北京格林伟迪科技有限公司
GW DELIGHT TECHNOLOGY CO., LTD.

EasyPath EPON

Operation Manual

V3.30

Statement

Because of the product version upgrades or other reasons, this manual will be updated from time to time. If you have any suggestions please feel free to contact us.
E-mail: gwdsupport@gwdelight.com

Technical Support

Technical Support E-mail: gwdsupport@gwdelight.com
Technical Support Telephone: (86-10)18901071077
Website: www.gwdelight.com

Content

1 OverView

This manual is for the EPON series product system administrator for configuration and management.

This manual detailed explains function characteristics and configuration method of EsayPath EPON GFA6000 series remote equipment OLT, also to illustrate some of the default configuration.

1 Use Basic

1.1On-line Help

EPON system command line interface (CLI) provides the following four types of online help:

- Help command
- Completeness help
- Partial help
- TAB help

1.2 Help Command

In any command mode, type “help” to obtain a brief description of the help system.For example:

```
GFA6700(config)#help
      GROS provides help feature as described below.
   1. Anytime you need help, just press "?" and don't
  press Enter, you can see each possible command argument
  and its description.
   2. You can also input "list" and then press Enter
  to execute this helpful command to view the list of
  commands you can use.
```

GFA6700(config)#

1.3 Completeness Help

In any command mode,type “?” to obtain all commands and a brief description of them.For example:

```
GFA6700(config)# ?
  access-list          Create an access-list
  active               Active pending onu
  add                  Add an onu mac address to authenticatiion
table
  alarm-class          Set e1 link alarm
  alarm-log            Config filter
  alarm-mask           Alarm mask configuration
  alarmlog-to-syslog   Config alarm log to syslog enable
  arp                  Config arp table
  auto-load            Onu auto-config or auto-upgrade by ftp
  auto-protect         Set a pon auto-protection
  batfile              Create a command file
  class-map            Traffic class map
  clear                Clear screen
  command              The command options setting
  config               Config system's setting
```

1.4 Partial Help

Type the command to enter a space, then type "?", If the position exists keyword, lists all of the optional keywords and a brief description; if there is parameter in the location, lists relevant parameters and their descriptions. For example:

```
GFA6700(config)#interface  ?
    ethernet  Config ethernet interface
```

```
    trunk        Config Trunk interface
    vlan         Config vlan interface
  GFA6700(config)# interface vlan ?
    <vlanname>   Vlan's name
```

Type a character or string, then enter "?", If there is the character or string at the beginning of the command, lists all of the character or string to the beginning of all the commands and their short description. For example:

```
 GFA6700(config)# s ?
   Save                 Save all batfile
   Screen               Set screen parameters
   Service              Config system's services
   Set                  Set system time
   Show                 Show running system information
   Software             Config software auto-update
   spanning-tree        Spanning tree
   statistic-history    Set the history statistic ttribute
```

1.5 TABHelp

Type a character or string, and then press the Tab key, GROS automatically filled command: If there are multiple character or string to the beginning of the command, lists all of the character or string to the beginning of all the commands, such as

```
 GFA6700(config)# t //Press TAB key at the same time
   telnet
```

If there is only one character or string to the beginning of the command, then the character or string to the beginning of the command completion, and to move the cursor to the end, waiting for further input, such as:

```
  GFA6700(config)# q    //Press TAB key at the same time
  GFA6700(config)# quit
```

Prompt:

If one command is too long, not easy to enter, you can only enter the first few characters of the command, then use the "Tab" key to help is lacking.

2. Command Grammer

Prompt:

- All of the commands in the command line are not case sensitive
- Password is case sensitive

2.1 Command Symbol

Various symbols can be seen in the command format, these symbols are not part of the command itself, which explains how to enter the section command. The meaning of the symbols in the format command as follows:

Symbol	Implication	Example
<>	This section must enter a parameter.	In the command of interface vlan <vlanname> {<1-4094>}*1, a legal VLAN name should be inputted at <vlanname> position.
[ ] and |	Square bracket is used with vertical curve. Part in brackets that this part	Command config syslog In [enable|disable], Included in brackets separated by a

	of the command has several vertical lines separated by an option, you must select the input one. In brackets if only one option, you can directly enter the option	vertical line of the two options, you must enter the enable or disable.
{ } and *	Braces is used with asterisk. Some braces can enter 0 ~ n times, n is equal to the number after the asterisk.	In command undo access-list{<1-5000>}*1, can directly enter the undo access-list, can also undo access-lis with a access-list after the serial number (range 1 to 5000).

2.2 Parameter Type

The angle brackets "<>" part of the enclosed command parameters, GROS command parameters have the following five types:

- **Value Range**

When the values of angle brackets are the two connected by a short horizontal line indicates that the parameter range between these two values. For example: <1-255> "means that the user can input is greater than or equal to 1 and less than any integer equal to 255, such as 20, is a legitimate argument.

- **IP address**

When the angle brackets are the "ABCD", it indicates that the parameter is an IP address, you must enter a valid IP address value, for example, 192.168.0.1 is a valid IP address value.

- **MAC address**

When the angle brackets are "HHH", it indicates that the parameter is a MAC address, you must enter a valid MAC address value, for example 000f.e901.0102 MAC address is a valid value.

- **Port list**

When the angle bracket is "portlist", it indicates that the parameter is an input port list. Port list in the format slot / port, which some available port comma "," to separate multiple ports, and if more than one port number is continuous to the serial port can be used together with the minimum port dash "-" plus The serial port's largest port said. For example: the list of input port 1 / 1, 1/3-6 expressed as: Slot 1 port on the board of 1, 3,4,5,6.

- **Character string**

When the angle brackets is not listed in the above three cases, you may need to enter the parameter that is a string or 16 hexadecimal numbers, you can enter commands specific to the parameters section, enter a question mark "?" Button to view some parameters of the command. For example: <macaddr> expressed the need to enter a 16 hexadecimal MAC address, enter 005023344325 as a valid MAC address, <name> said to enter a string as the name of an object.

2.3 Command Shortening

When enter the command, you can only enter part of a word or keyword in front of the letter of the command; as long as this part of the letter will not cause ambiguity,the switch will be able to identify the command,then the user can enter this command.Parmeters thar are require user input,such as VLAN names and so on,the it requires full input;

```
GFA6700(config)# interface vlan vlan1
```

This command also can be shortening as

```
GFA6700(config)# int vl vlan1
```

2.4 Command Mode

GROS command line offers two modes, one is read-only mode, the

other is the configuration mode. In the read-only mode, users can only view part of the system configuration information in configuration mode the user to view all system configuration information, and can modify the system configuration. In both modes, the command prompt at the end of symbols, the default command prompt is not the same. Read-only mode and configuration mode of the comparison table below:

	Read-only mode	Configuration mode
Function permission	Can only view partial system configuration information	Be able to view all system configuration information, and can modify the system configuration
Command prompt	>	#
Default command prompt	GFA6700>	GFA6700(config)#

Instead, enter the exit command to exit the current configuration mode and return to the previous command mode. In configuration mode, enter the exit command to return to the read-only mode.

In configuration mode, commands can be entered through a number of independent functional configuration mode, then the system will display the corresponding prompt. For example: GFA6700 (config-cst) # for the RSTP protocol configuration mode; GFA6700 (vlan-vlan1) # for the VLAN configuration mode.

For detailed configuration mode of each function,please refer to relevant sections of this manual.

2.5 Line Editing Command

At the command line interface (CLI),you can use the following line editing commands:

Command	Function
BackSpace key or Ctrl+h	Delete one character to the left
Up arrow or Ctrl+p	Call on a historical command
Left arrow or Ctrl+b	Move the cursor to the left one cell
Right arrow or Ctrl+f	Move the cursor to the right one cell
Down arrow or Ctrl+n	If you used the up arrow in front of a historic call to order, then click the down arrow key to display the next command history
Ctrl+a	Move the cursor to the line first
Ctrl+e	Move the cursor to end of line
Ctrl+d	Delete the character that the cursor position
Ctrl+k	Delete all characters after the cursor
Ctrl+t	Characters and the cursor is located left of the cursor that character interchangeable, and the cursor moves one space to the right
Ctrl+u	Delete entire row
Ctrl+w	Move the cursor left, space characters to the right to delete all the characters

2.6 undo Command

When configured to use some commands, you can use the undo command to cancel the corresponding configuration.

For example: The command debug spanning-tree all you can open the debug spanning-tree debugging, which corresponds to undo command undo debug spanning-tree all you can turn off the switch

2.7 Save Configuration

If you want to the current configuration is still valid when switch power down or restart,you must use the save configuration command to save the current configuration file.For example:

GFA6700(config)# save configuration

Trying to save configuration to flash, please wait... Preparing data for saving configuration...Done.

Starting writing configuration data to flash...Done. Configuration saved to flash successfully.

2 Equipment Management

1 System Management

1.1Basic Management Information

Users can configure the serial port cable connected to the system administration log in, can also log on via telnet system management system.

1.1.1 Usual Command

Usual commands in read-only mode, such as shown in Table 1-1:

Table 1-1 Usual commands in read-only mode

Command	Description
clear	Clear screen
enable	Enter configuration mode, you can configure the switch and write operations
exit	Exit the current configuration mode and return to the previous configuration mode

help	Shows how to use the command line grammar help
list	Displays the current list of available commands
logout	Log out, disconnect
quit	Exit the command line, disconnect the connection (and logout the same effect)
show command-history	Display history of commands entered
Show screen-idle-timeout	Display idle timeout time
show services	Displays the current system of services
who	Displays the current user connected to the switch

In addition to enable read-only mode, all commands other than the mode in the configuration are valid, are listed in Table 1-2 Common Configuration mode command to not repeat these commands.

Table 1-2Usual commands in configuration mode

Command	Description
enable-password	Modify own password into the configuration mode
erase config-file	Remove the switch startup configuration information stored in the system
hostname <hostname>	Renamed for the equipment

Screen idle-timeout <0-35791>	After setting the length of idle time, the system automatically log out
save {configuration}*1	To write the current running configuration switch and save
show running-config	Show running configuration of system
show startup-config	Show em boot configuration
screen lines <0-512>	Set the output terminal number of lines per screen

1.1.2 Show Version Information

Use the command show version to display version information. And the specific content related with the equipment of the type, specifications, software, and hardware version For example:

GFA6700(config)#show version

EasyPath Series PON Switch Software
GROS Version V1R03B216(Build on 15:19:35 Jul 13 2010)
Copyright (c) GW Technologies Co.,Ltd. All Rights Reserved

Running on EasyPath Ethernet-PON Hardware
Switch Chip : BCM56514_A0 , Driver : BCM56514_A0 (5.5.1)
Nvram Model : DS1746
Sysmac : 000F.E906.1188

	BootVersion	SoftwareVersion	FirmwareVersion
SLOT	1 : -	-	-
SLOT	2 : -	-	-
SLOT	3 : V1.22.0	V1R09B216	V1.6

SLOT 4 : - - -

SLOT 5 : - - -

SLOT 6 : - - -

SLOT 7 : V3.3.1 V5R03B520 V2.12.11.0

SLOT 8 : - - -

SLOT 9 : - - -

SLOT 10 : - - -

SLOT 11 : - - -

HardwareType HardwareVersion ManufactureDate SerialNo

CHASSIS : GFA6700 V1.0B0 - -

SLOT 1 : GFA-GET V1.0B0 2007-04-20 312065

SLOT 2 : - - - - -

SLOT 3 : GFA-SW V1.0B2 2010-6-29 67SWT100610031

SLOT 4 : - - - - -

SLOT 5 : - - - - -

SLOT 6 : - - - - -

SLOT 7 : GFA-EPON V1.0B1 2009-4-16 T09040160

SLOT 8 : - - - - -

SLOT 9 : GFA-PWU48 V1.0B1 2006-12-06 H6B282051

SLOT 10 : - - - - -

SLOT 11 : - - - - -

1.1.3 Set the line numbers of each show information of terminal

Use the command: screen lines <lines> to set the line numbers of the display information for each terminal.

By default the terminal screen displays information for each of 23 lines,

lines if the parameter is set to 0, then the number of lines per screen display no limit. For example, here set to 30 lines per screen display of information

```
GFA6700(config)# screen lines 30
```

1.1.4 Display the current status of the various services

Use the command show services can display the current status of the various services. And equipment specific display models, specifications, software, hardware version related. For example：

```
GFA6700(config)#show services
  telnet is up.
  snmp agent is up.
  snmp rmon is down.
  snmp trap support is up.
  sntp client is down.
  sntp server is down.
```

Telente service is started,SNMP related service close

1.1.5 Set Switch Name

Sometimes in order to manage, it can re-set the switch name, then, the system prompt will change. For example, set the host name for the GROS:

```
GFA6700(config)# config hostname GROS
GROS(config)#
```

1.1.6 Set and view the idle waiting time

Use command: screen idle-timeout <0-35791> Can set the system idle wait time.

Use command: show screen-idle-timeout can query the current system

idle wait time.

In default, the system is idle waiting time is 20 minutes.

For example, set the system idle wait time is 1 hour and check the configuration, use the following command:

```
GFA6700(config)# screen idle-timeout 60
GFA6700(config)# show screen-idle-timeout
Idle time out is set to 60 minutes.
```

If the user is not make any operation in 60 minutes on the system, it will automatically exit the super terminal management status, and disconnect the connection with the terminal into the log before the state. When the parameter is set to 0, does not automatically exit the system.

Prompt:

- If it is in learning stage or debug status, you can set this parameter larger or set to 0.
- Time unit of this command: minute.

1.1.7 View the current system configuration

In the case of fault diagnosis or other, “show running-config” command is often used to view the system's current configuration information. And equipment specific display models, specifications, software, hardware version related. For example:

```
GFA6700(config)#show running-config
!GROS system config file
!version V1R09B216

!Basic information config
```

config description EasyPath Ethernet-PON

!

!Login config

config login-authentication enable

!

!Usermanage config

user add admin login-password c133533ef746139ce83d12ff4e084691

user role admin admin enable-password c133533ef746139ce83d12ff4e084691

user add zhangxch login-password 7ff8c3b25586174c9337cbc63e331b6f

user role zhangxch admin enable-password 7ff8c3b25586174c9337cbc63e331b6f

user add yaol login-password ef89debfab65e0c083a88656f0d259f9

user role yaol admin enable-password ef89debfab65e0c083a88656f0d259f9

user add lijt login-password 9ca3c960815a9d6a2f8ac00a2159d7d0

user role lijt admin enable-password 9ca3c960815a9d6a2f8ac00a2159d7d0

user add xuyg login-password 662c45414a6bfb34e64ed851feea2737

user role xuyg admin enable-password 662c45414a6bfb34e64ed851feea2737

!

!OLT information config

```
!

!Pon port config
  pon 7/4
    add onu 1 000f.e903.4863
    add onu 2 000f.e903.b18e
    add onu 3 000f.e903.af18
    add onu 4 000f.e903.4e87
    add onu 5 000f.e903.ade0
    add onu 6 000f.e903.da5b
    add onu 11 000b.1616.2116
    add onu 15 000b.160c.0c0c
    onu p2p 1 2
    onu p2p 1 3
    onu p2p 1 4
    onu p2p 1 5
    onu p2p 1 6
    onu p2p 2 3
    onu p2p 2 4
    onu p2p 2 5
    onu p2p 2 6
    onu p2p 3 4
    onu p2p 3 5
    onu p2p 3 6
    onu p2p 4 5
    onu p2p 4 6
    onu p2p 5 6
  exit
!

!Onu config
```

```
 onu 7/4/1
  p2p forward address-not-found enable
 exit
 onu 7/4/2
  p2p forward address-not-found enable
 exit
 onu 7/4/3
  p2p forward address-not-found enable
 exit
 onu 7/4/4
  p2p forward address-not-found enable
 exit
 onu 7/4/5
  p2p forward address-not-found enable
 exit
 onu 7/4/6
  p2p forward address-not-found enable
 exit
!

!alarm config
   diagnose pon-link enable
!

!ETH loop detection config
!

!CTC ONU parameter mapping config
!

!onu autoconfig and upgrade config
```

```
!
!Trunk config
!

!VLAN config
   vlanmode dot1q
   vlantpid 0x8100 0x8100
   interface vlan default 1
    mcastmode 2
   exit
   interface vlan v3 3
    add port 7/4 tagged
    add port 1/4 untagged
    ip address 192.168.2.210 255.255.255.0
    mcastmode 2
   exit
!

!VLAN QinQ-Map ingress config
!

!VLAN QinQ-Map egress config
!

!Ethernet port config
   interface ethernet 1/1
    flowcontrol enable
   exit
   interface ethernet 1/2
    flowcontrol enable
   exit
```

```
   interface ethernet 1/3
    flowcontrol enable
   exit
!

!Forward-entry    config
!

!l2 user-entry    config
!

!Filter Config
!

!Mgt port config
!

!Stp config
!

!L2 multicast config
   igmp-snooping enable
!

!DoS config
!

!Arp config
!

!Sntp config
```

```
!

 !Static routes config
  ip route 0.0.0.0/0 192.168.2.254
 !

 !Global qos config
 !

 !Port qos config
 !

 !Syslog config
 !

 !Snmp config
    service snmp enable
    service snmp trap enable
 !

 !Nms config
 !

 !end of config

  ! *************************
  ! Total usage 2952 bytes
  ! Maximum         1310720 bytes
  ! *************************
```

1.1.8 View saved system configuration file

View saved system configuration file. Detailed show content is related

with type, specification, software and hardware version of equipment.

For example:

```
GFA6700(config)#show running-config
  !GROS system config file
  !version V1R09B216

  !Basic information config
    config description EasyPath Ethernet-PON
  !

  !Login config
    config login-authentication enable
  !

  !Usermanage config
    user add admin login-password
c133533ef746139ce83d12ff4e084691
    user role admin admin enable-password
c133533ef746139ce83d12ff4e084691
    user add zhangxch login-password
7ff8c3b25586174c9337cbc63e331b6f
    user role zhangxch admin enable-password
7ff8c3b25586174c9337cbc63e331b6f
    user add yaol login-password
ef89debfab65e0c083a88656f0d259f9
    user role yaol admin enable-password
ef89debfab65e0c083a88656f0d259f9
    user add lijt login-password
9ca3c960815a9d6a2f8ac00a2159d7d0
    user role lijt admin enable-password
9ca3c960815a9d6a2f8ac00a2159d7d0
```

```
        user add xuyg login-password
662c45414a6bfb34e64ed851feea2737
        user role xuyg admin enable-password
662c45414a6bfb34e64ed851feea2737
        !

        !OLT information config
        !

        !Pon port config
          pon 7/4
            add onu 1 000f.e903.4863
            add onu 2 000f.e903.b18e
            add onu 3 000f.e903.af18
            add onu 4 000f.e903.4e87
            add onu 5 000f.e903.ade0
            add onu 6 000f.e903.da5b
            add onu 11 000b.1616.2116
            add onu 15 000b.160c.0c0c
            onu p2p 1 2
            onu p2p 1 3
            onu p2p 1 4
            onu p2p 1 5
            onu p2p 1 6
            onu p2p 2 3
            onu p2p 2 4
            onu p2p 2 5
            onu p2p 2 6
            onu p2p 3 4
            onu p2p 3 5
            onu p2p 3 6
```

```
   onu p2p 4 5
   onu p2p 4 6
   onu p2p 5 6
  exit
!

!Onu config
   onu 7/4/1
     p2p forward address-not-found enable
   exit
   onu 7/4/2
     p2p forward address-not-found enable
   exit
   onu 7/4/3
     p2p forward address-not-found enable
   exit
   onu 7/4/4
     p2p forward address-not-found enable
   exit
   onu 7/4/5
     p2p forward address-not-found enable
   exit
   onu 7/4/6
     p2p forward address-not-found enable
   exit
  !

  !alarm config
     diagnose pon-link enable
  !
```

```
!ETH loop detection config
!

!CTC ONU parameter mapping config
!

!onu autoconfig and upgrade config
!
!Trunk config
!

!VLAN config
   vlanmode dot1q
   vlantpid 0x8100 0x8100
   interface vlan default 1
    mcastmode 2
   exit
   interface vlan v3 3
    add port 7/4 tagged
    add port 1/4 untagged
    ip address 192.168.2.210 255.255.255.0
    mcastmode 2
   exit
!

!VLAN QinQ-Map ingress config
!

!VLAN QinQ-Map egress config
!
```

```
!Ethernet port config
   interface ethernet 1/1
    flowcontrol enable
   exit
   interface ethernet 1/2
    flowcontrol enable
   exit
   interface ethernet 1/3
    flowcontrol enable
   exit
!

!Forward-entry    config
!

!l2 user-entry    config
!

!Filter Config
!

!Mgt port config
!

!Stp config
!

!L2 multicast config
   igmp-snooping enable
!
```

```
!DoS config
!

!Arp config
!

!Sntp config
!

 !Static routes config
  ip route 0.0.0.0/0 192.168.2.254
 !

 !Global qos config
 !

 !Port qos config
 !

 !Syslog config
 !

 !Snmp config
    service snmp enable
    service snmp trap enable
 !

 !Nms config
 !

 !end of config
```

! *************************

! Total usage 2952 bytes

! Maximum 1310720 bytes

! *************************

1.1.9 Save current configuration file

If you want the current configuration is still valid when swith power down or restart, you must use “save configuration” command to save current configuration file.

GFA6700(config)# save configuration

Trying save configuration to flash, please wait ..... Preparing configuration data to save...Done.

Starting write configuration data to flash...Done.

Configuration save to flash successfully.

1.1.10 Delete all the saved configuration information

If you want to re-configure the switch startup configuration information, use the “erase config-file” command to remove the previous configuration. This order need to restart the device to take effect. For example

---

 **Note!**

Remove the startup configuration; do not run before the reboot save config command.

GFA6700(config)# erase config-file

Are you sure want to erase config-file? [Y/N]y

Trying erase all configuration from flash, please wait ..... finished.

Successfully erase all configuration info from flash.

1.1.11 Show user information that connects to switch

Use the command “who” can show the user all the information connected to the switch, but “who am i” command displays only their own (switches) information.

GFA6700(config)#who

SessionID. - UserName ---------- LOCATION ---------- MODE ----

1030 yaol 192.168.4.197 CONFIG (That's me.)

Total 1 sessions in current system.

GFA6700(config)#who am i

I am *Session [1030] : user yaol connected from 192.168.4.197.

1.1.12 Force close connection of specific user

If there are unauthorized users to connect to the switch, the administrator can force users to disconnect their connection. An illegal user who commands from the session ID can be obtained. For example, forced to close off session ID of the user's session is 5, use the following command:

GFA6700(config)# kill session 5

Prompt:

If user use serial link, kill command can’t be used for force closed.

1.1.13 System Time

Each switch has its own system clock, to save the current date and time. Users can use the command static configuration.

The system's default start time is read from the RTC clock.

Can use the show system time display system time, for example:

GFA6700(config)# show system time

YYYY-MM-DD HH:MM:SS

2006-10-06 10:55:08

Using the “set system time” command to set the system time.For example:

GFA6700(config)# set system time 2006 9 10 7 8 18 28

Set time must comply with certain rules; the year must be between 1980 and 2079. Set the clock value is written to NVRAM.

1.1.14 Management IP Address of OLT

In-band management IP address or out-of-band management IP address of OLT equipment can be set.

Configure in-band management IP address.

Step	Command	Explain
Step 1	GFA6700(config)#interface vlan manage 4094 GFA6700(vlan-manage)#add port 1/3 untagged	Create one management VLAN, add in-band management port
Step 2	GFA6700(vlan-manage)#ip add 192.168.7.100/24	Configure management IP address in management VLAN.
Step 3	GFA6700(vlan-manage)#exit GFA6700(config)#	Quit management VLAN node

Configuration of out-of-band management IP address:

Step	Command	Explain
Step 1	GFA6700(config)#interface ethernet mgt	Enter out-of-band management node
Step 2	GFA6700(config-if-mgt)#ip add 192.168.7.100/24	Configure Out-of-band anagement IP ldress
Step 3	GFA6700(config-if-mgt)#exit	Quit out-of-band management port node

1.1.15 Restart System

Before you restart the switch, use the command save configuration to save the configuration file, otherwise it will lose all configuration information is not saved. Restart the switch, the following ways:

- **Re-power**

Equipment to re-power, through the system on the rear panel power switch to operate, the first switch set to OFF, then set to ON, re-power the system will automatically update after sync the device software version.

- **Restart the machine**

Enter configuration mode using the reboot command to restart the machine. For example

GFA6700(config)# reboot

Are you sure want to reboot switch system? [Y/N] y

- **Restart the specified board**

Enter configuration mode using the reboot <1-8> command to specify a piece of board to restart. For example:

GFA6700(config)#reboot 4

Are you sure want to reboot slot 4? [Y/N]y

Module 4 is going to reboot...

Pon(slot4) is pulled

Pon(slot4)/port1 is to be removed ... Ok

… …

… …

% DEVSM slot 4 board GFA_EPON is inserted...

% The insered time is: 24/01/2007, 17:20:20.430

SLOT 4 : GFA_EPON BOARD READY.

Start flow control initial....

SLOT 4 : GFA_EPON BOARD(SLAVE) RUNNING.

Prompt:

When the user specifies the main board to be reset with the control board, the equivalent to enter the Executive reboot, restart the machine.。

---

2 User Management

2.1 User Permission

GROS offers two user permissions:

- Ordinary users (NORMAL)
- Administrator (ADMIN)

Most ordinary users can view system information, but can not view the system of user information and system configuration information (mainly refers to the contents of the file system configuration and system global configuration information)). GROS ordinary users log on to the system, can only be read-only mode and can not enter into configuration mode. Administrator can enter the configuration mode and the system to view all parameters and settings

2.2 Default user account

The system default built a super user account administrator privileges, the user name is admin, default password is greenway. Default user admin account can not be deleted, the user name can not be modified, can only modify their passwords. Super administrator configuration mode privileged user to enter the password is greenway.

2.3 Enable User Manager

Change,configuration management with the user before the first use of config login-authentication enables command to enable user management.

GFA6700(config)#config login-authentication enable

2.4 Add User Account

With the user add command to add a user account. For example, adding a user account named Anna, and set the login password is 123456:

Each user account is only available for a user login. System for up to 5 users simultaneously landing a console user, four telnet users. 5 concurrent users if the administrator login, you can only have one user into the configuration node, the user only in view the regional node.

GFA6700(config)# user add Anna login-password 123456

The newly added user account permissions are normal user (NORMAL). For the ordinary user's permissions for the administrator or the administrator permissions for ordinary users need to log in via telnet to execute. Add, delete user accounts, and you do not need to modify the user password through the telnet login. Hypotheses have been through the telnet login, the following command in order to set the permissions the user account administrator (ADMIN) and users (NORMAL):

```
GFA6700(config)# user role Anna admin
GFA6700(config)# user role Anna normal
```

2.5 View user account

Current all users account can be viewed by following command:

```
GFA6700(config)# user list
  UserName ----------User_role ----------
  Admin                    ADMIN_USER
  Anna                     NORMAL_USER
  Total 2 users in system.
```

2.6 Delete user account

Use “user delete” command can delete one user accout

```
GFA6700(config)# user delete anna
```

Prompt:

Management has increased only the super user, modify user permissions, remove the user's permission to other administrative users do not have the permission。

2.7 Modify password

Administrator to modify password, use the command “login-password”, then prompted to enter the new password and confirm the new password.

Administrators to modify their own password to enter configuration mode, use the command “enable-password”. Then prompted to enter the new password and confirm the new password.

Administrator to reset the password of other users and configuration mode password, respectively, using the command “user login-password, user enable-password”, then prompted to enter the new password and confirm the new password.

3 Configure NMS

3.1Overview

NMS provides three access methods: Serial (Console), remote login (Telnet), Simple Network Management Protocol (SNMP), by default, telnet and SNMP is turned off, the opening must pass the appropriate command to configure access control to strengthen the management of access control switch.

In order to improve system security, in addition to the serial port, the network provides access control functions. Know a valid username and password to access the switch. Sometimes we have for safety consideration, and hope the user's IP address is a specific or a range, and then you can open Control access to services, the IP address to access the configuration table. When the user logs on, the switch first verify the legitimacy of the user IP address, if the IP legal, will verify the legitimacy of the user name and password

Before configure OLT visit control, you must first create a network access control “nms-access-profile”, network access control group, the

name of up to 19 characters, only by numbers, uppercase and lowercase letters and underscores.

3.2 Configure NMS

3.2.1 Default configuration information

The default configuration information as shown in the following table:

3.2.2 Configure NMS access control group

Network access control groups have used the premise that “service [telnet | snmp] enable” command to open a Telnet or SNMP service, the client can log in for access control.

For Telnet and SNMP access mode, the steps to configure access control similar to the control group are configured to access the unit, configure access control, including the IP address and IP network segment.

Telnet services as an example below to configure access control:

Configuration step:

Step	Command	Explain
Step 1	service telnet [enable|disable]	Enable Telnet service
Step 2	config access-control {[telnet|snmp]}*1 [enable|disable]	Open Telnet access control switch
Step 3	nms-access-profile <access_ profile_name>	Set SNMP read-only permissions authentication password

Step 4	config nms-access-profile <access_profile_name> telnet [enable|disable]	Set Telnet switch of access control group
Step 5	config nms-access-profile <access_profile_name> add ipaddress <A.B.C.D> <A.B.C.D> [enable|disable]	Add to the access control group to send trap IP address segment
Step 6	show nms-access-profile {<access_profile_name>}*1	Show configuration information of access control group

3.2.3 Match the order of access control

Access control system allows to create multiple groups, matches will traverse all the groups, the longest match of the IP address to determine the permissions. When the access control service is open, an IP can access the switch, first check whether the access control group, the IP address, if any, to take the control of the access permissions, and if not, see whether a particular IP subnet in, and take the appropriate permissions, priority rights to take the smallest subnet. If the access control group is not in the IP address, the IP can not access the switch

For example, the configuration group1 and group2 two groups, the configuration is as follows:

Configuration step

Step	Command	Explain
Step 1	service telnet [enable|disable]	Enable Telnet service
Step 2	config access-control enable	Open Telnet access control switch
Step 3	nms-access-profile group1	Open Telnet access control switch
Step 4	config nms-access-profile group1 telnet disable	Set forbidding access of Telnet switch of access control group 1
Step 5	config nms-access-profile group1 add ipaddress 192.168.7.0/24	Adding to the access control group allows IP address segment IP addresses belonging to this segment of the

		network can not Telnet connection
Step 6	nms-access-profile group2	Create one access control group 2
Step 7	config nms-access-profile group2 telnet enable	Control group group2 will visit the switch is set to allow access to Telnet
Step 8	config nms-access-profile group2 add ipaddress 192.168.7.0/24	Access control group group2 to add an address segment, making the IP address belongs to this segment of the network connection to Telnet

Which, group2 group1 in the segment included in the segment. Access control based on matching the order of the IP belongs to group1 can not Telnet to the switch, but is not part of group1 group2 but the IP can Telnet to the switch above.

