletes a created multicast profile. NAME: multicast profile name

To modify an existing multicast profile, use the following command.

Command	Mode	Description
multicast-profile *NAME* **modify**	Global	Modifies the existing multicast profile. NAME: multicast profile name

13.11.2 IGMP Configurations

To configure the multicast profile, use the following command.

Command	Mode	Description
igmp version <1-3>	Multicast-Profile	Sets an IGMP version on a current interface. 1-3: IGMP version (default: 2)
igmp function snooping		Enables the IGMP snooping.
igmp function suppression		Enables the IGMP snooping with proxy reporting (SRP).
igmp function proxy		Enables the IGMP proxy.
igmp immediate-leave enable		Enables the IGMP immediate leave. (Default: enable)
igmp querier address *A.B.C.D*		Specifies a querier address. A.B.C.D: querier address
igmp querier query-interval <0-3600>		Specifies a general query interval. 0-3600: query interval (default: 125 seconds)
igmp querier max-response-time <0-25>		Specifies a maximum query response time. 0-25: maximum response time (default: 10 seconds)
igmp robustness-variable <1-7>		Configures the Querier's Robustness Variable (QRV) value on an interface. (default: 2)
igmp access-list vid {**untagged** | *VLAN*} **dst-ip start** *A.B.C.D* **end** *A.B.C.D* [**bw** *VALUE* | **src-ip** *A.B.C.D* | **gem** *PORT* | **cos** <0-7>]		Configures the dynamic/static access control list table. It discards the IGMP join message from ONTs based on the access list. VLAN: 1 to 4095, VLAN ID for specific tagged downstream flow dst-ip: destination IP address A.B.C.D: start/end IP address of the multicast group range VALUE: imputed group bandwidth (unit: bytes/sec) src-ip: source IP address PORT: multicast GEM port ID
igmp static-access-list vid {**untagged** | *VLAN*} **dst-ip start** *A.B.C.D* **end** *A.B.C.D* [**bw** *VALUE* | **src-ip** *A.B.C.D* | **gem** *PORT* | **cos** <0-7>]		
igmp tag-control {**bypass** | **add vid** *VLANS* **cos** *VALUE* | **replace vid** *VLANS* [**cos** *VALUE*]}		Configures IGMP tag control attribute and the policy to define a VLAN ID and P-bits to add to upstream IGMP messages. bypass: pass upstream IGMP traffic transparently add: adds a VLAN tag (including P-bits) to upstream IGMP traffic replace: replaces the TCI (VLAN ID + P-bits or VLAN ID) VLANS: VLAN ID(s) (1-4095) VALUE: CoS (0-7)
igmp ds-tag-control {**remove** | **bypass** | **add vid** *VLANS* **cos** *VALUE* | **replace vid** *VLANS* [**cos** *VALUE*]}		Configures IGMP downstream tag control attribute and the policy to define a VLAN ID and COS value to add to IGMP messages. bypass: pass downstream IGMP traffic transparently add: adds a VLAN tag (including P-bits) to downstream IGMP traffic replace: replaces the TCI (VLAN ID + P-bits or VLAN ID)

		VLANS: VLAN ID(s) (1-4095) VALUE: CoS (0-7)
igmp upstream rate-limit <1-65535>		Configures the rate limit of upstream IGMP traffic 1-65535: IGMP message count (message/second)
igmp unauthorized-join-request allow		ONU will forward the IGMP join request or an IGMPv3 membership report for groups that is not authorized in the dynamic address control list table.
igmp unauthorized-join-request discard		ONU will silently discard an unauthorized IGMP join request.

To delete a specified IGMP configuration for multicast profile, use the following command.

Command	Mode	Description
igmp immediate-leave disable	Multicast-Profile	Deletes a specified IGMP configuration
no igmp robustness-variable		
no igmp querier address		
no igmp querier query-interval		
no igmp querier max-response-time		
no igmp {**access-list** | **static-access-list**} **all**		
no igmp access-list vid {**untagged** | *VLANS*} **dst-ip start** *A.B.C.D* **end** *A.B.C.D* [**bw** *VALUE* | **src-ip** *A.B.C.D* | **gem** *PORTS*]		
no igmp static-access-list vid {**untagged** | *VLANS*} **dst-ip start** *A.B.C.D* **end** *A.B.C.D* [**bw** *VALUE* | **src-ip** *A.B.C.D* | **gem** *PORTS*]		
no igmp tag-control		
no igmp ds-tag-control		
no igmp upstream rate-limit		

13.11.3 Saving Multicast Profile

After configuring a multicast profile, you need to save the profile with the following command.

Command	Mode	Description
apply	Multicast-Profile	Saves a multicast profile configuration.

Whenever you modify a multicast profile, you should apply the changes again using the **apply** command. If you do not, it will not be applied.

13.11.4 Applying Multicast Profile

If you want to apply a created multicast profile to a MAC bridge service profile, open *Traffic Profile Configuration* mode first, then you have to apply the multicast profile to MAC bridge service profile and its UNI-side port.

```
SWITCH(config-mcast-profile[TEST])# apply
SWITCH(config-mcast-profile[TEST])# exit
SWITCH(config)# traffic-profile 1 create
SWITCH(config-traffic-pf[1])# bridge 1
SWITCH(config-traffic-pf[1]-bridge[1])# uni eth 1
SWITCH(config-traffic-pf[1]-bridge[1]-uni[eth:1])# multicast-profile TEST
```

To apply the configured multicast profile to a specified UNI-side port of a traffic profile, use the following command.

Command	Mode	Description
multicast-profile *NAME*	Traffic Bridge-UNI	Applies the configured Multicast profile to a specified UNI port. NAME: Multicast profile name
no multicast-profile		Deletes the connections between a multicast profile and this UNI port.

13.11.5 Displaying Multicast Information

To display the information of Multicast profiles, use the following command.

