Nota Técnica sobre Boas práticas FK-C32

1. Objetivo

Instruir boas práticas de configuração e manutenção para o correto funcionamento da plataforma FK-C32.

2. Descrição

2.1. Limpeza das Tabelas

No chassis existem tabelas onde ficam armazenados registros das ONUs. Uma das tabelas é a "In host Memory", ela armaneza todo o histórico de ONUs tanto para a EPON1 quanto para a EPON2 (para a placa OLT 20/2 – nova).

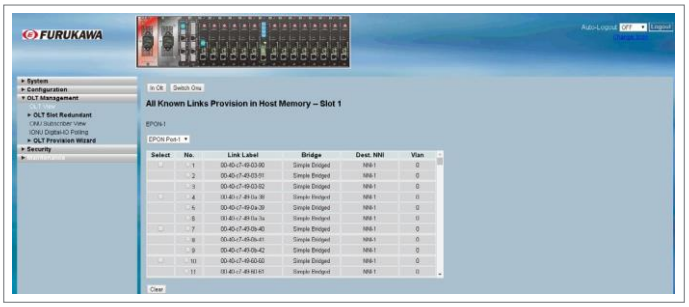

Figura 1 - Placa OLT 20/2 (nova)

Essa tabela suporta o registro de até 207 links lógicos por porta EPON (OLT20/2), porém o número máximo de 192 links lógicos ativos (64 ONUs x 3 links lógicos cada).
A outra tabela é a "In OLT" que exibe registro de todas as ONUs e links lógicos por slot (OLT 20 e OLT20/2).

Figura 2 - Placa OLT 20 (antiga)

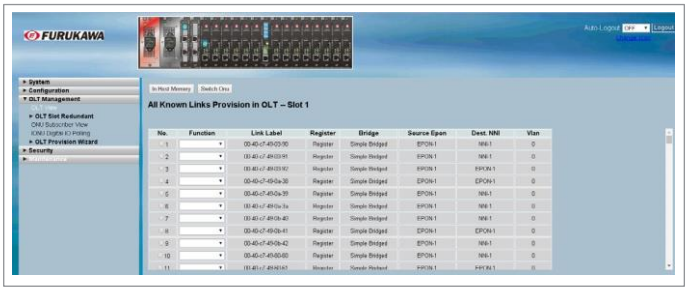

Figura 3 - Placa OLT 20/2 (nova)

A cada substituição de ONU em seu assinante é necessário deletar o registro dessa ONU.

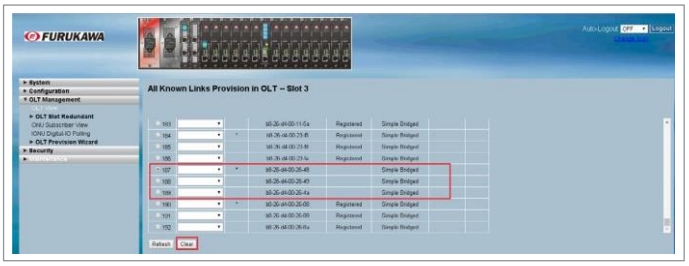

Figura 4 - Placa OLT 20 (antiga)

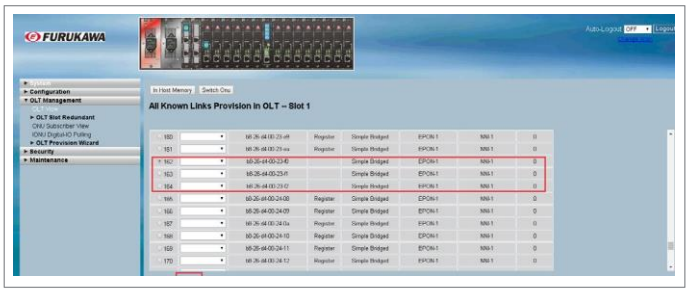

Figura 5 - Placa OLT 20/2 (nova)

Para isto é só confirmar se a ONU não está mais ativa, na tabela "In OLT" a ONU aparecerá sem o Status "Register" ou "Registered".