 **Note!**

For the same IP address, IP subnet is not able to configure multiple times, even in a different configuration of the access control group. When such a configuration, the system will not perform, and display the following message:% IP address conflicts with exist entry.

3.3 In-band NMS Route

When the NMS IP and the PC is not in the same network segment, you need to configure static routing can be achieved Telnet and SNMP access, EPON Although they are two-story device, but provides IP protocol and associated TCP / IP protocol stack supports simple three-routed function, and supports static routing configuration, in order to achieve across different segments of the IP packet forwarding, the key segment for cross-band network management functions。

3.3.1 Static route

Static routing is configured by the user route. When the user reaches a certain segment should be forwarded to an address, you can configure this through the command ip route static routing.

Configuration step

Step	Command	Explain
Step 1	ip route [<A.B.C.D/M> | <A.B.C.D>	Configure static route

Step 2	show ip route	View route
Step 3	undo ip route <A.B.C.D/M> <A.B.C.D>	Cancel set of static route

3.3.2 Default route

There is a special kind of routing is called a default route (or default route), that is the destination address and mask of 0.0.0.0 / 0 route. It can match any destination address, so each packet can not find the corresponding route are forwarded will be the default route. Default routes are usually considered necessary by the user static route configuration.

Configuration step:

Step	Command	Explain
Step 1	ip route 0.0.0.0/0 <A.B.C.D>	Configure default route
Step 2	show ip route	View route

3.4 Configuration case

3.4.1 Create one access control group

Case Description: Creating an access control group group1, configure an IP network segment so that the IP addresses belonging to this segment can log in Telnet.

Configuration step:

Step	Command	Explain
Step 1	GFA6700 (config)# service telnet enable	Enable Telnet service
Step 2	GFA6700 (config)# config access-control enable	Open swith of access control
Step 3	GFA6700 (config)# nms-access-profile group1	Create one access control group 1
Step 4	GFA6700 (config)# config nms-access-profile group1 telnet enable	Telnet access to the control group will be set to allow access to switches
Step 5	GFA6700 (config)# config nms-access-profile group1 add ipaddress 192.168.7.0/24	Add to address access control segment, making the IP address belongs to this segment Telnet to log in
Step 6	GFA6700 (config)# config nms-access-profile group1 delete ipaddress 192.168.7.0/24	Just added you want to modify the network segment, starting with the access control group,

		deleting this segment
Step 7	GFA6700 (config)# config nms-access-profile group1 add ipaddress 192.168.7.0/24	Re-added to the access control group, the address segment
Step 8	GFA6700 (config)# show services telnet is up. snmp agent is down. snmp rmon is down. snmp trap support is down. GFA6700(config)# show nms-access-profile ========== ========== Access profile name : group1 Telnet access status : enable SNMP access status : disable ---------- Address List: ---------- No ID Network-IP NetMask ---------- 1 0 192.168.7.0 255.255.255.0 ---------- Total 1 Addresses. ==========	Use “show” command to view configuration result

	========== Total 1 access profile in system.	

3.4.2 View route

Use command “show ip route” to view route, for example:

GFA6700(config)#show ip route

Codes: C - connected, S - static,

> - Selected route, * - Selected nexthop

S>* 0.0.0.0/0 [1/0] via 192.168.2.254, v3, weight 8

C>* 192.168.2.0/24 is directly connected, v3

C at the beginning of the route that is the route of the switch ports, it only shows the direct connection of local network segment; S at the beginning of the static route, which is user configurable; ">" sign followed by "*" symbol, it shows When the next hop IP routing when there are multiple, including the next hop which was in force. Destination address, next hop address and interface name (the example of the VLAN "v1"), followed by weight and, finally, the survival time of routing.

Note!

When the interface state is DOWN, the associated routing will fail or be removed. Because then the switch can not forward the packets out the interface was. When the interface state to UP, the interfaces and static route will take effect immediately, while the dynamic routing should be restored in a relatively short period of time.

---

4 Configuration SNMP

4.1 Overview

With the rapid development of network technology, increasing the number of networks, and network equipment from different manufacturers, how to manage these devices becomes very important. SNMP is based on this need arise.

SNMP (Simple Network Management Protocol) is used in the data communications network, the most widely used network management protocol, is widely accepted and the actual use of industry standards. Its design goal is to make management information can be transmitted between any two points in the network, enabling network administrators to any node in the network to retrieve information, modify the preparation, troubleshooting, fault diagnosis, planning and traffic and generate reports. It uses the polling mechanism, providing the most basic feature set. SNMP is an application layer protocol, the transport layer using UDP protocol.

Based on TCP / IP network management is divided into two processes,

Users of the network management station, also known as management Processes,

Managed device and management of related software client called the agent (Agent) or the agent process.

Based on TCP / IP network management consists of 3 components:

A Management Information Base MIB (Management Information Base), management information repository that contains all the agents process (SNMP Agent) of all that can be queried and modified parameters.

On the MIB's structure and that a common set of symbols.

Management process and the communication protocol between the proxy processes, called the Simple Network Management Protocol SNMP (Simple Network Management Protocol), SNMP use UDP for the process management process and the communication between agents.

SNMP protocol defines 5 types of message

- **get-request**
- **get-next-request**
- **set-request**
- **get-response**
- **trap** // Agent process the initiative to send the message management process, notification of certain events, such as the port dropped and so on.

4.2 Configuration SNMP

4.2.1 Default configuration information

Table 2-4 SNMP default configuration information

Content	Default configuration	Remark
SNMP Agent startup/close (up/down)	down	Set can be changed
SNMP Trap startup/close (up/down)	down	Set can be changed
SNMP access password (community strings)	Read-only permission password public; Read and write permission password: private	Set can be changed

4.2.2 Startup SNMP service/configuration SNMP TRAP

Configuration step as following of startup SNMP service:

Configuration step:

Step	Command	Explain
Step 1	service snmp enable	Enable SNMP agent service
Step 2	service snmp trap enable	Enable SNMP trap service
Step 3	config snmp community readonly <string>	Set SNMP read-only permissions authentication password
Step 4	config snmp community readwrite <string>	Set SNMP read and write permissions authentication password
Step 5	config snmp trapreceiver add <A.B.C.D> version [v1|v2c] {community <string>}*1	Adding a host address to receive TRAP
Step 6	show service	Show whether SNMP is startup
Step 7	show snmp community-string	Show the current authentication password

		permissions

4.3 Configuration case

4.3.1 Set one PC is trap receive station

Case description:

GFA6000 series with a networked PC, OLT OLT receives the information issued by the trap, PC machine's IP address is 11.1.1.100. Ping through the switch and the PC function.

Figure 2-1 SNMP networking

Configuration step

Step	Command	Explain
Step 1	GFA6700 (config)# service snmp enable GFA6700 (config)# service snmp trap enable GFA6700 (config)# config snmp trap type all on	Enable SNMP switch service that allows to send all types of trap
Step 2	GFA6700 (config)# config snmp trapreceiver add 11.1.1.100 version v2c	IP addresses of known

		added as a trap station PC
Step 3	GFA6700 (config)# show services telnet is down. snmp agent 120is up. snmp trap support is up. . . GFA6700 (config)# show snmp trap type Interface trap is on Stp trap is on Start trap is on GFA6700(config)#show snmp trapreceiver IP address Version Community 192.168.2.72 v2c public Total 1 trapreceiver IP address in system.	View configuration result

4.4 Fault Analysis

4.4.1trap receiving station not receive trap

Phenomenon	Configuration of the trap station, but not received trap.
Analysis	If the SNMP configuration is correct, may be between the switch and trap station network communication is not normal.
Resolve	Ping from the switch about receiving station, if the ping barrier, then between the switch and the receiving station can not be network communications. Check two or

	three-forward set of network hardware.

5 Software upgrade

5.1 Overview

EPON equipment supports BSP, software, firmware remote upgrade by FTP, be achieved to support FTP configuration data, configuration data such as automatic backup and recovery.

5.2 OLT Software Upgrade

5.2.1 Upgrade File Explain

- **APP file:** Application files, it is GFA6000 series of OLT when the normal operation of the software used.
  Sample file name: OLTV1R09B216.BIN
- **Boot file:** System boot files, when the device is powered up after the first run of this software, its main job is to initialize the hardware, and load the app file into memory to run, run to completion after the software is to replace it by the app work.
  Sample file name: GFA6700BootV1.22.0.BIN
- **Firmware file:** PON chips running software stored in memory chips in the exchange board, each time the device is restarted, the exchange board must download this file to each PON chip. PON system board so the more the longer start.
  Sample file name: OLTFWV5.2.44.1.BIN
- **DBA file:** This is the PON chip bandwidth allocation algorithm running on the file, and the PAS5001 files, is stored in the exchange board, each time the system restarts, downloaded from the exchange board to each PON chip. Generally do not upgrade the file.

Sample file name: OLTDBAV3.3.BIN

5.2.2 Upgrade preparation

- Ensure that the FTP Server can communicate with each other and OLT
- Prepare documents related to the upgrade
- Backup configuration file, the software running the current system to prevent problems, you can back version

5.2.3 File Upgrade Command

Command	Explain
download ftp [app] <A.B.C.D> <user> <pass> <filename> [olt|onu] {[CRC-check]}*1	Upgrade OLT APP file or ONU APP file
download ftp [boot] <A.B.C.D> <user> <pass> <filename>	Upgrade boot file
download ftp [config] <A.B.C.D> <user> <pass> <filename>	Import configuration file
download ftp [driver] <A.B.C.D> <user> <pass> <filename> [firmware|dba]	Upgrade firmware and DBA file
download ftp [tdm] <A.B.C.D> <user> <pass> <filename>	In the OLT with SIG or TDM cards, use this command to upgrade the card

	application

Note!

- Please confirm normal communication between FTP Server and OLT when upgrading BOOT file, and ensure to equipment can't power off. If above coditions occuers, BOOT file will be imperfect caused by upgrading process interrupt, and equipment can't startup normal.
- System software with the version number after V1R09B216 can provide this function that use of CRC-check parameter when upgrading APP file.

5.2.4 Configuration case

Step	Command	Explain
Step 1	GFA6700(config)#save configuration Trying to save configuration to flash, please wait... Preparing data for saving configuration...Done. Starting writing configuration data to flash...Done. Configuration saved to flash successfully.	Save current system configuration
Step 2	GFA6700(config)#interface vlan internet GFA6700 (vlan-internet)#add port 1/1 untagged	OLT equipment configurati

	GFA6700(vlan-internet)#ip address 192.168.7.126/24 GFA6700 (vlan-internet)#exit GFA6700(config)#	on of a IP address to the network and the FTP Server can communic ate
Step 3	GFA6700(config)#ping 192.168.7.72 PING 192.168.7.72 : 56 data bytes. Press Ctrl-c to Stop. Reply from 192.168.7.72 : bytes=56: icmp_seq=0 ttl=128 time<=10 ms Reply from 192.168.7.72 : bytes=56: icmp_seq=1 ttl=128 time<=10 ms Reply from 192.168.7.72 : bytes=56: icmp_seq=2 ttl=128 time<=10 ms Reply from 192.168.7.72 : bytes=56: icmp_seq=3 ttl=128 time<=10 ms Reply from 192.168.7.72 : bytes=56: icmp_seq=4 ttl=128 time<=10 ms	OLT can be recognize d and FTP Server (assuming it's IP is 192.168.7. 72) normal communic atio-n
Step 4	GFA6700(config)#upload ftp app 192.168.7.72 test aaaaaa GFA6700V1R09B216.BIN olt Get ftp operational popedom! Connecting to server: 192.168.7.72 Uploading file to server... Upload file ...ok Release ftp operational popedom!	Backup configurati on file and the current file system operation APP

	GFA6700(config)#upload ftp config 192.168.7.72 test aaaaaa config-olt.txt Get ftp operational popedom! Connecting to server: 192.168.7.72 Uploading file to server... Upload file ...ok Release ftp operational popedom!	
Step 5	GFA6700(config)#show online-onu [TOTAL ONLINE ONU COUNTER = 6] Idx Mac addr type running-time userName ---------- Pon(slot7)/port4 [online onu counter = 6] 1 000f.e903.4863 GT811_A 0000:02:30:36 GT811A 2 000f.e903.b18e GT812_A 0004:23:04:01 GT812A 3 000f.e903.af18 GT812_A 0000:05:22:42 GT812 A 4 000f.e903.4e87 GT812_A 0004:23:04:01 GT812 A 5 000f.e903.ade0 GT812_A 0004:23:04:01 GT812 A 6 000f.e903.da5b GT866 0004:23:04:01 GT866	Confirmed before the upgrade online ONU, check after the upgrade to prepare for

Step 6	GFA6700(config)#download ftp app 192.168.2.75 test aaaaaa OLTV1R09B216.bin olt Get ftp operational popedom! Connecting to server: 192.168.2.75 Downloading file from server... Received size: 2eb502 byte Download file ...ok Write to flash...ok Release ftp operational popedom! GFA6700 (config)#download ftp driver 192.168.2.109 test 1 OLTDBAV3.3.BIN dba Get ftp operational popedom! Connecting to server: 192.168.2.109 Downloading file from server... Received size: d0a0 byte Download file ...ok Write to flash...ok Release ftp operational popedom! GFA6700(config)#download ftp driver 192.168.2.109 test aaaaaa OLTFWV5.2.44.1.BIN firmware Get ftp operational popedom! Connecting to server: 192.168.2.109 Downloading file from server... Received size: 53248 byte Download file ...ok Write to flash...ok Release ftp operational popedom!	Download new version of APP，DBA，Firmware and BOOT file

	GFA6700(config)#download ftp boot 192.168.2.109 test aaaaaa GFA6700BootV1.22.0.BIN Get ftp operational popedom! Connecting to server: 192.168.2.109 Downloading file from server... Received size: 53248 byte Download file ...ok Write to flash...ok Release ftp operational popedom!	
Step 7	GFA6700(config)#reboot Are you sure want to reboot switch system? [Y/N]	Restart the OLT, so that the new version of the software into force

5.3 ONU Software Upgrade

5.3.1 File upgrade command

Command	Explain
download ftp [app] <A.B.C.D> <user> <pass> <filename> [olt|onu] {[CRC-check]}*1	Use "ONU" parameters, download software to the OLT

	on the ONU
update onu file <onuid_list>	PON access to a node, upgrade the software ONU

5.3.2 Configuration case

Step	Command	Explain
Step 1	GFA6700(config)#save configuration Trying to save configuration to flash, please wait... Preparing data for saving configuration...Done. Starting writing configuration data to flash...Done. Configuration saved to flash successfully. GFA6700(config)#	Save ONU system configuration
Step 2	GFA6700(config)#interface vlan internet GFA6700 (vlan-internet)#add port 1/1 untagged GFA6700(vlan-internet)#ip address 192.168.7.126/24	OLT equipment configuration of a IP address to

	GFA6700 (vlan-internet)#exit GFA6700(config)#	the network and the FTP Server can communicate
Step 3	GFA6700(config)#ping 192.168.7.72 PING 192.168.7.72 : 56 data bytes. Press Ctrl-c to Stop. Reply from 192.168.7.72 : bytes=56: icmp_seq=0 ttl=128 time<=10 ms Reply from 192.168.7.72 : bytes=56: icmp_seq=1 ttl=128 time<=10 ms Reply from 192.168.7.72 : bytes=56: icmp_seq=2 ttl=128 time<=10 ms Reply from 192.168.7.72 : bytes=56: icmp_seq=3 ttl=128 time<=10 ms Reply from 192.168.7.72 : bytes=56: icmp_seq=4 ttl=128 time<=10 ms	OLT can be recognized and FTP Server (assuming it's IP is 192.168.7.72) normal communicatio-n
Step 4	GFA6700(config)#download ftp app 192.168.7.72 test aaaaaa GT811_A_app_V1R02B089.bin onu Get ftp operational popedom! Connecting to server: 192.168.7.72 Downloading file from server... Received size: f4e98 byte Download file ...ok Write to flash...ok Release ftp operational popedom!	Download new version of APP file to OLT

Step 5	GFA6700(config)#pon 7/4 GFA6700(epon-pon7/4)#update onu file 1-4	Into which the PON ONU to be upgraded node, upgrade the software ONU

6 ONU Management

6.1 ONU Remote Management

6.1.1 Create ONU remote management channel

For up to the OLT on each ONU, through the OAM, and the ONU terminal control module management channel established, centralized remote management. Establish a management channel, which can be configured on the ONU and management. Management channel established command: pty

Configuration step:

Step	Command	Explain
Step 1	GFA6700(config)#onu 7/4/1 GFA6700(epon-onu7/4/1)#	Enter one ONU node that want to be managed

Step 2	GFA6700(epon-onu7/4/1)#pty
	GROS(tm)
	Easypath Series ONU Software
		Create OAM managem

	Version 1.2(Build 089 on May 7 2010, 17:03:46) Copyright (c) GWTT Technology Limited. All Rights Reserved Running on Easypath GT811 Hardware GT811_A-7/4/1>enable GT811_A-7/4/1(config)#	ent channel to enter ONU managem ent
Step 3	 GT811_A-7/4/1(config)#quit Quit. Disconnected. Thanks for using GW Technologies product. Bye! GFA6700(epon-onu7/4/1)#	If you configure the end, the managem ent need to exit the ONU, the command quit, then quit to the OLT of the ONU node.

6.1.2 ONU Basic Management Information

View ONU online (registered) situation. Status marked as "up" means that the ONU-line; "down" means that the ONU registered, but currently offline, can not manage, the business also interrupt status; "powerDown" means that the ONU has been off the electricity.

GFA6700(config)#show onu-list

[TOTAL ONU COUNTER = 10]

Idx Mac addr type status Lastedtime userName

Pon(slot7)/port4 [Onu counter = 10]

1 000f.e903.4863 GT811_A up 0000:16:17:23 GT811A

2 000f.e903.b18e GT812_A up 0000:16:08:01 GT812A

3 000f.e903.af18 GT812_A up 0000:16:05:18 GT812A

4 000f.e903.4e87 GT812_A up 0000:16:08:01 GT812A

5 000f.e903.ade0 GT812_A up 0000:16:08:02 GT812A

6 000f.e903.da5b GT866 up 0000:16:08:02 GT866

7 000f.e903.4807 GT811_A down 0000:16:12:50 GT811_A

8 000f.e903.72fc GT811_A powerDown 0000:16:11:21 GT811

View on-line ONU:

GFA6700(config)# show online-onu

[TOTAL ONLINE ONU COUNTER = 6]

Idx Mac addr type running-time userName

Pon(slot7)/port4 [online onu counter = 6]

1	000f.e903.4863	GT811_A	0000:16:21:13	GT811A
2	000f.e903.b18e	GT812_A	0000:16:11:51	GT812A
3	000f.e903.af18	GT812_A	0000:16:09:07	GT812A
4	000f.e903.4e87	GT812_A	0000:16:11:51	GT812A
5	000f.e903.ade0	GT812_A	0000:16:11:51	GT812A
6	000f.e903.da5b	GT866	0000:16:11:51	GT866

View the system version information for all registered ONU and the current fiber distance:

GFA6700(config)#show onu-version

Idx	type	range	HW-version	SW-version	userName
7/4/1	GT811_A	60	V1.0B0	V1R02B089	GT811A
7/4/2	GT812_A	48	V1.0B0	V1R02B040	GT812A
7/4/3	GT812_A	60	V1.0B0	V1R02B073	GT812A
7/4/4	GT812_A	70	V1.0B0	V1R02B076	GT812A
7/4/5	GT812_A	51	V1.0B0	V1R02B073	GT812A
7/4/6	GT866	80	V1.0B0	V1R01B015 V1R01B027(VOICE)	GT866
7/4/7	GT811_A	N/A	V1.0B0	V1R02B089A	GT811_A
7/4/8	GT811_A	N/A	V1.0B0	V1R02B089A	

6.2 ONU Bandwidth Management

6.2.1 Default Bandwidth of ONU

6.2.1.1 Overview

The default bandwidth of ONU means configuration default bandwidth of all ONU, and this configuration is valid global Generally, it will use the default bandwidth allocation when the ONU registered for the first time.It can be a default bandwidth for all ONU unified configuration in order to simplify the configuration process,improve the efficiency of all allocation,convenient user operation.

The system default ONU downlink speed disable.For the default bandwidth configuration, the downlink bandwidth will not occupy the system bandwidth when ONU register and the downlink bandwidth don't speed disable.So it will not happen that the ONU can't register because the lack of the downlink bandwidth allocation.It will use the downlink assurance of the default bandwidth to ensure the registration and occupy the downlink bandwidth even the downlink speed disable close enable for the mechanism before the GFA6000 system.Maybe it will can't register due to the shortage of the downlink bandwidth,so please pay attention to distinguish.

Add function:Open the function of the ONU downlink bandwidth limit;Configure the downlink guarantee and maximum bandwidth of the default bandwidth to 0,it means it don't occupy the downlink bandwidth when ONU register and the downlink bandwidth don't limit ;While the default bandwidth downlink maximum bandwidth can be configured to any value except 0;ONU could occupy bandwidth dynamically as long as not exceed the maximum bandwidth.Morever the downlink speed limit enable can achieve PON levels,i.e.on a single PON opening the PON port downlink speed limit enable function.

There will be part of the ONU can't register becauset of the insufficient

bandwidth allocation if lots of ONU register.If the the bandwidth is not enough when configure the default bandwidth, then it will allocate the bandwidth according to the number of the regidtered ONU and the bandwidth allocation.The ONU will maintain the existing configuration for the short parts of bandwidth in order to ensure the normal use.The bandwidth allocation will be allotted one time when the ONU offline.The configuration is the current system default bandwidth configuration for the ONU that haven't configured the assigned bandwidth.And it uses the mechanism of occuping bandwidth to register,so the registered firstly ONU has the priority to grab the bandwidth.

Default bandwidth and traditional specified bandwidth allocation has a certain relationship.The specified bandwidth means configure one or more ONU alonely on the PON port.If some one has assigned the specified bandwidth, then it can't accept the default bandwidth allocation.Conversely,if the ONU is not configured to assign bandwidth,then the ONU will accept the system default bandwidth configuration.Another if the speficied bandwidth allocation and the default bandwidth allocation are same,then the seficied bandwidth allocation will be displayed independently in the show running-config in order to distinguish its using is the specified bandwidth allocation.

Note that ,ONU downlink speed limit is disable,so it will occupy the bandwidth of system according to its guaranteed bandwidth when ONU register.If the guaranteed bandwidth sum of the configuration of multiple ONU exceeds the bandwidth of the system,then it will prompts the shortage of the bandwidth and the configuration is not successful.

6.2.1.2The default configuration of default bandwidth

The downlink bandwidth dpeed limit of system enables, the default uplink and downlink guaranteed bandwidth and the default maximum bandwidth as shown in the following table:

Content	Default	Remark

	configuration	
Onu downlink-policer	disable	configure
Uplink assured-bw	15000	15M，configure
Uplink best-effort-bw	100000	100M，configure
Downlink assured-bw	15000	15M，configure
Downlink best-effort-bw	100000	100M，configure

6.2.1.3Default commands of bandwidth configuration

Using the bandwidth command to configure the uplink and downlink guaranteed bandwidth and the maximum bandwidth, and it also can view the default bandwidth configuration and cancel the default bandwidth configuration to resume the default value of default bandwidth.The command of configuration and related specificatiions as shown bellows:

Command	Specification
onu default-bandwidth uplink <64-1000000> <64-1000000> {downlink [0|<64-1000000>] [0|<64-1000000>]}*1	Configure default uolink and downlink guaranteed and maximum bandwidth
show onu default-bandwidth	View the default bandwidth configuration
undo onu default-bandwidth	Delete the default bandwidth configuration

6.2.1.4 Configuration case

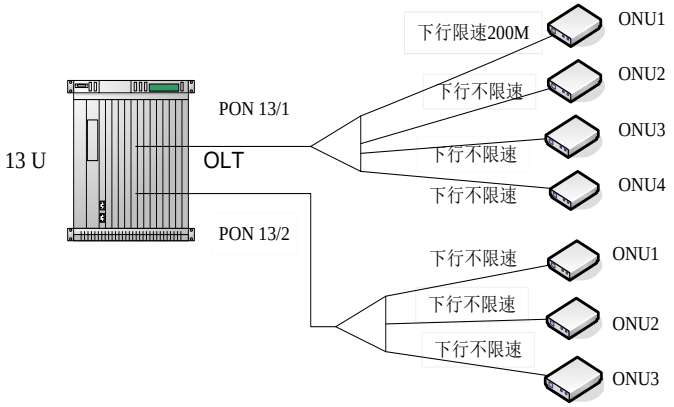
Case 1

According to the ONU downlink bandwidth limit in the practical

application,part of the ONU downlink rate-limit,the rest ONU don't rate-limit.Accordign to the relation of the specified bandwidth and default bandwidth,and the PON class ONU downlink rate-limit function of system,use the examples to descripte the configuration of bandwidth in the actual application.

Case description

Configure the bandwidth of PON port 13/1 ,priority to ensure the ONU1 downlink bandwidth 200M;ONU2-4 downlink bandwidth don't rate-limit,ONU1-3 of PON13/2 configured to no downlink rate-limit.The uplink bandwidth of PON 13/1 and 13/2 don't change,i.e to ensure the uplink 15M and the maximum 100M.



Configuration

Steps	Command	Specification
Step1	GFA6900(epon-pon13/1)# bandwidth class 2 delay low assured-bw 200000 best-effort-bw 200000 down 1	Configure downlink bandwidth 200M for the ONU under the PON 13/1

Step2	GFA6900(config)#onu default-bandwidth uplink 15000 100000 downlink 0 0	Configure the default bandwidth of system to uplink guarantee 15M,and the maximum is 100M,the downlink has no rate-limit
Step3	GFA6900(epon-pon13/1)# onu downlink-policer	PON 13/1 open the ONU downlink bandwidth rate-limit
Step4	GFA6900(epon-pon13/1)#show bandwidth logical-link 1	View the bandwidth configuration of ONU1 again
Step5	GFA6900(epon-pon13/1)#show bandwidth logical-link 2-4	View the bandwidth configuration of ONU2-4
Step6	GFA6900(epon-pon13/2)# show onu downlink-policer	View the ONU downlink bandwidth rate-limit

		enable under the PON 13/2

The result of configuration shows that the uplink guarantee is15M in the step6 to view the bandwidth configuration of ONU1,the maximum bandwidth is 100M,and the downlink bandwidth is 200M;the ONU has no downlink bandwidth rate-limit under the PON 13/2 in the step6

Note!

We can realize the single ONU downlink rate-limit for a PON port,and we can also realize ONU downlink rate-limit of PON class.We best first configure the bandwidth of the rest that don't need to rate-limit and single ONU downlink rate-limit bandwidth for the configuration of single ONU downlink bandwidth rate-limit under a PON port,open the downlink bandwidth rate-limit enable of ONU last.

The default downlink rate-limit enable of ONU in the system is closed, while for the default banwidth, the downlink bandwidth doesn't take part in the bandwidth allocation when ONU register.The default downlink guarantee bandwidth can configure exceed 1G bandwidth,i.e view bandwidth allocation corresponding to the allocated bandwidth more than 1G,but the activated bandwidth is No policer,so it can't affect the ONU's registration.

Note!

The default bandwidth configuration downlink when the system ONU downlinks rate-limit enable.0 0 indicates it doesn't occupy the bandwidth when ONU register.,the maximum bandwidth 0 indicates that downlink don't

rate-limit.While the default bandwidth configuration is downlink 0,200000M,it indicates that it don't occupy the bandwidth when ONU register,and the maximum bandwidth is dynamic,the maximum value is 200M.If the default bandwidth configuration is downlink 200000,200000 indicates it has occupies 200M bandwidth when ONU register,and the maximum bandwidth is 200M.

Case 2

The default bandwidth configuration exceed the bandwidth of system and the insufficient bandwidth can cause the failure of ONU's registration.The detailed introduction as follows.When the default bandwidth configuration exceed thebandwidth of system,it will configure the default bandwidth according to the registered ONU number and the bandwidth using circumstance for the registered ONU,and due to the insufficient bandwidth ,part of ONU will maintaine the original bandwidth configuration;Once the ONU under the PON port offline a time ,the default bandwidth send down a time ,and the bandwidth configurationof all the ONU become the current default bandwidth configuration of system ONU;It will use the preemptive registration bandwidth mechanism for registration if regiser once again,to grab the first registration;And the ONU will come into the Pending queue due to the insufficient bandwidth;If reprogramme the bandwidth of ONU rationally, when the bandwidth use normally, then the ONU can restore the registry; with the premise of the insufficient system bandwidth, new register a ONU, ONU registration failed.

Case description

Open the downlink rate-limit enable of system ONU,7 ONU registre at the same PON port ,the default bandwidth configuration is the uplink guaranteed 198M,the maximum 300M,the downlink guaranteed 100M,the maximum 300M.

Configuration

Steps	Command	Specification
Step1	GFA6900(config)# onu downlink-policer	Configure ONU downlink rate-limit enable in the global mode
Step2	GFA6900(config)#onu default-bandwidth uplink 198000 300000 downlink 100000 300000	Configure the default bandwidth：The uplink guaranteed 198M,the maximum 300M,the downlink guaranteed 100M,the maximum 300M.
Step3	GFA6900(config)#show onu default-bandwidth	View the default bandwidth configuration
Step4	GFA6900(epon-pon13/1)# show bandwidth	View the bandwidth allocation and the activation
Step5	GFA6900(epon-pon13/1)#show bandwidth	View the

	logical-link 1-7	bandwidth allocation of ONU

When the default bandwidth configuration exceeds the bandwidth of system, the series process of bandwidth configuration and the renew registration as shown follows:

1. **System has registered 7 ONU,the first 4 ONU are the default bandwidth and the rest maintane the original bandwidth configuration after the default bandwidth configuration.View the bandwidth configuration of ONU as shown follows:**

GFA6900(epon-pon13/1)#show bandwidth logical-link 1-7

OnuIdx direction class fixbw assured-bw(kbit/s) best-effort-bw(kbit/s)

1 Uplink 2 0 198000 300000

Downlink -- -- 100000 --

2 Uplink 2 0 198000 300000

Downlink -- -- 100000 --

3 Uplink 2 0 198000 300000

Downlink -- -- 100000 --

4 Uplink 2 0 198000 300000

Downlink -- -- 100000 --

5 Uplink 2 0 15000 100000

Downlink -- -- 15000 --

6 Uplink 2 0 15000 100000

Downlink -- -- 15000 --

7 Uplink 2 0 15000 100000

Downlink -- -- 15000 --

2. **Once the ONU under the PON port offline a time ,the default bandwidth send down a time ,and the bandwidth configurationof all the ONU become the current default bandwidth configuration of system,the bandwidth configuration of ONU shown as follows:**

GFA6900(epon-pon13/1)#show bandwidth logical-link 1-7

OnuIdx direction class fixbw assured-bw(kbit/s) best-effort-bw(kbit/s)

1 Uplink 2 0 198000 300000

Downlink -- -- 100000 --

2 Uplink 2 0 198000 300000

Downlink -- -- 100000 --

3 Uplink 2 0 198000 300000

Downlink -- -- 100000 --

4 Uplink 2 0 198000 300000

Downlink -- -- 100000 --

5 Uplink 2 0 198000 300000

Downlink -- -- 100000 --

6 Uplink 2 0 198000 300000

Downlink -- -- 100000 --

7 Uplink 2 0 198000

300000

Downlink -- -- 100000 --

3. **If the ONU register again, then there will two ONU can't register due to the insufficient bandwidth.The system will give the corresponding alarm information, and these ONU come into the pending queue.**

2011-06-13,21:42:13 GT831_B (13/1/7) register fail for bandwidth lack

2011-06-13,21:42:33 GT815(13/1/8) register fail for bandwidth lack

GFA6900(config)#show pending-onu

PON	LLID	macAddress	reason
13/1	2	000f.e904.b339	Reg_Failed
13/1	1	000f.e906.ee8f	Reg_Failed

View the current bandwidth allocation of PON port, and it has activated 990M uplink bandwidth

GFA6900(epon-pon13/1)#show bandwidth

4-EPN(slot13)/port1 bandwidth Info

max upstream bandwidth: 1000000Kbit/s

allocated upstream bandwidth: 1386000Kbit/s

(fixed bandwidth:0Kbit/s)

left upstream bandwidth: 0Kbit/s

Activated upstream bandwidth: 990000Kbit/s

max downstream bandwidth: 1000000Kbit/s

allocated downstream bandwidth: 700000Kbit/s

left downstream bandwidth: 300000Kbit/s

Activated downstream bandwidth: 500000Kbit/s

bandwidth allocation arithmetic: DBA

Another: With the premise of the insufficient system bandwidth, new register a ONU, ONU register failed.