Command	Mode	Description
show multicast-profile [*PROFILE*]	Enable Global Interface [GPON] Multicast-Profile	Shows the information of Multicast profiles PROFILE: Multicast profile name

13.11.6 Multicast Access List

The multicast access list is used for ONU (ONT) to handle the multicast traffic using the dynamic/static IGMP access list commands. For each dedicated multicast access list, it can permit/discard the IGMP message and multicast traffic of the specified IP multicast groups and ranges. It is the responsibility of the OLT to manage the members of a multicast group and control the multicast connection in ONTs. To implement this multicast access list per ONT, the specified multicast profile should be already configured on these ONTs.

13.11.6.1 Creating Multicast ACL

To create a multicast access list, use the following command.

Command	Mode	Description
multicast-access-list *NAME* **create**	Global	Creates a multicast access list. NAME: multicast access list name

i The maximum number of access list tables can be configurable up to 5 within a multicast access list.

After opening *Multicast Access Control List Configuration* mode, the prompt changes from SWITCH(config)# to SWITCH(config-mcast-acl-profile[*NAME*])#.

To delete a created multicast access list, use the following command.

Command	Mode	Description
no multicast-access-list {*NAME* | **all**}	Global	Deletes a created multicast access list. NAME: multicast access list name

To modify an existing multicast access list, use the following command.

Command	Mode	Description
multicast-access-list *NAME* **modify**	Global	Modifies the existing multicast access list. NAME: multicast access list name

13.11.6.2 IGMP Access List Configuration

To configure the multicast access list, use the following command.

Command	Mode	Description
igmp access-list vid {**untagged** | *VLAN*} **dst-ip start** *A.B.C.D* **end** *A.B.C.D* [**bw** *VALUE* | **src-ip** *A.B.C.D* | **gem** *PORT* | **cos** <0-7>]	Multicast-ACL	Configures the dynamic/static access control list table. It discards the IGMP join message from ONTs based on the access list. VLAN: 1 to 4095, VLAN ID for specific tagged downstream flow dst-ip: destination IP address A.B.C.D: start/end IP address of the multicast group range VALUE: imputed group bandwidth (unit: bytes/sec) src-ip: source IP address PORT: multicast GEM port ID
igmp static-access-list vid {**untagged** | *VLAN*} **dst-ip start** *A.B.C.D* **end** *A.B.C.D* [**bw** *VALUE* | **src-ip** *A.B.C.D* | **gem** *PORT* | **cos** <0-7>]		

To remove the dynamic/static access control list configuration from the multicast access list, use the following command.

Command	Mode	Description
no igmp {**access-list** | **static-access-list**} **all**	Multicast-ACL	Removes the dynamic/static access control list configuration from the multicast access list.
no igmp access-list vid {**untagged** | *VLANS*} **dst-ip start** *A.B.C.D* **end** *A.B.C.D* [**bw** *VALUE* | **src-ip** *A.B.C.D* | **gem** *PORTS*]		
no igmp static-access-list vid {**untagged** | *VLANS*} **dst-ip start** *A.B.C.D* **end** *A.B.C.D* [**bw** *VALUE* | **src-ip** *A.B.C.D* | **gem** *PORTS*]		

13.11.6.3 Saving Multicast ACL

After configuring a multicast ACL, you need to save the profile using the following command.

Command	Mode	Description
apply	Multicast-ACL	Saves a multicast ACL configuration.

i Whenever you modify a multicast ACL, you should apply the changes again using the **apply** command. If you do not, it will not be applied.

13.11.6.4 Applying Multicast Access List

To apply the configured multicast access list to a specified ONU ID, use the following command.

Command	Mode	Description
onu multicast-access-list *ONU-ID NAME* [**multicast-profile** *NAME*]	Interface [GPON]	Applies the dynamic/static multicast access control list table to ONU ID. It discards the IGMP join message from ONTs based on the access list. ONU_ID: ONU ID or ONU serial number NAME: multicast access list name multicast-profile: applies the multicast ACL to the specified ONUs on the Multicast profile. NAME: multicast profile name
no onu multicast-access-list *ONU-ID NAME* [**multicast-profile** *NAME*]		Removes the specified multicast access list configuration from ONU ID.

i Up to 8 multicast access lists can be configured per ONU ID.

13.11.6.5 Displaying Multicast Access List

To display the information of multicast access list, use the following command.

Command	Mode	Description
show multicast-access-list [*NAME*]	Enable Global Interface [GPON] Multicast-ACL	Shows the information of multicast access lists. NAME: Multicast access list name

To display the information of IGMP access control list per ONU, use the following command.

Command	Mode	Description
show onu multicast-access-list gpon *OLT-ID*	Enable Global	Shows the information of multicast access control lists per ONU.
show onu multicast-access-list [*ONU-ID*]	Interface [GPON]	

13.12 Rate-limit Profile

Basically the rate-limit configuration can be set in ‘Traffic Profile’. And the ‘Traffic Profile’ is assigned to ONT through 'ONU Profile'. When the service rate should be changed, you don’t need to modify all the 'Traffic Profiles' in the OLT. If an OLT has so many 'Traffic Profiles', you can create 'Rate-limit profile' and all Traffic Profiles can share this 'Rate-limit profile'. So when the service rate needs to be changed, you simply can modify the 'Rate-limit profile'.

13.12.1 Creating Rate-limit Profile

To create an Rate-limit profile, use the following command.

Command	Mode	Description
rate-limit-profile *NAME* **create**	Global	Creates an Rate-limit profile. NAME: Rate-limit profile name

After opening *Rate-limit Profile Configuration* mode, the prompt changes from SWITCH(config)# to SWITCH(config-rate-limit-profile[*NAME*])#.

To delete the created Rate-limit profile, use the following command.

Command	Mode	Description
no rate-limit-profile {*NAME* | **all**}	Global	Deletes the created Rate-limit profile. NAME: Rate-limit profile name

To modify an existing Rate-limit profile, use the following command.