Para a Placa OLT 20/2 (nova), acessar novamente a tabela "In host Memory" e selecionar a ONU que não está mais ativa na porta EPON e clicar em "clear".

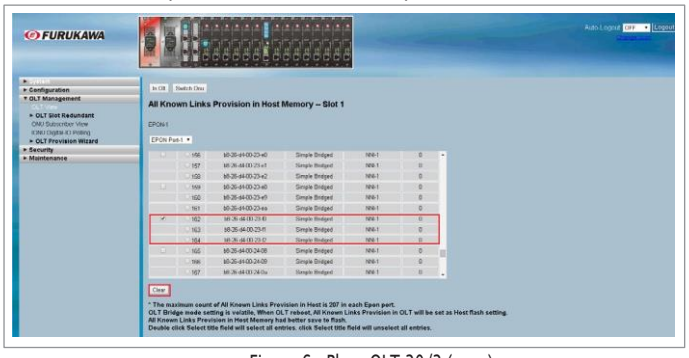

Figura 6 - Placa OLT 20/2 (nova)

Para a Placa OLT 20 (Antiga) é necessário selecionar o último Link Lógico da ONU e clicar em "clear", e refazer o processo para os demais Links Lógicos sempre do último para o primeiro.

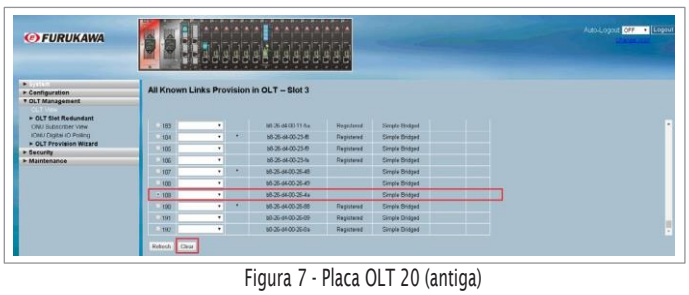

Figura 7 - Placa OLT 20 (antiga)

Os registros serão excluídos.

2.2. Limite de Aplicação dos Modos Shared

Para a placa OLT 20/2 (nova) os modos shared (compartilhar a mesma vlan para diversas ONUs) permite que sejam cadastradas 64 ID's de vlans diferentes em cada porta EPON (somando todos os modos shared diferentes disponíveis que são: "Shared Vlan", "Double Tagged Shared Vlan", "Transparent Priority Shared Vlan", "Transparent Shared Vlan with Broadcast", "Priority Remapping Shared Vlan" e "Priority Shared Vlan").

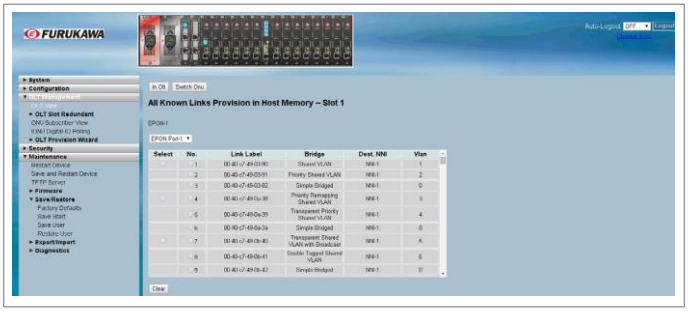

Figura 8 - Placa OLT 20/2 (nova)

Para a placa OLT 20 (Antiga) o modo shared (compartilhar a mesma vlan para diversas ONUs) permite que sejam cadastradas 15 ID's de vlans diferentes por slot (somando todos os modos shared diferentes disponíveis que são: "Shared Vlan", "Double Tagged Shared Vlan", "Transparent Priority Shared Vlan", "Transparent Shared Vlan with Broadcast", "Priority Remapping Shared Vlan" e "Priority Shared Vlan").