The system configure the circumstance of default bandwidth, it needs

to use the default bandwidth configuration for the new registered ONU. It has activated uplink 990M bandwidth of the PON port in the upper system..The default bandwidth configuration is the uplink guaranteed 198M,the maximum 300M,the downlink guaranteed 100M,the maximum 300M.New register a ONU at this time,it will failed due to the insufficient bandwidth ,and the ONU will come into the Pending queue,as follows:

2011-06-13,21:56:49 onu13/1/3(13/1/3) register fail for bandwidth lack

GFA6900(config)#show pending-onu

PON	LLID	macAddress	reason
13/1	2	000f.e904.b339	Reg_Failed
13/1	1	000f.e906.ee8f	Reg_Failed
13/1	3	000f.e903.b0d7	Reg_Failed

Summary:If find the ONU register failed,please view the bandwidth using circumstance of PON port and whether exceed the bandwidth of system, if yes,please adjust the bandwidth allocation again,or adjust the number of ONU to ensure the normal registration of ONU.

6.2.2 ONU Bandwidth Configuration

Downstream direction, for each up to a PON ONU is under the support of the rate-limit and not limited to speed in two ways, by default is not limited to rate, open and close the PON link the rate-limiting function for ONU The command is:

onu downlink-policer //Open ONU downlink rate-limit of PON link

undo onu downlink-policer // Cancel ONU downlink rate-limit of PON link

When setting rate-limit, can use command to set different bandwidth:

bandwidth class <0-7> delay [high|low] {fixed-bw <0-1000000>}*1

assured-bw <64-1000000> best-effort-bw <64-1000000> [up|down] <onuid_list>

Configuration step:

Step	Command	Explain
Step 1	GFA6700(config)#onu downlink-policer	Open uplink/ downlink rate-limit of PON link
Step 2	GFA6700(config)#pon 7/4 GFA6700(epon-pon7/4)#bandwidth class 2 delay low assured-bw 35000 best-effort-bw 100000 down 1	Enter PON node, configure downlink bandwidth of ONU
Step 3	GFA6700(epon-pon7/4)#show bandwidth logical-link 1-10 OnuIdx direction class fixbw assured-bw(kbit/s) best-effort-bw(kbit/s) 1 Uplink 2 0 15000 100000 Downlink -- -- 35000 -- 2 Uplink 2 0 15000 100000 Downlink -- -- 15000 -- 3 Uplink 2 0 15000 100000	View downlink bandwidth of configured ONU

		Downlink	--	--		
	15000		--			
	4	Uplink	2	0		
	15000		100000			
		Downlink	--	--		
	15000		--			
	5	Uplink	2	0		
	15000		100000			
		Downlink	--	--		
	15000		--			
	6	Uplink	2	0		
	15000		100000			
		Downlink	--	--		
	15000		--			

Upstream direction, support dynamic allocation bandwidth allocation (DBA), does not support the way the static bandwidth allocation (SBA); By default, the uplink direction for each registered ONU bandwidth allocation to ensure 15Mbits, maximum bandwidth is 100Mbits:
Configuration step:

Step	Command	Explain
Step 1	GFA6700(config)#pon 7/4	Enter one PON node
Step 2	GFA6700(epon-pon7/4)#bandwidth class 2 delay low assured-bw 35000 best-effort-bw 100000 up 1	Configure ONU bandwidth

Step 3	GFA6700(epon-pon7/4)#show bandwidth logical-link 1-10 OnuIdx direction class fixbw assured-bw(kbit/s) best-effort-bw(kbit/s) 1 Uplink 2 0 35000 100000 Downlink -- -- 35000 -- 2 Uplink 2 0 15000 100000 Downlink -- -- 15000 -- 3 Uplink 2 0 15000 100000 Downlink -- -- 15000 -- 4 Uplink 2 0 15000 100000 Downlink -- -- 15000 -- 5 Uplink 2 0 15000 100000 Downlink -- -- 15000 -- 6 Uplink 2 0 15000 100000 Downlink -- -- 15000 --	View configured ONU uplink bandwidth

Note!

Minmal bandwidth increment is 64kbit/s

ONU's downstream bandwidth allocation for the command. Dynamic bandwidth allocation for downlink is not, so parameter "best-effort-bw" is not active, so there will be in the settings "Note: class, delay, best-effort-bw on the onu is inactive." Prompt. For the downlink bandwidth allocation, bandwidth size is the actual configuration parameters "assured-bw" behind the value

---

6.3 Registration and Cerftification of ONU

6.3.1 ONU registration in default

GT800 Series ONU following conditions are met by default, you can automatically register to the central office OLT equipment:

- ONU at the downstream optical power in the between-7dBm ~-24dBm
- ONU from the OLT to the fiber length can not exceed 20Km

6.3.2 ONU Certified Regisered

GFA6000 Series OLT ONU certification can open up ONU, in order to prevent illegal automatic registration to the central office OLT ONU equipment:

Command	Explain
onu-register authentication enable {[auth-all]}*1	Enable registration certificatio n function

	of ONU
add onu-register authentication entry <slot/port> <H.H.H>	Add one legal registration certificatio n table item of ONU
delete onu-register authentication entry <slot/port> {<H.H.H>}*1	Delete one legal registration certificatio n table item of ONU
show onu-register authentication enable	View whether registration certificatio n function of ONU is enabled
show onu-register authentication entry {<slot/port>}*1	View machine or a PON port has been added under the ONU

	registration certificate entries
undo onu-register authentication enable	Close registration certificatio n function of ONU

6.3.3 ONU Certified registered configuration case

Step	Command	Explain
Step 1	GFA6700(config)#onu-register authentication enable	Open authentica tion.For the registered ONU, will automatic ally be added to the certificatio n table. If you add the parameter s after auth-all, it has been registered

		as an illegal ONU ONU also be forced offline
Step 2	GFA6700(config)#add onu-register authentication entry 7/4 000f.e901.0203	The ONU (MAC address 000f.e901.0203) as a legitimate ONU to the PON 7 / 1 of the authentication table entry
Step 3	GFA6700(config)#show onu-register authentication entry pon 7/4 Authentication Onu table: 1 000f.e903.b18e 2 000f.e903.af18 3 000f.e903.4e87 4 000f.e903.ade0 5 000f.e903.da5b 6 000f.e901.0203	View certification registry key legal ONU

6.4 Automatic upgrade and configuration of ONU

6.4.1 Overview

Remote ONU EPON products in large quantities, widely distributed, diversified business features, management and maintenance of open and caused great difficulty, repeat the configuration data in particular great effort. Using FTP mode Ethernet services by the ONU through the channel automatically downloaded via FTP way to get the configuration file and automatically update the local configuration or software. This approach not only to achieve a flexible and automatic configuration features, but also can be extended to remote configuration data backup and pre-configuration.

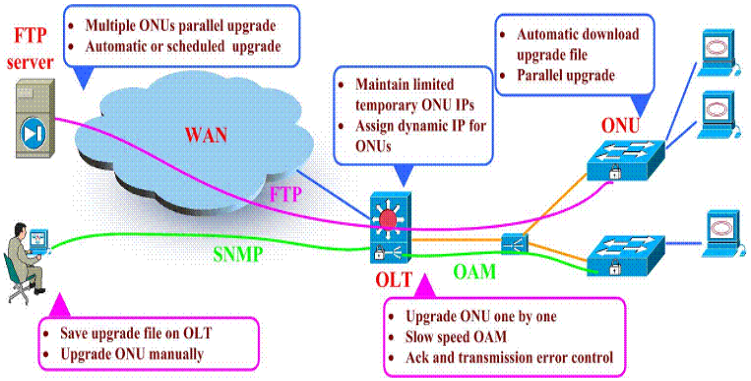


Figure 2-2 ONU automatic upgrade and configuration Schematic

It can be seen from Figure 2-2, in the use of this feature to deploy a FTP server, FTP client and ONU as FTP Server automatically take the appropriate file (version of the software / configuration files).

6.4.2 ONU Automatic upgrade/configuration deploy of ONU

Configure FTP Server / assigned IP address pool to use FTP Client:

Command	Explain

auto-load ftpserver <A.B.C.D> <ftpservername> <password> {[ftpport]<1-65535>}*1	Specify FTP server's IP address, user name, password, and application port (default 21)
auto-load client-ip <A.B.C.D/M> gateway <A.B.C.D> vid <1-4094>	Configured to use FTP Client IP address pool, you can configure up to 5
undo auto-load ftpserver undo auto-load client-ip <A.B.C.D/M>	Delete FTP Server configuration information Delete FTP Client configuration information
show auto-load client-information show auto-load ftpserver	View FTP Server and Client configuration information

show auto-load onu [waiting-config|configing|configed|config-failure|config-abort] show auto-load onu [waiting-upgrade|upgrading|upgraded|upgrade-failure|upgrade-abort]	View ONU upgrades or configuration state list

ONU automatic upgrade commands:

Command	Explain
auto-load upgrade pon <slotId/port> {<onuid_list>}*1	Under the ONU based on a PON to determine the scope of ONU to be upgraded
auto-load upgrade type [<onu_type>|all-onu]	Based on a type of ONU ONU to determine the scope to be upgraded
auto-load upgrade-file <onu_type> [boot|app|fw|voip|fpga] <ver>	Set the type to be upgrading the software version information ONU

auto-load upgrade {[start-time] <start_time>}*1 {[end-time] <end_time>}*1	Configuration and automatically update the time automatically end
auto-load upgrade	Immediately trigger the upgrade process to manually configure
auto-load upgrade stop	Manual configuration to stop the upgrade process
undo auto-load upgrade-file <onu_type> {[boot|app|fw|voip|fpga]}*1	ONU type set to delete the upgrade file version information
show auto-load upgrade-file	View set to upgrade file information
show auto-load	View a summary of the information function

	deployment

ONU automatic configuration related commands:

Command	Explain
auto-load config <slotId/port> {[onu] <onuid_list>}*1 {[direction] [server2onu|onu2server]}*1 {[filename] <namestring>}*1	ONU upload or download configuration settings range, direction and configuration file name
auto-load config start	Enable automatic configuration function
auto-load config stop	Disable automatic configuration function

6.4.3 ONU automatic upgrade/configuration case

6.4.3.1 Case 1

Plan to August 20, 2010 03:00:00 for a type of OLT ONU under all GT812_A upgrade the software version to V1R02B089.

Configuration step

Step	Command	Explain
Step 1	GFA6700(config)#show system time YYYY-MM-DD HH:MM:SS 2010-08-16 13:33:50	Verify that the system time is correct. If the system time is not correct, correct system configuration time
Step 2	GFA6700(config)#interface vlan v4094 4094 GFA6700(vlan-v4094)#add port 1/1 untagged GFA6700(vlan-v4094)#add port 7/1-4,8/1-4 tagged GFA6700(vlan-v4094)#exit	In the OLT is configured VLAN, to ensure that through this VLAN, ONU communication can FTP Server
Step 3	GFA6700(config)#auto-load ftpserver 192.168.2.72 test 123456 ftpport 21	Set software version stored in the FTP Server's IP address and user name, password
Step 4	GFA6700(config)#auto-load client-ip 192.168.2.100/24 gateway 192.168.2.254 vid 4094 GFA6700(config)#auto-load client-ip 192.168.2.101/24 gateway	Configure FTP Client terminal (ONU) can use IP address pool, and set to

	192.168.2.254 vid 4094 GFA6700(config)#auto-load client-ip 192.168.2.102/24 gateway 192.168.2.254 vid 4094 GFA6700(config)#auto-load client-ip 192.168.2.103/24 gateway 192.168.2.254 vid 4094 GFA6700(config)#auto-load client-ip 192.168.2.104/24 gateway 192.168.2.254 vid 4094	communicate VLAN. Can be set up to 5 IP addresses. ONU to be upgraded all the upgrade will automatically create a temporary VLAN, VID is the command to set the VID. ONU upgrade is complete, ONU will automatically delete this temporary set in the VLAN on the ONU
Step 5	GFA6700(config)#auto-load upgrade-file GT812_A app V1R02B089	ONU configuration GT812_A type version of the software upgrade
Step 6	GFA6700(config)#auto-load upgrade type GT812_A	Set all GT812_A need to be upgraded

Step 7	GFA6700(config)#auto-load upgrade start-time 2010-08-20,03:00:00	Set automatic updates started. If the latter without end-time parameter, the default counting from the start time, stop automatically after 24 hours
Step 8	GFA6700(config)#auto-load upgrade stop	After all to be upgraded, in order to prevent misuse, turn off the automatic update feature

6.4.3.2 Case 2

Plan to August 20, 2010 03:00:00 for a OLT's PON7 / 4 under all ONU, including GT811_A, GT812_A. Upgrade the software version, respectively, to V1R02B084, V1R02B089.

Configuration step:

Step	Command	Explain

Step 1	GFA6700(config)#show system time YYYY-MM-DD HH:MM:SS 2010-08-16 13:33:50	Verify that the system time is correct. If the system time is not correct, correct system configuration time
Step 2	GFA6700(config)#interface vlan v4094 4094 GFA6700(vlan-v4094)#add port 1/1 untagged GFA6700(vlan-v4094)#add port 7/1-4,8/1-4 tagged GFA6700(vlan-v4094)#exit	In the OLT is configured VLAN, to ensure that through this VLAN, ONU communication can FTP Server
Step 3	GFA6700(config)#auto-load ftpserver 192.168.2.72 test 123456 ftpport 21	Set software version stored in the FTP Server's IP address and user name, password
Step 4	GFA6700(config)#auto-load client-ip 192.168.2.100/24 gateway 192.168.2.254 vid 4094 GFA6700(config)#auto-load client-ip 192.168.2.101/24 gateway 192.168.2.254 vid 4094 GFA6700(config)#auto-load client-ip	Configure FTP Client terminal (ONU) can use IP address pool, and set to communicate VLAN. Can be

	192.168.2.102/24 gateway 192.168.2.254 vid 4094 GFA6700(config)#auto-load client-ip 192.168.2.103/24 gateway 192.168.2.254 vid 4094 GFA6700(config)#auto-load client-ip 192.168.2.104/24 gateway 192.168.2.254 vid 4094	set up to 5 IP addresses. ONU to be upgraded all the upgrade will automatically create a temporary VLAN, VID is the command to set the VID. ONU upgrade is complete, ONU will automatically delete this temporary set in the VLAN on the ONU
Step 5	GFA6700(config)#auto-load upgrade-file GT812_A app V1R02B089 GFA6700(config)#auto-load upgrade-file GT811_A app V1R02B084	The type of configuration GT812_A and GT811_A software upgrade version of the ONU
Step 6	GFA6700(config)# auto-load upgrade pon 7/1	Set PON 7 / 1, all you need to upgrade ONU

Step 7	GFA6700(config)#auto-load upgrade start-time 2010-08-20,03:00:00	Set automatic updates started. If the latter without end-time parameter, the default counting from the start time, stop automatically after 24 hours
Step 8	GFA6700(config)#auto-load upgrade stop	After all to be upgraded, in order to prevent misuse, turn off the automatic update feature

6.4.3.3 Case 3

Batch at a time plan to deploy more than one installation of the new ONU (GT811_A), connected to the fiber, the automatic registration to the new PON port unused 7 / 1, 7 / 2, and auto-complete data configuration, the opening of user services, Automatic completion of ONU deployment. (Use this function on the premise that the deployment of these ONU configuration in the data is completely consistent)

Configuration step:

Step	Command	Explain
Step 1	The data will be GT811_A configuration file template named after GT811_A_CONFIG.txt, placed on FTP Server	
Step 2	GFA6700(config)#interface vlan v4094 4094 GFA6700(vlan-v4094)#add port 1/1 untagged GFA6700(vlan-v4094)#add port 7/1-4,8/1-4 tagged GFA6700(vlan-v4094)#exit	In the OLT is configured VLAN, to ensure that through this VLAN, ONU communication can FTP Server
Step 3	GFA6700(config)#auto-load ftpserver 192.168.2.72 test 123456 ftpport 21	Set software version stored in the FTP Server's IP address and user name, password
Step 4	GFA6700(config)#auto-load client-ip 192.168.2.100/24 gateway 192.168.2.254 vid 4094 GFA6700(config)#auto-load client-ip 192.168.2.101/24 gateway 192.168.2.254 vid 4094 GFA6700(config)#auto-load client-ip 192.168.2.102/24 gateway 192.168.2.254 vid 4094	Configure FTP Client terminal (ONU) can use IP address pool, and set to communicate VLAN. Can be set up to 5 IP addresses.

	GFA6700(config)#auto-load client-ip 192.168.2.103/24 gateway 192.168.2.254 vid 4094 GFA6700(config)#auto-load client-ip 192.168.2.104/24 gateway 192.168.2.254 vid 4094	ONU all be configured in the configuration will automatically create a temporary VLAN, VID is the command to set the VID. After the upgrade is complete ONU, ONU will automatically delete this temporary set in the VLAN on the ONU
Step 5	GFA6700(config)#auto-load config 7/1 direction server2onu filename GT811_A_CONFIG.txt GFA6700(config)#auto-load config 7/2 direction server2onu filename GT811_A_CONFIG.txt	ONU with the upgrade to set the scope and data configuration file name
Step 6	GFA6700(config)#auto-load config start	Manually set the auto-configuration feature is turned on.

		Auto-configuration feature can only be manually turned off
Step 7	GFA6700(config)# auto-load config stop	Data configuration files are automatically configured, in order to prevent misuse, manually turn off the feature

Note!

- In order to prevent errors caused by misoperation upgrades, misconfigurations, after each use functions, to close the function.
- When using the automatic upgrade, if you set the range, use the command auto-load upgrade pon <slotId/port> {<onuid_list>} * 1 only configure parameters <slotId/port>, not followed by configuration parameters <onuid_list>, At this time all of the following will be the PON ONU ONU are as dealing with the upgrade. That is, if a new ONU to get up to the PON port, will automatically initiate the upgrade ONU.
- When using the automatic configuration, and as described above.

6.5 P2P Access control

6.5.1 ONU isolation and interworking at the same PON port

P2P access control is under the same PON ONU ports between the access control: isolation or exchange.

In default, under the same PON ONU between port isolation. Access control list on P2P configuration, you can make configuration exchange between the ONU and other ONU.

Command	Explain
onu p2p <onuid_list> <onuid_list>	Cofigure P2P interworking ONU list
onu p2p <onuid_list> forward address-not-found [enable|disable]	ONU is configured to open interoperability between P2P unknown unicast forwarding, if the configuration ONU exchange, they must turn the feature
show onu p2p <onuid_list>	View P2P interworking ONU list

undo onu p2p <onuid_list> <onuid_list>	Delete P2P interworking ONU list

6.5.2 Isolation and interworking between different PON ports

In default, the difference is isolated between PON, EPON system can not communicate directly. PON filter list can be configured to implement different PON port, the EPON system in direct communication.

Command	Explain
filter <filtername> in_port <slot/port> out_portlist <portlist> permit	Configure PON filter list
show filter [all|<filtername>]	View current configured PON filter list
show filter port <slot/port>	View the current configuration of a PON port which corresponds to the exchange port
undo filter <filtername>	Delete one PON filter list

6.6 Configuration file of ONU（ONU pre configuration）

6.6.1 Overview

In comparison with the data form of ordinary ONU, this function provides

method of ONU configuration by using file, and it makes the configuration data of ONU stored in the OLT unity.The OLT will alot its configuration file to this ONU when it registered in line.

6.6.1.1Types of configuration file

- **Shared Configuration File**

It means multiple ONU shared using the configuration file.There is a special shared configuration and it's a onuconfdef,it is an empty configuration file.The first registered ONU will be associated to this configuration file defaultly if it not specified the associated configuration in advance.The actual implementation of the effect is do not any configuration operations to the ONU.

- **Private Configuration File**

It's the configuration file that can be used by a single ONU.The private configuration file is named by onuid and its name always like ONUX/X/X.They are all created by the system and unable to manually create.

For the private configuration file,it can't create private configuration file if the ONU is not onlie,i.e. it can't use private configuration file to achieve the pre configuration of ONU

6.6.1.2Using of a configuration file

The steps of configuring ONU by using the configuration file:

1）Firstly,create a configuration file on the OLT

2）The configuration file will automatically issued and applied to these ONU when they are associated with the configuration file.

What we needs to pay attentaion is the saved command of ONU's and OLT's configuration file are associated with each other.So remember to execute a save command under the config port after every revision. This command will save the content of configuration file of ONU, and it also will save it to the OLT.

It will realize the function of batch configurations when multiple ONU

share the same configuration file.And it can realize pre configuration of ONU by configuring associated configuration file of ONU in advance.

6.6.2 Comman of configuration file

6.6.2.1 Command Transmission（The open and close of ONU's configuration file ）

Command	Specification
OLT(config)#onu transmission-flag [enable|disable]	Open / closed ONU command transmission function. System default open command line transmission function.

 Notice!

Directly configure on the ONU port ,not using configuration file if open command line transmission.But if the function of comman line transmission is closed then using the configuration file to configure.

6.6.2.2 Create/Edit configuration of ONU

Command	Specification

OLT(config)#config onu-profile <name>	If the file not exists then create a shared configuration file;But if it exists then edit it.
OLT(config)# ONU <slot/pon/onuid>	When the state of the command transmission is disable,then into the ONU port to create or edit a private configuration file for this ONU

6.6.2.3 Associate with the configuration file of ONU

Command	Specification
OLT(config)#onu-profile associate <slot/port> <onuid_list> <name>	Associated with a configuration file to a / some ONU. under a PON

OLT(epon-pon10/2)#onu-profile associate <onuid_list> <name>	Associated with the this PON port to the relation between some ONU and the configuration

The configuration of the configuration file will be alloted to the ONU after execute some related association.The original ONU memory configuration is cleared, updated for the configuration file configuration.

6.6.2.4Display the lists of ONU configuration files

Command	Specification
OLT(config)# show onu-profile list {counter}*1	Not with counter parmeter,shows the system lists information of configuration files,including the serial number 、file name 、file attributes and whether it is being used. With counter parmeter,show

	s the number of configuration file in the system
OLT(config)# show onu-profile name <name>	Shows the ONU information that associated with some configuration file,including onuid 、 mac address and show-name
OLT(config)# show onu-profile onu <x/x/x>	Shows the configuration file information that associated with some ONU,including onuid 、 the name of associtsed configuration file 、 file attribute、ONU mac address and the

	show-name.
OLT(epon-onu10/2/2)#show profile	Shows configuration file information of this ONU
OLT(config)# show onu-profile pon [all|<slot/port>] [all|<onuid_list>]	Shows the configuration file information that associated with some or all ONU under some or all PON port ,including onuid 、 the name of associtsed configuration file 、 file attribute、ONU mac address and the show-name.
OLT(epon-pon10/2)#show onu-profile list	Shows the configuration file information that associated

	with all ONU under this PON port

6.6.2.5 Display data content of ONU configuration file

Command	Specificatio
OLT(config)# show onu-profile text <name>	Show configuration content of some configuration file
onu-profile(test)#show profile To display the OLT stored in the configuration file and related information	Show configuration content of some configuration file at this configuration port

6.6.2.6 Display the saved configuration file informationand related information in the OLT

Command	Specification
OLT(config)# show onu-profile startup	Show the saved configuration file information and related

	information in the OLT,including the saved configuration file、content of the file and th related information associated with the ONU.

6.6.2.7 Copy the content of ONU configuration file

Command	Specification
OLT(config)#onu-profile copy <soure> <destination>	Copy the configuration content of the source file to the destination file

 Notice!

- This command requires the existence of the destination file,if not exists,the it needs to create a destination to execute the copy operation.
- This copy command only copies the contents of the configuration file not the attributes.

6.6.2.8 Migration the association of the ONU configuration file

Command	Specification
OLT(config)#onu-profile switch <slot/pon> <slot/pon>	Migrate the association from the source PON port to the destination PON, the first parmeter specifies the source port and the second parmeter specifies destination port.

Rules about the migration of ONU configuration file on the PON port:

The association relation of the source PON port is constant. The ONU id after the migration is the previous registered id for the ONU that once registered on the destination PON port. But for the ONU that never register on the destination PON port, the transfer id is allotted orderly by the id according to the id number that register on the source PON from the first available id on the destination PON port. The association relation between the ONU and the configuration file and the MAC information are also transferred.

For the ONU that associate with the shared configuration file, they also associate with this shared file after transfer. But for the ONU that

associate with the private configuration file, the system will create automatically a private configuration file named by the transferred ONU id after the transfer. And also copy the source private configuration file to the new private configuration file.

6.6.2.9 Lift the association of ONU configuration file

Command	Specification
OLT(config)#undo onu-profile associate <name>	Lift association between some configuration file with all ONU,lift the default associataion betweeb the ONU with the onuconfedf files
OLT(config)# undo onu-profile associate <slot/port> <onuid_list>	Lift association between soconfiguratio n file with some ONU,lift the default associataion betweeb the ONU with the onuconfedf files

6.6.2.10 Delete ONU configuration file

Command	Specification
OLT(config)#delete onu-profile name <name>	Delete some configuration file that have no association,if the file also exists association then it's not allowed to delete.
OLT(config)# delete onu-profile all-disused	Delete all configuration files that not associate with ONU

6.6.2.11Backup and restore the information of ONU configuration file

Command	Specification
OLT(config)#upload ftp [onu-profile] <A.B.C.D> <user> <pass> <filename>	Backup the stored configuration files and the association information to the server

OLT(config)# download ftp [onu-profile] <A.B.C.D> <user> <pass> <filename>	Restore the configuration files and the association information to the OLT from the server.

6.6.3 Configuration case

6.6.3.1 Case 1

Case description:

Register GT811(ONUID from 1~10,20~30) and GT812ONUID from 11~19,31~39) under the PON (6/3) of a OLT.The configuration mode is 1~3 port's VLAN is 100,port 4's VLAN is 200 for GT811; while the configuration mode is 1~7 port's VLAN is 100,port 8's VLAN is 200 for GT812

In this case, we can use ONU configure files way to create two shared configuration files on the OLT, GT811_CONIFG and GT812_CONIFG, and it's convenient for the management and maintance.

Configuration steps:

Step	Command	Specification
Step1	OLT(config)#onu transmission-flag disable	Close the command transmission function(equals to open ONU configuration function)

Step2	OLT(config)#config onu-profile GT811_CONFIG	Create shared configuration files of GT811_CONIFG
Step3	onu-profile(GT811_CONFIG)#vlan dot1q_add 100 onu-profile(GT811_CONFIG)#vlan dot1q_port_add 100 1-3 1 onu-profile(GT811_CONFIG)#vlan dot1q_add 200 onu-profile(GT811_CONFIG)#vlan dot1q_port_add 200 4 1 onu-profile(GT811_CONFIG)#exit	Configure specifical data content:port 1~3 locate VLAN 100,untag way;port 4 locate VLAN 200,untage way
Step4	OLT(config)#onu-profile associate 6/3 1~10 GT811_CONFIG OLT(config)#onu-profile associate 6/3 20~30 GT811_CONFIG	Make the configuration of GT811_CONIFG and ONUID to 1~10,20~30 relevance application
Step5	OLT(config)#config onu-profile GT812_CONFIG	Create shared configuration files of GT812_CONIFG
Step6	onu-profile(GT812_CONFIG)#vlan dot1q_add 100 onu-profile(GT812_CONFIG)#vlan	Configure specifical data content:port

	dot1q_port_add 100 1-7 1 onu-profile(GT812_CONFIG)#vlan dot1q_add 200 onu-profile(GT812_CONFIG)#vlan dot1q_port_add 200 8 1 onu-profile(GT812_CONFIG)#exit	1~7 locate VLAN 100,untag way;port 8 locate VLAN 200,untage way
Step7	OLT(config)#onu-profile associate 6/3 11~19 GT811_CONFIG OLT(config)#onu-profile associate 6/3 31~39 GT811_CONFIG	Make the configuration of GT812_CONIFG and ONUID to 11~19,31~39 relevance application
Step8	OLT(config)#save	Save the configurations after the modification

6.6.3.2 Case 2

Case description

Plan to deploy to open ONU1~32 of PON PORT 6/3,and the configuration of ONU1~31is exactly the same,all ports are in the VLAN 100.While the ONU32 is slightly different,port1~3 are in the VLAN 100,port 4 is in the VLAN 200.It's hoped to ONU pre-deploy,so it's only need to connect with the optical fiber and register on the ONT.The configuration data of ONU is configured in advance on the OLT by the ONU configuration files function.Because the configuration files of ONU is correlated to the ONU by the ONU,it's best to subscribe the ONUID

after register on the OLT for the ONU 32.Through the ONU equipment MAC address bind with the ONUID on the OLT.If the MAC address of ONU32 is 000F E901 0101,for ONU 1~31 use the CONFIG_1 configuration file and use CONFIG_2 for ONU32.