Command	Mode	Description
rate-limit-profile *NAME* **modify**	Global	Modifies the existing Rate-limit profile. NAME: Rate-limit profile name

13.12.2 Configuring Rate-limit Profile

To configure the rate limit profile, use the following command.

Command	Mode	Description
downstream *PIR_VALUE* [*SIR_VALUE*]	Rate-limit Profile	Sets the downstream traffic bandwidth. SIR_VALUE: SIR bandwidth range of 0 to 2147483584 (in steps of 64Kbps) PIR_VALUE: PIR bandwidth range of 0 to 2147483584
upstream *PIR_VALUE* [*SIR_VALUE*]		Sets the upstream traffic bandwidth. SIR_VALUE: SIR bandwidth range of 0 to 2147483584 (in steps of 64Kbps) PIR_VALUE: PIR bandwidth range of 0 to 2147483584
no downstream		Deletes the configured rate limit for downstream traffic.
no upstream		Deletes the configured rate limit for upstream traffic.

13.12.3 Saving Rate-limit Profile

After configuring an Rate-limit profile, you need to save the profile with the following command.

Command	Mode	Description
apply	Rate-limit Profile	Saves an Rate-limit profile configuration.

Whenever you modify an rate-limit profile, you should apply the changes again using the **apply** command. If you do not, the changes will not be applied.

13.12.4 Applying Rate-limit Profile

To apply the configured Rate-limit profile for GEM ports, use the following command.

Command	Mode	Description
gemport *RANGE* **rate-limit profile** *NAME*	Traffic-Mapper	Applies the configured Rate-limit profile to specified GEM port. NAME: Rate-limit profile name
no gemport *RANGE* **rate-limit profile**		Removes the Rate-limit profile from the GEM port.

For the details of how to create and configure the Rate-limit profile, see 13.4.2 Creating a Mapper.

To apply the configured Rate-limit profile for an UNI-side port of ONU, use the following command.

Command	Mode	Description
rate-limit profile *NAME*	Traffic Bridge-UNI	Applies the configured Rate-limit profile to specified UNI port. NAME: Rate-limit profile name
no rate-limit profile		Removes the Rate-limit profile from connected UNI port.

For the details of how to create and configure the Rate-limit profile, see 13.4.3.6 UNI Port Configuration.

13.12.5 Displaying Rate-limit Profile

To display the information of Rate-limit profile, use the following command.

Command	Mode	Description
show rate-limit-profile [*NAME*]	Enable Global Interface [GPON] Rate-limit-profile	Shows the information of Rate-limit profile. NAME: Rate-limit profile name

13.13 ONU Service Profile

The LD3032 provides numerous functions to customize a GPON network with many CLI commands and parameters. Each ONU profile can be designed with several profiles such as T-CONT, DBA and VoIP to meet the requirement of data bandwidth, VoIP access and the advanced security issues. The LD3032 also provides the service ONU profile for customer convenience. You can apply one of ONU profiles as the default profile to all ONUs or apply an ONU profile to specified ONUs with a given model name.

To apply a default ONU profile to all ONUs(ONTs), use the following command.

Command	Mode	Description
olt service-profile default *PROFILE*	Global	Applies a default ONU profile to all ONUs. PROFILE: existing ONU profile name

To apply an ONU profile to specified ONUs(ONTs) with a given model name, use the following command.

Command	Mode	Description
olt service-profile model-name *NAME PROFILE*	Interface [GPON]	Applies an ONU profile to specified ONUs with a given model name. NAME: ONU model name PROFILE: existing ONU profile name

i

If you try to configure a default profile for all ONUs when a specified service ONU profile is already applied to ONUs with a given model name, the default ONU profile will be applied only to the ONUs that do not have specific profiles.

To release the default ONU profile from all ONUs(ONTs), use the following command.

Command	Mode	Description
no olt service-profile	Interface [GPON]	Releases a default/service ONU profile from all ONUs.
no olt service-profile default		
no olt service-profile model-name *NAME*		

To display the service ONU profile from all ONUs(ONTs), use the following command.

Command	Mode	Description
show olt service-profile	Enable Global Interface [GPON]	Shows the configured service ONU profiles.

13.14 GPON Debug

To enable debugging of all GPON or a specific feature of GPON, use the following command.

Command	Mode	Description
debug gpon { **all** | **func** | **db** | **comm** | **ugrd** | **profile** | **queue** | **statistics** | **rauth**}	Global	Enables GPON debugging. all: all GPON features func: GPON function db: GPON database comm.: GPON communication ugrd: GPON auto-upgrade profile: GPON profile queue: GPON queue statistics: GPON statistics rauth: RADIUS authentication
no debug gpon {**all** | **func** | **db** | **comm** | **ugrd** | **profile** | **queue** | **statistics**| **rauth** }		Disables GPON debugging.

To display the debugging status of GPON, use the following command.

Command	Mode	Description
show debug gpon	Enable Global	Shows the debugging status of GPON.

