BOAS PRÁTICAS PARA EVITAR INDISPONIBILIDADE DE SERVIÇO EM REDES GPON

1 Situações de Risco de *Loop*

Uma situação de vulnerabilidade comum a que estão sujeitas redes de dados é o *loop* de pacotes. Um *loop* caracteriza-se pela existência de dois caminhos físicos distintos na interconexão entre elementos de rede e que causam um fluxo indesejado de pacotes ingressando e retornando ao mesmo caminho de origem de maneira constante. Esse fluxo pode chegar ao ponto de causar uma indisponibilidade total na rede.

A utilização da tecnologia *Gigabit Passive Optical Network* (GPON) em redes *enterprise* minimiza a possibilidade de ocorrência de *loops Layer* 2 (L2) na rede, dada a quantidade reduzida de equipamentos ativos e funções bem definidas dos equipamentos *Optical Line Termination* (OLT) e *Optical Network Unit* (ONU). Aos equipamentos terminais da rede PON, ONUs, recomenda-se, por exemplo, que sejam conectados somente equipamentos terminais de usuários, condição que, se seguida, não resultaria em *loops* L2.

Entretanto, uma rede GPON não está livre de erros de conexão ou conexões não autorizadas de *Access Points* (*Rogue APs*) ou *switches* L2 aos ONUs. Para esses casos, é importante que os projetos de solução Laserway considerem a configuração de um protocolo de *loop avoidance* conforme recomendações e considerações descritas neste documento.

Em topologias GPON usando as OLTs da Furukawa existem duas situações onde se está vulnerável a *loops*: Ligação entre portas de ONTs conectadas à mesma OLT e ligação entre portas de ONTs conectadas a portas de OLT distintas.

1.1 Mesma porta de OLT

Um *loop* lógico poderá ser causado pela conexão entre portas de duas ONTs conectadas na mesma OLT (figura 1), ou pela conexão entre duas portas da mesma ONT (figura 2) se, e somente se, as interfaces conectadas pertencerem à mesma VLAN e a porta de OLT tiver a funcionalidade de *port-bridge* habilitada.

A funcionalidade de *port-bridge* é normalmente utilizada em redes empresariais e permite a comunicação entre computadores ou telefones IP que trabalham em ONTs pertencentes à mesma OLT.

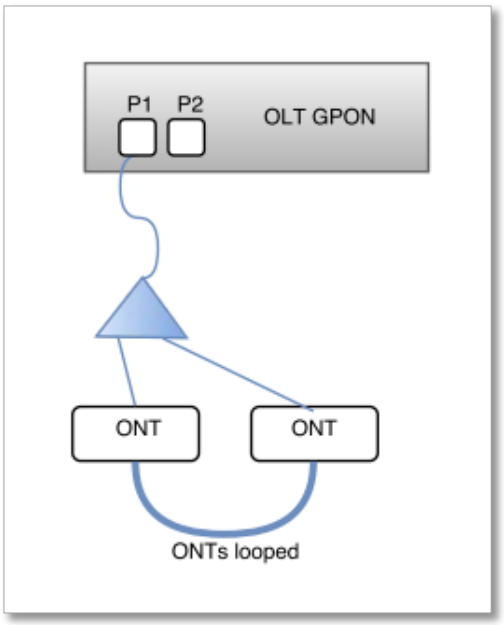

Figura 1 – ONTs conectadas entre si pertencentes à uma mesma porta de OLT (P1).

Este documento pode estar desatualizado. Baixe sempre a versão atual no site da Furukawa

Argentina 0800 800 9701 | Brasil 0800 41 2100 | Bolivia 800 10 2222 5445 | Chile 123 00209395 | Colombia 01800 518 1160 | Paraguay 00 812 800 5446 | Perú 0800 54089 | Uruguay 0004 019 0337 | Venezuela 08001008511