Configuration steps

Step	Comand	Specification
Step1	OLT(config)#onu transmission-flag disable	Close the command transmission function(equals to open ONU configuration function)
Step2	OLT(epon-pon6/3)#add onu 32 000f.e901.0101	Bind the ONU to ONUID 32 by the MAC address of ONU32
Step3	OLT(config)#config onu-profile CONFIG_1	Create shared configuration file CONFIG_1
Step4	onu-profile(GT811_CONFIG)#vlan dot1q_add 100 onu-profile(GT811_CONFIG)#vlan dot1q_port_add 100 1-4 1 onu-profile(GT812_CONFIG)#exit	Configure specifical data content:port 1~4 locate VLAN 100,untag way

Step5	OLT(config)#onu-profile associate 6/3 1～31 CONFIG_1	Make the configuration of CONIFG_1 and 1~31 ONUID relevance application
Step6	OLT(config)#config onu-profile CONFIG_1	Create shared configuration files CONFIG_2
Step7	onu-profile(GT811_CONFIG)#vlan dot1q_add 100 onu-profile(GT811_CONFIG)#vlan dot1q_port_add 100 1-3 1 onu-profile(GT811_CONFIG)#vlan dot1q_add 200 onu-profile(GT811_CONFIG)#vlan dot1q_port_add 200 4 1 onu-profile(GT812_CONFIG)#exit	
Step8	OLT(config)#onu-profile associate 6/3 32 CONFIG_1	Make the configuration of CONIFG_2 and 32 ONUID relevance application
Step9	OLT(config)#save	Save the configurations after the modification

After the above configuration steps,ensure that there is no ONU register on the PON 6/3 port,I.e the ONUID 1~32 are not occupied,only need connect each ONU to fiber and register on the OLT ,then all configuration is effective.

6.6.3.3 Case 3

Case description

If a ONU (6/3/1) under PON port 6/3 has failure,then it needs a new ONU to replace the faulty equipment.And still use CONFIG_1,the configuration file of the original fault ONU

Configuration steps

Step	Command	Specification
Step1	OLT(config)#show onu-profile onu 6/3/1 Pon6/3: onuid name share mac addr device name 1 CONFIG_1 yes 0011.2233.4405 GT811_C	View the associated sharing configuration files of the fault ONU
Step2	GFA6900(config)#pon 6/3 GFA6900(epon-pon6/3)#add onu 33 000f.e907.704d GFA6900(epon-pon6/3)#exit	Add registration information of new ONU,bind it to a unused ONUID.
Step3	OLT(config)#onu-profile associate 6/3 33 CONFIG_1	Associate the shared configuration files with the new ONU

Step4	OLT(config)#save	Save the configurations after the modification

6.6.3.4 Case 4

Case description

If some ONU has faults,then it needs to register to the other PON port for this ONU.There are two circumastaces for using the file transfer command to transfer the registration information and association information of configuration to the new pon port:

1） If the transfered ONU never registered on the new pon port,then according to the original registration id order to register.And the association of ONU and the mac information are also transfered .If it is a shared configuration file before the transfer,then it will also associate with this shared configuration file after the transfer .If the associated file of ONU is the private configuration file,then create a onux./x/x file of the new pon port,and copy the configuration content to the new file.Examples are as follows:

Step	Command	Specification
Step1	OLT(config)#show onu-profile pon 10/2 1-4 pon10/2: Onuid name share mac addr device name 1 test yes 000f.e903.c992 GT811_A 2 onu10/2/2 no 0011.2233.4405 GT811_C 3 test yes 000f.e907.704d	View the association information of fault PON port.

	GT811_C 4 onuconfdef yes ffff.ffff.ffff	
Step2	OLT(config)#show onu-profile pon 10/3 1-4 pon10/3: onuid name share mac addr device name 1 onuconfdef yes 000f.e903.7995 2 onuconfdef yes ffff.ffff.ffff 3 onuconfdef yes ffff.ffff.ffff 4 onuconfdef yes ffff.ffff.ffff	View and change the registration information of PON port,and find that there is no registration information on the pon port for the ONU of fault port
Step3	OLT(config)#onu-profile switch 10/2 10/3	Use the migration command to migrate the association information of default PON port to the replaced pon port
Step4	OLT(config)#show onu-profile pon 10/3 1-4 pon10/3: onuid name share mac addr device name 1 onuconfdef yes 000f.e903.7995	View the onu registration information and the association information of

	2 test yes 000f.e903.c992 3 onu10/3/3 no 0011.2233.4405 4 test yes 000f.e907.704d	the replaced PON port
Step5	OLT(config)#save	Save the configurations after the modification

2） If some transfered ONU once registered on the new pon port,then according to the original registration id to register,and these not registered ONU register in accordance with the new registration id.The transfer rules of the shared and private files are the same ,examples are as follows:

Step	Command	Specification
Step1	OLT(config)#show onu-profile pon 10/2 1-3 pon10/2: onuid name share mac addr device name 1 test yes 000f.e903.c992 GT811_A 2 onu10/2/2 no 0011.2233.4405 GT811_C 3 test yes 000f.e907.704d GT811_C	View the association information of the fault PON port
Step2	OLT(config)#show onu-profile pon 10/4 1-3 pon10/4: onuid name share mac addr device name	View and change the registration information of PON port,and

	1 onuconfdef yes 000f.e907.704d GT811_C 2 onuconfdef yes ffff.ffff.ffff 3 onuconfdef yes ffff.ffff.ffff	find that there is registration information on the pon port for the ONU of fault port
Step3	OLT(config)#onu-profile switch 10/2 10/4	Use the migration command to migrate the association information of default PON port to the replaced pon port
Step4	OLT(config)#show onu-profile pon 10/4 1-3 pon10/4: onuid name share mac addr device name 1 test yes 000f.e907.704d GT811_C 2 test yes 000f.e903.c992 3 onu10/4/3 no 0011.2233.4405	View the onu registration and t association information of the replaced PON port
Step5	OLT(config)#save	Save the configurations after the modification

Finally, all onu under the fault pon port are physical transferred to the

new PON port, issued to ONU after correct configuration.

Note!

For the PON port transfer function,it's recommended to set the transfer command first ,then physical transfer the onu.Otherwise,there will be some problems.

---

7 Protection function

7.1 PON trunk optical fiber protection

GFA6000 Series OLT support the CTC / ITU G.983.5 Class B definition of fiber protection, OLT optical transceiver modules can fail or break the case of trunk optical fiber PON network quickly recover business functions to improve the PON network reliability and survivability.

7.1.1 PON trunk optical fiber protection principle

The PON network configuration of class B protection as shown below.Redundant OLT ports、redundant trunk optical fiber to achieve the fiber protection.

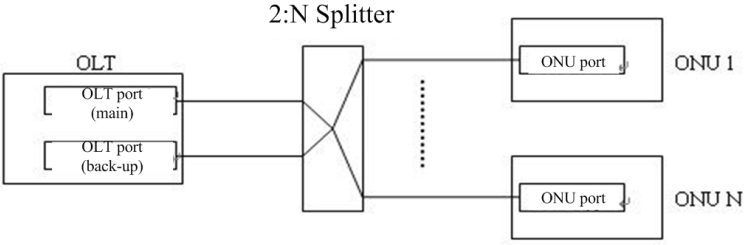


Figure2-3 Class B optical fiber protection

Each OLT of the PON port can only belong to a protected group. By

default, PON does not belong to any protected group. In GFA6000 Series OLT equipment, with the board from time to time between any two inter-board PON ports can form a protection group.

PON port for protection switching of the trigger conditions are the following:

- PON fiber link port failure or malfunction, such as optical signal loss, etc
- Use the command or the network management operation, forced switching, etc

7.1.2 PON trunk optical fiber protection configuration

Make the same protection group of the two PON must meet the followings conditions:

- Standby PON ports not install and register any ONU equipment
- Main and standby PON ports are all up status
- Make a backup PON port, we can not directly configure the operating

Configuration commands:

Command	Explain
auto-protect pon <slot/port> partner <slot/port>	PON protection on or off, and the two PON port set to a protection group
undo auto-protect pon <slot/port>	Close protection function
show auto-protect {pon <slot/port>}*1	Show PON port protection status and related information

7.2 Backup protection of Main control board

EsayPath GFA6000 Series OLT can support the control board of the backup protection, thus further improving system reliability. In slot3 and slot4 control board installed by default slot3 the control board in the active state, slot4 the control board is in standby state. System is in standby state board to synchronize automatically every 1 hour in the active state board data configuration, so that the two board configuration files in sync, and save configuration command each time you run the two boards will also synchronize the configuration file.

Command	Explain
sync-file [sw-app|sw-boot|pon-firm|pon-dba|onu-app|cfg-data|tdm-config|ctc-config|sysfile]	The file manually synchronize the two plates
switchover	Manually switch the state of the two boards

7.3 PON protectionof double OLT

7.3.1 Overview

Cross OLT equipment PON protection switchingfunction can be realized by configuring PON protection switching of two or multiple OLT equipments and realize cross equipment optical path protection function of two PON port.

The core idea of realizing cross OLT equipment is to consider the remote device as a logic slot of the OLT equipment, and the PON port of the remote device as a logic port of the logic slot.So we can use

“logical slot number/logic port number” to refer to a PON port of remote device in this OLT device, and with the PON port of the local “physical slot/physical port” configure to cross optical path protection pairs of equipment.

Two OLT equipments need to establish a UDP connection, use the IP address and port number as the device address (the default service port: 22222).To ensure the security of remote access, we can configure authentication mode (enabled default authentication) when the connection of crossing OLT device is created.It’s not allowed to create the connection with the local OLT device if not pass the authentication.Whether the connection is required for the authentication,it can be configured according to the actual needs of users.

A OLT device can support 4 logical slot at most, i.e. can configure cross OLT devices PON protection with up to 4 OLT devices at the same time.Each logical slot support 16 logical ports at most,and the system supports 64 logical port at most,i.e. can configure cross OLT devices PON protection with up to 64 OLT devices.

The switching time is about 1-2s of crossing OLT device PON protection switching when use the command switching.When use fiber switching, the time is 3s of configuring PON switching,and the real switching time is about 4-5s.

It can realize the cross OLT equipment PON protection switching in the same type device or different types devices in GFA6900, GFA76700 and GFA6100 three devices.

7.3.2 Configuration commands

7.3.2.1 Configure equipment PON protection switching across OLT

Command	Specification

OLT(config)#auto-protect pon <slot/port> partner <gslot/gport> mode [sensitive|slowness]	Configure PON protection mode between devices
OLT(config)# force-switching pon <gslot/gport>	Use commands to realize the PON protection switching between devices

7.3.2.2 Configure logic slot service

Command	Specification
OLT(config)# logical-slot service [enable|disable]	Configure logic slot service enable/close
OLT(config)#logical-slot service port <0-65535>	Configure port number of logic slot service
OLT(config)#undo logical-slot service port	Cancle the port number configuration of logic slot service,restore the default value 22222

OLT(config)# logical-slot service auth [enable|disable]	Configure logic slot service authentication enable/close
OLT(config)#show logical-slot service	View the configuration of logic slot service

7.3.2.3 Configure logic slot and port number

Command	Specification
OLT(config)# logical-slot <65-68>	Enter into a logical slot configuration node
OLT(config-logical-slot65)#device name	Configure the label of 65 logical slot
OLT(config-logical-slot65)#device ip <A.B.C.D> {port <0-65535>}*1	Configure the IP address and port number for the careation need of the pon protection between the logical slot 65 and remote OLT device

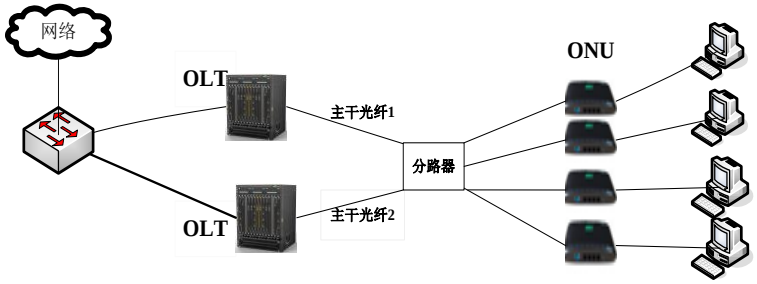
OLT(config-logical-slot65)#device user <username>	Configure the username of authentication
OLT(config-logical-slot65)#device password <password>	Configure the password of authentication
OLT(config-logical-slot65)#logical-port <1-16>	Enter into the logical slot configuration node
OLT(config-logical-slot65)#delete logical-port <1-16>	Delete the logical port
OLT(config-logical-slot65)#show logical-port {<1-16>}*1	View the configuration of the logical port
OLT(config-logical-port65/1)#device port <rslot/rport>	Configure the actual PON port of OLT device that corresponding to the logical port 65/1 port

7.3.3 Configuration case

Case description

Two GFA6900 equipments ,respectively marked 6900_1、6900_2.The requipment is making the PON3/1 of 6900_1 and the PON4/1 of 6900_2 to be optical path protection each other.Cretation of the connection need to a one-way authentication, i.e the remote device connects to thelocal OLT device needs to authenticate, and the

username of authentication is test and the password is 123456.The local device connects to the remote device does not requires authentication.The logical slot serivceport number for two OLT connection is respectively:remote device connect to this local OLT is using the 32005 port number;this local device connect to the remote device is using the 43006 port number.The two OLT manage the vlan by using the default vlan,and the data forwarding VLAN is using the VLAN 100.



Configuration steps:

It needs to configure cross OLT device PON protection switching on the two OLT devices. If 6900_1 IS the local OLT device and 6900_2 is the remote device,then the corresponding configuration steps on the local OLT device and the remote device are as shown following：

Configuration of remote device in the local OLT device that cross OLT device PON protection switching as shown bellows:

Step	Command	Specification
Step1	GFA6900(vlan-default)#ip address 192.168.2.145/24	Configure management IP address of OLT

Step2	GFA6900(config)#interface vlan v100 100 GFA6900(vlan-v100)#a port 3/1 tagged GFA6900(vlan-v100)#a port 14/1 untagged	Create VLAN V100, add PON port and uplink port
Step3	GFA6900(config)#auto-protect pon 3/1 partner 65/1 mode slowness	Configure cross OLT device PON protection switching ,use the logical port 65/1
Step4	GFA6900(config)# logical-slot service enable	Configure logical slot service enable,the default is disable
Step5	GFA6900(config)#logical-slot service port 32005	Configure port 32005
Step6	GFA6900(config)#user add test login-password 123456	Configure the username and password of remote device connect to the authentication
Step7	GFA6900(config)#show logical-slot service	View the enable,port number and authentication configuration

		of logical slot service
Step8	GFA6900(config-logical-slot65)#device ip 192.168.2.90 port 43006	Configure the end IP address and port number
Step9	GFA6900(config-logical-slot65)#logical-port 1	Enter into the 65/1 logical port configuration node
Step10	GFA6900(config-logical-port65/1)#device port 4/1	Configure remote OLT PON port corresponding to the 65/1 port

Configuration of remote device that cross OLT device PON protection switching as shown bellows:

Step	Command	Specification
Step1	GFA6900(vlan-default)#ip address 192.168.2.90/24	Configure management IP address of OLT
Step2	GFA6900(config)#interface vlan v100 100 GFA6900(vlan-v100)#a port 4/1 tagged GFA6900(vlan-v100)#a port 1/1 untagged	Create VLAN V100, add PON port and uplink port

Step3	GFA6900(config)# logical-slot service enable	Configure logical slot service enable,the default is disable
Step4	GFA6900(config)#logical-slot service port 43006	Configure port 43006
Step5	GFA6900(config)#logical-slot service auth disable	Configure authentication close,the default is autheitication enable
Step6	GFA6900(config)#show logical-slot service	View the enable,port number and authentication configuration of logical slot service
Step7	GFA6900(config-logical-slot65)#device ip 192.168.2.145 port 32005	Configure the end IP address and port number
Step8	GFA6900(config-logical-slot65)#device user test GFA6900(config-logical-slot65)#device password 123456	Configure the username and password of remote device connect to the

		authentication

8 Configure SNTP

8.1 Overview of SNTP

Simple Network Time Protocol SNTP (Simple Network Time Protocol) is the Network Time Protocol (NTP), a simplified version. NTP protocol is applied to the clock synchronization of devices on the Internet. In the case that not needs to implement full functional of NTP, then you can use SNTP. It has the same functiona with the NTP, but easier than it. SNTP client / server operating mode, either in unicast mode (point to point), the operation can also be in the broadcast mode (point to multipoint) operating.It's good for the management and maintance if running the SNTP protocol in the network devices.

Working mode of SNTP：

SNTP protocol in the maintenance of network equipment of the time when there are three different modes:

- **Unicast**

Client sent to the designated server that contains the local time of the request message, the server returns a response message, response message containing the server receives a client request packets of the time and server response packets sent. The client receives the server response packet by packet contains a variety of time value, the packet can be calculated and the local device cycle time value and time value of the deviation of the server.

- **Multicast**

Server periodically broadcasts its time value. The client receives the broadcast packet; modify the value of their time repair, and the server broadcast messages to the time value of the same.

■ **Unicast/multicast（Anycast）**

When the client does not know the address of time server used in this way that the client sent to the specified network multicast or broadcast request message, the network server after receiving the broadcast request message, all the way to unicast response to the client, but the client only receives the first response packet received, and record the address of this server, after which the client and the server will work in unicast mode.

Prompt:

- Unicast mode for the switch as a SNTP client and SNTP server, the Internet communication between.
- Prompted multicast mode and unicast / multicast mode (Anycast) for SNTP communication between the two switches, one of which as a SNTP client, another as an SNTP server

---

8.2 Configuration of SNTP

Command	Specification
GFA6700(config)#sntp-server disable GFA6700(config)#sntp-server enable	Open or close SNTP server
GFA6700(config)#sntp-server mode {[unicast]}*1 {[multicast] subnet <A.B.C.D/M>}*1 {[anycast] subnet <A.B.C.D/M>}*1	Configure working mode of SNTP server
GFA6700(config)#sntp-server update-interval <16-1024>	When the SNTP server operating in multicast mode (Multicast)

	next, the server to a certain period in the specified time, the network broadcast their values. Configure SNTP server broadcast cycle
GFA6700(config)#sntp-client disable GFA6700(config)#sntp-client enable	Open or close SNTP client
GFA6700(config)#sntp-client mode [anycast] subnet <A.B.C.D/M> GFA6700(config)#sntp-client mode [unicast|multicast] server ipaddr <A.B.C.D>	Configure working mode of the SNTP client
GFA6700(config)#sntp-client update-interval <16-1024>	When the client work in the unicast / multicast mode (Anycast) or unicast mode (Unicast) under, you need to configure the client refresh period of time,

	that is how often configure the client to the server sends a request message time。
GFA6700(config)#show sntp-client GFA6700(config)#show sntp-server	View SNTP configuration information

8.3 Configuration case

Unicast mode (Unicast) for the switch to the Internet in the SNTP SNTP client or server communications; If SNTP communication between two switches, one of which is the client, the other is the server, select Multicast Mode (Multicast) or unicast / multicast mode (Anycast). If SNTP communication between two switches, one switch of the SNTP mode for multicast mode (Multicast), another switch must also be configured for multicast mode (Multicast); when the switch as a SNTP client mode for the unicast / multicast mode (Anycast) t, as a SNTP server mode switch can be unicast mode (Unicast), it can be unicast / multicast mode (Anycast).

Two GFA6700 below to be an example, introduce the configuration and application methods of SNTP protocol.

GFA6700-1 as a SNTP Server, IP address is 192.168.2.100, GFA6700-2 as the SNTP Client:

Configuration steps:

Step	Command	Explain

Step 1	GFA6700-1(config)# sntp-server mode multicast subnet 192.168.2.100/24	Configure working mode of GFA6700-1 server
Step 2	GFA6700-1(config)# sntp-server enable	Enable SNTP server of GFA6700-1
Step 3	GFA6700-2(config)#sntp-client mode multicast server ipaddr 192.168.2.100	Configure working mode of GFA6700-2 client
Step 4	GFA6700-2(config)# sntp-client enable	Enable SNTP client of GFA6700-2
Step 5	GFA6700-2(config)# sntp-client update-interval 200	In order to adapt to different accuracy requirements, but also can modify the client's time refresh rate

3 Port Configuration

1 Configure Ethernet Port

All the parameters of the optical port can't be configured apart from the negotiation parameter.Power port working in the auto-negotiation mode for the default configuration.The interface speed、duplex mode and flow control mode are negotiated by the switch and the to end device.The users also can configure them, but it should to ban the auto-negotiation of the interface before change these configurations.

 **Note!**

Only open the communication device interfaces which interconnected each other at the same time can ensure get the correct protocol result

---

1.1 Default configuration

The default setting information on the Ethernet interfaces as shown in the following table:

Table3-1The default configuration information of the Ethernet interface

Content	Default setting	Remark
Encapsulation	DIX	
MTU	Depend on the binded interface	

Auto-negotiation	enable	
Duplex	Full -duplex	
Flowcontrol	Disable	
Hardware	Ethernet	
MAC address	Equipment MAC	
Max speed	1000M	
Accesslimit	disable	Can’t change the settings
Layer2 interface	Enable	Can’t change the sttings
Interface admin state	admin up	Can change the settings

1.2 Basic configuration of Ethernet interface

Command	Explain

GFA6700(config)# interface ethernet <slot/port>	Enter to port node
GFA6700(if-eth1/1)# auto [enable|disable]	Open/close port autonegotiation
GFA6700(if-eth1/1)# description <string> {<string>}*29	Configure description information of port
GFA6700(if-eth1/1)# duplex [full|half]	Configure half-duplex/full-duplex mode for port
GFA6700(if-eth1/1)# flowcontrol [enable|disable]	Configure traffic control open/close of port
GFA6700(if-eth1/1)# learning [enable|disable]	Configure the port MAC address learning on / off, on by default
GFA6700(if-eth1/1)# speed [10|100|1000]	Configure port rate
GFA6700(if-eth1/1)# shutdown GFA6700(if-eth1/1)# undo shutdown	Close/open port
GFA6700(if-eth1/1)# show interface ethernet {<portlist>}*1	View port basic configuration information

1.3 Port mirroring

GROS support port mirroring, mirror all the data packets of the specifiedport to the another configuration port to facilitate the diagnostic errors

Configuration case

Need to port 1 / 3 of the upstream and downstream data are mirrored to 1 / 4 port.

Cofiguration step:

Step	Command	Explain
Step 1	GFA6700(config)#interface ethernet 1/4	Enter node of port 1/4
Step 2	GFA6700(if-eth1/4)#mirror ingress 1/3 egress 1/3	Configure port 1 / 3 of the upstream and downstream data are mirrored to 1 / 4
Step 3	GFA6700(config)#show mirror	Exit to the config node, view the port mirroring configuration
Step 4	GFA6700(if-eth1/4)#undo mirror	When not mirroring

		feature, the feature off

2 Configure Trunk port

2.1 Over of Trunk

Trunk is bound to multiple physical ports together as a logical port, also known as multi-port load-balancing group (Load Sharing Group). Trunk only used between the connections of the switches for the purpose of enhancing the communication bandwidth Trunk bundled user profiles specified port, the switch port configuration based on user decision packet routing strategy (Packet) is sent to from a member of the port on the side of the switch. When the switch detects that a member of the port link down, it will not continue to send packets at this port until the link of the interruptted port back to normal. When two or more of a switch port to simultaneously send data to the adjacent switch, the creation Trunk can greatly improve the transmission speed.

Default configuration information:

Default configuration information on the Trunk shown in the following table:

Table 3-2 Trunk default configuration information

Content	Default configuration	Remard
MTU	1500	Set can be changed
Hardware	Ethernet	Set can’t be changed

MAC address	Switch MAC	Set can't be changed
Policy	srcdstmac-based	Set can be changed
VLAN name	Default	Set can't be changed
Interface admin state	admin up	Set can be changed

2.2 Configure Trunk

Command	Explain
interface trunk < trunkname >	Create a TRUNK port, and into the trunk port node
grouping <portlist>	The specified port as a trunk port binding
policy [srcmac-based|dstmac-based|srcdstmac-based]	Configure the routing strategy Trunk Port
show interface trunk {<trunkname>}*1	Show TRUNK information

In TRUNK configuration mode, you can cancel the configuration using

the undo policy strategy; use undo grouping is bound to remove the Ethernet port; use the undo shutdown interface management can be restored to the default admin up state of the state.

 **Note！Each Trunk follows the following rules:**

- Members of the port must be in the same slot of the module.
- Members of the port must have the same type (Gigabit power port, Gigabit optical port, Fast electrical interface, etc.) and rate.
- Members of the port must operate in full duplex mode.
- Each trunk can bind up to 8 ports.
- Trunk in the user profile, the user's input must meet the above principles, if you do not meet the.
- The above principles, it will prompt the user configuration error

---

2.3 Configuration case

Description of case

Case One：

Create a Trunk, tied the port 1, 2, 3 of slot 1 and named uplink 1.Make the Trunk group joine d to the VLAN 100 in the way of TAG and joined to the VLAN 4094 by untag .The port routing strategy is based on the source and destination MAC address.

Steps of configuration：

Step	Command	Specification
Step1	GFA6700(config)#interface trunk uplink1	Create a trunk named uplink1

Step2	GFA6700(config)#vlan 100 trunk uplink1 tagged GFA6700(config)#vlan 4094 trunk uplink1 untagged	The empty trunk join to all the VLAN port to ensure the consistency with the port
Step3	GFA6700(trunk-uplink1)# grouping 1/1-3	Binding port 1,2 and 3 on the slot 1
Step4	GFA6700 (trunk-uplink1)# policy srcdstmac-based	Specifies the strategy
Step5	EPON_V2R1(trunk-uplink1)#show Interface Trunk uplink1 is down. Physical status is down, administrator status is up. MTU 1500 bytes. Max speed 3000 M, current speed 0 M, Bandwidth 0 Kbit. Srcdstmac-based Policy. Trunk ID is 0. Be added into vlan(s): Vlan name:vlanAuto100, vlan ID:100 Vlan name:vlanAuto4094, vlan ID:4094 Port member list: eth1/1 eth1/2 eth1/3	Show configuration information of trunk

	Interface eth1/1 is down. Physical status is down, administrator status is up. MTU 1500 bytes. Port type is 1000BASE-SX. UrTypeName is SFP. Loopback mode is None-Loopback. AutoNegotiation enabled. DIX encapsulation. Ingress Discard disable. Egress Discard disable. Duplex full. FlowControl disabled. Hardware is ethernet. Max speed 1000 M, current speed 1000 M, Bandwidth 1000000 Kbits. Accesslimit disabled.	

Case Two:

Add/delete port number for the existing Trunk group.This trunk group has already included port1/1-2 and it's in normal using,then add1/3 port .

Steps of configuration：

Step	Command	Specification
Step1	GFA6700(config)#interface trunk uplink1	Enter into the trunk configuration node

Step2	GFA6700(trunk-uplink1)# grouping 1/3	Add the 1/3 port to the Trunk Group
Step3	GFA6700 (trunk-uplink1)# policy srcdstmac-based	Specifies the strategy
Step4	EPON_V2R1(trunk-uplink1)#show Interface Trunk uplink1 is down. Physical status is down, administrator status is up. MTU 1500 bytes. Max speed 3000 M, current speed 0 M, Bandwidth 0 Kbit. Srcdstmac-based Policy. Trunk ID is 0. Be added into vlan(s): Vlan name:vlanAuto100, vlan ID:100 Vlan name:vlanAuto4094, vlan ID:4094 Port member list: eth1/1 eth1/2 eth1/3 Interface eth1/1 is down. Physical status is down, administrator status is up. MTU 1500 bytes. Port type is 1000BASE-SX. UrTypeName is SFP. Loopback mode is None-Loopback. AutoNegotiation enabled. DIX encapsulation.	Show configuration information of trunk

	Ingress Discard disable. Egress Discard disable. Duplex full. FlowControl disabled. Hardware is ethernet. Max speed 1000 M, current speed 1000 M, Bandwidth 1000000 Kbits. Accesslimit disabled.	

Notice！The present network Trunk configuration

- Trunk firstly join to the VLAN, then grouping,it will reduce the service interruption time.
- The configuration of Trunk and VLAN such as tag and untag should be kept consistent strictly with port ,to ensure the remote operation service can't be interrupted
- The modified trunk refer to VLAN，but the number disposable should not excess 200,keep the remote operation is not interrupted.

2.4 Fault analysis

Phenomanon	OLT can't execute remote management after the grouping port
Analysis	All the undefault vlan at the port will first deleted ,then associate with all the vlan of the trunk.But it's should insure that the vlan which make the trunk joined and the previous port are consistent completely,so please notice the management of VLAN especially!

Reslove	If the service of management interrupts, it should be configure d by the console port.But if the management is normal ,and only some services are interrupted,plese check whether the configurations of port and the trunk in this VLAN are consistent.

4 VLAN configuration

Virtual LAN (VKAN) can be a physical local area network divided into many sub logical sense, without having to consider the specific physical location, each VLAN can correspond to a logical unit, such as department, workshops and project group and so on. Within the same VLAN as the transfer of data between hosts will not affect the other hosts on the VLAN, thus reducing the possibility of data exchange, greatly enhanced network security.

In a physical LAN, the switch port through the division of the LAN equipment is divided into several independent groups, group internal communications between devices can be free, and when the different groups of equipment to conduct communication, must be three routes forward; this way as a physical LAN to be divided into several isolated local area network, these different groups is called a virtual LAN (VLAN). For VLAN by port, any port in the collection (or even all ports on the switch) can be viewed as a VLAN. VLAN classification is not the physical connection hardware limitations, the user can command the flexibility to divide the port, create a defined VLAN. VLAN can be used to help control traffic, provide greater security, make changes and mobile network equipment is more convenient.

1 Configure VLAN

Note!

Should be integrated planning across the network name the VLAN. 2, the use of 802.1Q tagged packets may lead to packet length than the existing IEEE 802.3 / Ethernet frame is 1518 the maximum number of bytes a little larger, which may lead to other devices in the packet count errors, so in the presence of non- 802.1Q bridges or routers in the network connections may cause problems.

1.1 VLAN mode

EsayPath support VLAN mode 3: 802.1Q, qinq mode (stack) and pass-through mode. Default mode is the 802.1Q (dot1q).

Command	Explain
GFA6700(config)#vlanmode [dot1q|transparent|stack]	Configure VLAN mode
GFA6700(config)#show vlanmode	View current configured VLAN mode information

1.2 VLAN configuration based on port

Creating Port-based VLAN, and configure the IP address.

Command	Explain

interface vlan <vlanname> {<1-4094>}*1	Create a VLAN, and enter into the VLAN interface node
[add|delete] port <portlist> [tagged|untagged] [add|delete] trunk <trunkname> [tagged|untagged]	Eth port or trunk port will be added to the VLAN, or remove from the VLAN in
ip address <A.B.C.D/M>	Configure one IP address on VLAN port
show interface vlan {[count]}*1 {[port-based]}*1 {<name>}*1	Show VLAN information

In the VLAN port configuration mode, use the undo shutdown interface management can be restored to the default admin up state of the state

1.3 Bath configuration of VLAN

Command	Explain
vlan <vlanlist> {port <portlist> [tagged|untagged]}*1 vlan <vlanlist> {trunk <trunkname> [tagged|untagged]}*1	Create a VLAN, and the appropriate ports to the VLAN in

For the bulk created VLAN, the VLAN name is a specific format, the system automatically generated and can not be modified. Name prefix is vlanAuto, followed vid, for example vlanAuto100.