13.15 Sample Configuration

Configuration Example 1

```
SWITCH(config)# voip-profile voip create
SWITCH(config-voip-profile[voip])# codec-nego 1 codec pcma packet-period 10
silence-suppression 1
SWITCH(config-voip-profile[voip])# codec-nego 2 codec pcmu packet-period 10
silence-suppression 1
SWITCH(config-voip-profile[voip])# codec-nego 3 codec g729 packet-period 10
silence-suppression 1
SWITCH(config-voip-profile[voip])# codec-nego 4 codec g723 packet-period 10
silence-suppression 1
SWITCH(config-voip-profile[voip])# pstn-protocol-variant 616
SWITCH(config-voip-profile[voip])# protocol sip
SWITCH(config-voip-profile[voip]-sip)# proxy-server proxy.xxxxx.com
SWITCH(config-voip-profile[voip]-sip)# outbound-proxy-server proxy.xxxxx.com
SWITCH(config-voip-profile[voip]-sip)# register-server proxy.xxxxx.com
SWITCH(config-voip-profile[voip]-sip)# host-part-server proxy.xxxxx.com
SWITCH(config-voip-profile[voip]-sip)# dns primary 168.126.63.1
SWITCH(config-voip-profile[voip]-sip)# exit
SWITCH(config-voip-profile[voip])# apply
SWITCH(config-voip-profile[voip])# exit

SWITCH(config)# pm-profile pm_ces create
SWITCH(config-pm-profile[pm_ces])# pm uni-ces
SWITCH(config-pm-profile[pm_ces])# pm pseudowire
SWITCH(config-pm-profile[pm_ces])# apply
SWITCH(config-pm-profile[pm_ces])# exit

SWITCH(config)# dba-profile sr_100m create
SWITCH(config-dba-profile[sr_100m])# mode sr
SWITCH(config-dba-profile[sr_100m])# sla fixed 128
SWITCH(config-dba-profile[sr_100m])# sla maximum 102400
SWITCH(config-dba-profile[sr_100m])# apply
SWITCH(config-dba-profile[sr_100m])# exit

SWITCH(config)# pw-maintenance-profile pw_m create
SWITCH(config-pw-maintenance-profile[pw_m])# apply
SWITCH(config-pw-maintenance-profile[pw_m])# exit

SWITCH(config)# tdm-pw-profile tdm create
SWITCH(config-tdm-pw-profile[tdm])# payload-size 256
SWITCH(config-tdm-pw-profile[tdm])# timing-mode adaptive
SWITCH(config-tdm-pw-profile[tdm])# apply
SWITCH(config-tdm-pw-profile[tdm])# exit

SWITCH(config)# traffic-profile g-60a create
SWITCH(config-traffic-pf[g-60a])# tcont 1
SWITCH(config-traffic-pf[g-60a]-tcont[1])# gemport 1/1-1/4
SWITCH(config-traffic-pf[g-60a]-tcont[1])# dba-profile sr_100m
SWITCH(config-traffic-pf[g-60a]-tcont[1])# exit

SWITCH(config-traffic-pf[g-60a])# tcont 2
SWITCH(config-traffic-pf[g-60a]-tcont[2])# gemport 2/1-2/4
SWITCH(config-traffic-pf[g-60a]-tcont[2])# dba-profile sr_100m
SWITCH(config-traffic-pf[g-60a]-tcont[2])# exit

SWITCH(config-traffic-pf[g-60a])# tcont 3
SWITCH(config-traffic-pf[g-60a]-tcont[3])# gemport 4/1-4/4
SWITCH(config-traffic-pf[g-60a]-tcont[3])# dba-profile sr_100m
SWITCH(config-traffic-pf[g-60a]-tcont[3])# exit

SWITCH(config-traffic-pf[g-60a])# mapper 1
SWITCH(config-traffic-pf[g-60a]-mapper[1])# gemport count 4
SWITCH(config-traffic-pf[g-60a]-mapper[1])# exit

SWITCH(config-traffic-pf[g-60a])# mapper 2
SWITCH(config-traffic-pf[g-60a]-mapper[2])# gemport count 4
SWITCH(config-traffic-pf[g-60a]-mapper[2])# exit
SWITCH(config-traffic-pf[g-60a])# mapper 3
SWITCH(config-traffic-pf[g-60a]-mapper[3])# gemport count 4
SWITCH(config-traffic-pf[g-60a]-mapper[3])# exit

SWITCH(config-traffic-pf[g-60a])# bridge 1
SWITCH(config-traffic-pf[g-60a]-bridge[1])# ani mapper 1
SWITCH(config-traffic-pf[g-60a]-bridge[1])# uni eth 1
SWITCH(config-traffic-pf[g-60a]-bridge[1]-uni[eth:1])# exit
SWITCH(config-traffic-pf[g-60a]-bridge[1])# uni eth 2
SWITCH(config-traffic-pf[g-60a]-bridge[1]-uni[eth:2])# exit
SWITCH(config-traffic-pf[g-60a]-bridge[1])# uni eth 3
SWITCH(config-traffic-pf[g-60a]-bridge[1]-uni[eth:3])# exit
SWITCH(config-traffic-pf[g-60a]-bridge[1])# uni eth 4
SWITCH(config-traffic-pf[g-60a]-bridge[1]-uni[eth:4])# exit
SWITCH(config-traffic-pf[g-60a]-bridge[1])# exit

SWITCH(config-traffic-pf[g-60a])# bridge 2
SWITCH(config-traffic-pf[g-60a]-bridge[2])# ani mapper 2
SWITCH(config-traffic-pf[g-60a]-bridge[2]-ani[mapper:2])# exit
SWITCH(config-traffic-pf[g-60a]-bridge[2])# link ip-host-config 1
SWITCH(config-traffic-pf[g-60a]-bridge[2])# exit

SWITCH(config-traffic-pf[g-60a])# bridge 3
SWITCH(config-traffic-pf[g-60a]-bridge[3])# ani mapper 3
SWITCH(config-traffic-pf[g-60a]-bridge[3]-ani[mapper:3])# exit
SWITCH(config-traffic-pf[g-60a]-bridge[3])# link ip-host-config 2
SWITCH(config-traffic-pf[g-60a]-bridge[3])# exit

SWITCH(config-traffic-pf[g-60a])# ip-host-config 1
SWITCH(config-traffic-pf[g-60a]-iphost[1])# ip address dhcp
SWITCH(config-traffic-pf[g-60a]-iphost[1])# vlan-operation us-oper overwrite
100 0
SWITCH(config-traffic-pf[g-60a]-iphost[1])# vlan-operation ds-oper remove
SWITCH(config-traffic-pf[g-60a]-iphost[1])# link voip-service 1
SWITCH(config-traffic-pf[g-60a]-iphost[1])# exit

SWITCH(config-traffic-pf[g-60a])# ip-host-config 2
SWITCH(config-traffic-pf[g-60a]-iphost[2])# ip address static
SWITCH(config-traffic-pf[g-60a]-iphost[2])# dns primary 168.123.0.1 secondary
168.123.0.2
SWITCH(config-traffic-pf[g-60a]-iphost[2])# vlan-operation us-oper overwrite
200 0
SWITCH(config-traffic-pf[g-60a]-iphost[2])# vlan-operation ds-oper remove
SWITCH(config-traffic-pf[g-60a]-iphost[2])# link tdm-service 1
SWITCH(config-traffic-pf[g-60a]-iphost[2])# exit

SWITCH(config-traffic-pf[g-60a])# voip-service 1
SWITCH(config-traffic-pf[g-60a]-voip[1])# manage-method omci
SWITCH(config-traffic-pf[g-60a]-voip[1])# voip-profile voip
SWITCH(config-traffic-pf[g-60a]-voip[1])# uni pots 1
SWITCH(config-traffic-pf[g-60a]-voip[1]-uni[1])# exit
SWITCH(config-traffic-pf[g-60a]-voip[1])# exit

SWITCH(config-traffic-pf[g-60a])# ces 1
SWITCH(config-traffic-pf[g-60a]-ces[1])# tdm-service 1 mode pw-ip
SWITCH(config-traffic-pf[g-60a]-ces[1]-svc[1]-pw-ip)# tdm-profile tdm
SWITCH(config-traffic-pf[g-60a]-ces[1]-svc[1]-pw-ip)# udp port 10 tos 20
SWITCH(config-traffic-pf[g-60a]-ces[1]-svc[1]-pw-ip)# exit
SWITCH(config-traffic-pf[g-60a]-ces[1])# exit
SWITCH(config-traffic-pf[g-60a])# apply
SWITCH(config-traffic-pf[g-60a])# exit

SWITCH(config)# onu-profile g-60a create
SWITCH(config-onu-profile[g-60a])# traffic-profile g-60a
SWITCH(config-onu-profile[g-60a])# pm-profile pm_ces
SWITCH(config-onu-profile[g-60a])# circuit-pack card-config c-ds1-e1 e1
SWITCH(config-onu-profile[g-60a])# apply
SWITCH(config-onu-profile[g-60a])# exit
SWITCH(config)#
```