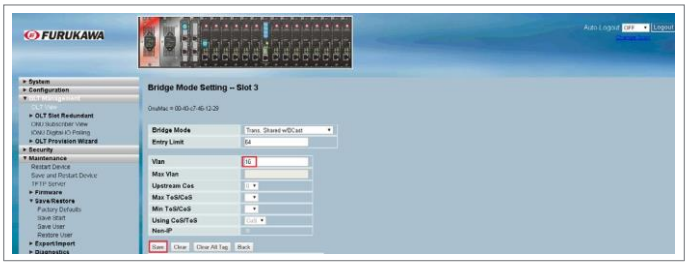

Figura 9 - Placa OLT 20 (antiga)

Ao tentar adicionar a 16ª vlan aparecerá mensagem de "Parameter Out Of Range", significa que o limite foi atingido.

Figura 10 - Placa OLT 20 (antiga)

Lembrando que um ID já utilizado para um determinado modo bridge não poderá ser reutilizado em outro modo brigde na mesma OLT.

2.3. ONU Authorization

A lista "ONU Authorization" permite o registro de até 64 ONUs, tanto para a placa nova (64 por porta EPON), quanto para a placa antiga.

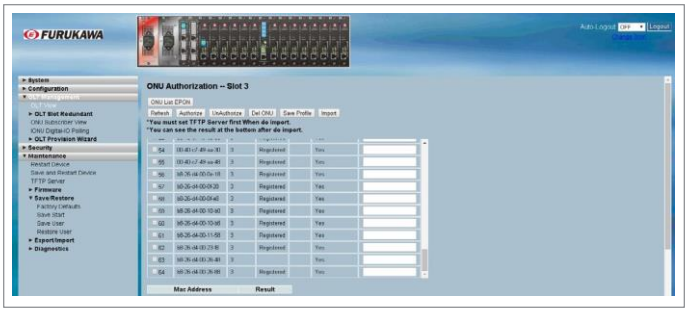

Figura 11

Se tentar adicionar a 65ª ONU à lista de autorização, será exibida a seguinte mensagem de erro: "The Authorization List is full and can't be added" Significa que a lista de autorização já está cheia e o MAC da ONU selecionado não pode ser adicionado.

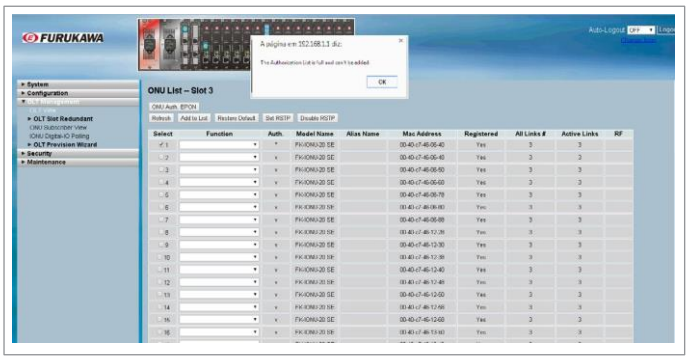

Figura 12

Para poder incluir uma nova ONU à lista de autorização é necessário apagar o registro de alguma ONU que não esteja mais registrada nesse slot. Para deletar a ONU, selecione o MAC e clique em "Del ONU".

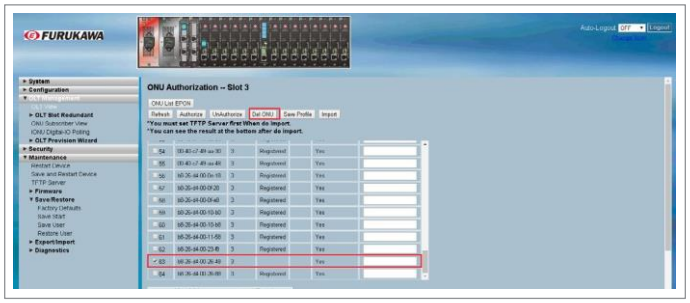

Figura 13

Após exlcuir ONUs que não estejam mais ativas no slot é possível adicionar as novas ONUs a lista de autorização. Basta selecionar as ONUs e clicar em "Add to list".
Selecione a ONU e clique em "Authorize".