2 Configuration case

2.1 Case 1（Batch configure VLAN1000～VLAN2000）

Configuration data in the business, often encounter a large number of VLAN configuration of the business situation. For example, the need to follow each ONU port (user) or on a per ONU to divide VLAN, so you need to configure 2-3000 VLAN. This volume can be used to establish the time of the method to reduce the workload VLAN. Suppose you need to pon port 6 / 1 of the user, based on the division of each ONU port VLAN, this requires the establishment of the OLT 1000 to 2000 VLAN. The uplink service port is 1 / 1.

Step	Command	Explain
Step 1	GFA6700(config)#vlan 1000-2000 port 1/1 tagged	Create vlan1000 ~ vlan2000, and port 1 / 1 to the VLAN in
Step 2	GFA6700(config)#vlan 1000-2000 port 6/1 tagged	The port 6 / 1 is also added to the VLAN in
Step 3	GFA6700(config)# show interface vlan	View VLAN configuration

2.2 Case2（Configure VLAN Trunk Link）

In practice, OLT's need to receive an uplink port aggregation switch in the middle with TRUNK LINK connection, host multiple VLAN services.

In GFA6000 Series OLT, the only way to this port to tagged VLAN of these can be added to.

Step	Command	Explain
Step 1	GFA6700(config)#vlan 1000-2000 port 1/1 tagged	Create vlan1000 ~ vlan2000, and port 1 / 1 to add to the VLAN tagged in
Step 2	GFA6700(config)#vlan 1000-2000 port 6/1 tagged	The port 6 / 1 is also added to the VLAN in
Step 3	GFA6700(config)# show interface vlan	View VLAN configuration

5 Multicast configuration

1 Overview of IGMP Snooping（Proxy）

IP Multicast is a network layer multicast, study its original meaning is to reduce the IP packet to the transmission of the address do not need it. However, the second floor of the exchange in the general lack of network layer with IP Multicast IGMP protocol layer interaction

management protocol, multicast packets and broadcast packets are indiscriminately broadcast to all ports, resulted in the loss of multicast in mind. IGMP Snooping is born to resolve this contradiction. The switch supports IGMP Snooping IGMP packets can read and parse out the port from multicast group membership information with the information switch to multicast group members to build their own tables, so that only the host to the group members to forward multicast packets, and The host did not join the group will not receive their unwanted messages. IGMP Snooping violation of the hierarchical principle, it provides a flexible tool to solve the problem. IGMP Snooping can avoid the use of multicast traffic in the VLAN in the broadcast, according to the port forwarding necessary to accurately.

In GFA6000 Series OLT and ONU on the GT800 series, respectively, using the IGMP Proxy and IGMP snooping in two ways.

IGMP Snooping is relatively simple; it is through listening between the client and the router side of IGMP packets, so in the establishment of a multicast for multicast table entry. Include the multicast address, physical port and VLAN mapping.

IGMP Proxy is blocked by the user and IGMP packets between routers to establish multicast table, Proxy device uplink ports perform the role of the host, the second line port the role of the implementation of the router.

- Downlink port the role of the implementation of the router, IGMP V2 in full accordance with the mechanism specified in the implementation, including inquiries by the election mechanism to regularly send a general query information, receive a packet to send out a specific query.
- uplink ports perform the role of the host in response to a query from the router, when the new user group or a group of the last user exits, take the initiative to send members of the reporting package or leave package

2 Configure IGMP Proxy of OLT

2.1 Default configuration information

The default settings on the IGMP Snooping information such as the following table

Table 5-1 IGMP Proxy default configuration information of OLT

Content	Default set	Remark
Enable/disable	disable	Set can be changed
Survival time of the multicast group	250s	Set can be changed
Member query interval	125s	The default setting is recommended
Robustness parameter	2	The default setting is recommended

2.2 Configuration commands

Command	Explain
igmp-snooping [enable|disable]	Open or close igmp proxy
igmp-snooping grouplife [<10-1000>|default]	Set aging time of multicast group
igmp-snooping queryinterval [<10-300>|default]	Set the query interval
igmp-snooping responsetime [<10-25>|default]	After receiving query message to set the response

	time
igmp-snooping robust [<1-100>|default]	Set robust parameter
igmp-snooping [add|del] group <vlanname> <A.B.C.D>	Configured to add or remove a static multicast group
igmp-snooping [add|del] member <vlanname> <A.B.C.D> <portlist>	Configured to add or remove a static multicast group member port
igmp-snooping deldyngroup <vlan> [<A.B.C.D>|all]	Delete the dynamic multicast group
show igmp-snooping show igmp-snooping groupcount show igmp-snooping grouplife show igmp-snooping hosttimeout show igmp-snooping queryinterval show igmp-snooping responsetime show igmp-snooping robust	IGMP query some configuration information

3 Configure IGMP Snooping of ONU

3.1 Configuration commands

Manage the ONU through PTY, go to the config node. Management commands as basic and OLT side

Command	Explain
igmp-snooping [enable|disable]	Open or close igmp proxy
igmp-snooping grouplife [<10-1000>|default]	Aet aging time of multicast group
igmp-snooping queryinterval [<10-300>|default]	Set the query interval
igmp-snooping responsetime [<10-25>|default]	After receiving query message to set the response time
igmp-snooping robust [<1-100>|default]	Set robust parameter
igmp-snooping max-group <0-256>	Set number of multicast groups to establish the maximum
igmp-snooping [add|del] group <vlanname> <A.B.C.D>	Configured to add or remove a static multicast group

igmp-snooping [add|del] member <vlanname> <A.B.C.D> <portlist>	Configured to add or remove a static multicast group member port
igmp-snooping deldyngroup <vlan> [<A.B.C.D>|all]	Delete the dynamic multicast group
show igmp-snooping show igmp-snooping groupcount show igmp-snooping grouplife show igmp-snooping hosttimeout show igmp-snooping queryinterval show igmp-snooping responsetime show igmp-snooping robust	IGMP query some configuration information

4 Cross VLAN multicast function

Standard IGMP Snooping feature is only available within the same VLAN multicast function, while most carriers use the current port users by way 802.1qVLAN isolation and location, so the implementation of the multicast, the user is usually in a different VLAN being, if this time also using the standard IGMP Snooping, VLAN causes each to be established within a multicast stream, and ultimately unable to achieve the effect of network bandwidth savings. Cross-VLAN multicast technology can be a good solution to this problem.

Command	Explain

igmp-snooping-tvm [enable|disable]	Open or close cross VLAN multicast function
igmp-snooping-tvm add <A.B.C.D> <A.B.C.D> <1-4094>	Add VLAN and multicast group IP address mapping table entries
igmp-snooping-tvm del <1-4094> igmp-snooping-tvm del <A.B.C.D> <A.B.C.D> igmp-snooping-tvm del all	Delete mapping items
igmp-snooping-tvm sync-interval [<10-120>|default]	OLT and ONU configuration Multicast configuration between the cross-VLAN OAM synchronization time. This parameter is not recommended to modify, you can keep the default value
show igmp-snooping-tvm {<1-4094>}*1	View the current configuration of the mapping table entry information

show igmp-snooping-tvm sync-interval	View inter-VLAN multicast configuration OAM configuration synchronization time

5 Multicast authentication

System also supports two multicast authentication methods for a user-based MAC address authentication, hereinafter referred to as MAC authentication or authentication method BMA; the other is based ONU port authentication, hereinafter referred to as BPA port authentication method or authentication method. Both authentication modes should to provide different authentication information. Multicast authentication information is configured to concentrate in the OLT.

Command	Explain
igmp-snooping auth [enable|disable]	Open or close multicast authentication

5.1 MAC authentication method

BMA authentication required authentication information: ONU's ID, where the user connects the ONU port VLAN ID, multicast group address, the user device MAC address.

Command	Explain
igmp-auth-gw <slotId/port/onuId> <1-4094> <H.H.H.H> <H.H.H> <1-4094>	Adding multicast MAC authentication authentication information entry
igmp-auth-gw status <slotId/port/onuId> <1-4094> <H.H.H.H> <H.H.H> <authstatus>	Set multicast authentication information state
igmp-auth-gw delete all	Delete all entries authentication information
undo igmp-auth-gw <slotId/port/onuId> <1-4094> <H.H.H.H> <H.H.H>	Delete an authentication information entry
show igmp-auth-gw	View the current configuration of the multicast authentication information entry

5.2 Port authentication method

BPA authentication credentials required to: ONU's ID, the user takes the ONU port number, multicast group address

Command	Explain
igmp-auth <slotId/port/onuId> <1-24> <H.H.H.H> <1-3> <1-4094>	Add user port multicast authentication authentication information entry
igmp-auth status <slotId/port/onuId> <1-24> <H.H.H.H> <level> {[preview-time|preview-interval|preview-counter|used-counter] <set_value>}*1	Set multicast authentication information state
igmp-auth delete all	Delete all entries authentication information
undo igmp-auth <slotId/port/onuId> <1-24> <H.H.H.H>	Delete an authentication information entry
show igmp-auth	View the current configuration of the

	multicast authentication information entry

6 Configuration case

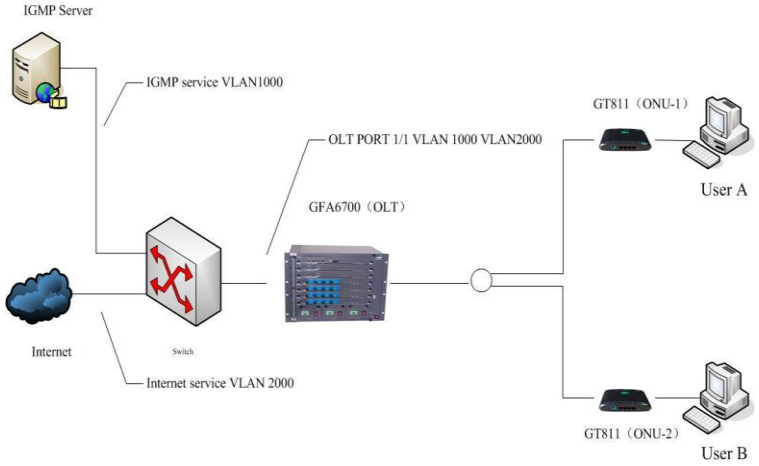
For the simple case of just carrying the multicast service to both sides of the OLT and ONU IGMP Snooping (Proxy) feature can be enabled.

Step	Command	Explain
Step 1	GFA6700(config)# igmp-snooping enable	
Step 2	PTY administered by ONU, ONU side of the same command to enable IGMP Snooping	

6.1 Case 1 (Cross VLAN multicast)

Multicast server deployment in the VLAN 1000, Internet access services in the VLAN 2000; User A and User B respectively, and ONU2 received ONU1 port 1, VLAN 2000; and User A and User B has a multicast service. In this case, we need a function of inter-VLAN multicast.

Figure 5-1 Cross VLAN multicast topology



Configuration step:

Step	Command	Explain
Step 1	GFA6700(config)#igmp-snooping enable	Enable IGMP Snooping（Proxy）function of OLT
Step 2	GFA6700(config)#igmp-snooping-tvm enable	Enable cross VLAN multicast function
Step 3	GFA6700(config)#igmp-snooping-tvm add 224.1.1.1 224.1.1.1 2000 GFA6700(config)#igmp-snooping-tvm add 225.1.1.1 225.1.1.1 2000	Add mapping items
Step 4	GFA6700(config)#interface vlan v1000 1000 GFA6700(vlan-v1000)#add port 1/1,6/1 tagged	Establish multicast service VLAN 1000 VLAN 2000 and

	GFA6700(config)#interface vlan v2000 2000 GFA6700(vlan-v1000)#add port 1/1,6/1 tagged	internet service
Step 5	GT811-6/1/1(config)#igmp-snooping enable	Enable IGMP Snooping function of ONU1
Step 6	GT811-6/1/1 (config)#interface vlan v1000 1000 GT811-6/1/1 (vlan-v1000)#add port 1/1,6/1 tagged	In ONU1 VLAN can be established on Internet business, without the need to establish the multicast service VLAN
Step 7	GFA6700(config)#show igmp-snooping IGMP snooping is enable. IGMP snooping auth is disable. IGMP snooping multivlan translation is disable. VLAN group type router member v2000 224.1.1.1 (D) 6/1(d) v2000 225.1.1.1 (D) 6/1(d)	Exit to the OLT's config node View the multicast forwarding

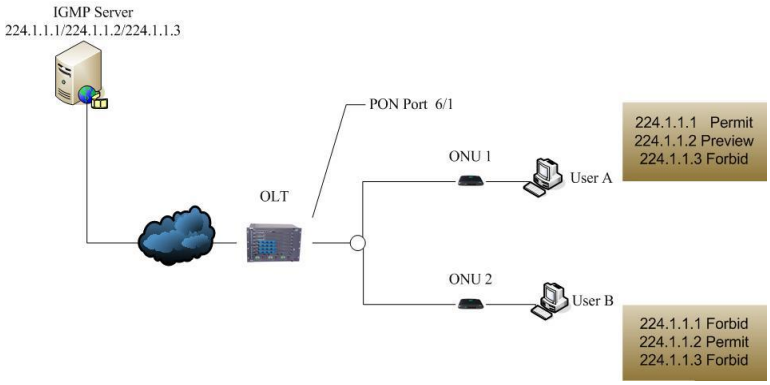
Step 8	GT811-6/1/1(config)#show igmp-snooping-tvm igmp-snooping tvm is enabled No. GroupStart GroupEnd IVid ---------- 1 224.1.1.1 224.1.1.1 2000 2 225.1.1.1 225.1.1.1 2000	View from the OLT to the ONU over the map on the synchronization

6.2 Case 2 (Multicast authentication)

Two users User A and User B. User A can broadcast a program 224.1.1.1 permission (Permit), for programs 224.1.1.2 there is a preview (Preview) permission, no permission to broadcast programs 224.1.1.3 (Forbid);

And User B 224.1.1.1 and 224.1.1.2 for the program is not playing privileges (Forbid), only shows 224.1.1.2 broadcast rights (Permit). Port-based user authentication method

Figure 5-2 Multicast authentication topology



Configuration step:

Step	Command	Explain
Step 1	GFA6700(config)#igmp-snooping enable	Open IGMP Snooping function of OLT
Step 2	GFA6700(config)#igmp-snooping auth enable	Open OLT side multicast authentication
Step 3	GFA6700(config)#igmp-auth 6/1/1 1 224.1.1.1 1 2000	Configuring User A user's programs 224.1.1.1 permissions Permit. (1-Permit; 2-Preview; 3-Forbid)

Step 4	GFA6700(config)#igmp-auth 6/1/1 1 224.1.1.2 2 2000	Configuring User A user's programs 224.1.1.2 permissions Preview
Step 5	GFA6700(config)#igmp-auth 6/1/1 1 224.1.1.3 3 2000	Configuring User A user of the program authority is Forbid 224.1.1.3
Step 6	GFA6700(config)#igmp-auth 6/1/2 1 224.1.1.1 3 2000 GFA6700(config)#igmp-auth 6/1/1 1 224.1.1.2 1 2000 GFA6700(config)#igmp-auth 6/1/1 1 224.1.1.2 3 2000	Configuring User B of the program the user's permission.
Step 7	GFA6700(config)#igmp-auth status 6/1/1 1 224.1.1.2 2 preview-counter 10 GFA6700(config)#igmp-auth status 6/1/1 1 224.1.1.2 2 preview-interval 20 GFA6700(config)#igmp-auth status 6/1/1 1 224.1.1.2 2 preview-time 60	For a preview of the program's user privileges, you must configure state information, including the number of preview (preview-conte r), the time interval

		between the two preview (preview-interval), each time for a preview Length (preview-time)
Step 8	GT811_A-6/1/1(config)#igmp-snooping enable GT811_A-6/1/1(config)#igmp-snooping auth enable GT811_A-6/1/2(config)#igmp-snooping enable GT811_A-6/1/2(config)#igmp-snooping auth enable	Configuration, respectively, the two ONU, the IGMP Snooping and Multicast authentication open

6 STP/RSTP/MSTP configuration

1 Overview

Current and STP related agreements: IEEE 802.1D (STP), 802.1W (RSTP), 802.1S (MSTP).

802.1D STP which is the first on the standard. RSTP (Rapid Spanning Tree Protocol) is the extension of STP, the main feature is the addition of the port state fast switching mechanism to achieve fast switching network topology. MSTP (Multiple Spanning Tree Protocol) proposed the concept of multi-spanning tree can be mapped to a different vlan to a different spanning tree, so as to achieve network load balancing purposes

STP is a Layer Management Protocol, the basic role is to bridge through the exchange of protocol data packets, the network structure of the

actual consultation network is calculated as the tree (Spanning Tree), to ensure that any two sites in the network has one and only a path to avoid network loops and thus inhibit the purpose of broadcast storm.

STP Election of a switch as the spanning tree root bridge (Root Switch), the other loop-free path through the switch and the root bridge is connected, the other redundant lines in the block (blocking) state. This, STP switching mechanism to provide dynamic redundancy: When the main line work, the backup line is off; when the main line fails, the backup line automatic recovery, switch the data stream.

 **Note!**

GROS support STP, RSTP, MSTP three kinds of spanning tree protocol, for the RSTP, MSTP these two protocols, GROS CST and MST, respectively, both models use to achieve, but for the STP protocol, the product can not be configured, but can be compatible.

---

2 Configure STP/RSTP

Generally speaking the benefits of using STP: in an extended LAN switches in all STP bridge protocol data unit by exchanging BPDU (Bridge Protocol Data Unit) to realize; as a stable spanning tree topology to select a root bridge; selected for each segment of a specified exchange switch; will switch on the redundant path is set to Blocking, to eliminate network loops.

Default configuration information

On the STP / RSTP / MSTP default settings as in the following table:

Content	Default set	Remark

enable/disable	enable	Set can be changed
Bridge ID Priority	32768	Set can be changed
cst/mst	cst	Set can be changed
forwarddelay	15s	The default setting is recommended
BPDU Hello Time	2s	The default setting is recommended
Bridge Max Age	20s	The default setting is recommended

2.1Set mode

STP into CST, MST two modes, the user can select a reasonable model:

- **CST mode**

CST (Common Spanning Tree) to form a spanning tree across the network, STP port settings based on the state. STP settings, such as port blocking, all VLAN on the port are in a blocked state.

The model is characterized by a configuration is simple and suitable for small networks. The concept of disadvantage is not vlan, VLAN topology configuration when the user is different, it may cause some VLAN can not communicate properly.

- **MST mode**

MST (Multiple Spanning Tree) is an extension of CST, which has the following characteristics: multiple switches can be a virtual domain into a MST, the MST field, a bridge similar to CST, and CST bridge interoperability.

In the MST area, with the same topology can be mapped to a multiple spanning tree instance vlan that MSTI (Multiple Spanning Tree Instance).

In the area of each MSTI can have different topologies, the purpose of achieving a balanced flow

Configuring Spanning Tree mode, follow these steps:

Step	Command	Explain
Step 1	GFA6700(config)#stp	Enter the spanning-tree configuration mode and configure the spanning tree mode
Step 2	GFA6700(config-mst)# spanning-tree mode cst	Select spanning tree mode
Step 3	GFA6700(config-cst)# spanning-tree enable	Enable spanning tree
Step 4	GFA6700(config)#show spanning-tree	View RSTP configuration and status information

2.2 Set fast features

RSTP introduced the mechanism of rapid state transitions, a reasonable allocation of port property, the network can achieve fast switching.

- **Edge property**

At the edge of the network switch is typically connected with the terminal equipment, such as PC, workstation. And the terminal equipment connected to the port configured as Edge ports, port status can be achieved fast conversion without Forwarding the conversion, Learning the need for Discarding process.

Edge attributes configuration steps:

Step	Command	Explain
Step 1	GFA6700(config)#stp	Enter the spanning-tree configuration mode and configure the spanning tree mode
Step 2	GFA6700(config-cst)# spanning-tree port <slot/port> [edge] [yes|no]	Configure the switch port is specified in the STP protocol specified domain calculation
Step 3	GFA6700(config)#show spanning-tree	View RSTP configuration and status information

■ **P2P property**

Switch ports and switch ports directly connected, the port is the P2P interface. RSTP negotiation mechanism used for P2P interfaces, port status can be achieved rapid conversion (Discarding Forwarding).

P2P attributes configuration steps:

Step	Command	Explain

Step 1	GFA6700(config)#stp	Enter the spanning-tree configuration mode and configure the spanning tree mode
Step 2	GFA6700(config-cst)#spanning-tree port <slot/port> [p2p] [yes | no | auto]	P2p properties configure the switch port
Step 3	GFA6700(config)#show spanning-tree	View RSTP configuration and status information

Note!

If the port is not connected and shared media, as the port is set to P2P properties;

2.3 Set time prameter

CST has 3 time parameters that can be configured

Hello-time: Transmit interval of STP message

Forward-delay: Port is from Discarding -> Learning -> Forwarding state time'

Maximum-age: Life cycle of the largest packet

The following shows the time parameters of CST mode interface configuration

Step	Command	Explain
Step 1	GFA6700(config)#stp	Enter the spanning-tree configuration mode and configure the spanning tree mode
Step 2	GFA6700(config-cst)#spanning-tree [hello-time] <1-10>	Configuration when the switch is selected as the root bridge sends BPDU interval, in seconds, default is 2. hello-time must be less than equal to the forward-delay - 2
Step 3	GFA6700(config-cst)# spanning-tree [forward-delay]<4-30>	When the switch is selected to set the root bridge, the port state switching time interval, in seconds, default is 15. forward-delay time must be greater than equal to the

		hello-time + 2
Step 4	GFA6700(config-cst)#spanning-tree [maximum-age] <6-40>	Configure the switch in the specified domain BPDU packets maximum time interval of aging, in seconds, default is 20, received more than this time BPDU packets directly discarded. maximum-age time must be greater than equal to 2 * (hello-time + 1), less than or equal 2 * (forward-delay-1)
Step 5	GFA6700(config)#show spanning-tree	View RSTP configuration and status information

2.4 Set bridge priority

Users can manually configure the bridge priority of the rational planning

of the network. The highest bridge priority (the value of the smaller) is the root of the network bridge. When the distance from the two links to the root bridge is same, choose to specify the path of high priority bridges.

The priority of the bridge configuration steps:

Step	Command	Explain
Step 1	GFA6700(config)#stp	Enter the spanning-tree configuration mode and configure the spanning tree mode
Step 2	GFA6700(config-cst)# spanning-tree [priority] <0-61440>	Configure the switch in the specified domain STP priority, the bridge priority. Must be an integer multiple of 4096, the default values: 32768, priority, the lower the value, the more likely to become the root of the network bridge priority value of 0 represents the

		highest priority
Step 3	GFA6700(config)# show spanning-tree	View RSTP configuration and status information

2.5 Set port priority

When the two links, like the distance to the root bridge, designated as the bridge priority, port priority decisions based on topology. Port Priority Configuration steps:

Step	Command	Explain
Step 1	GFA6700(config)#stp	Enter the spanning-tree configuration mode and configure the spanning tree mode
Step 2	GFA6700(config-cst)# spanning-tree port <slot/port>[priority] <0-240>	Configuration calculated in the specified area STP port priority, default is 128, the lower the priority value, the port more easily become a root

		port, the priority value of 0 represents the highest priority
Step 3	GFA6700(config)# show spanning-tree	View RSTP configuration and status information

2.6 Set port path

After the root bridge selection, port path on the network topology is of great significance. The smaller the distance to the root are, the more likely to be a pathway. After choosing a root bridge, under the port speed, etc., a reasonable path to the configuration of the port, can form the ideal topology. Set port path configuration steps:

Step	Command	Explain
Step 1	GFA6700(config)#stp	Enter the spanning-tree configuration mode and configure the spanning tree mode
Step 2	GFA6700(config-cst)# spanning-tree port <slot/port>[path-cost] [auto |<1-200000000>]	Configure the port path cost, port path cost default value of a relationship with the port rate is

		generally higher port speed, port path cost less.
Step 3	GFA6700(config)# show spanning-tree	View RSTP configuration and status information

2.7 Set port non-stp feature

RSTP can be some of the port is set to the port does not participate in the protocol computation; the method is to set the non-stp property. Characteristics of non-stp set port configuration steps:

Step	Command	Explain
Step 1	GFA6700(config)#stp	Enter the spanning-tree configuration mode and configure the spanning tree mode
Step 2	GFA6700(config-cst)# spanning-tree port <slot/port>[none-stp] [yes|no]	Configure whether to participate in STP port operations, port does not participate in STP after the operation, in the Forward state

Step 3	GFA6700(config)# show spanning-tree	View RSTP configuration and status information

3 Configure MSTP

3.1 Set mode

STP into CST, MST two modes, the user can select a reasonable model:

- **CST mode**

CST (Common Spanning Tree) to form a spanning tree across the network, STP port settings based on the state. STP settings, such as port blocking, all VLAN on the port are in a blocked state.

The model is characterized by a configuration is simple and suitable for small networks. The concept of disadvantage is not vlan, VLAN topology configuration when the user is different, it may cause some VLAN can not communicate properly.

- **MST mode**

MST (Multiple Spanning Tree) is an extension of CST, which has the following characteristics:

Virtual switches can be multiple domains into a MST, the MST CST domain like a bridge, and the CST bridge interoperability. In the MST area, with the same topology can be mapped to a multiple spanning tree instance vlan that MSTI (Multiple Spanning Tree Instance). In the area of each MSTI can have different topologies, the purpose of achieving a balanced flow.

Configuring Spanning Tree mode, follow these steps:

Step	Command	Explain

Step 1	GFA6700(config)#stp	Enter the spanning-tree configuration mode and configure the spanning tree mode
Step 2	GFA6700(config-mst)# spanning-tree mode mst	Select spanning tree mode
Step 3	GFA6700(config)# show spanning-tree mst <0-64>	Show MSTP configuration, mst-instance is 0 when the information is displayed IST, and other parameters for MSTI

3.2 Set fast feature

MSTP introduces a mechanism for rapid state transitions, a reasonable allocation of port property, you can quickly convert to the network.

- **Edge property**

At the edge of the network switch is typically connected with the terminal equipment, such as PC, workstation. And the terminal equipment connected to the port configured as Edge ports, port status can be achieved fast conversion without the need for Discarding Learning Forwarding the conversion process.

Edge property configuration step:

Step	Command	Explain
Step 1	GFA6700(config)#stp	Enter the spanning-tree configuration mode and configure the spanning tree mode
Step 2	GFA6700(config-mst)#Spanning-tree mode mst	Configure mst working mode
Step 3	GFA6700(config-mst)# spanning-tree port <slot/port>[edge] [yes | no]	Configure the switch port is specified in the specified domain of STP protocol computation, the default is involved in the calculation
Step 4	GFA6700(config)# show spanning-tree mst <0-64>	Show MSTP configuration, mst-instance is 0 when the information is displayed IST, and other parameters for MSTI

■ **P2P property**

Switch ports and switch ports directly connected, the port is the P2P

interface. RSTP negotiation mechanism used for P2P interfaces, port status can be achieved rapid conversion (Discarding Forwarding).

P2P property configuration step:

Step	Command	Explain
Step 1	GFA6700(config)#stp	Enter the spanning-tree configuration mode and configure the spanning tree mode
Step 2	GFA6700(config-mst)#Spanning-tree mode mst	Configure mst working mode
Step 3	GFA6700(config-mst)#spanning-tree port <slot/port> [p2p] [yes | no | auto]	Configure the switch port is specified in the specified domain of STP protocol computation, the default is involved in the calculation
Step 4	GFA6700(config)# show spanning-tree mst <0-64>	Show MSTP configuration, mst-instance is 0 when the information is displayed IST, and

		other parameters for MSTI

Note!

If the port is not connected and shared media, as the port is set to P2P properties.

3.3 Set time parameter

MST has four time parameters can be configured:

Hello-time: STP message transmission interval

Forward-delay: Port is from Discarding -> Learning -> Forwarding state time

Maximum-age: Life cycle of the largest message

Max-hops: MST within the maximum message lifetime

The following shows the time parameters of MST configuration mode interface:

Step	Command	Explain
Step 1	GFA6700(config)#stp	Enter the spanning-tree configuration mode and configure the spanning tree mode
Step 2	GFA6700(config-mst)#Spanning-tree mode mst	Configure mst working mode

Step 3	GFA6700(config-mst)#spanning-tree [hello-time] <1-10>	Configuration when the switch is selected as the root bridge sends BPDU interval, in seconds, default is 2. hello-time must be less than equal to the forward-delay - 2
Step 3	GFA6700(config-mst)#spanning-tree [forward-delay]<4-30>	When the switch is selected to set the root bridge, the port state switching time interval, in seconds, default is 15. forward-delay time must be greater than equal to the hello-time + 2
Step 4	GFA6700(config-mst)#spanning-tree [maximum-age]<6-40>	Configure the switch in the specified domain BPDU packets maximum time interval of aging, in seconds, default is 20, received more than this time BPDU packets directly discarded. maximum-age time must be greater than equal to 2 * (ello-time + 1) less than or equal 2 * (forward-delay-1)

Step 5	GFA6700(config-mst)# spanning-tree [max-hops] <6-40>	Configuring Bridge Forward delay parameter
Step 6	GFA6700(config)# show spanning-tree mst <0-64>	Show MSTP configuration, mst-instance is 0 when the information is displayed IST, and other parameters for MSTI

3.4 Set bridge case priority

Users can manually configure the bridge priority of the rational planning of the network. The highest bridge priority (the value of the smaller) is the root of the network bridge.