Configuration Example 2

```
SWTICH(config)# pm-profile PM_PROFILE create
SWTICH(config-pm-profile[PM_PROFILE])# pm gemport
SWTICH(config-pm-profile[PM_PROFILE])# pm aniport
SWTICH(config-pm-profile[PM_PROFILE])# apply
SWTICH(config-pm-profile[PM_PROFILE])# exit
SWTICH(config)# onu-profile ONU_PROFILE create
SWTICH(config-onu-profile[ONU_PROFILE])# traffic-profile TRAFFIC_PROFILE
SWTICH(config-onu-profile[ONU_PROFILE])# pm-profile PM_PROFILE
SWTICH(config-onu-profile[ONU_PROFILE])# apply
SWTICH(config-onu-profile[ONU_PROFILE])# exit
SWTICH(config)# interface gpon 2/2
SWTICH(config-if[GPON2/2])# show onu statistics
------------------------------------------------------------------------------
OLT : 2/2 ONU : 1
------------------------------------------------------------------------------
Enabled PM : gemport aniport
Elapsed time after clear : 0d 1h 32m 33s
Elapsed time after update : 0d 0h 5m 3s
------------------------------------------------------------------------------
GEM port PM counter | 15Min | Prev-15Min | Total
------------------------------------------------------------------------------
Lost Packets      |   0    |      0 |   0
Misinserted Packets       |   0    |      0 |   0
Received Packets |  131   |    126|  642
Received Blocks  |  366   |    356| 1799
Transmitted Blocks       |  578   |    567| 2836
Impaired Blocks  |   0    |      0 |   0
------------------------------------------------------------------------------
------------------------------------------------------------------------------
```

```
ANI port PM counter | 15Min | Prev-15Min | Total
------------------------------------------------------------------------------
Discarded Frames |   0    |     0 |   0
------------------------------------------------------------------------------
SWITCH(config-if[GPON2/2])# show onu statistics current 1
--------------------------------------------------------------
OLT : 2/2 ONU : 1
--------------------------------------------------------------
Enabled PM : gemport aniport
Elapsed time after clear : 0d 1h 33m 4s
Elapsed time after update : 0d 0h 5m 34s
--------------------------------------------------------------
GEM port PM counter | Current | Total + Current
--------------------------------------------------------------
Lost Packets     |   0    | 0
Misinserted Packets       |  0    | 0
Received Packets |   26   | 668
Received Blocks  |   73   | 1872
Transmitted Blocks        |  106  | 2942
Impaired Blocks  |   0    | 0
------------------------------------------------------------------------------
--------------------------------------------------------------
ANI port PM counter | Current | Total + Current
--------------------------------------------------------------
Discarded Frames |    0   | 0
--------------------------------------------------------------
SWITCH(config-if[GPON2/2])#
```

14 System Software Upgrade

14.1 SFU Upgrade

For the system enhancement and stability, new system software may be released. Using this software, the LD3032 can be upgraded without any hardware change. You can simply upgrade your system software with the provided upgrade functionality via the CLI.

14.1.1 General Upgrade for SFU

The LD3032 supports the dual system software functionality, which you can select applicable system software stored in the system according to various reasons such as the system compatibility or stability.

To upgrade the system software of the switch, use the following command.

Command	Mode	Description
copy {**ftp** | **tftp**} **os download** {**os1** | **os2**}	Enable	Upgrades the system software of the switch via FTP or TFTP. os1 | os2: the area where the system software is stored
copy {**ftp** | **tftp**} **os upload** {**os1** | **os2**}		Uploads the system software image of the switch to FTP or TFTP

⚠ To upgrade the system software, FTP or TFTP server must be set up first! Using the **copy** command, the system will download the new system software from the server.