CENTRAL DE SERVIÇO AO CLIENTE
CENTRAL DE SERVICIO AL CLIENTE

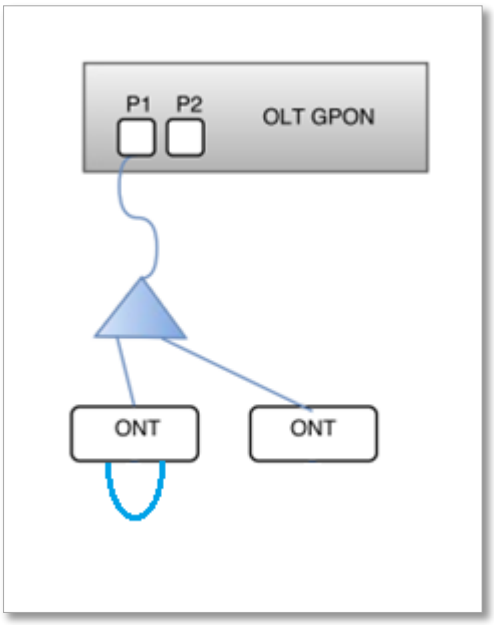

Figura 2 – Portas de uma ONT conectadas entre si.

1.1.1 Port-bridge

As OLTs GPON Furukawa suportam a funcionalidade *port bridge* de camada 2 (L2), que permitem o encaminhamento de pacotes para a mesma interface que o originou. Quando o endereço MAC de destino é encontrado, o pacote é encaminhado normalmente, ainda que na mesma porta OLT de origem.

Uma alternativa ao *port-bridge* é a configuração da funcionalidade *ARP alias*.

1.1.2 ARP alias

Para permitir a comunicação entre *hosts* específicos que estejam conectados à mesma porta de OLT, as OLTs GPON Furukawa suportam o comando *arp alias,* que faz com que o switch de concentração responda as requisições ARP dos clientes dessa OLT.

1.2 Portas de OLT distintas

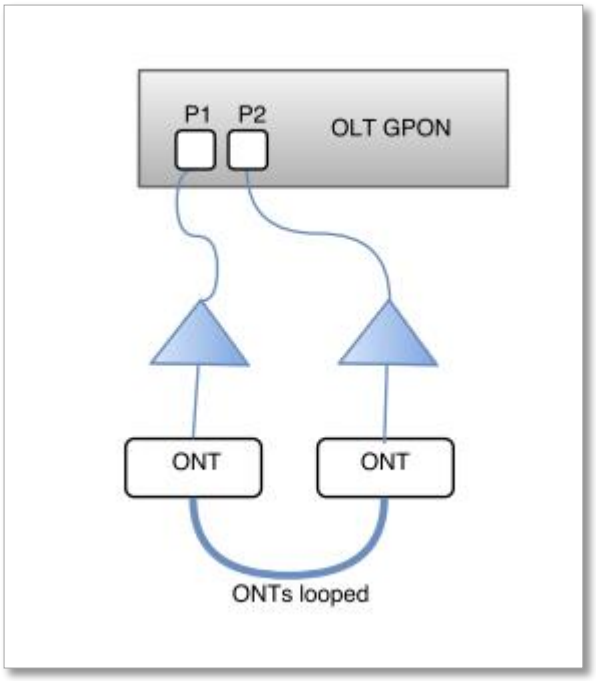

Figura 3 - ONTs conectadas entre si pertencentes à portas de OLT distintas (P1 e P2)

É possível a formação de um *loop* conectando-se ONTs que pertençam a portas de OLT distintas mas que estejam trabalhando no mesmo regime de VLANs. Nesse caso o *loop* ocorre entre as portas de OLT e recomenda-se habilitar um modo de *spanning-tree* para evitar tal fenômeno.

1.3 Identificação do *Loop*

O primeiro registro que deve ser consultado para identificação de problemas (*troubleshooting*) com as OLTs GPON é o *syslog* do equipamento.

Verifique o syslog da OLT através do seguinte comando:

```
SWITCH(config)# show syslog local non-volatile reverse
```

Eventos de *loop* podem ser identificados por entradas no syslog como as seguintes:

Este documento pode estar desatualizado. Baixe sempre a versão atual no site da Furukawa

Argentina 0800 800 9701 | Brasil 0800 41 2100 | Bolivia 800 10 2222 5445 | Chile 123 00209395 | Colombia 01800 518 1160 | Paraguay 00 812 800 5446 | Perú 0800 54089 | Uruguay 0004 019 0337 | Venezuela 08001008511

CENTRAL DE SERVIÇO AO CLIENTE
CENTRAL DE SERVICIO AL CLIENTE

```
Jun 23 15:54:47  GPON[278]: ONU(2/2,13)
Found afflict Mac(00:24:21:fe:52:ba).
Stats(TC:4999,IC:2527, MC:2443)

Jun 23 15:54:47  GPON[278]: ONU(2/2,14)
Found afflict Mac(00:24:21:fe:52:ba).
Stats(TC:4999,IC:2527, MC:2443)
```

2 Configurações recomendadas

Para diminuir os efeitos indesejáveis causados por *loop* recomenda-se agregar ao sistema as configurações que seguem neste capítulo.