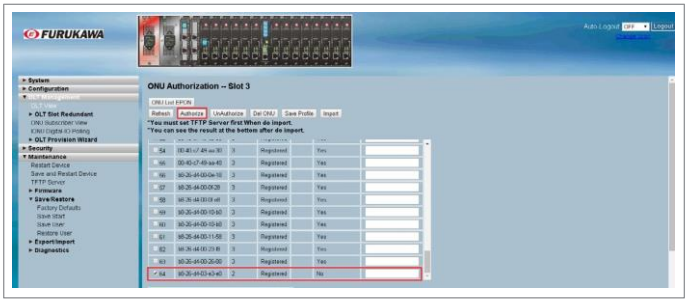

Figura 14

A ONU foi autorizada.

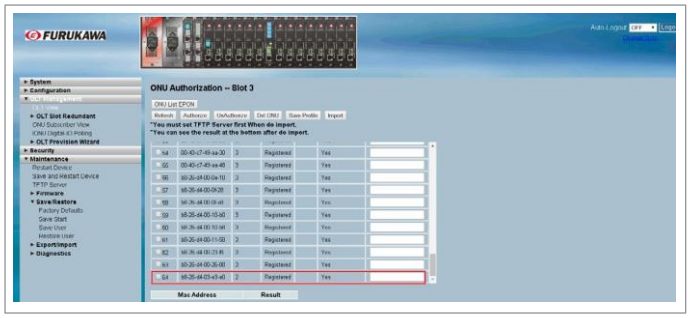

Figura 15

2.4. Adicionar Servidor para Armazenamento de Logs

Logs são registros que devem ser armazenados, pois contém dados importantes para análise de problemas. É possível através de um servidor de Syslog ou Servidor TFTP.
Para adicionar um Servidor de Syslog: Acessar Menu "System", clicar em "Syslog", clicar em "Configuration", Habilitar o "Server Mode" para "Enabled", inserir o endereço IP do Servidor em "Server Address" e clicar em "Apply".

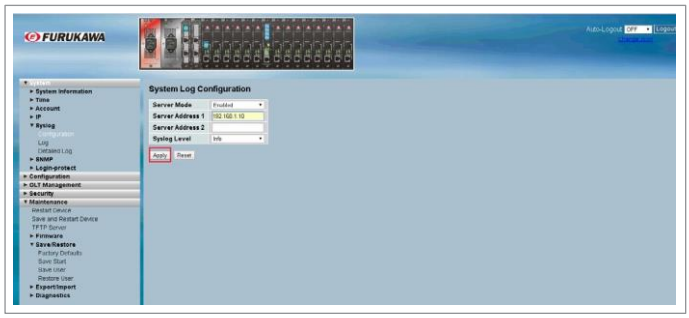

Figura 16

Para armazenar os Log's em um Servidor TFTP: Acessar Menu "Maintenance", clicar em "TFTP Server", inserir o endereço IP do Servidor e clicar em "Save".

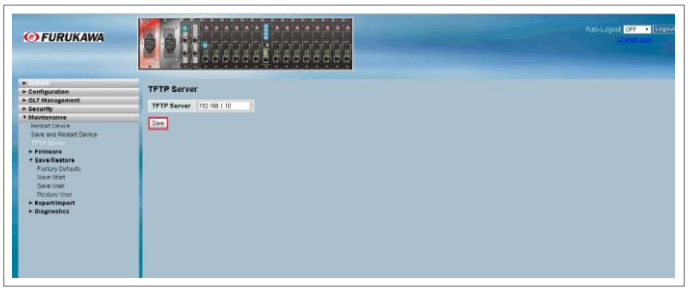

Figura 17

Após inserir o endereço IP do Servidor TFTP é necessário habilitar o Auto-Upload dos arquivos de Log para serem enviados ao servidor ao atingir 200 registros.
Acessar o menu "System", acessar o menu "Syslog", clicar em "Log", alterar a opção "Auto Upload" para "Enable" e clicar em "Save".