⚠ To reflect the downloaded system software, the system must restart using the **reload** command! For more information, see Section 4.1.4.1.

The following is an example of upgrading the system software stored in **os2**.

```
SWITCH# show flash

Flash Information(Bytes)
 Area                     total     used(%)     free
 -----------------------------------------------------------------------------
 OS1(default)(running)  33554432   17764738   15789694   1.23 #1037 R001-0008
 OS2                  33554432     17776442   15777990   1.23 #1038 R001-0008
 CONFIG                  4194304      356352      3837952
 ------------------------------------------------------------------------
 Total                  71303168 35897532( 50%)    35405636

SWITCH# copy ftp os download os2

 To exit : press Ctrl+D
--------------------------------------
IP address or name of remote host (FTP): 10.55.2.202
Download File Name : LD3032/SFU/zMRA4072/LD3032_SFU.3.01-1037-01.x
User Name : qa
Password:
Hash mark printing on (1024 bytes/hash mark).
```

```
Downloading NOS ....
May 30 15:57:03  ftp: writing a file(LD3032/SFU/zMRA4072/LD3032_SFU.3.01-1037-
01.x) to flash(os2) : request

#############################################################################
#############################################################################
#############################################################################
#############################################################################
#############################################################################
###############################################

17764738 bytes download OK.

May 30 15:57:21  system: erasing and writing flash(os2) : start

Upgrading NOS : 100%May 30 15:59:16  system: NOS upgrade : success

 Standby is not available

SWITCH# show flash

Flash Information(Bytes)
 Area                     total     used(%)     free
 ----------------------------------------------------------------------------
 OS1(default)(running)  33554432   17764738  15789694   1.23 #1037 R001-0008
 OS2                    33554432  17776442   15777990   3.01 #1037 R001-0008
 CONFIG                  4194304    356352     3837952
 -----------------------------------------------------------------------
 Total                 71303168 35897532( 50%)    35405636

SWITCH# default-os os2
SWITCH# reload
Do you want to save the system configuration? [y/n]y
Do you want to reload the system? [y/n]y

Broadcast message from admin (ttyp0) (Fri Aug 18 15:15:41 2006 +0000):

The system is going down for reboot NOW!

SWITCH login: admin
Password:
SWITCH> enable
SWITCH# show flash

Flash Information(Bytes)
 Area                     total     used(%)     free
 ----------------------------------------------------------------------------
 OS1                    33554432   17764738  15789694   1.23 #1037 R001-0008
 OS2(default)(running)   33554432  17776442   15777990   3.01 #1037 R001-0008
 CONFIG                  4194304    356352     3837952
 -----------------------------------------------------------------------
 Total                 71303168 35897532( 50%)    35405636

Flash Information(Bytes)
```

14.1.2 Boot Mode Upgrade

In case that you cannot upgrade the system software with the general upgrade procedure, you can upgrade it with the boot mode upgrade procedure. Before the boot mode upgrade, please keep in mind the following restrictions.

- A terminal must be connected to the system via the console interface. To open the boot mode, you should press <**S**> key when the boot logo is shown up.
- The boot mode upgrade supports TFTP only. You must set up TFTP server before upgrading the system software in the boot mode.
- In the boot mode, the only interface you can use is MGMT interface. So the system must be connected to the network via the MGMT interface.
- All you configures in the boot mode is limited to the boot mode only!

To upgrade the system software in the boot mode, perform the following step-by-step instruction:

Step 1 To open the boot mode, press <**S**> key when the boot logo is shown up.

```
*************************************************************
*                                                           *
*                 Boot Loader Version                       *
*              Furukawa Electric Latam                      *
*                                                           *
*************************************************************
Press 's' key to go to Boot Mode:  0
Boot>
```

Step 2 To enable the MGMT interface to communicate with TFTP server, you need to configure a proper IP address, subnet mask and gateway on the interface.

To configure an IP address, use the following command.

Command	Mode	Description
ip *A.B.C.D*	Boot	Configures an IP address.
ip		Shows a currently configured IP address.

To configure a subnet mask, use the following command.

Command	Mode	Description
netmask *A.B.C.D*	Boot	Configures a subnet mask. (e.g. 255.255.255.0)
netmask		Shows a currently configured subnet mask.

To configure a default gateway, use the following command.

Command	Mode	Description
gateway *A.B.C.D*	Boot	Configures a default gateway.
gateway		Shows a currently configured default gateway.

To display a configured IP address, subnet mask and gateway, use the following command.

Command	Mode	Description
show	Boot	Shows a currently configured IP address, subnet mask and gateway.

The configured IP address, subnet mask and gateway on the MGMT interface are limited to the boot mode only!

The following is an example of configuring an IP address, subnet mask and gateway on the MGMT interface in the boot mode.

```
Boot> ip 10.27.41.83
Boot> netmask 255.255.255.0
Boot> gateway 10.27.41.254
Boot> show
IP          = 10.27.41.83
GATEWAY     = 10.27.41.254
NETMASK     = 255.255.255.0
MAC         = b8:26:d4:00:0d:83
MAC1        = ff:ff:ff:ff:ff:ff
Boot>
```

Step 3 Download the new system software via TFTP using the following command.

Command	Mode	Description
load {**os1** | **os2**} *A.B.C.D FILENAME*	Boot	Downloads the system software. os1 | os2: the area where the system software is stored A.B.C.D: TFTP server address FILENAME: system software file name

To verify the system software in the system, use the following command.

Command	Mode	Description
flashinfo	Boot	Shows the system software in the system.

To upgrade the system software in the boot mode, TFTP server must be set up first! Using the **load** command, the system will download the new system software from the server.