2.1 Source MAC address Monitoring (SRC-MAC-MON) e Loop Detection (LD)

2.1.1 Source MAC address Monitoring (SRC-MAC-MON)

A funcionalidade *Source MAC address Monitoring* (SRC-MAC-MON) permite que a OLT identifique ONUs problemáticas através da análise do endereço MAC de origem dos frames recebidos (SRC-MAC). Caso a OLT identifique um frame cujo SRC-MAC seja igual ao MAC de sistema da OLT, caracterizando um *loop* L2, é realizado o bloqueio da ONU que enviou o *frame*.

O desbloqueio de uma ONU em *loop* pode ser configurado para ocorrer de forma administrativa ou de forma automática, baseado em uma temporização (*expire-timeout*). Caso seja utilizado o modo automático de desbloqueio, recomenda-se utilizar temporização de no mínimo 300 segundos a fim de permitir a remoção do *loop* físico:

Configuração de srcmac-monitor nas interfaces PON 1 e 2 da OLT: desbloqueio automático em 300s:

```
configure terminal
gpon
 !
gpon-olt 1/1
olt srcmac-monitor enable auto-onu-block
expire-timeout 300
 gpon-olt 1/2
olt srcmac-monitor enable auto-onu-block
expire-timeout 300
```

Configuração de srcmac-monitor nas interfaces PON 1 e 2 da OLT: desbloqueio manual:

```
configure terminal
 gpon
  !
  gpon-olt 1/1
   olt srcmac-monitor enable auto-onu-block
  gpon-olt 1/2
   olt srcmac-monitor enable auto-onu-block
```

Verificação e desbloqueio manual de ONU

```
show onu block status OLT-ID [ONU-ID]
!
configure terminal
gpon
 !
 gpon-olt OLT-ID
  onu unblock ONU-ID
```

A eficiência da funcionalidade SRC-MAC-MON na identificação e bloqueio de loops depende da geração de frames pela OLT capazes de circular por toda a rede L2. A funcionalidade *Loop Detection* descrita a seguir necessita ser configurada nas interfaces PON que se deseja proteger a fim de garantir a geração periódica de *frames* para monitoração de MAC.

2.2 *Loop Detection* (LD)

Este documento pode estar desatualizado. Baixe sempre a versão atual no site da Furukawa

Argentina 0800 800 9701 | Brasil 0800 41 2100 | Bolivia 800 10 2222 5445 | Chile 123 00209395 | Colombia 01800 518 1160 | Paraguay 00 812 800 5446 | Perú 0800 54089 | Uruguay 0004 019 0337 | Venezuela 08001008511

CENTRAL DE SERVIÇO AO CLIENTE
CENTRAL DE SERVICIO AL CLIENTE

A funcionalidade de *Loop Detection* (LD) permite que as interfaces configuradas enviem periodicamente *frames broadcast loop-detect* cujo SRC-MAC é o endereço MAC de sistema da OLT. As interfaces, então, monitoram o recebimento desses *frames* identificando também a condição de *loop*, mas não bloqueando, por *default*, as interfaces envolvidas. Dessa forma, é possível combinar as funcionalidades SRC-MAC-MON e LD nas interfaces PON a fim de identificar e bloquear seletivamente apenas as ONUs envolvidas na condição de loop L2.

Por utilizar *frames broadcast*, o LD não depende de qualquer configuração adicional em equipamentos conectados ao acesso ONU; STP por exemplo. Os *frames broadcast loop-detect* são enviados em todas as *bridges* associadas às interfaces PON da OLT, incluindo *frames untagged* caso a interface esteja configurada para tal.

A fim de garantir a eficiência na detecção de *loop*, o período de envio dos frames *loop-detect* (*period*) deve ser sintonizado em 3 segundos.