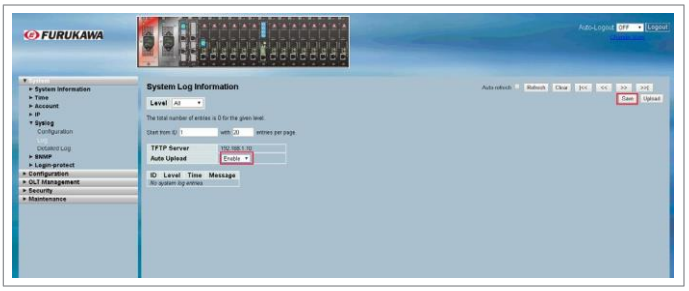

Figura 18

2.5. Cadastrar Outras Contas de Usuários/Senha

Por questões de segurança se faz necessário a criação de senha do usuário admin diferente do padrão. Para alterar a senha do usuário admin basta acessar o Menu "System", clicar em "Account", clicar em admin na opção "User Name".

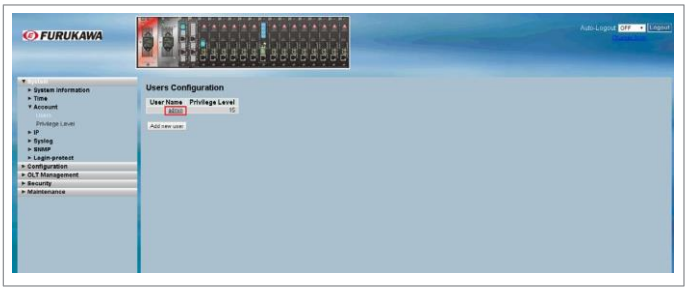

Figura 19

A tela para edição do Usuário será aberta, basta inserir a senha e clicar em "Apply".

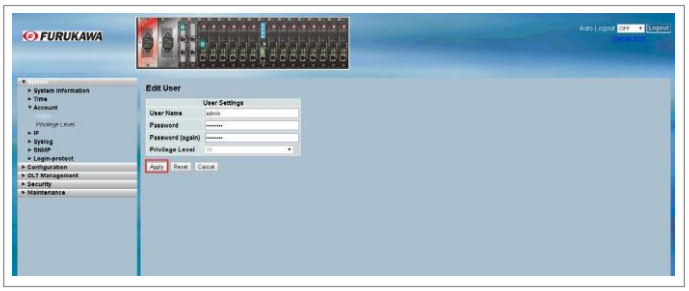

Figura 20

Outro quesito de segurança é a criação de usuário com privilégio menor apenas para consulta, assim o acesso admin fica restrito a quem precisa fazer alterações. Ainda dentro do menu "System" na opção "Account" clicar em "Add new user".

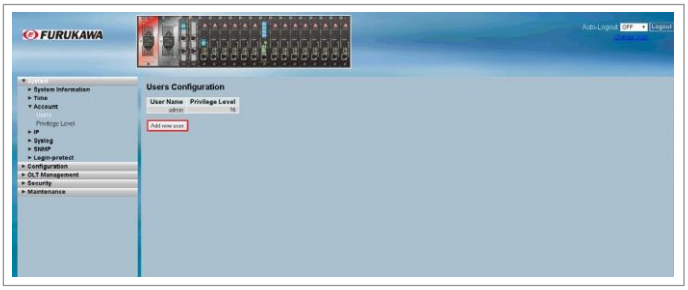

Figura 21

Designar um nome para o usuário em "User Name", inserir a senha e selecionar o nível de privilégio que o usuário terá e clicar em "Save".