The following is an example of upgrading the system software stored in **os1** in the boot mode.

```
Boot> load os1 10.27.41.82 LD3032_SFU.3.01-1032.x
TFTP from server 10.27.41.82; our IP address is 10.27.41.83
Filename 'LD3032_SFU.3.01-1032.x'.
Load address: 0xffffe0
Loading: #####################################################################
         #####################################################################
```

```
          ######################################################################
          ######################################################################
          ######################################################################
          (Omitted)
          ######################################################################
          ######################################################################
          ######################################################################
          ######################################################################
          ######################################################################
          ####
done
Bytes transferred = 13661822 (d0767e hex)

Update flash: Are you sure (y/n)? y
 Erasing      : 0x01D00000 - 0x01D1FFFF
 Programming  : 0x01D00000 - 0x01D1FFFF
 Verifying    : 0x01D00000 - 0x01D1FFFF
Boot> flashinfo
Flash Information(Bytes)
Area     OS size      Default-OS     Standby-OS     OS Version
--------------------------------------------------------------
os1       13661806        *              *         3.01 #1032
os2       13661412                                 1.23 #1026

Boot>
```

Step 4 Reboot the system with the new system software using the following command.

Command	Mode	Description
reboot [**os1** | **os2**]	Boot	Reboots the system with specified system software. os1 | os2: the area where the system software is stored

If the new system software is a current standby OS, just exit the boot mode, then the interrupted system boot will be continued again with the new system software.

To exit the boot mode, use the following command.

Command	Mode	Description
exit	Boot	Exits the boot mode.

14.2 IUs Upgrade

14.2.1 General Upgrade for IUs

To upgrade the system software of a specific module, perform the following step-by-step instruction:

Step 1 Download the system software image of IU, use the following command.

Command	Mode	Description
copy {**ftp** | **tftp**} **iu download**	Enable	Downloads the system software of the Interface unit from FTP/TFTP server.

Step 2 Select an IU in the specified slot and uploads the new system software using the following command.

Command	Mode	Description
slot upgrade-mode iu *SLOT_NUMBER* **manual**	Global	Enable IU manual upgrade mode. SLOT_NUMBER: slot number
slot upgrade iu *SLOT_NUMBER*		Select a slot number of IU and performs the upgrade.

Step 3 Restart a specific IU in the slot using the following command.

Command	Mode	Description
slot restart iu *SLOT_NUMBER*	Global	Resets an interface module in the specified slot number.

Step 4 Display the new system software using the following command.

Command	Mode	Description
show slot nos iu {**all** | *SLOT_NUMBER*]	Enable Global	Shows the system software of each slot.

The following is an example of upgrading the SIU_GPON16 software image.

```
SWITCH# copy ftp iu download

 To exit : press Ctrl+D
--------------------------------------
IP address or name of remote host (FTP): 10.55.2.202
Download File Name : LD3032/SIU_GPON16/1.x/LD3032_SIU_GPON16.3.01_1025-02.x
User Name : qa
Password:
Hash mark printing on (1024 bytes/hash mark).
Downloading file ....
##############################################################################
##############################################################################
##############################################################################
##############################################################################
```

```
#############################################################################
#############################################################################
#######################################################

9078904 bytes download OK.

SWITCH#

SWITCH# show slot nos iu 2
-------------------------------------
|     IU Slot [02] Nos Info        |
-------------------------------------
 Version  : 1.23
 Revision : 1026
 Size     : 8623784
 Status   : -

-------------------------------------
|   Released Nos Image on SFU       |
-------------------------------------
 * GPIU Released Nos
   Version  : 3.01
   Revision : 1025
   Size     : 9078904

* SFU Released Nos
   Version  : -
   Revision : -
   Size     : 0


SWITCH# configure terminal
SWITCH(config)# slot upgrade iu  2
SWITCH(config)# May 30 15:51:10  EQM[231]: EQM: SIU[3] Nos Upgrade Start

SWITCH(config)# show slot nos iu 2
-------------------------------------
|      IU Slot [02] Nos Info      |
-------------------------------------
 1. Running Nos ----------------------
 Version  : 1.01
 Revision : 0005
 Size     : 14633875
 Status   : Upgrading
 Area     : OS2
 2. Standby Nos ----------------------
 Version  : 1.00.HW4
 Revision : 0
 Size     : 14528229
 Area     : OS1
-------------------------------------
|   Released Nos Image on SFU     |
-------------------------------------

   * SIU_GPON16 Released Nos
   Version  : -
   Revision : -
   Size     : 0
```

```
SWITCH(config)#

SWITCH(config)# May 30 15:52:20  EQM[231]: EQM: SIU[3] Nos Upgrade Done

SWITCH(config)# show slot nos iu 2
-------------------------------------
|     IU Slot [02] Nos Info         |
-------------------------------------
 Version  : 3.01
 Revision : 1026
 Size     : 8623784
 Status   : Upgrade Complete.

-------------------------------------
|   Released Nos Image on SFU      |
-------------------------------------
 * GPIU Released Nos
   Version  : 3.01
   Revision : 1025
   Size     : 9078904

  * SFU Released Nos
   Version  : -
   Revision : -
   Size     : 0


SWITCH(config)# slot restart iu 2

May 30 15:53:02  system: port 3/1 removed
May 30 15:53:02  system: port 3/1 link off(operational)
May 30 15:53:03  system: port 3/2 removed
May 30 15:53:03  system: port 3/2 link off(operational)
May 30 15:53:03  system: port 3/3 removed
May 30 15:53:03  system: port 3/3 link off(operational)
May 30 15:53:03  system: port 3/4 removed
May 30 15:53:03  system: port 3/4 link off(operational)
May 30 15:53:03  GEPON[262]: GEPON: OLT(3/1) DEACTIVATION
May 30 15:53:03  GEPON[262]: GEPON: OLT(3/2) DEACTIVATION
May 30 15:53:03  GEPON[262]: GEPON: OLT(3/3) DEACTIVATION
May 30 15:53:03  GEPON[262]: GEPON: OLT(3/4) DEACTIVATION

(Omitted)

May 30 15:54:12  GEPON[262]: ONU(3/1,1) ACTIVATION (SN:DSNWcb5a447b)
May 30 15:54:12  GEPON[262]: ONU(3/2,1) ACTIVATION (SN:DSNWcb5a4a62)
May 30 15:54:12  GEPON[262]: ONU(3/3,1) ACTIVATION (SN:DSNWcbc47f88)
May 30 15:54:12  GEPON[262]: ONU(3/4,1) ACTIVATION (SN:DSNWcbc47f51)

SWITCH(config)# show slot nos iu 2

-------------------------------------
|     IU Slot [02] Nos Info      |
-------------------------------------
 Version  : 3.01
 Revision : 1025
 Size     : 9078904
 Status   : -

-------------------------------------
```

```
|    Released Nos Image on SFU     |
-------------------------------------
 * GPIU Released Nos
   Version  : 3.01
   Revision : 1025
   Size     : 9078904

  * SFU Released Nos
   Version  : -
   Revision : -
   Size     : 0
```