A funcionalidade LD, mesmo configurada para apenas identificar um *loop*, apesar de não bloquear a interface, utiliza uma temporização para iniciar uma nova detecção de *loop* (*timer*). Assim, considerando a detecção de *loop* na interface PON, o tempo de detecção controla o intervalo mínimo entre detecções de *loop* em ONUs de uma mesma interface PON. Por isso, o tempo de detecção deve ser sintonizado em 5 segundos.

Configuração de loop-detect nas interfaces PON 1 e 2 da OLT: intervalo de envio de 3s e tempo de detecção de 5s:

```
configure terminal
bridge
 loop-detect enable
 loop-detect 1-2
 loop-detect 1-2 period 3
 loop-detect 1-2 timer 5
```

2.3 Monitoração e localização de loops

Os logs gerados pela funcionalidade SRC-MAC-MON permitem apontar as ONUs envolvidas no loop L2.

Exemplo de log evidenciando loop entre as ONUs (1,1) e (1,2):

Este documento pode estar desatualizado. Baixe sempre a versão atual no site da Furukawa

Argentina 0800 800 9701 | Brasil 0800 41 2100 | Bolivia 800 10 2222 5445 | Chile 123 00209395 | Colombia 01800 518 1160 | Paraguay 00 812 800 5446 | Perú 0800 54089 | Uruguay 0004 019 0337 | Venezuela 08001008511

CENTRAL DE SERVIÇO AO CLIENTE
CENTRAL DE SERVICIO AL CLIENTE

```
Aug  4 15:03:39  system: port 1 is looping

Aug  4 15:03:39  GPON[121]: ONU(1,1) Found
NEW MAC is System MAC

Aug  4 15:03:40  GPON[121]:
notify_priority_function_call(3747) Receive
updated Block Status of ONU(1,1)

Aug  4 15:03:40  GPON[121]: ONU(1,1) is
Blocking Status

Aug  4 15:03:40  GPON[121]: ONU(1,2) Found
NEW MAC is System MAC

Aug  4 15:03:40  GPON[121]:
notify_priority_function_call(3747) Receive
updated Block Status of ONU(1,2)

Aug  4 15:03:40  GPON[121]: ONU(1,2) is
Blocking Status

Aug  4 15:03:41  GPON[121]: ONU(1,1) eth
port 4 link off(operational)

Aug  4 15:03:42  GPON[121]:
notify_priority_function_call ONU(1,1) MIb
Sync Data 0

Aug  4 15:03:44  GPON[121]: ONU(1,1) eth
port 4 link on(operational)

Aug  4 15:03:44  system: port 1 is moved to
loop-detect detecting list by timeout

Aug  4 15:03:51  GPON[121]: ONU(1,1) eth
port 4 link off(operational)

Aug  4 15:03:52  GPON[121]:
notify_priority_function_call ONU(1,2) MIb
Sync Data 0
```


Este documento pode estar desatualizado. Baixe sempre a versão atual no site da Furukawa

Argentina 0800 800 9701 | Brasil 0800 41 2100 | Bolivia 800 10 2222 5445 | Chile 123 00209395 | Colombia 01800 518 1160 | Paraguay 00 812 800 5446 | Perú 0800 54089 | Uruguay 0004 019 0337 | Venezuela 08001008511

CENTRAL DE SERVIÇO AO CLIENTE
CENTRAL DE SERVICIO AL CLIENTE

Exemplo de log do desbloqueio automático das ONUs (1,1) e (1,2):

```
Aug  4 15:04:40  GPON[121]: ONU(1,2)
Success to check the traffic profile

Aug  4 15:04:40  GPON[121]:
notify priority function call(3747) Receive
updated Block Status of ONU(1,2)

Aug  4 15:04:40  GPON[121]: ONU(1,2) is
Unblocking Status

Aug  4 15:04:41  GPON[121]: ONU(1,1)
Success to check the traffic profile

Aug  4 15:04:41  GPON[121]:
notify_priority_function_call(3747) Receive
updated Block Status of ONU(1,1)

Aug  4 15:04:41  GPON[121]: ONU(1,1) is
Unblocking Status

Aug  4 15:04:42  GPON[121]:
notify_priority_function_call ONU(1,2) MIb
Sync Data 73

Aug  4 15:04:43  GPON[121]:
notify_priority_function_call ONU(1,1) MIb
Sync Data 49
```

Os *logs* podem ser redirecionados para servidor *Syslog remote* através do comando abaixo.