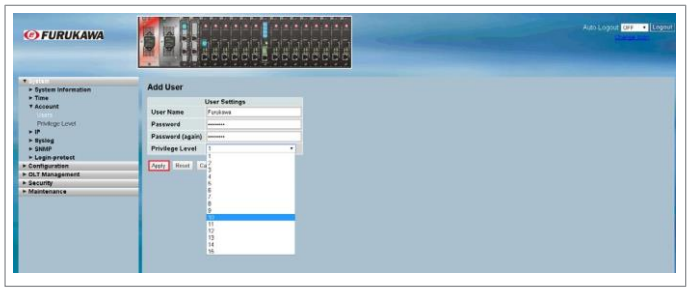

Figura 22

2.6. IP da Gerência

Com a gerência na internet o risco de ataques à plataforma é grande. O principal tipo de ataque é o de acessos simultâneos que pode gerar um mau funcionamento da placa por travamento da interface de gerência. Instruímos manter um IP inválido.

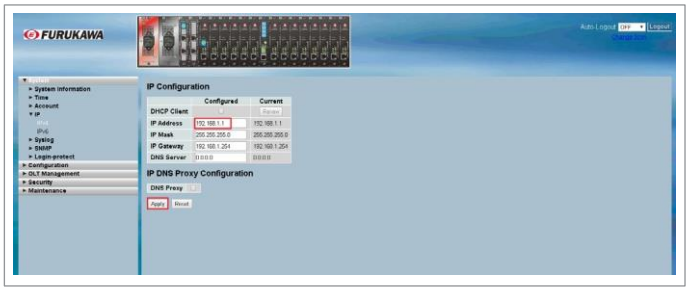

Figura 23

Esse é um arquivo de Log onde é possível verificar que a gerência está sofrendo tentativas de acesso não autorizado de usuários não cadastrados.

```
ID      Level   Time    Message
1       Warning 2014-06-09 17:22:42     Login passed for user 'furukawa'
2       Warning 2014-06-09 17:14:49     Bad password attempt for user 'vyos'
6       Warning 2014-06-09 16:50:59     Bad password attempt for user 'jjjjee'
7       Warning 2014-06-09 16:50:50     Bad password attempt for user 'jjjj'
14      Warning 2014-06-09 16:44:50     Bad password attempt for user 'yyy
yyMMSyyyyNSPlayer
15      Warning 2014-06-09 16:44:30     Bad password attempt for user 'OPTIONS sip:nm SIP
16      Warning 2014-06-09 16:44:20     Bad password attempt for user 'GET
17      Warning 2014-06-09 16:44:15     Bad password attempt for user 'yMB@@yPC NETWORK PROGRAM 1.0'
18      Warning 2014-06-09 16:44:15     Bad password attempt for user 'qjynOykyyyy^O\y
PyNMy'
19      Warning 2014-06-09 16:43:47     Bad password attempt for user 'OPTIONS
20      Warning 2014-06-09 16:43:47     Bad password attempt for user 'OPTIONS
21      Warning 2014-06-09 16:43:47     Bad password attempt for user 'GET
22      Warning 2014-06-09 16:38:22     Bad password attempt for user 'GET
23      Warning 2014-06-09 16:38:17     Bad password attempt for user 'yMB@@yPC NETWORK PROGRAM 1.0'
24      Warning 2014-06-09 16:38:17     Bad password attempt for user 'qjynOykyyyy^O\y
PyNMy'
25      Warning 2014-06-09 16:37:50     Bad password attempt for user 'OPTIONS
26      Warning 2014-06-09 16:37:50     Bad password attempt for user 'OPTIONS
27      Warning 2014-06-09 16:37:50     Bad password attempt for user 'GET
28      Warning 2014-06-09 16:25:10     Bad password attempt for user 'root'
29      Warning 2014-06-09 16:25:10     Bad password attempt for user 'root'
34      Warning 2014-06-09 15:55:31     Login passed for user 'admin'
36      Warning 2014-06-09 15:29:50     Login passed for user 'admin'
37      Warning 2014-06-09 15:24:34     Bad password attempt for user 'root'
38      Warning 2014-06-09 15:24:33     Bad password attempt for user 'root'
39      Warning 2014-06-09 15:24:33     Bad password attempt for user 'root'
40      Warning 2014-06-09 15:24:30     Bad password attempt for user 'root'
41      Warning 2014-06-09 15:24:29     Bad password attempt for user 'root'
42      Warning 2014-06-09 15:24:29     Bad password attempt for user 'root'
43      Warning 2014-06-09 15:24:28     Bad password attempt for user 'root'
44      Warning 2014-06-09 15:24:28     Bad password attempt for user 'root'
45      Warning 2014-06-09 15:24:27     Bad password attempt for user 'root'
46      Warning 2014-06-09 15:24:27     Bad password attempt for user 'root'
47      Warning 2014-06-09 15:24:26     Bad password attempt for user 'root'
48      Warning 2014-06-09 15:24:25     Bad password attempt for user 'root'
```