When the distance from the two links to the root bridge is same, choose to specify the path of high priority bridges. Configure the switch on the specified MSTID MSTI bridge priority, default is 32768, MSTI Bridge Priority must be a multiple of 4096. Bridge priority of instance configuration steps:

Step	Command	Explain
Step 1	GFA6700(config)#stp	Enter the spanning-tree configuration mode and configure the spanning tree mode
Step 2	GFA6700(config-mst)#Spanning-tree mode mst	Configure mst working mode

Step 3	GFA6700(config-mst)# spanning-tree priority <0-61440>mst <0-64>	Configure the bridge priority of instance
Step 4	GFA6700(config)# show spanning-tree mst <0-64>	Show MSTP configuration, mst-instance is 0 when the information is displayed IST, and other parameters for MSTI

3.5 Set port priority

When the two links, like the distance to the root bridge, designated as the bridge priority, port priority decisions based on topology. Port Priority Configuration steps:

Step	Command	Explain
Step 1	GFA6700(config)#stp	Enter the spanning-tree configuration mode and configure the spanning tree mode
Step 2	GFA6700(config-mst)#Spanning-tree mode mst	Configure mst working mode
Step 3	GFA6700(config-mst)#spanning-tree port <slot/port>priority <0-240> mst <0-64>	Configure port priority
Step 4	GFA6700(config)#show spanning-tree mst <0-64>	Show MSTP configuration,

		mst-instance is 0 when the information is displayed IST, and other parameters for MSTI

3.6 Set port path

After the root bridge selection, port path on the network topology is of great significance. The smaller the distance to the root are, the more likely tobe a pathway. After choosing a root bridge, under the port speed, etc., a reasonable path to the configuration of the port, can form the ideal topology. Port pathcost configuration steps:

Step	Command	Explain
Step 1	GFA6700(config)#stp	Enter the spanning-tree configuration mode and configure the spanning tree mode
Step 2	GFA6700(config-mst)#Spanning-tree mode mst	Configure mst working mode
Step 3	GFA6700(config-mst)# spanning-tree port <slot/port>path-cost [auto | <1-200000000>] mst <0-64>	Configure port pathcost
Step 4	GFA6700(config)#show spanning-tree mst <0-64>	Show MSTP configuration, mst-instance is 0

		when the information is displayed IST, and other parameters for MSTI

3.7 Set port non-stp feature

MSTP can be some of the port is set to the port does not participate in the protocol computation; the method is to set the non-stp property. non-stp attribute configuration steps:

Step	Command	Explain
Step 1	GFA6700(config)#stp	Enter the spanning-tree configuration mode and configure the spanning tree mode
Step 2	GFA6700(config-mst)#Spanning-tree mode mst	Configure mst working mode
Step 3	GFA6700(config-mst)# spanning-tree port <slot/port>[none-stp] [yes|no]	Configure whether to participate in STP port operations, port does not participate in STP after the operation, in the

		Forward state
Step 4	GFA6700(config)#show spanning-tree mst <0-64>	Show MSTP configuration, mst-instance is 0 when the information is displayed IST, and other parameters for MSTI

3.8 Set MSTP domain

MSTP is a domain must meet the same: the physical connection between the device cases, names, revision, Vlan mapping with the MSTI exactly. MSTP domain configuration steps

Step	Command	Explain
Step 1	GFA6700(config)#stp	Enter the spanning-tree configuration mode and configure the spanning tree mode
Step 2	GFA6700(config-mst)#Spanning-tree mode mst	Configure mst working mode

Step 3	GFA6700(config-mst)# spanning-tree mst [name] <name>	Configuring MSTP domain name identifier
Step 4	GFA6700(config-mst)# spanning-tree mst revision<0-65535>	Configuring MSTP domain identifier version
Step 5	GFA6700(config-mst)# spanning-tree map vlan <vlans>mst <0-64>	Configuring MSTP mapping domain and vlans
Step 7	GFA6700(config)#show spanning-tree mst <0-64>	Show MSTP configuration, mst-instance is 0 when the information is displayed IST, and other parameters for MSTI

4 Configuration case

4.1 RSTP configuration case

Case description

In this case the main switch is configured with RSTP. In bridge1, bridge2, bridge3, respectively, to enable rstp, by agreement between the calculation will block one of three bridges, one of the port. In this case, bridge1 the MAC is: 22:22:22:22:22:22, bridge2 the MAC is: 00:05:3 b: 81:12:78, Bridge3 the MAC to 00:05:3 b: 00.00 : 00.

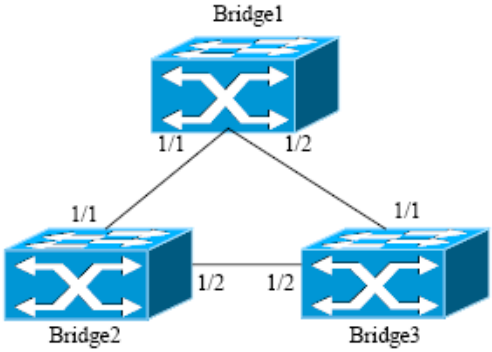


Figure 6-1 Configure RSTP

Configure step:

(The first step to third step is to configure RSTP bridge1 on the steps to configure RSTP bridge2 and bridge3 steps and bridge1 the same).

Step	Command	Explain
Step 1	GFA6700(config)#stp	Enter the spanning-tree configuration mode and configure the spanning tree mode
Step 2	GFA6700(config-mst)#Spanning-tree mode cst	Configure cst working mode
Step 3	GFA6700(config-cst)# spanning-tree enable	Enable RSTP

Step 4	GFA6700(config-mst)# show spanning-tree ----------SPANNING TREE information in STP domain 0 ------- Designated Root : 22:22:22:22:22:22 Designated Root Priority : 32768 Designated Root Path Cost: 0 Root Port : none Root Max Age 20 Hello Time 3 Forward Delay 15 Bridge ID Mac Address : 22:22:22:22:22:22 Bridge ID Priority : 32768 Bridge ForceVersion : 2 Bridge Max Age 20 Hello Time 3 Forward Delay 15 ---------- All ports information in STP domain 0 ---------- Name pri cost role span-state lk p2p eg Desi-bridge-id Dcost D-port Eth1/1 128 2000000 Desi Forwarding Y Y N 32768:222222222222 0 0x8081 Eth 1/2 128 20000 Desi Forwarding Y Y N 32768:222222222222 0	Show configuration of brideg1

	0x8082 Eth 1/3 128 20000 Dis Discarding N N N ----------	
Step 5	GFA6700(config-cst)# show spanning-tree ----------SPANNING TREE information in STP domain 0 --------- Designated Root : 22:22:22:22:22:22 Designated Root Priority : 32768 Designated Root Path Cost : 20000 Root Port : 1/1 Root Max Age 20 Hello Time 2 Forward Delay 15 Bridge ID Mac Address : 00:05:3b:81:12:78 Bridge ID Priority : 32768 Bridge ForceVersion : 2 Bridge Max Age 20 Hello Time 3 Forward Delay 15 ---------- All ports information in STP domain 0 ---------- Name pri cost role span-state lk p2p eg Desi-bridge-id Dcost D-port Eth 1/1 128 20000 Root	Show configuration of brideg2

	Forwarding Y Y N 32768:00053b811278 20000 0x8041 Eth 1/2 128 20000 Alt Discarding Y Y N 32768:00053b811278 20000 0x8042	
Step 6	GFA6700(config -cst)# show spanning-tree ----------SPANNING TREE information in STP domain 0 --------- Designated Root : 22:22:22:22:22:22 Designated Root Priority : 32768 Designated Root Path Cost : 20000 Root Port : 1/1 Root Max Age 20 Hello Time 2 Forward Delay 15 Bridge ID Mac Address : 00:05:3b:00:00:00 Bridge ID Priority : 32768 Bridge ForceVersion : 2 Bridge Max Age 20 Hello Time 3 Forward Delay 15 ---------- All ports information in STP domain 0 ---------- Name pri cost role span-state lk	Show configuration of brideg3

	p2p eg Desi-bridge-id Dcost D-port Eth 1/1 128 20000 Root Forwarding Y Y N 32768:222222222222 20000 0x8031 Eth 1/2 128 20000 Desi Forwarding Y Y N 32768:00053b000000 0 0x8032	

4.2 MSTP configuration case

Case description

In this case the main switch is configured with MSTP domain. Respectively in the three switches create a single MST Region, and in which to create the three Instance. Priority by configuring the instance makes Instance1 in bridge1 (MAC: 0005:3 b80: 03cf) is the root bridge, Instance 2 in bridge2 (MAC: 0005.3b81.1278) is the root bridge in Instance3 in bridge3 (MAC: 2222:2222: 2222) as the root bridge.

MSTP entire network is divided into multiple domains (different domains with different distinguished name and revision), each field can contain up to 64 instances of spanning tree for each instance of the internally generated; each instance can also contain more than a VLAN, multiple vlan mapping to a Spaning Tree, all of the VLAN in Instance 0 in default. In the MST configuration, if the final configuration with Instance <1-64>, spanning tree to change to only valid in a specific Instance, Instance Spanning Tree on the other has no effect; default, change the parameters of only the Region (Instance 0) in the spanning tree affected.

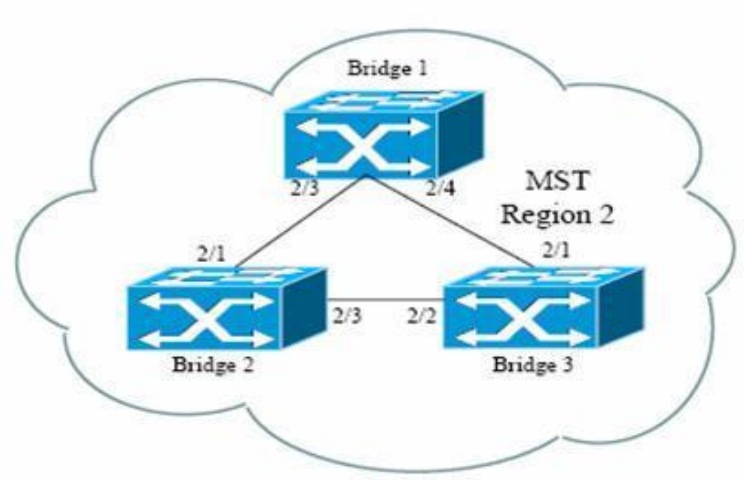


Figure 6-2 MSTP configuration

Configuration steps on the Bridge1:

Step	Command	Explain
Step 1	GFA6700(config)#interface vlan vlan10 10 GFA6700 (vlan-vlan10)#add port 2/1-4 tag GFA6700 (vlan-vlan10)#exit GFA6700 (config)#interface vlan vlan20 20 GFA6700 (vlan-vlan20)#add port 2/1-4 tag GFA6700 (vlan-vlan20)#exit GFA6700 (config)#interface vlan vlan30 30 GFA6700 (vlan-vlan30)#add port	Create vlan，and add port

	2/1-4 tag GFA6700 (vlan-vlan30)#exit	
Step 2	GFA6700 (config) # stp GFA6700 (config -cst) # spanning-tree mode mst	Enter config –mstp configuration mode
Step 3	GFA6700 (config -mst)# spanning-tree mst name region2 GFA6700 (config -mst)# spanning-tree mst revision 2	Create one mst region
Step 4	GFA6700 (config -mst)# spanning-tree enable	Enable MSTP
Step 5	GFA6700 (config -mst)# spanning-tree map vlan 10-19 mst 1 GFA6700 (config -mst)# spanning-tree map vlan 20-29 mst 2 GFA6700 (config -mst)# spanning-tree map vlan 30-39 mst 3	Create three instances
Step 7	GFA6700 (config -mst)# spanning-tree priority 4096 mst 1 GFA6700 (config -mst)# spanning-tree priority 32768 mst 2 GFA6700 (config -mst)# spanning-tree priority 61440 mst 3	Configure instance priority

Configuration steps on the Bridge2:

Step	Command	Explain

Step 1	GFA6700 (config)#interface vlan vlan10 10 GFA6700 (vlan-vlan10)#add port 2/1-4 tag GFA6700 (vlan-vlan10)#exit GFA6700 (config)#interface vlan vlan20 20 GFA6700 (vlan-vlan20)#add port 2/1-4 tag GFA6700 (vlan-vlan20)#exit GFA6700 (config)#interface vlan vlan30 30 GFA6700 (vlan-vlan30)#add port 2/1-4 tag GFA6700 (vlan-vlan30)#exit	Create vlan，and add port
Step 2	GFA6700 (config) # stp GFA6700 (config -cst) # spanning-tree mode mst	Enter config –mstp configuration mode
Step 3	GFA6700 (config -mst)# spanning-tree mst name region2 GFA6700 (config -mst)# spanning-tree mst revision 2	Create one mst region
Step 4	GFA6700 (config -mst)# spanning-tree enable	Enable MSTP
Step 5	GFA6700 (config -mst)# spanning-tree map vlan 10-19 mst 1 GFA6700 (config -mst)# spanning-tree map vlan 20-29 mst 2 GFA6700 (config -mst)#	Create three instances

	spanning-tree map vlan 30-39 mst 3	
Step 6	GFA6700 (config -mst)# spanning-tree priority 61440 mst 1 GFA6700 (config -mst)# spanning-tree priority 4096 mst 2 GFA6700 (config -mst)# spanning-tree priority 32768 mst 3	Configure instance priority

Configuration steps on the Bridge3:

Step	Command	Explain
Step 1	GFA6700 (config)#interface vlan vlan10 10 GFA6700 (vlan-vlan10)#add port 2/1-4 tag GFA6700 (vlan-vlan10)#exit GFA6700 (config)#interface vlan vlan20 20 GFA6700 (vlan-vlan20)#add port 2/1-4 tag GFA6700 (vlan-vlan20)#exit GFA6700 (config)#interface vlan vlan30 30 GFA6700 (vlan-vlan30)#add port 2/1-4 tag GFA6700 (vlan-vlan30)#exit	Create vlan，and add port

Step 2	GFA6700 (config) # stp GFA6700 (config -cst) # spanning-tree mode mst	Enter config –mstp configuration mode
Step 3	GFA6700 (config -mst)# spanning-tree mst name region2 GFA6700 (config -mst)# spanning-tree mst revision 2	Create one mst region
Step 4	GFA6700 (config -mst)# spanning-tree enable	Enable MSTP
Step 5	GFA6700 (config -mst)# spanning-tree map vlan 10-19 mst 1 GFA6700 (config -mst)# spanning-tree map vlan 20-29 mst 2 GFA6700 (config -mst)# spanning-tree map vlan 30-39 mst 3	Create three instances
Step 6	EPON V2R1(config -mst)# spanning-tree priority 32768 mst 1 EPON V2R1(config -mst)# spanning-tree priority 61440 mst 2 EPON V2R1(config -mst)# spanning-tree priority 4096 mst 3	Configure instance priority

7 QinQ configuration

1 QinQ overview

IEEE802.1Q defined in the VLAN Tag field is only 12 bits used to represent VLAN ID, so the device can support up to 4094 VLAN. In practice, it often requires the user to isolate a large number of VLAN,

VLAN 4094 can not meet demand.

QinQ characteristics of the port devices is a simple, flexible layer VPN technology, which the service provider network edge devices for the user's private network packets encapsulated outer VLAN Tag (S-VLAN), to carry two packets VLAN Tag layer through the carrier's backbone network (public network). In the public network, the device only in accordance with the outer VLAN Tag (S-VLAN) to forward packets, and packet source MAC address table entries to learn where the outer VLAN Tag of the MAC address table, and the user's private Network VLAN Tag (C-VLAN) in the transmission process will be treated as part of the data packets for transmission.

QinQ feature allows the network to provide up to 4094X4094 a VLAN, VLAN number to meet the needs of the metro, which mainly address the following issues:

- Alleviate the growing shortage of resources the public network VLAN ID.
- Users can plan their own private network VLAN ID, will not lead to conflict and the public network VLAN ID.
- For small metropolitan or enterprise network to provide a relatively simple two-story VPN solution

2 General QinQ configuration

The VLAN mode should be setted to stack mode in the use of general QinQ function.

Command	Specification
GFA6900(config)#vlanmode stack	Enable double VLAN recognition mode

GFA6900(config)#vlantpid <outertpid> <innertpid>	Configure the TPID of inner layer and outer layer

Command	Specification
vlan add ingress vlantrans <slot/port> <1-4094> <1-4094> <0-7> <0-1> {<0-1>}*1	Based on the inner VID,configure ingress rules,add corresponded outer label or usie the new VID to replace VID
vlan add egress vlantrans <slot/port> <1-4094> <1-4094> <0-7> <0-1>	Based on the inner VID,configure engress rule,use the new VID to replace the original VID
vlan del egress vlantrans <slot/port> <1-4094> vlan del ingress vlantrans <slot/port> <1-4094>	Delete the configuration rules
show egress vlantrans {<slot/port>}*1 show ingress vlantrans {<slot/port>}*1	View the current rules information of configuration

3 PON QinQ Configuration

As its name suggests, PON QinQ function refers to the double VLAN label function which realized by the PON chip.In this realize way,the switching chip of OLT don’t need to add /peel the labels,but it

need to identify the data label to forward the data flow correctly。

When using PON QinQ, the corresponding mode of OLT VLAN is dot1q.

Command	Specification
vlanmode [dot1q|transparent|stack]	Switch VLAN mode to dot1q, monolayer recoginition mode
uplink vlan-tag-add <1-64> inter-vid [all|<1-4094>] outer-vid <1-4094> priority [<0-7>|original] tpid [0x8100|0x9100|0x88a8|user-defined]	At the PON node ,configure the uplink direction to add the outer VID rules according to the LLID(ONUID)
uplink vlan-tag-exchange <1-64> [all|null-tagged|<1-4094>] <1-4094> [original|<0-7>] [0x8100|0x9100|0x88a8|user-defined]	At the PON node ,configure the uplink direction to replace the VID rules
downlink vlan-tag-striped <1-4094>	At the PON node ,configure the downlink direction to peel the outer VID rules according to the LLID(ONUID)
downlink vlan-tag-exchange <1-4094> <1-4094> [original|<0-7>]	At the PON node ,configure the downlink direction to replace the VID rules

show downlink vlan-tag-manipulation {<1-4094>}*1 show uplink vlan-tag-manipulation <1-64>	View the current configuration rules information of the uplink or downlink direction

When using PON QinQ, the corresponding mode of OLT VLAN is srack.

Command	Specification
vlanmode [dot1q|transparent|stack]	Switch VLAN mode to stack, double layer recoginition mode
vlan stack nni enable	Set the eth interface which corresponding to the PON port to nni mode (or port will not identify the outer label of the pon uplink)
The rst configuration on the PON port refer to the examples that VLAN mode is dot1q，exactly the same	Ellipsis

4 Flexible QinQ configuration

EsayPath EPON QinQ provide a more flexible configuration rules can be based on more conditions to the corresponding configuration outer

VID.

 **Note!**

In the use of GFA6700, only configuration GFA-SW-B0 main control board, the only support flexible QinQ function. GFA6100 and GFA6700 configuration GFA-SW-A0, you can not support flexible QinQ function, only supports VLAN Stacking feature.

Command	Explain
qinq-map [ingress|egress] <map_name>	Create one qinq map，and enter to this node.
match dip <A.B.C.D> <A.B.C.D> match dmac <H.H.H> <H.H.H> match dscp <0-63> <0-63> match ethertype <hex_value> <hex_mask> match ingress-port <slot/port> match inner-priority <0-7> match inner-vid <1-4094> <1-4094> match l3-protocol <0-255> match l4-dport <0-65535> <1-65535> match l4-sport <0-65535> <1-65535> match outer-priority <0-7> match outer-vid <0-4094> <1-4095> match sip <A.B.C.D> <A.B.C.D> match smac <H.H.H> <H.H.H> match snap-head <hex_string>	In qinq map node can be configured based on a variety of conditions to match the rules

<mask_string>	
policy [noop|drop|nodrop] {[vlannoop|vlanadd|vlanrep] <0-4094> [chgpri|nochgpri] <0-7>}*1	In qinq map node, configure the matching rules, set to add or replace the outer layer VID
apply	Enable rules currently configured QINQ
show config	View current rule configuration

5 Port QinQ property configuration

There are sereval properties to be configured for the port in some scenes application

Command	Explain
vlan stack nni [enable|disable]	Enable or cancel the port property. When the port is NNI property, you can identify the double-layer VLAN.
vtenable [ingress|egress] [enable|disable]	Enable or cancel the port VLAN ingress or egress of the

	conversion
vtmiss [untag|tag]	Configure port vtmiss properties. The default is untag way. If the data packet does not match a QinQ rule, the corresponding set of attributes vtmiss. The property must first enable port vtenable property to take effect

6 Configuration case

6.1 Case 1

Case description

User network C-VLAN100 ~ 200 in all data packets have to add S-VLAN 2001. Below:

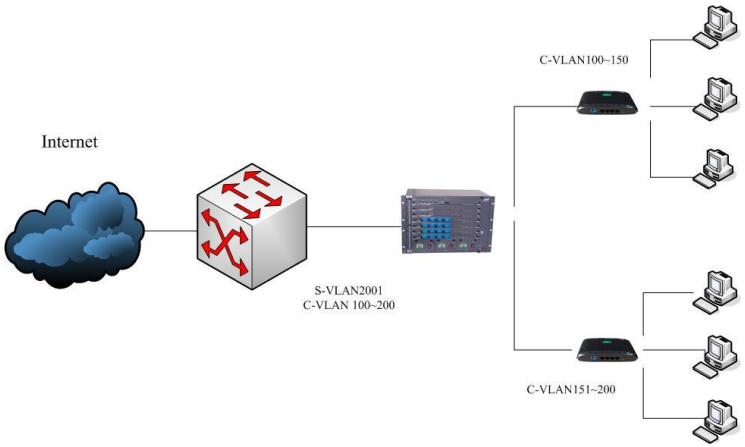


Figure 7-1 Case 1

Step	Command	Explain
Step 1	GFA6700(config)#vlanmode stack	Set VLAN mode as stack mode
Step 2	GFA6700(config)#qinq-map ingress test	Create one ingress qinq map，name is test
Step 3	GFA6700(config-qinq-ingmap-test)# match inner-vid 100 200 GFA6700(config-qinq-ingmap-test)# match ingress-port 5/1	Configure match condition
Step 4	GFA6700(config-qinq-ingmap-test)# policy nodrop vlanadd 2001 nochgpri 0	Configure policy. SVLAN vid 2001
Step 5	GFA6700(config-qinq-ingmap-test)# apply	Apply the rules, policy configuration

Step 6	GFA6700(config)#show qinq-map ingress Totol Map Count 1 ---------- QinQ-Map Name : test QinQ-Map Stat : Enable QinQ-Map Index: 0 QinQ-Map Type : Ingress Map QinQ-Map Apply: Has Applied after QinQ-Map creation or DATA modification QinQ-Map MATCH RULES: Inner_VID : 100 - 200 QinQ-Map Policy: Packet_Drop : nodrop Change_Vlan : add New_VlanID : 2001 Change_PRI : nochange New_Priority: 0 ---------- GFA6700(config)#	View current all ingress qinq map
Step 7	GFA6700(config)#interface vlan v2001 2001 GFA6700(vlan-v2001)#add port 1/1，5/1 tagged	Create S VLAN 2001

6.2 Case 2

Case description

For each onu under OLT can be divided into S VLAN. For example, the ONU 1 ~ 32 PON5 / 1 under, respectively tag S VLAN to 101 ~ 132.

Step	Command	Specification
Step1	GFA6900(config)#vlanmode stack	Set VLAN mode to stack mode
Step 2	GFA6900(if-eth1/1)#vlan stack nni enable GFA6900(if-eth5/1)#vlan stack nni enable	Set the corresponding uplink port and pon port to NNI mode
Step 3	GFA6900(epon-pon5/1)#uplink vlan-tag-add 1 inter-vid all outer-vid 101 priority original tpid 0x8100 GFA6900(epon-pon5/1)#uplink vlan-tag-add 2 inter-vid all outer-vid 102 priority original tpid 0x8100 GFA6900(epon-pon5/1)#uplink vlan-tag-add 3 inter-vid all outer-vid 103 priority original tpid 0x8100 .... GFA6900(epon-pon5/1)#uplink vlan-tag-add 32 inter-vid all outer-vid 132 priority original tpid 0x8100	Configure 32 ONU at the PON node,all uplink direction data of each ONU plus the crrespording SVLAN
Step4	GFA6900(epon-pon5/1)#downlink vlan-tag-striped 101	Configure downlink data

	GFA6900(epon-pon5/1)#downlink vlan-tag-striped 102 GFA6900(epon-pon5/1)#downlink vlan-tag-striped 103 . . . . . GFA6900(epon-pon5/1)#downlink vlan-tag-striped 132	direction and peel the outer SVLAN at the PON node
Step 5	GFA6900(config)#interface vlan v101 101 GFA6900(vlan-v101)#add port 1/1,5/1 tagged GFA6900(config)#interface vlan v102 102 GFA6900(vlan-v101)#add port 1/1,5/1 tagged . . . . GFA6900(config)#interface vlan v132 132 GFA6900(vlan-v101)#add port 1/1,5/1 tagged	Configure the corresponding SVLAN

6.3 Case 3

Case description

VoIP voice services using a single layer VLAN550, Internet services and the user VLAN in the aggregation switch interface needs to receive a double VLAN, SVLAN is 1001, CVLAN101 and 201. VoIP services and Internet use at the OLT at the same uplink ports.

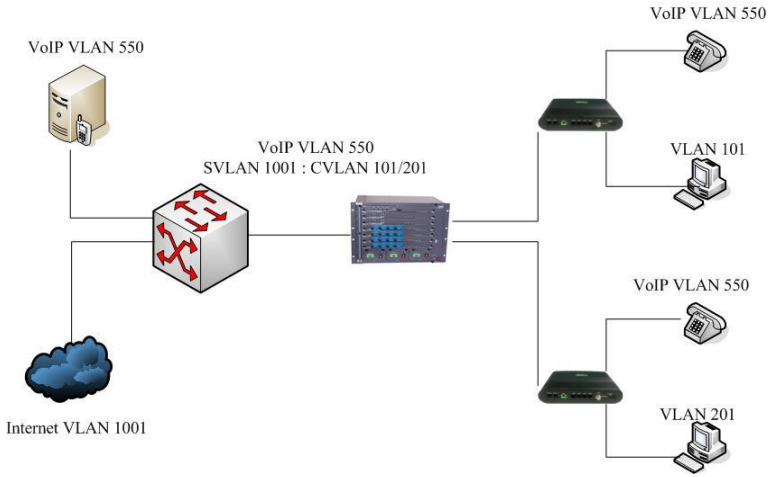


Figure 7-2 Case 3

This is a very specific scene, the VLAN configuration on the need to pay attention

Step	Command	Specification
Step1	GFA6900(config)#vlanmode stack	Set the VLAN mode to stack mode
Step2	GFA6900(if-eth1/4)#vlan stack nni enable	Set the corresponding uplink port to NNI mode
Step3	GFA6900(config)#qinq-map ingress test1 GFA6900(config-qinq-ingmap-test1) #match inner-vid 101 101 GFA6900(config-qinq-ingmap-test)# match ingress-port 11/3	Configure internet service CVLAN101 needs to plus outer VID1001 of SVLAN

	GFA6900(config-qinq-ingmap-test)# policy outervlan vid add 1001 GFA6900(config-qinq-ingmap-test1) #apply	

Step4	GFA6900(config)#qinq-map ingress test2
	GFA6900(config-qinq-ingmap-test1)
	#match inner-vid 201 201
	GFA6900(config-qinq-ingmap-test)#
	match ingress-port 11/3
	GFA6900(config-qinq-ingmap-test)#
	policy outervlan vid add 1001
	GFA6900(config-qinq-ingmap-test1)
	#apply
		Configure internet service CVLAN201 needs to plus outer VID1001 of SVLAN

Step5	GFA6900(config)#qinq-map ingress test3
	GFA6900(config-qinq-ingmap-test2)
	#match inner-vid 550 550
	GFA6900(config-qinq-ingmap-test)#
	match ingress-port 11/3
	GFA6900(config-qinq-ingmap-test)#
	policy outervlan vid add 550
	GFA6900(config-qinq-ingmap-test1)
	#apply
		Although the VoIP voice service requires for a single VLAN,550.while because the attribute of uplink port,it needs to configure the outer layer of VID550 of SVLAN,and with the stp 6 at the same time ,peeling the outer VID550.

Step6	GFA6900(config)#interface vlan v550 550 GFA6900(vlan-v500)#add port 1/4 untagged GFA6900(vlan-v500)#add port 11/3 tagged	With the step3,peel the outer VID layer of uplink VLAN 550
Step7	GFA6900(config)#interface vlan v1001 1001 GFA6900(vlan-v500)#add port 1/4 tagged GFA6900(vlan-v500)#add port 11/3 untagged	Note that the 11/3 port join the VLAN by untag way,to peel the 1001 outer layer on downlink direction
Step8	GFA6900(config)#interface ethernet 11/3 GFA6900(if-pon11/3)#vtenable ingress disable GFA6900(if-pon11/3)#vtenable egress disable	Set the attributes of ingress and egress to disable of 11/3 port
Step9	GFA6900(epon-onu11/3/2)#vlan dot1q 0	Set the ONU transmission,or careate the corresponding inner VLAN

8 Qos Configuration

1 Overview of Qos

In traditional IP networks, all packets are treated the same no difference, each network device on all packets are used first in first out (FIFO) strategy for processing, it is best efforts the packet to the destination,

but the reliability of packet transmission, transmission delay and other performance does not provide any guarantee.

Rapid network development, with the IP network, the continual emergence of new applications on the IP network quality of service is also put forward new requirements, such as VoIP (Voice over IP, IP voice), and other real-time services on packet transmission delay on the proposed high requirements, if sending the message delay is too long, it will be unacceptable to the user (in relative terms, E-Mail and FTP services are not sensitive to the time delay). Have different service needs to support voice, video and data services, requiring the network to distinguish between different communications, and then provide them the appropriate services. Best of traditional IP network service can not identify and distinguish the various communications networks category, and have communication ability is the distinction between types of communication for different services provide different premise, so that the traditional networks can not meet the best service model applications. QoS (Quality of Service, Quality of Service) technology there has been dedicated to solve this problem.

QoS is intended to address the different needs of various applications, to provide different quality of service, for example: to provide dedicated bandwidth and reduce packet loss rate and lower packet delivery delay and delay jitter

2 Configure Qos

2.1 Traffic classfication

EasyPath EPON supports a number of flexible terms to distinguish different business traffic, the class-map node show bellows:

Command	Specification

match destination-address ip <A.B.C.D/M> match destination-address ip <A.B.C.D> <A.B.C.D>	Execute business flow classification based on the destination IP address
match destination-address mac <mac_address>	Execute business flow classification based on the destination MAC address
match destination-port <0-65535>	Execute business flow classification based on the 4 layer destination port number
match dscp [<0-63>|ef|default|af11|af12|af13|af21|af22|af23|af31|af32|af33|af41|af42|af43|cs1|cs2|cs3|cs4|cs5|cs6|cs7]	Execute business flow classification based on the DSCP
match ethernet-type [<0x0000-0xffff>|<0-65535>]	Execute business flow classification based on the type of Ethernet.The wildcard “f” stands for matching
match inner-user-priority <0-7>	Execute the business flow classification base on the 802.1P priority of inner VLAN.Only function

	for the NNI mode port
match inner-vlan-id <1-4094>	Execute the business flow classification base on the inner VID.Only function for the NNI mode port
match ip-precedence <0-7>	Execute business flow classification based on the priority of IP
match ip-protocol [<0x00-0xff>|<0-255>]	Execute business flow classification based on the IP protocol number
match port <slot/port>	Execute business flow classification based on the interface of Ethernet
match source-address ip <A.B.C.D/M> match source-address ip <A.B.C.D> <A.B.C.D>	Execute business flow classification based on the source IP address
match source-address mac <mac_address>	Execute business flow classification based on the source MAC

	address
match source-port <0-65535>	Execute business flow classification based on the 4 layer source port number
match user-priority <0-7>	Execute business flow classification based on the priority of 802.13
match vlan-id <1-4094>	Execute business flow classification based on the destination IP address

2.2 Qos strategy

It can support a variety of QoS strategies in the EasyPath EPON.Under the node of Policy-map:

Command	Specification
drop	Execute the discard strategy for the matched business flow
police cir <cir_value> cbs <cbs_value>	Execute the speed limit strategy for the matched business

	flow
set counter	Set the counter for the matched business flow
set dscp [<0-63>|ef|default|af11|af12|af13|af21|af22|af23|af31|af32|af33|af41|af42|af43|cs1|cs2|cs3|cs4|cs5|cs6|cs7]	Change the value of DSCP for the matched business flow
set ip-precedence <0-7>	Change the priority of IP for the matched business flow
set mirror port <slot/port>	Mirror to some Ethernet port for the matched business flow
set redirect port <slot/port>	Specify to some Ethernet port for the matched business flow
set user-priority <0-7> {[internal|external]}*1	Change the priority of 802.1p for the matched business flow
set drop-precedence <0-1>	Set the priority of discarding for the matched business flow

set out-drop set out-drop-precedence <0-1> set out-dscp [<0-63>|ef|default|af11|af12|af13|af21|af22|af23|af31|af32|af33|af41|af42|af43|cs1|cs2|cs3|cs4|cs5|cs6|cs7]	Set the strategy of discarding for the matched business flow

2.3 Queue scheduling

For the congestion management, generally use the queue scheduling technology, to make the message temporary cache to the queue according to a certain strategy in the network equipment., and then take out the message from the wueue according to a certain strategy,and send out on the interface.EasyPath EPON supports multiple queue scheduling modes;

- FIFO，First In First Out Queuing
- PQ，Priority Queuing.Also called strict priority queue scheduling,，SP
- WRR，Weighted Round Robin
- DRR，Deficit Round-Robin
- WRR+PQ，DRR+PQ

Under the config node：

Command	Specification
config queue-mode drr <w0,w1,w2,w3,w4,w5,w6,w7>	Configure queue scheduling for all the drr queue in the global
config queue-mode fifo	Configure queue scheduling for all the Fifo ports in the

	global The default scheduling is fifo queue scheduling
config queue-mode hybrid drr <w0,w1,w2,w3,w4,w5,w6,w7>	Configure mix queue scheduling for all the DRR+PO ports in the global
config queue-mode hybrid wrr <w0,w1,w2,w3,w4,w5,w6,w7>	Configure mix queue scheduling for all the WRR+PO ports in the global
config queue-mode pq	Configure PQ queue scheduling for all ports in the global
config queue-mode wrr <w0,w1,w2,w3,w4,w5,w6,w7>	Configure WRR queue scheduling for all ports in the global
show queue-mode	View queue scheduling configuration information

Note!