Redirecionamento de log para servidor Syslog remoto:

```
configure terminal
syslog output info remote SERVER_IPV4_ADDR
!
```

Exemplo de log no servidor Syslog

```
configure terminal 08/08/2016 10:43:51
[363] From: (10.150.4.25) Fac:0 Sev:6 Msg
>>> system: port 1 is looping

08/08/2016 10:43:52 [367] From:
(10.150.4.25) Fac:0 Sev:6 Msg >>> system:
port 2 is moved to loop-detect detecting
list by timeout

08/08/2016 10:43:52 [364] From:
(10.150.4.25) Fac:1 Sev:4 Msg >>>
GPON[121]: ONU(1,2) Found NEW MAC is System
MAC

08/08/2016 10:43:52 [365] From:
(10.150.4.25) Fac:1 Sev:4 Msg >>>
GPON[121]: ONU(1,2) is Blocking Status

08/08/2016 10:43:52 [366] From:
(10.150.4.25) Fac:1 Sev:6 Msg >>>
GPON[121]: ONU(2,2) eth port 3 link
on(operational)

08/08/2016 10:43:57 [368] From:
(10.150.4.25) Fac:1 Sev:6 Msg >>>
GPON[121]: ONU(2,2) eth port 3 link
off(operational)

08/08/2016 10:43:59 [369] From:
(10.150.4.25) Fac:1 Sev:6 Msg >>>
GPON[121]: ONU(2,2) eth port 3 link
on(operational)

08/08/2016 10:43:59 [370] From:
(10.150.4.25) Fac:1 Sev:6 Msg >>>
GPON[121]: ONU(1,2) eth port 4 link
on(operational)

08/08/2016 10:44:11 [371] From:
(10.150.4.25) Fac:1 Sev:6 Msg >>>
IMISH[2300]: show onu block status 1

08/08/2016 10:44:14 [372] From:
(10.150.4.25) Fac:1 Sev:6 Msg >>>
IMISH[2300]: show onu block status 2

08/08/2016 10:44:37 [373] From:
(10.150.4.25) Fac:1 Sev:6 Msg >>>
GPON[121]: ONU(2,2) eth port 3 link
off(operational)

08/08/2016 10:44:37 [374] From:
(10.150.4.25) Fac:1 Sev:6 Msg >>>
GPON[121]: ONU(1,2) eth port 4 link
off(operational)

08/08/2016 10:44:48 [375] From:
(10.150.4.25) Fac:1 Sev:4 Msg >>>
GPON[121]: ONU(1,2) is Unblocking Status
08/08/2016 10:44:59 [376] From:
(10.150.4.25) Fac:1 Sev:6 Msg >>>
IMISH[2300]: show onu block status 1
```

É possível também verificar o estado de bloqueio de ONU através de comando CLI.

Verificação de ONU (1,2) bloqueada:

```
Aug  8 10:44:14  system: port 1 is looping
Aug  8 10:44:14  GPON[121]: ONU(1,2) Found
NEW MAC is System MAC
Aug  8 10:44:15  GPON[121]:
notify_priority_function_call(3747) Receive
updated Block Status of ONU(1,2)
Aug  8 10:44:15  GPON[121]: ONU(1,2) is
Blocking Status
Aug  8 10:44:15  GPON[121]: ONU(2,2) eth
port 3 link on(operational)
Aug  8 10:44:19  system: port 2 is moved to
loop-detect detecting list by timeout
Aug  8 10:44:25  GPON[121]: ONU(2,2) eth
port 3 link off(operational)
Aug  8 10:44:27  GPON[121]: ONU(2,2) eth
port 3 link on(operational)
Aug  8 10:44:27  GPON[121]: ONU(1,2) eth
port 4 link on(operational)
Aug  8 10:44:27  GPON[121]:
notify_priority_function_call ONU(1,2) MIb
Sync Data 0
SWITCH(config)# show onu block status 1
---------------------------------------
  OLT | ONU | Block Status | Block Reason
---------------------------------------
    1 |   1 |  Unblock     | None
    1 |   2 |  Auto Block  | SRCMAC
    1 |   3 |  Unblock     | None
    1 |   4 |  Unblock     | None
    1 |   5 |  Unblock     | None
```

2.4 Cenários de proteção de loops suportados pelo SRC-MAC-MON e LD

Conforme citado, o LD não depende de qualquer configuração adicional em equipamentos conectados ao acesso ONU para detecção de *loops*, já que utiliza frames *broadcast*. Dessa forma, não existem cenários conhecidos em que a combinação SRC-MAC-MON e LD não consiga identificar e bloquear ONUs com acesso em *loop*. Esta recomendação não considera arquiteturas redundantes de conexão na uplink OLT, sendo necessário avaliar o uso de xSTP ou *Link Aggregation Group* (*LAG*) nessas condições.