Figura 24

7. Utilização SNMP

SNMP v1/v2 vem habilitado com as comunidades padrão. Se essa opção é utilizada em sua operação, instruímos alterar os nomes das comunidades diferentes do padrão para reduzir o risco de atividade maliciosa e o uso não autorizado do serviço SNMP.

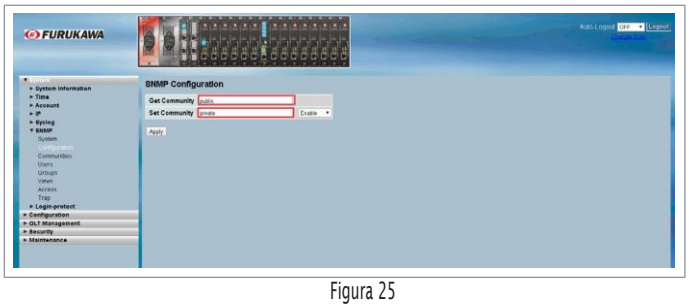

Figura 25

Para alterar os nomes das comunidades, basta acessar o Menu "System", clicar em "SNMP", clicar em "Configuration", alterar "Get Community" e "Set Community" e clicar em "apply".

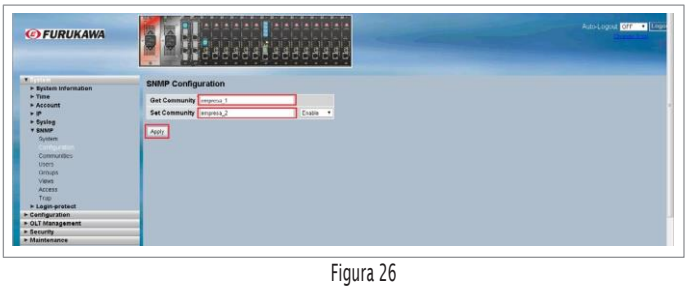

Figura 26

Caso não utilizem os recursos do protocolo SNMP é necessário desabilitá-lo. Pois como no SNMP versão 2 não é necessária autenticação e a configuração de comunidades é padrão e previsível, o chassis fica vulnerável.
Acessar o Menu “System”, clicar em “SNMP”, clicar em “System”, selecionar a opção “disable” e clicar em “Apply”.

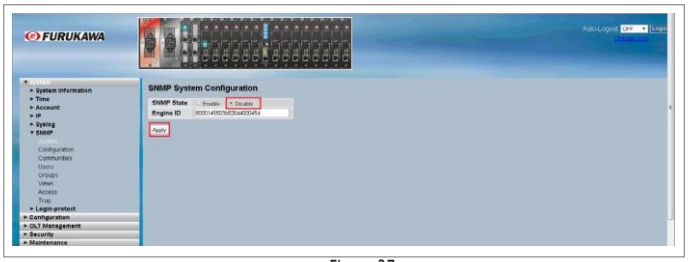

Figura 27

3. Conclusão

Este procedimento auxilia nas boas práticas de configuração para o correto funcionamento da plataforma FK-C32.