14.2.2 Auto Upgrade

Upgrade SIU by enabling IU auto upgrade using the following command.

Command	Mode	Description
slot upgrade-mode iu *SLOT_NUMBER* **auto**	Global	Enable IU auto upgrade function. SLOT: IU slot number, 1 to 2
slot upgrade iu *SLOT_NUMBER*		Select a slot number of IU and performs the upgrade.

When auto upgrade function is enabled, the LD3032 compares the downloaded SFU firmware in the system with the firmware currently loaded in the inserted SIUs. If the version of the firmware from IU side is lower than that of the firmware from the SFU side, then the firmware upgrade will automatically start.

15 Abbreviations

ACL	Access Control List
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
ASM	Any Source Multicast
BGP	Border Gateway Protocol
BSR	Bootstrap Router
CE	Communauté Européenne
CIDR	Classless Inter Domain Routing
CLI	Command Line Interface
CLNS	Connectionless Network Service
CoS	Class of Service
CSNP	Complete Sequence Number PDU
DA	Destination Address
DBA	Dynamic Bandwidth Allocation
DHCP	Dynamic Host Configuration Protocol
DIS	Designated IS
DR	Designated Router
DSCP	Differentiated Service Code Point
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
EGP	Exterior Gateway Protocol
EMC	Electro-Magnetic Compatibility
EN	Europäische Norm (European Standard)
ERP	Ethernet Ring Protection
FDB	Forwarding Data Base
FE	Fast Ethernet
FSM	Finite State Machine
FTP	File Transfer Protocol
GB	Gigabyte
GE	Gigabit Ethernet
GenID	Generation ID

GSP	Generic Status Portal
HW	Hardware
ID	Identifier
IEC	International Electrotechnical Commission
IEEE 802	Standards for Local and Metropolitan Area Networks
IEEE 802.1	Glossary, Network Management, MAC Bridges, and Internetworking
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IFSM	Interface Finite State Machine
IGMPv1	Internet Group Management Protocol Version 1
IGMPv2	Internet Group Management Protocol Version 2
IGMPv3	Internet Group Management Protocol Version 3
IGP	Interior Gateway Protocol
IP	Internet Protocol
ISP	Internet Service Provider
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union - Telecommunications standardization sector
IU	Interface Unit
KAT	Keep Alive Time
L2	Layer 2
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LCT	Local Craft Terminal
LLDP	Link Layer Discover Protocol
LLID	Logical Link ID
LS	Link-State
LSP	Link-State PDU
MAC	Medium Access Control
McFDB	Multicast Forwarding Database
MFC	Multicast Forwarding Cache
MPCP	Multi-point Control Protocol
MRIB	Multicast Routing Information Base

MTU	Maximum Transmission Unit
MVR	Multicast VLAN Registration
NBMA	Non-Broadcast Multi-Access
NE	Network Element
NET	Network Entity Title
NFSM	Neighbor Finite State Machine
NTP	Network Time Protocol
OAM	Operation, Administration and Maintenance
OIF	Outgoing Interface
OLT	Optical Line Termination
ONT	Optical Network Terminal
OS	Operating System
OSPF	Open Shortest Path First
PC	Personal Computer
PDU	Protocol Data Unit
PIM-DM	Protocol Independent - Multicast Dense Mode
PIM-SM	Protocol Independent - Multicast Sparse Mode
PIM-SSM	Protocol Independent - Multicast Source-Specific Multicast
PON	Passive Optical Network
PSNP	Partial Sequence Number PDU
PVID	Port VLAN ID
QoS	Quality of Service
QRV	Querier’s Robustness Variable
RFC	Request for Comments
RIP	Routing Information Protocol
RMON	Remote Monitoring
RP	Rendezvous Point
RPF	Reverse Path Forwarding
RPT	Rendezvous Point Tree
RSTP	Rapid Spanning Tree Protocol
RTC	Real Time Clock
SA	Source Address
SFP	Small Form Factor Pluggable

SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SNPA	Sub-Network Point of Attachment
SNTP	Simple Network Time Protocol
SPT	Shortest Path Tree
SSH	Secure Shell
SSM	Source-Specific Multicast
STP	Spanning Tree Protocol
SW	Software
TCN	Topology Change Notification
TCP	Transmission Control Protocol
TIB	Tree Information Base
TFTP	Trivial FTP
ToS	Type of Service
TTL	Time-To-Live
UDP	User Datagram Protocol
UMN	User Manual
VBD	VoiceBand Data
VID	VLAN ID
VIF	Virtual Interface
VLAN	Virtual Local Area Network
VoD	Video on Demand
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VRF	Vortual Routing and Forwarding
xDSL	Any form of DSL