2.5 Broadcast storm-control

Essa funcionalidade permite controlar o efeito da transmissão massiva de pacotes broadcast e multicast.

É possível estabelecer uma taxa máxima de pacotes broadcast à serem processados por segundo em uma determinada interface de OLT.

2.6 Spanning-tree

Verifique a sessão “Spanning-tree protocol (STP)” do manual de usuário para configurar o modo desejado de spanning-tree e evitar o loop lógico de pacotes entre portas da OLT.

2.7 Acesso serial

Em algumas situações, um evento de negação de serviço (DoS) como os gerados por *loop* podem impedir o acesso à gerência do equipamento por rede (telnet / SSH) e impedem a coleta de informação e configurações.

Neste caso, a única forma de acessar o equipamento é através da interface console (conexão serial).

Recomenda-se manter sempre um computador com acesso à console da OLT Furukawa disponível para situações de emergência.

Existem alguns concentradores de console no mercado que permitem o acesso serial à

Este documento pode estar desatualizado. Baixe sempre a versão atual no site da Furukawa

Argentina 0800 800 9701 | Brasil 0800 41 2100 | Bolivia 800 10 2222 5445 | Chile 123 00209395 | Colombia 01800 518 1160 | Paraguay 00 812 800 5446 | Perú 0800 54089 | Uruguay 0004 019 0337 | Venezuela 08001008511

CENTRAL DE SERVIÇO AO CLIENTE
CENTRAL DE SERVICIO AL CLIENTE

equipamentos de rede de forma remota através de uma LAN de administração (*out-of-band*).

2.8 Configuração de um servidor de syslog

Recomenda-se também configurar um servidor de syslog na rede de administração para manter atualizadas as informações de saúde do sistema e identificar mais facilmente situações de risco.

Os sistemas operacionais Linux já possuem servidores de syslog embarcados, portanto não precisam de aplicações extras para implementação do servidor de syslog.

Para os sistemas operacionais Windows recomendamos:

1 – KIWI Syslog Server for Windows

http://www.kiwisyslog.com/products/kiwi-syslog-server/product-overview.aspx

Software pago. Existe uma versão free mas para apenas 5 equipamentos.

2 – Aonaware Syslog Daemon

http://www.aonaware.com/syslog.htm

Software livre. É necessário instalar o Microsoft SQL Server 2005 ou superior no servidor que terá o servidor de syslog instalado. É bastante simples e não possui ferramentas para filtrar/analisar as informações, no entanto é uma solução robusta do ponto de vista de armazenamento dos logs em base de dados.

3 – Syslog Server

https://sourceforge.net/projects/syslog-server/

Software livre.

3 Conclusão

As informações apresentadas nessa Nota Técnica visam auxiliar na identificação e na mitigação de efeitos indesejados em redes GPON quando submetidas a inundação de pacotes de dados.

O uso combinado das funcionalidades Source MAC address Monitoring e Loop Detection é indicado como mecanismo eficiente de detecção, bloqueio e localização de loops L2 nas interfaces de usuários de redes GPON utilizando OLTs GPON FK-OLT-G2500 ou FK-OLT-G8S ou FK-OLT-G4S.

Para maiores informações sobre as funcionalidades apresentadas ou esclarecimento de dúvidas técnicas pesquise a documentação do produto ou abra um chamado pelo endereço abaixo:

http://suporte.furukawa.com.br

Este documento pode estar desatualizado. Baixe sempre a versão atual no site da Furukawa

Argentina 0800 800 9701 | Brasil 0800 41 2100 | Bolivia 800 10 2222 5445 | Chile 123 00209395 | Colombia 01800 518 1160 | Paraguay 00 812 800 5446 | Perú 0800 54089 | Uruguay 0004 019 0337 | Venezuela 08001008511

CENTRAL DE SERVIÇO AO CLIENTE
CENTRAL DE SERVICIO AL CLIENTE