This configuration can also be configured individually queue scheduling mode for this port at the port node

2.4 Queue map

Config node：

Command	Specification
config dscp <0-63> cos-queue <0-7>	Configure dscp and mapping relations between queues for all ports In the global
config user-priority <0-7> cos-queue <0-7>	Configure 802.1p and mapping relationl between queues for all ports In the global

 **Note！**

It’s generally not recommended to modify the mapping relation In addition, this configuration can also be configured individually queue scheduling mode for this port at the port node

2.5 Congestion Avoidance

Excessive congestion can cause great harmto the cyber source,so it must take certain measures to lift.Congestion Avoidance is a flow control mechanism,it can monitor the use of cyber source(such as a ueue or memory buffer),actively discarded message when the congestion has exacerbated trend,and it can remove the network overload by adjusting the network flow..

This flow control has more extensive meaning compare with end-to-end

flow control ,it affect more business stream load of equipments.When equipment discard the messge,it not excluse the action to match the end flow control (such as TCP fmicrolfuidic) and better adjustement of network ttraffic to a reasonable load condition.The eddective combination between packet discard strategy and the source end mechanism,can make the throughout and efficiency of network maximization,and make the discard and delay of message minimizing,

EasyPath EPON supports twodiscard stretgies, Tail-Drop and RED.

- **Tail-Drop**

All the new messages will be discarded when the length of queue has got a maximum value.

- **RED**

Set the upper and lower limit for each queue, do the following handles with the messages in the queue:

- Don't discard the message when the length of queue less than the lower limit
- Discard the message when the length of queue excessive than the limit
- When the length of the queue between the upper and lower limits,it begins to random discard the arrived messages.Longer queue,the drop probability is higher,but there is a maximum drop probability.

Command	Specification
GFA6700(config)#qos drop-policy red <1-5000> GFA6700(config)#qos drop-policy red <red_name>	Create a red discard strategy

GFA6700(config-drop-policy)# set queue <1-8> minThreshold <1-100> maxThreshold <1-100>	Configure 0~7 queuediscard threshold range

3 Configuration case

Case description

A large business customers need to give priority to ensuring the data bandwidth, then it's assigned to the business VLAN is the VLAN 1001 for this client.The configuration of the data business priority is 7 for the customer based on the VID, while we should configure the monitoring for the user service flow.

Configuration steps

Step	Command	Specification
Step1	GFA6700(config)#class-map customer1	Create a class map 。Named customer1。
Step2	GFA6700(config-cmap)#match vlan-id 1001	Distinguish the customer service flow with the exclusive VID
Step3	GFA6700(config)#policy-map ingress customer1	Create a policy map,named customer1
Step4	GFA6700(config-policymap)#match class-map customer1	Bind the prior created class map and policy map

Step5	GFA6700(config-policymap-c)#set user-priority 7	Set the priority 7 of this client's service flow
Step7	GFA6700(config-policymap-c)#set counter	Configure the monitor for this client's service flow
Step8	GFA6700(config)#interface ethernet 5/1 GFA6700(if-eth5/1)#service-policy ingress customer1 GFA6700(config)#interface ethernet 1/1 GFA6700(if-eth1/1)#service-policy ingress customer1	Bind the strategy for the uplink/downlink interface
Step9	GFA6700(if-eth1/1)#show counter ingress	View the service flow statistics at the port node
Step10	GFA6700(config)#config queue-mode pq	Configure the queue scheduling mode of global or single port according to the actual needs.

9 ACL Configuration

1 Overview of ACL

ACL (Access Control List) by providing a series of matching the data packet classification, then classification of the data packet is to allow or

filter (deny) policy

2 Configure ACL

Command	Specification
config access-list service [enable|disable]	Enable or close ACL function
access-list <1-5000>	Create and enter acces-list node
rule <1-5000> [permit|deny] any rule <1-5000> [permit|deny] icmp dip [<A.B.C.D/M>|any] sip [<A.B.C.D/M>|any] rule <1-5000> [permit|deny] ip dip [<A.B.C.D/M>|any] sip [<A.B.C.D/M>|any] rule <1-5000> [permit|deny] mac destination [<dst_mac> |any] source [<src_mac> |any] rule <1-5000> [permit|deny] tcp dip [<A.B.C.D/M>|any] dst-port [<0-65535>|any] sip [<A.B.C.D/M>|any] src-port [<0-65535>|any] rule <1-5000> [permit|deny] udp dip [<A.B.C.D/M>|any] dst-port [<0-65535>|any] sip [<A.B.C.D/M>|any] src-port [<0-65535>|any]	Configure the matching conditions and acl atrategies at the access-list node.
access-list type [ip|pppoe]	Configure the application styles of the access-listt,it should to set

	pppoe parqmeter for the PPPoE application
access-list priority <1-5000>	Configure prorities of accesslist which created currnet,and the high priority is matching the priority effect.
GFA6700(if-eth1/1)# access-list <1-5000>	Bound the created acl to the port at the port node ,and enter into force

Note!

No need to enter the access-list node, the node can directly create config acl match the conditions and configuration.

3 Configuration case

Case description

All from the port 1 / 1 to enter, send to the destination IP address is 192.168.34.76 to filter out ICMP messages

Step	Command	Explain

Step 1	GFA6700(config)#config access-list service enable	Enable ACL function
Step 2	GFA6700(config)#access-list 1 deny icmp dip 192.168.34.76/32 sip any	Create a access list, and configure the match conditions
Step 3	GFA6700(config)#interface ethernet 1/1	Enter to port 1/1 node
Step 4	GFA6700(if-eth1/1)#access-list 1	Access-list 1 will bind to port 1 / 1
Step 5	GFA6700(config)#show access-list Total 1 access-list(s) ========== ========== access-list index: 1 type: ip priority: 1 port number bound: 1 rule number : 1 ---------- --- rule index: 10 action: deny IP protocol: ICMP destination IP address: 192.168.34.76/32 source IP address: any	View configured access-list

	========== ==========	

10 Voice Service Configuration

1. Overview of SIP

SIP (Session Initiation Protocol) is a control protocol of application layer for the establishment, change and termination of multimedia session.And the session can be the IP telephony, multimedia session or multimedia conference.SIP is the core protocol(the latest document of RFC is RC 3261) of IETF multimedia data and control system structure.I ts main purpose is to solve the IP network signling control and the exchange communication with the software platform,to form the next generation of value-added service platform of telecommunication,banking ,finance and other industries to provide better value-added service.

SIP is used to launch a session; it can control the establishment and termination of the multimedia session, and also can adjust and modify session attributes dynamically, such as session bandwidth requirements, transmission media type (voice, video and data), media codec format, support of the multicast and unicast. The SIP protocol is based on the text encoding, draws heavily on mature HTTP protocol, and has the characteristics of easy expansion, easy realization , so it is very suitable for multimedia communication system Internet base on Internet.

1.1 Basic concept of SIP

1.1.1 Multimedia session

According to the definitions of RFC 2327, the multimedia session refers to a group of multimedia senders and receivers, as well as the data

stream from a sender to a recipient. For example, a multimedia conference is a multimedia session. A session is determined by a set of user names, session ID, network type, type address and address of each unit .

1.1.2 User Agent

User agent (UA, User Agent) or SIP terminal refers to the multimedia session terminal which supports SIP protocol. Generally, the router which supports SIP protocol considered to be the SIP UA. UA includes user agent client (UAC, User Agent Client) and user agent server (UAS, User Agent Server). When we say UA, it always refers to the two, because a SIP terminal not only can be the UAC, but also can be UAS. User agent client launch a session request actively in a SIP session establishment process. For example, call the SIP terminal. When the agent server sends a session request to the called terminal, it becomes the user agent client. User agent server receives a session request in SIP session establishment process. For example, call the SIP terminal. When the agent server receives a calling terminal sends a session request, also as a user agent server.

1.1.3 Proxy Server

The function of the proxy server is to transfer the session request to the called UA from the caller UA,then send back the response from the called UA,so it's equivalent to be a message bridge between the caller UA and the called UA.It will find the position and calling strategy information of the called UA firstly when the proxy server receive the session request from the caller UA.Only to find the called UA and the calling is allowed,the proxy server will send the session request .Generally,proxy server is required in the SIP session.

1.1.4 Redirect Server

Redirect server is to specify the location of the recalled UA calling UA specified to caller UA. If the caller UA calling called UA, it will search the

location information when the server receive the session request messsage from the caller UA,, and then send it back to the calling UA, enabling the caller UA initiate a session request back to this position. This position can be the position of called UA, and it can also be a proxy server location. Then the next process is same to the proxy server.

1.1.5 Loacation Server

Location server supply the information of UA to the proxy server and the redirect server, it record the information of the UA fron the registrar server.The location server and the registrar server are on the same device generally.

1.1.6 Registrar Server

Registrar server accept the users's registrations,and the content (such as the locate number and other information) are always stored on the location server for subsequent queries using .All two are all logic components and store on the same server generally.

1.2 The function and feature of SIP

1.2.1 Function

Five basic functions of SIP:

- Locate the called SIP user's position:.We can use the registration information or other positioning server to achieve user positioning, such as DNS, LDAP and so on,it can provides location-based services to enhance its positioning function.
- Determine availability of user: Make sure that the called terminal can attend this session. SIP supports multiple address description and addressing modes, including: name @ host address (such as ab@172.18.24.10), called number @PSTN gateway address (123456@172.18.24.11) and ordinary telephone number (such as 010-12345678) and so on. So, SIP caller can identify the called whether in the traditional telephone network according to the called

address,, and then through a traditional telephone network connected to the gateway initiated and call create calling.

- Determine the capacity of user: Identifying the media type and media parameters of the called terminal that can be used to participate in a session.Their own carried media type and media parameters of SIP terminal in the process of message interaction makes the session both can identify their conversationl capacities.
- Create session : SIP sessions, the two parties, finally chose the ability which both has to establish a session through the consultation about media type and media parameters
- Manage session:You can change session parameters or abort session

1.2.2 Feature

Features of SIP are as follows:

- Open standard:Different new features, products and services introduced by the operators work together for the free choose.
- Flexibile configuration:Compatible with a variety of dialing mode, achieve on a wired or wireless device, highly flexible configuration, work collaboratively together with other systems.
- Expandability: With the expansion of enterprise scale, system also can be expanded.
- Support remote users: The network of enterprise can extend to anywhere no matter where the users are.
- Same communication aggrement between the differenet departmentals of enterprise .Branch office, home office and business workers use the same dialing method and system access method, and it's ease to manage.
- Start quickly. The system should do some corresponding change quickly when establishing new branches, recruit new employees, rearranging the staffs or change their workingplaces.
- Easy install and maintenance: Unprofessionals also can install or maintain SIP system

1.3 SIP message

SIP message use text encoding, including message request and message response.

SIP message request include INVITE、ACK、 OPTIONS、 BYE 、 CANCEL and REGISTER.INVTE message use for inviting a user joins a calling.RFC3262 defines the request message include the following five kinds.

- INVITE :Invite a user joins a calling
- ACK: Comfirmation of response message to the request message.
- OPTIONS:Use for request negotiation capacity information
- BYE:Use for releasing the established calling
- CANCEL：Use for releasing the unestablished calling
- REGISTER: Use for registering location information of the user to the SIP registar server.

The SIP response message is used to responed the request message, indicating a success or failure condition from the calling or registaration. Different types of response messages can be distinguished by the state codes.The status code contain three integers, the first used to define the type of response; the other two are used to further detailed description to the response. The classification of the response message classification is shown in table 1.

Table1 Number of response message

Number of state code	Message meaning	Message classification
100~199	Receive request and being processed	Temporary message
200~299	Request has received and being processed successfully Accept the request	Process successfully
300~399	To complete the	Redirect

	request require further operation	
400~499	Message has syntax error, the server cannot process the request	Client error

1.4 Brief introduction of SIP working principle

1.4.1 Registration

In a complete SIP system, all of the SIP terminal as User Agent should register on the registar server, to inform their position, conversational ability, calling strategy and other information. Usually, it will send a registration to the registar server when the SIP terminal boot or perform the registration operation, and the message carries all the necessary information for the registration. Register server transmits a response message to the terminal after receiving the registration request message, to inform that the request message has been received. If the registration is successful, then transmits “OK" news to the terminal. As shown in figure 1.

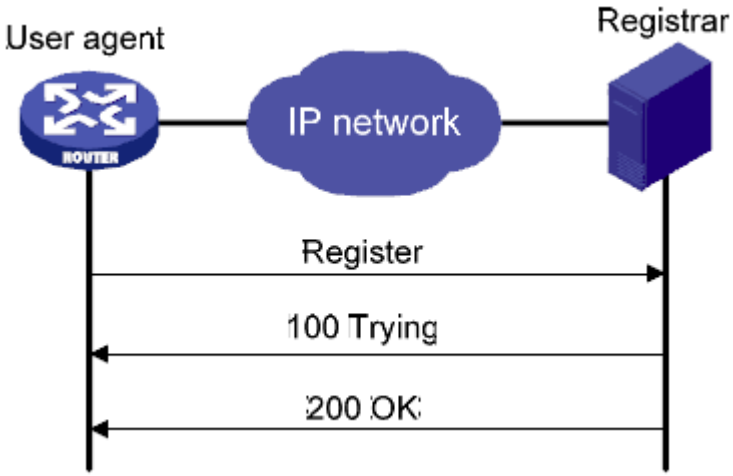


Figure1 Registration message interfaction between the UA and the Registrar

1.4.2 Establish calling

The SIP protocol uses Client/Server model, it mainly through the communication between the UA and proxy servers to complete the calling process of the user.

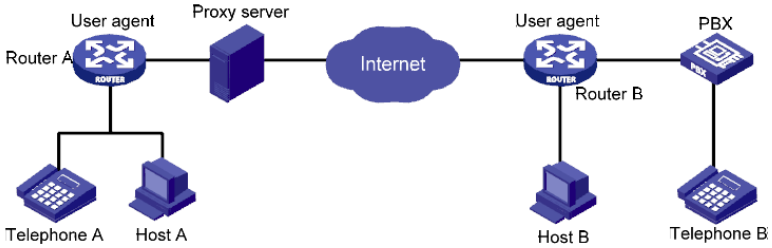


Figure2 UA UA Estabilsh the calling through Proxy Server

As shown in figure 2, the Telephone A need to call Telephone B,and the two router as SIP the terminal(UA).Router A will send the session request message to the Proxy Server after Telephone A dial the phone number of Telephone B . Proxy Server sends a session request to the router B through the search the corresponding information of Telephone B number .Router B receives the request, if it is available, and then sends the response to Proxy Server, and the Telephone B ringing. Proxy Server sends the response message to the Router A after receiving the response. And this transponder should include: two temporary response (100 Trying and 180 Ringing) and a successful response (200 OK). The message interaction of the whole process is as shown in figure 3.

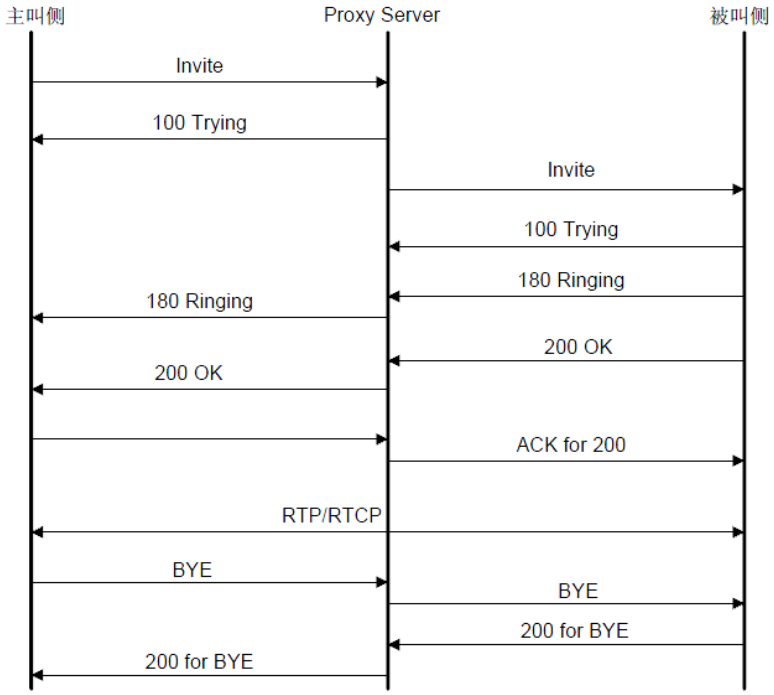


Figure 3 Process figure of calling creation by Proxy Server

This example is a simple application, it only use a proxy server. But in a complex application, it can have multiple proxy servers and registration servers.

1.4.3 Redirect calling

If SIP redirect server receives a session request message, it will not forward the session request message, but inform the called terminal SIPS address in the response message. The calling terminal sends the session request message directly to the called terminal. The called terminal will also directly sends a response message to the calling terminal. The interaction message of the calling progress as shown in Figure 4

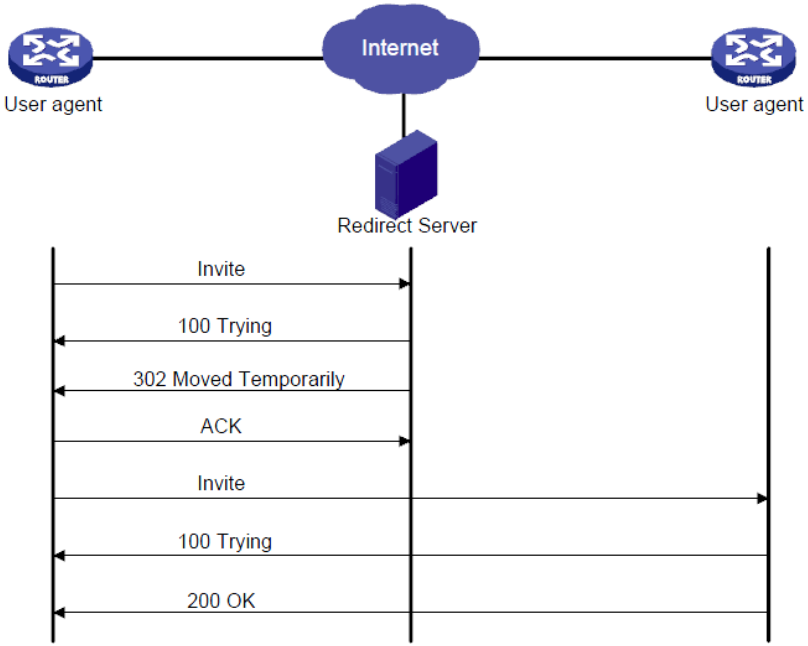


Figure 4 UA redirects calling progress

This is common application. From the principle of speaking, redirect server can also reply the address of the proxy server to the calling terminal, then the next calling process are the same with the proxy server .

2 Voice service configuration of ONU

2.1Overview of voice system

GT83x/86x series of voice gateway equipment support the SIP UA function, provide the following voice calling mode:

- Calling via the SIP server:ONU telephone user registers on Proxy/Registar server,calling(include the caller and the called) need to through proxy server.And this model is applied to the carrier network as long as the proxy assigned telephone number to the ONU telephone user (to allow the registration, it may also need authentication information), you can dial the telephone

number to initiate a calling or accept a calling(without the manual configuration to the SIP URI address of all end users); this mode supports large network, and support user mobility .The server platform can also provide billing, authentication, private network penetration management mode;

The following graphic describle the network topology diagram of calling mode (The device that unrelated to the SIP voice business is not marked)

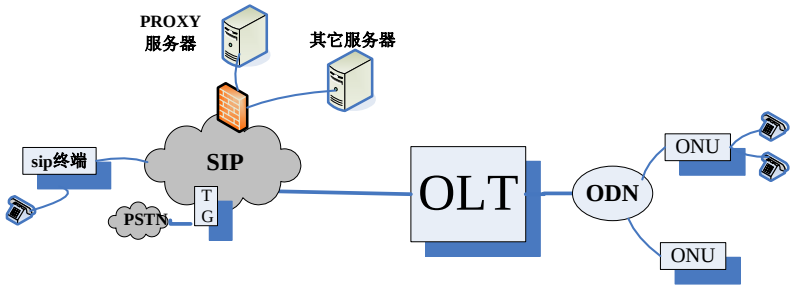


图 经由proxy的呼叫模式

The most basic configuration content of SIP server :

- System configuration(such as the network addres used by voice service and the default router information)
- Protocol configuration（such as the monitor port of SIP protocol message）;
- Local phone number;
- Configuration of proxy server;
- if required certification, also need to configure user authentication information

With the support of SIP platform server support, GT83x/86x can achieve:

- Interconnection with the SIP terminal,including SIP IAD、

SIP PHONE、video phone and SIP soft phone;

- Interconnection with the un-SIP VOIP terminal,include H.323,MGCP,H.248 terminal and so on(sSIP platform need to supply the intercommunication capability with H.323 network, CA GK MGCP network)
- Interconnection with the traditional PSTN telephone（the server platform need provide the interconnection via a TG gateway and PSTN network ）

2.2 System configuration

GT83x/86x series voice gateway equipment must configure system network parameter, and only in this way that the device can work normally.

Support configuration static network address or through the DHCP server get the network address dynamiclly, (if the configuration command under the ONU node, GT83x can directly into the ONU node; GT86x requires advanced to PTY mode, then go to the ONU node) the related configuration commands are as follows:

Command	Specfication
voice ip address <A.B.C.D/M> voice ip address <A.B.C.D> <A.B.C.D>	Configure IP addres of voice module
voice ip gateway <A.B.C.D>	Configure IP gateway addres of voice module
voice ip address dhcp	Configure IP address which get from the DHCP server of voice module
show voice ip address	Display IP address information of voice module
show voice ip gateway	Display IP gateway address information of voice module
voice dns [enable|disable]	Enable/Close DNS CLINET function

voice dns server add <A.B.C.D> {[primary]}*1	Add address of DNS server < A.B.C.D >：the need added server IP address of DNS Primary： Set< A.B.C.D > tp DNS server，parameter is optional
voice dns server del {<A.B.C.D>}*1	Delete addddres of DNS server s
show voice dns info	Display DNS service information of voice module

Note:1) in the use of dynamic IP address mode, no longer need to manually configure IP address, mask; (the default route whether need configure depending on the DHCP server capacity)

2) Part of the DHCP server may not provide a default route, the users should manually configure a default route; ONU will report access failure alarm to route.

2.3 Configuration of SIP protocol

Configuration of SIP protocol:

- Because ONU supports SIP, H.248 and other voice protocols, ONU initial default all voice protocol is closed, so first to enable SIP protocol when configure SIP protocol,
- Configuration of SIP server
- It requires to provide authentication information for accessing to prevent unauthorized users (optional)
- Configure telephone number
- Configure username for management and maintenance(optional)

Command	Specification
sip enable	Enable SIP protocol
sip	Enable or close appointed telephon,the default

[phone1|phone2|phoneall] [enable|disable]	is enable
sip [phone1|phone2|phoneall] username <name>	Configure username of SIP local port,it's always telephone number
sip [phone1|phone2|phoneall] account <account>	Configure username of SIP
sip [phone1|phone2|phoneall] password <pass>	Configure password of SIP
sip [phone1|phone2|phoneall] displayname <name>	Configure display name of local port, the name will be included in the URI of SIP
sip [phone1|phone2|phoneall] outboundproxy address <address>	Configure address of proxy server;(it can be the DNS)
sip [phone1|phone2|phoneall] outboundproxy port <1-65535>	Configure UDP port number of proxy server
sip [phone1|phone2|phoneall] server address <address>	Configure address of SIP server(It can be the DNS)
sip [phone1|phone2|phoneall] server port <1-65535>	Configure port number of SIP server
sip [phone1|phone2|phoneall]	Configure domain name of SIP registar server(or IP address)

registar realm <realm>	
sip [phone1|phone2|phoneall] registar port <1-65535>	Configure port number of SIP registration server
sip [phone1|phone2|phoneall] local port <1-65535>	Configure port number of local UDP
sip [phone1|phone2|phoneall] expires <60-3600>	Configure the default server cycle
sip [phone1|phone2|phoneall] server-heart [enable|disable]	Enable or disable the server-heart function
sip [phone1|phone2|phoneall] server-heart interval <10-600>	Configure server-heart interval of SIP phone
sip [phone1|phone2|phoneall] session-heart [enable|disable]	Enable or disable session-heart function
sip [phone1|phone2|phoneall] session-heart interval <1-60>	Configure session-heart interval of SIP phone
sip user-agent <string>	Configure user-name of SIP
sip dns srv-record [enable|disable]	Configure SIP DNS-SRV address selection, when a domain name corresponding to multiple IP addresses, it can retry another address if an

	address failure
sip prack {[enable|disable]}*1	Display、enable or disable PRACK No parameter:Display PARCK whether enable,and PRACK is the default
sip replaces {[enable|disable]}*1	Display、enable or disable replace session function No parameter:Display PARCK whether enable,and replace session is the default
sip number-prefix 0 {<name>}*1	Display or configure the first number 0 represents the number prefix None of the parameters: displays the current number 0 represents the code prefix Prefix number, general national number, default is" +86"
sip tel-uri {[enable|disable]}*1	Display、enabel or disable URL format of Telephone,such as(tel:+86075987654321) None of parameter:Display the URL format of current using telephone whether Tel format Default disable Tel URL format
sip cwring-normal {[enable|disable]}*1	Display, enable or disable the special response ring number for call waiting None of the parameters: displays the response ring number of current call waiting The default value is disable: the special response ring number is 182 of calling waiting
sip dist-ring {<0-4>}*1	Display or configure the special ringtone for distinguish different rings None of the parameters: show the special ringtone for distinctive ringing selection

	<0-4>: Special tone of the group ringing ,0 is the ringing tone of out-group , the default is 1
sip call-forward {[refer|302]}*1	Display or configure the call -forward method None of the parameters: displays the current call -forward method The default value is refer: using the REFER method to realize call -forward
sip server-heart method {[options|register]}*1	Display or configure server-heart detection method of registration server None of the parameters: displays the current call -forward method The default value is options: Use the OPTIONS method to realize the server-heart detection of registration server
sip session-heart method {[options|info]}*1	Display or configure session-heart detection method of registration server None of the parameters: displays the current call -forward method The default value is options: Use the OPTIONS method to realize the session-heart detection of registration server
sip dtmf-relay {[info|in-band]}*1	Display or configure DTMF transmission method None of the parameters: displays the current call -forward method The default value is Info: using the INFO method, to transmit the DTMF This command only works in the command of voice dtmf-relay disable Use RFC2833 telephone-event to transmit DTMF for Voice dtmf-relay enable

2.4 Dialing rules of SIP terminal

In SIP or H323 protocol, need to collect user dial in IAD before reporting, IAD achieve number collection by digitmap. The default digitmap of IAD is : *XX|XX.T|XX.#|****, wherein XX.T represents random digit dial, report after 5 seconds; XX.# represnts random digit dial and # as the end; *XX * means the start number report after received two digits immediately, report immediately when dial continuous 4 * in the using of the supplementary service, and it's used when IAD use telephone configuration and query . The detailed description about digitmap please refers to the RFC3435.

Command	Specification
dial-plan add <dialplan>	Configure dialing rules of SIP terminal
dial-plan delete <dialplan>	Display mapping rules of the called number
dial-plan match-mode {[longest|shortest]}*1	Display or configure the match rules of dial plan
dial-plan buildin	Use the built-in dialing plan of the system, the default is domestic dialing plan

2.5 Configuration of voice interface

Support service configuration on pots user port of ONU

- Configuration of supplement-servce
- Configuration of voice quality capacity
- Fax service

Commnd	Specification
voice dtmf-relay [enalbe|disable]	Configure signal relay mode of DFTM enable:Enable dtmf signal through RFC2833 telephone-event relay

	disable:dtmfvsignal tranmsit by band-in
voice ecan [enalbe|disable]	Configure canceller of echo
voice fax [t38|pass-through]	Configure FAX transmission mode; T38:FAX transmission mode is T38-relay mode, does not support currently Pass-through:FAX transmission mode for belt transmission
voice phone <1-2> [rx-gain|tx-gain] [m|p] [<0-18>|default]	Configure telephone gain Rx-gain: receive gain Tx-gain: transmission gain M/p : the negative / positive (Minus value/Positive value) 0-18: gain value, the unit is DB
voice vad [enalbe|disable]	Configure MUTE detection
voice prefer_codec [pcmu|pcma|g723|g726_32|g729]	Configure the prefer_code of voice
show voice [vad|dtmf-relay|ecan|gain|fax]	Show voice configuration
show voice running-config	Show running configuration of voice module
show voice startup-config	Show the startup configuration of voice module
show voice call-status	Show the call-status of current voice
show voice phone-status	Show the phone-status of current voice
show voice codec-statistics	Show the codec-statidtics of voice
voice codec-statistics clear [phone1|phone2]	Clear the codec-statistics of voice

voice acl [limitedout|blacklist] [add|delete] <number_template>	Configure call restriction function of telephone, limitedout and limitedin. Limitedout: configure call limitedout lists Blacklist:configure call limitedin black list Add: add a call restriction Delete: remove a call restriction <number_template>: number templates, similar to the input of dialing rule, but It only supports " +.X[-]"
show voice acl	Show all calling limited items

2.6 Configuration of supplement-service

Command	Specification
sip supplement_service {[local|soft-switch]}*1	Display the support way of the configuration of SIP supplement-service None of the parameters: displays current SIP supplement-service support way The default value of soft-switch : select the server to support the supplement- service
voice supplement-service [phone1|phone2|phoneall] dont_disturb [enable|disable]	Configure the dont_disturb service of the enable terminal
voice supplement-service	Configure the call_hold service of

[phone1|phone2|phoneall] call_hold [enable|disable]	the enable terminal
voice supplement-service [phone1|phone2|phoneall] call_waiting [enable|disable]	Configure the call_ waiting service of the enable terminal
voice supplement-service [phone1|phone2|phoneall] call_transfer [enable|disable]	Configure the call_ transfer service of the enable termina
voice supplement-service [phone1|phone2|phoneall] fwd_busy <fwd_number> [enable|disable]	Configure the fwd_busy service of the enable terminal
voice supplement-service [phone1|phone2|phoneall] fwd_no_reply <fwd_number> [enable|disable]	Configure the fwd_no_reply service of the enable terminal
voice supplement-service [phone1|phone2|phoneall] fwd_uncond <fwd_number> [enable|disable]	Configure the fwd_uncond service of the enable terminal
voice supplement-service [phone1|phone2|phoneall] hot_line <hotline_number> [enable|disable]	Configurre the hot_line service of the enable terminal
show voice supplement-service	Show the configuration information of the supplement-service

2.7 Configuration of voice QOS

Support VLAN ID and COS parameters of setting the ONU voice protocol flow / mediad stream:

Command	Specification
vlan dot1q_add <2-4094>	Create voice transmit VLAN
vlan dot1q_port_add <2-4094> <port_list> [1|2]	Add voice port into the voice vlan The voice port of GT831 is 5, and the GT866 is 17. The voice port of GT863 is 25. Choose the untag voice port mode
qos vlan priority_mode {[up|down] [priority_translation|priority_vid]}*1	Enable priority based on vlan-id
qos classifier vlan-id <vid> [up|down] <0-7> <0-7> [0|1]}*1	Set the COS parameter of ONU voice VLAN ID <0-7> Priority <0-7> Queue [0|1] [Disable|Enable]

2.8 Save of ONU configuration

Command	Specification
mgt config save	Save the configuration into the flash of ONU

3 Configuration of OLT

The package and unpackage of SIP voice data can be realized at ONU side, and OLT only provide transmission channel. In order to cooperate with the ONU to transmit voice data, OLT need to configure VLAN, and set the Qos priority of voice data, configure the uplink DBA.of ONU

3.1 Configuration of vlan

Command	Specification
interface vlan <vlanname> {<1-4094>}*1	Create vlan,enter into vlan configuration mode
[add|delete] port <portlist> [tagged|untagged]	Add or delete port to the VLAN

3.2 Configure prority transmittion based on VLAN

Create business flow classification

Command	Specification
class-map <class_map_name>	Create business flow classification in the configuration mode of config
match vlan-id <1-4094>	Add the rule match to the vid in the configuration mode of Class Map

Create supervision strategy of traffic

Command	Specification
policy-map ingress <policy_map_name>	Create supervision strategy of traffic in the config configuration mode
policy-map ingress <policy_map_name>	Match business flow in the Policy Map configuration
set user-priority <0-7>	Set COS in the traffic classification configuration mode

Apply traffic policy strategy at the uplink port

Command	Specification
interface ethernet <slot/port>	From config configuration mode into interface configuration mode
service-policy ingress [<1-5000>|<policy_name>]	Applying strategy

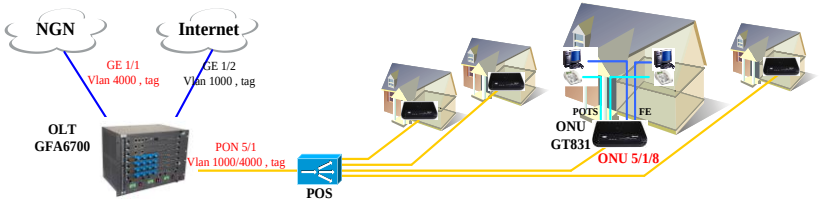
3.3 Configure uplink DBA of ONU

Configure uplink DBA of ONU under the PON configuration node

Command	Specification
bandwidth class <0-7> delay [high|low] {fixed-bw <0-1000000>}*1 assured-bw <64-1000000> best-effort-bw <64-1000000> [up|down] <onuid_list>	Configure uplink DBA of ONU

4 Configuration case

Application topology：



Configuration content：

EPON_V2R1(config)#int vlan NGN 4000

EPON_V2R1(vlan-Voip)#add port 1/1,5/1 tagged

EPON_V2R1(vlan-Voip)#exit

GFA6700(config)#class-map NGN

GFA6700(config-cmap)#match vlan-id 4000

GFA6700(config-cmap)#exit

GFA6700(config)#policy-map ingress NGN

GFA6700(config-policymap)#match class-map NGN

GFA6700(config-policymap-c)#set user-priority 7

GFA6700(config-policymap-c)#exit

GFA6700(config-policymap)#exit

GFA6700(config)# interface ethernet 1/1

GFA6700(if-eth1/1)#service-policy ingress NGN

GFA6700(if-eth1/1)#exit

GFA6700(config)# pon 5/1

GFA6700(epon-pon5/1)#bandwidth class 2 delay low fixed-bw 5000 assured-bw 10000 best-effort-bw 50000 up 8

GFA6700(epon-pon5/1)#onu 8

GFA6700(epon-onu5/1/8)#voice ip address 58.240.118.242/30

GFA6700(epon-onu5/1/8)#voice ip gateway 58.240.118.241

GFA6700(epon-onu5/1/8)#sip phoneall registar realm 58.241.184.4

GFA6700(epon-onu5/1/8)#sip phoneall registar port 5060

GFA6700(epon-onu5/1/8)#sip phoneall outboundproxy address 58.241.184.4

GFA6700(epon-onu5/1/8)#sip phoneall outboundproxy port 5060

GFA6700(epon-onu5/1/8)#sip phoneall server address 58.241.184.4

GFA6700(epon-onu5/1/8)#sip phoneall server port 5060

GFA6700(epon-onu5/1/8)#sip phoneall local port 5060

GFA6700(epon-onu5/1/8)#sip phone1 username 02566695004

GFA6700(epon-onu5/1/8)#sip phone1 displayname 02566695004

GFA6700(epon-onu5/1/8)#sip phone1 account 02566695004

GFA6700(epon-onu5/1/8)#sip phone1 password 5064712807

GFA6700(epon-onu5/1/8)#sip phone2 username 02566695014

GFA6700(epon-onu5/1/8)#sip phone2 displayname 02566695014

GFA6700(epon-onu5/1/8)#sip phone2 account 02566695014

GFA6700(epon-onu5/1/8)#sip phone2 password 2079934815

GFA6700(epon-onu5/1/8)# dial-plan add 13XXXXXXXXX

GFA6700(epon-onu5/1/8)# dial-plan add 15XXXXXXXXX

GFA6700(epon-onu5/1/8)#voice dtmf-relay disable

GFA6700(epon-onu5/1/8)#sip enable

Change the system mode to SIP,Please save config and restart your system!

GFA6700(epon-onu5/1/8)#vlan dot1q_add 4000

GFA6700(epon-onu5/1/8)#vlan dot1q_port_add 4000 5 2

GFA6700(epon-onu5/1/8)#qos vlan priority_mode up priority_vid

Setting up stream qos vlan priority mode to priority_vid SUCCESS.

GFA6700(epon-onu5/1/8)#qos vlan priority_mode down priority_vid

Setting down stream qos vlan priority mode to priority_vid SUCCESS.

GFA6700(epon-onu5/1/8)#qos classifier vlan-id 4000 up 7 7 1

Add priority manipulate rule for ether-type 100 SUCCEED.

GFA6700(epon-onu5/1/8)#qos classifier vlan-id 4000 down 7 7 1

Add priority manipulate rule for ether-type 100 SUCCEED.

GFA6700(epon-onu5/1/8)#mgt config save % Config data save finished.

Config file saved success.

Config file saved success.

GFA6700(epon-onu5/1/8)# mgt reset

GFA6700(epon-onu5/1/8)#exit

GFA6700(epon-pon5/1)#exit

GFA6700(config)# save configuration

11 TDM service configuration

1 Overview

In EsayPath EPON products, the use of GFA6700 (OLT) configured GFA-TDM card, remote use GT861A (ONU) configurations GT-4E1 card, you can carry TDM (E1) Transmission service.

GFA-TDM E1 cards provide three clusters (E1 FPGA), each cluster provides eight E1 E1 ports, a total of 24 E1 links.

Note!

GFA-TDM and GFA-SIG board can not be used in GFA6700.

2 Configure E1 link

2.1 Confirm board status

GFA-TDM board can be inserted in any slot between slot5 and slot8.

GFA6700(config)#show slot

Slot	CfgType	InsertType	RunningState	WorkMode	Redundancy
1	AUTO	GFA-GET	RUNNING	SLAVE	-
2	AUTO	EMPTY	-	-	-
3	AUTO	GFA-SW	RUNNING	MASTER	ACTIVE
4	AUTO	EMPTY	-	-	-
5	AUTO	EMPTY	-	-	-
6	AUTO	GFA-TDM	RUNNING	SLAVE	-
7	AUTO	EMPTY	-	-	-
8	AUTO	GFA-EPON	RUNNING	SLAVE	-

9 AUTO EMPTY - -
-
10 AUTO EMPTY - -
-
11 AUTO GFA-PWU220 RUNNING
SLAVE -

2.2 Enter into TDM-E1 node

Command	Specification
GFA6700(config)# tdm e1 GFA6700(epon-tdm-e1)#	Enter into TDM-E1 node

2.3 Configure E1-VLAN

Because TDM-E1 service jitter and delay sensitive, so in order to prevent other broadband data services for the same business within the system hosted TDM impact method using the E1-VLAN TDM E1 service and other services separated. And configure a certain priority (802.1P) to ensure the transmission of TDM-E1 business performance.

Command	Explain
GFA6700(epon-tdm-e1)#e1-vlan <slot/fpgaportlist> vlan-id <1-4094> priority <0-7> GFA6700(epon-tdm-e1)#undo e1-vlan <slot/fpgaportlist>	Create and delete E1 VLAN

2.4 Configure E1 link

Create E1 link between OLT and ONU

Command	Explain
GFA6700(epon-tdm-e1)#add e1-link <slot/e1portlist> onu-e1 <slot/port/onuid> <slot/e1portlist> GFA6700(epon-tdm-e1)# delete e1-link <slot/e1portlist>	Create and delete E1 VLAN

2.5 Configure E1 port loop-back

When doing the link test is often necessary to observe the E1 port loopback link status. In GROS system, there are two each E1 port loopback mode: circuit and system.

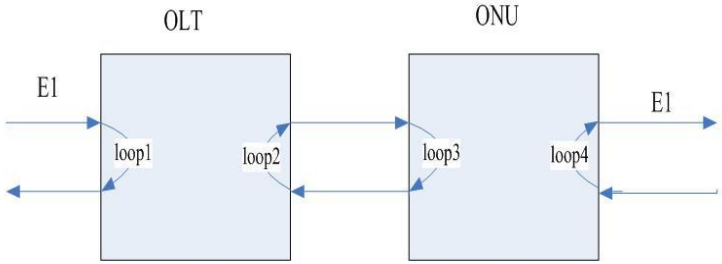


Figure 11-1 E1 port loop-back

Figure in loop1 and loop4 the circuit loopback mode, loop2 and loop3 the system loopback mode.

Command	Explain
GFA6700(epon-tdm-e1)#olt-e1-port loopback <slot/e1portlist> {[circuit|system]}*1 GFA6700(epon-tdm-e1)#onu-e1-port loopback	OLT-side configuration, and to cancel,

<slot/port/onuid> <slot/e1portlist> {[circuit|system]}*1 GFA6700(epon-tdm-e1)#undo olt-e1-port loopback <slot/e1portlist> GFA6700(epon-tdm-e1)#undo onu-e1-port loopback <slot/port/onuid> <slot/e1portlist>	ONU side of the E1 port loopback

2.6 Configure E1 alarm screen

Command	Explain
GFA6700(epon-tdm-e1)#alarm-mask olt-e1-port <slot/e1portlist> [all|los|ais] GFA6700(epon-tdm-e1)#alarm-mask onu-e1-port <slot/port/onuid> <slot/e1portlist> [all|los|ais] GFA6700(epon-tdm-e1)#undo alarm-mask olt-e1-port <slot/e1portlist> [all|los|ais] GFA6700(epon-tdm-e1)#undo alarm-mask onu-e1-port <slot/port/onuid> <slot/e1portlist> [all|los|ais]	OLT-side configuration, and to cancel, ONU side shielded E1 alarm

3 Configuration case

Note!

Each E1 link will occupy a certain bandwidth of PON link, so ONU configuration E1 link bandwidth allocation, in addition to considering the bandwidth of broadband services, but also take into account to the E1 link with sufficient bandwidth . Generally an E1 link, use the link in the PON about 3Mbits bandwidth.

Step	Command	Explain
Step 1	GFA6700(config)#interface vlan e1_vlan 1000 GFA6700(vlan-v1000)#add port 1/1,6/1 tagged GFA6700(vlan-v1000)#exit	Configuring VLAN, as the bearer of a dedicated E1 service VLAN. Port 6 / 1 that <slot/E1fpga_id>.
Step 2	GFA6700(epon-pon5/1)#bandwidth class 2 delay low assured-bw 30000 best-effort-bw 100000 up 4	For service with E1 ONU, to allocate sufficient bandwidth
Step 3	GFA6700(epon-tdm-e1)#e1-vlan 6/1 vlan-id 1000 priority 7	Into the E1 node, configuration E1 VLAN, and configure a certain priority (802.1P)
Step 4	GFA6700(epon-tdm-e1)#add e1-link 6/8 onu-e1 7/1/23 2/1	OLT and ONU-side configuration side E1 link connection establishment. Where 6 / 8 that <slot/e1

		port>
Step 5	GFA6700(epon-tdm-e1)#show e1-link	View the current link configuration of E1

12 System Maintenance

1 FDB table

The central office equipment in the EsayPath EPON FDB in two forms, the exchange of chips and PON chips; for the remote device is only one FDB table

1.1 Overview of FDB table

Switch receives Media Access Control (MAC) address information from its all ports to form a MAC address table and maintain it.When the switch receive a frame,it will decide whether filter or forward the frame according to its MAC address table.At this point,the maintained MAC address table is the FDB address table.

Content of FDB

FDB address table contains multiple entries; different products FDB address table entries contain a different number. Each FDB entry address table composed of the following:

- Received data source device MAC address
- Connect the data source device port symbol
- Flag symbol
- Belongs to VLAN name

If the purpose of data frames received MAC address is not in the MAC

address table, then the data will be sent to the data source device VLAN that belongs to all ports

Address table type of FDB table

There are three address Mac address table entries:

- Dynamic address entries

Initially, the switch to all MAC addresses in the address table entries are dynamic; If after a period of time (aging time Agingtime), the device has no data, then the address table entry will be deleted, this can prevent the address table items become too large; when convinced that a device from the network after the removal, put the address of the device entry removed; when the switch off after a reboot or reset, all dynamic address entries will be deleted.

- Fixed address table entries

If the aging time is set to 0, then the address entries stored in the MAC address table and will not be dynamically removed until the switch off or restart. Permanent address entry will remain a permanent address entries stored in the MAC address table, even if the switch off or restart.

- Static address table entries

It must be manually setted by the system administrator. All input from the command line static address entries will be stored as a static address entry.

Way to add address entries

FDB address in the address table entries can be added through the following two ways:

- Switch from learning. Can switch packets received by the source MAC address, the port received the packet, the port received a packet where the address of VLAN to automatically update the FDB table
- Manual configuration. Command line interface can be added manually to the address table entry address table in the FDB

1.2 Configuration of FDB table

1.2.1 Aging time of configuration entry

Command	Specification
GFA6700(config)#forward-entry agingtime [0|<10-1000000>]	Configure FDB table aging time of switch chip
GFA6700(epon-pon7/1)#aging-mac-time <5-86400>	Configure FDB table aging time of PON chip
GT811_A-7/4/1(config-onu-mgt)#atuaging {[0|<15-3825>]}*1	Enter into the ONU node to configure FDB table aging time of ONU in the PTY mode

1.2.2 FDB table to create a static address table entries

Command	Explain
GFA6700(config)# forward-entry mac <H.H.H> vlan <vlanname> <slot/port>	FDB configuration switch chip static address table entry (Ethernet port)
GFA6700(config)# forward-entry mac <H.H.H> vlan <vlanname> <trunkname>	FDB configuration switch chip static address table entry (TRUNK ports)

GT811_A-7/4/1(config-onu-mgt)#atu static_add <mac> [0|1] <portlist> {<1-4094>}*1 {<0-7>}*1 GT811_A-7/4/1(config-onu-mgt)#atu static_del <mac> {<1-4094>}*1	PTY mode, enter the ONU nodes, configure or remove the ONU of the FDB table static address table entries

 **Note!**

Central office equipment PON chips FDB table can not add a static address entry.

1.2.3 Delete FDB table address table entries

Command	Explain
GFA6700(config)# delete forward-entry mac <H.H.H> vlan <vlanname>	Delete entry FDB Switch Chip
GFA6700(epon-pon7/1)# delete fdbentry mac <H.H.H>	Delete FDB entries PON chips
GT811_A-7/4/1(config-onu-mgt)#atu clear {[all|dynamic]}*1	PTY mode, enter the ONU nodes, delete the FDB entry ONU

1.2.4 Drop table address illegal FDB entries

Command	Explain
GFA6700(config)#forward-entry mac <H.H.H> vlan <vlanname> <slot/port> drop [src_drop|dest_drop|all]	FDB table drops, the address of illegal entry
GFA6700(config)# delete forward-entry drop mac <H.H.H> vlan <vlanname>	FDB table to cancel the address configuration discarding illegal entry
GT811_A-7/4/1(config-onu-mgt)#atu filter {[source|dest] <mac> [drop|cpu|dp|both] [0|1]}*1	PTY mode, enter the ONU nodes, configure or cancel the drop table address illegal FDB entries

 **Note!**

Central office equipment PON chips FDB FDB table can not be set to discard the illegal entry.

1.2.5 View FDB table address table entries

Command	Explain
show forward-entry agingtime show forward-entry count port <slot/port> vlan <vlanname> {[static|dynamic]}*1 show forward-entry count port <slot/port>	According to various search criteria, view the exchange of chips

{[static|dynamic]}*1 show forward-entry count trunk <trunkname> vlan <vlanname> {[static|dynamic]}*1 show forward-entry count trunk <trunkname> {[static|dynamic]}*1 show forward-entry count vlan <vlanname> {[static|dynamic]}*1 show forward-entry count {[static|dynamic]}*1 show forward-entry drop show forward-entry port <slot/port> vlan <vlanname> {[static|dynamic]}*1 show forward-entry port <slot/port> {[static|dynamic]}*1 show forward-entry static {[mac] <H.H.H>}*1 {[vlan] <vlanname>}*1 show forward-entry trunk <trunkname> vlan <vlanname> {[static|dynamic]}*1 show forward-entry trunk <trunkname> {[static|dynamic]}*1 show forward-entry vlan <vlanname> {[static|dynamic]}*1 show forward-entry {[mac] <H.H.H>}*1 {[vlan] <vlanname>}*1	FDB address table entries
show fdbentry mac <H.H.H> show fdbentry mac counter show fdbentry mac {onu <1-64>}*1	According to various search criteria, view PON chips FDB address table entries

atu show counter atu show static {[unicast|multicast|all]}*1 atu show {<mac>}*1 atu show {<portlist>}*1	PTY mode, enter the ONU node, according to various search criteria, view the FDB address entry ONU

2 Loop-back detection function

Between the Ethernet switch port connected to the inappropriate or switch port failure resulting from the ring itself, which may cause network loops, and if the switch is not open STP-related functions, this loop will lead to endless packets Repeat forward to form a broadcast storm issues, resulting in network failure. In EsayPath EPON, the support loop automatic detection function, because the loop resulting from the reduction of network failures.

2.1 Overview of Function

For the EasyPath EPON loop detection, it default detecte all onu loop only below all the PON port and the the uplink port.

It will use the “report after detect loop” method for the lopp detection of uplink port, and it will not shundown the corresponfing uplink port.

For the onu port loop, it will shutdown the corresponding port if it has detected loop to avoid affecting the other users in the whole network.And it will also detect whether the loop is eliminated in the follow-up.For the instaneous loop (eliminated automatically in 3 detection period),it will make the port up again after a certain time.But for the uneliminated loop(uneliminate in 3 detection period),it will close the management of this port.

In addition, it can specify the MAC address of uplink BRAS or the gateway device on the PON port to avoid loop affects.And it can also

avoid affect the other users online if the MAC address of uplink BRAS or the gateway devce learned by the onu AFTER onu looped.

2.2 Function configuration

Step	Command	Specification
Step1	GFA6700(config)#loop-detection enable	Open loop-back detect function
Step2	GFA6700(config)#config loop-detection [mac] [<H.H.H>|default]	Configure loop detection packet source MAC address. The default device is the OLT MAC address.
Step3	GFA6700(config)#config loop-detection [vlan] [<1-4094>|all]	VLAN configuration loop detection range. The default is the system all of the VLAN
Step4	GFA6700(config)#config loop-detection port [<portlist>|all|default]	Loop Detection configured port range. By default only the detection system under all the PON port loop (ie, ONU side), the OLT

		uplink direction is not detected
Step5	GFA6700(config)#config loop-detection interval-time [<10-3600>|default]	Configured to send the message loop detection time interval. The default is 2 minutes
Step6	GFA6700(config)#loop-detection control enable	Configuration loop control enabled. When a loop, it will automatically close the loop port
Step7	GFA6700(config)#config loop-detection up-times <0-10> threshold <0-10>	Closed loop control of the port configuration detection time interval and the re-detection threshold
Step8	GFA6700(config)#show loop-detection	View loop alarms have occurred
Step9	GFA6700(config)#show loop-detection config	View configuration information loop detection

Step10	GFA6700(config)#olt-mac add 0000.0000.0088 to cni GFA6700(config)#olt-mac delete 0000.0000.0088	Add/remove PON static MAC address entries.All pon port will have the entry after the global adding.The main purpose for adding this configuration is to bind the BRAS MAC address,to prevent MAC address table learn the error BRAS mac address because the loop.
Step11	GFA6700(config)#show olt-mac	View pon static mac configuration

3 Optical power detection function

3.1 Overview of function

EsayPath EPON supporting infrastructure equipment and remote equipment, optical power detection. With this feature you can start and optical equipment failures and other issues play a supporting role. This feature can check the PON OLT port output power, received optical power and other parameters. And can set a certain threshold, which for

the occurrence of optical breakdown and other issues can play a preventive role

3.2 Function configuration

3.2.1 OLT-side optical power detection configuration

Command	Specification
optical-power [enable|disable]	Open or close the optical power detection function
optical-power interval <1-86400>	Configure detection cycle
optical-power alarm-threshold [olt|onu] <Tx_high> <Tx_low> <Rx_high> <Rx_low> optical-voltage alarm-threshold [olt|onu] <high> <low> optical-current alarm-threshold [olt|onu] <high> <low> optical-power threshold-deadzone <power> <tempertaure> <voltage> <current> optical-temperature alarm-threshold [olt|onu] <high> <low>	Configure alarm thresholds range for each parameter
show optical-power olt <slot/port> {[temperature|voltage|bias|power]}*1	View OLT PON parameters such as light-emitting power
show optical-power olt-rx <slot/port> <onuid_list>	View an ONU OLT side of the direction of the

	received power

3.2.2 ONU-side optical power detection configuration

Manage the ONU in the PTY method,enter into ONU ports.

Command	Explain
transceiver moniter {[0|<10-3600>]}*1	Enable optical power detection, and set the test period
transceiver threshold {[temperature|voltage|bias|rxpower|txpower] <low> <high>}*1	Set alarm thresholds for each parameter range
show transceiver {[temperature|voltage|bias|power]}*1	View the value of each parameter
show transceiver [config]	Viewing configuration information

4 Traffic/Performance statistics

4.1 Port traffic statistics

Command	Explain

GFA6700(if-eth1/1)#show statistics	Port node, view the statistics of each port
GFA6700(if-eth1/1)#clear statistics	Port node, clear the current value of all statistical projects and re-start statistics
GFA6700(epon-pon8/3)#show statistic pon	View PON port statistics

4.2 Performance statistics

Performance statistics for the OLT PON port, respectively, the history of statistics, ONU PON port historical statistics and real-time statistics.

Configuring OLT pon port and port historical statistics ONU pon

OLT PON port equipment is divided into 15-minute historical statistics and historical statistics 24 hours a historical statistics. Can be set for each survey cycle, statistical data stored items. Maximum 15-minute survey cycle, save the data set of 200 statistical items (> 2 days); 24-hour survey cycle 61 maximum set of statistical data stored items (> = 2 months); these data are consistent for each port in the config node configuration.

Historical statistics of the port, 15 minutes and 24 hours alone start.

Configuration step:

Step	Command	Explain
Step 1	GFA6700(config)# statistic-history bucket-num 15m <1-200>	Set all ports of the Historical

		Statistics of the PON 15 minutes cycle / Statistics of 24-hour cycle
Step 2	GFA6700(config)# statistic-history bucket-num 24h <1-60>	Set all ports of the Historical Statistics of the PON 15 minutes cycle / Statistics of 24-hour cycle
Step 3	GFA6700(config)# show statistic-history bucket-num	Show bucket num information
Step 4	GFA6700(config)# show statistic-history table [pon|onu]	Show olt pon or onu pon historical statistics to enable the table

Step	Command	Explain
Step 1	GFA6700(epon-pon8/3)#statistic-history [pon|<1-64>] {[15m|24h]}*1	PON port to enable the current or historical statistics to the PON port under the historical statistics onu
Step 2	GFA6700(epon-pon8/3)#show statistic-history data [15m|24h] {<1-1440>}*1	History shows the current PON port statistics. 15

		minutes / 24 hours of statistical data / bucketnum Information
Step 3	GFA6700(epon-pon8/3)#show statistic-history	The following shows the current PON port statistics to enable the port history

Configuration case

Case description

15-minute set of historical statistics, the number of 24-hour bucket

Configuration step:

Step	Command	Explain
Step 1	GFA6700 (config)#statistic-history bucket-num 15m 30 GFA6700 (config)#statistic-history bucket-num 24h 20	Configuration in config node
Step 2	GFA6700 (config)#show statistic-history bucket-num interval type bucket number 15Min 30 24h 20	Show configuration result

Enable pon4 / 1 port historical statistics, the history of statistics can onu

2

Configuration step:

Step	Command	Explain
Step 1	GFA6700 (config)#pon 4/1 GFA6700 (epon-pon4/1)#	
Step 2	GFA6700 (epon-pon4/1)#statistic-history pon 15m GFA6700 (epon-pon4/1)#statistic-history pon 24h GFA6700 (epon-pon4/1)#statistic-history 2	Pon ports were enabled for 15 minutes, 24 hours of historical statistics
Step 3	GFA6700 (epon-pon4/1)#show statistic-history port 1 history 15Min is enable port 1 history 24Hour is enable onuIdx history enable status 4/1/2 history 15Min is enable history 24Hour is enable	View configuration enable information
Step 4	GFA6700 (epon-pon4/1)#show statistic-history 15m-data 2007.1.27 19:31:27(MillSec 0) : History DropEvents : 0 History RevOctets : 259618238 History RevPackets : 3605677	Show OLT PON port historical statistical data for 15 minutes

	History RevBroadcastPkts : 700 History MulticastPkts : 3605404 History CRCAlignErrors : 0 History UndersizePkts : 0 History OversizePkts : 0 History Fragments : 0 History Jabbers : 0 History Collisions : 0	
Step 5	GFA6700 (epon-onu4/1/1)#show statistic-history 15m-data 2007.1.27 19:31:27(MillSec 0) : History DropEvents : 0 History RevOctets : 0 History RevPackets : 0 History RevBroadcastPkts : 0 History MulticastPkts : 0 History CRCAlignErrors : 0 History UndersizePkts : 0 History OversizePkts : 0 History Fragments : 0 History Jabbers : 0 History Collisions : 0	Show ONU PON port historical statistical data for 15 minutes

5 Alarm

5.1 Configuration and view of alarm

Command	Specification

config alarm-log [enable|disable]	Configure whether open the alarm log recording function
pwu-alarm [disable|enable]	Configure whether open power alarm function
temperature-monitor [enable|disable]	Configure whether open temperature alarm function
fan-monitor [enable|disable]	Configure whether open fan alarm function
fan alarm-threshold <rev>	Configuration the threshold of fan alarm
temperature alarm-threshold <high> {<low>}*1	Configuration the threshold of temperature alarm
mem-usage alarm-threshold [system|user] {<0-100>}*1	Configuration the threshold of memory utilization
cpu-usage alarm-threshold {<0-100>}*1	Configuration the threshold of CPU utilization
show alarm log [today|yestoday] show alarm log {[device|name|onu] <value>}*1 {[class] <1-5>}*1 {[trap] <1-151>}*1 {[start-time] [yestoday|today|<start_time>]}*1 {[end-time] <end_time>}*1	Query according to various search criteria alarm log

show environment-monitor show temperature	View the current information of fan and temperature
show current alarms {[level] <1-3>}*1 {[device] <dev_idx>}*1 clear current alarms {[level] <1-3>}*1 {<device_index>}*1	View/Delete the current alarm information according to thetype pf the device or the level of alarmThe most serious is the small level. The corresponding alarm presence / elimination and board the warning indicator light / destroy synchronization

5.2 Alarm screen

In many scenarios, often there are some unnecessary alarm information is recorded, reported. For example, in the application of FTTH scenario, ONU port UP / DOWN is very frequent, and the information is basically worthless. In this case, we can block out this information. Can prevent a large number of unwanted alarms reported to the network management system, a waste of resources

Command	Specification

alarm-mask olt-device [all|power|fan|cpu|temperature|register|present]	EsayPath EPON alarm conditions to provide shielding
alarm-mask olt-e1 <port_list> [all|los|lof|ais|rai|smf|lofsmf|crc3|crc6]	
alarm-mask olt-eth <slot/port> [all|link|fer|flr|ti]	
alarm-mask olt-pon <slot/port> [all|ber|fer|abnormal|aps|link]	
alarm-mask onu <onu_type> [all|power|fan|cpu|temperature|register|present|eth-link|eth-fer|eth-flr|eth-ti|eth-loop|pon-ber|pon-fer|pon-abnormal|pon-aps|pon-link|onuLaserAlwayOn|onuOpticalPowerLow|onuOptic alPowerHigh]	
alarm-mask onu-device <slot/port/onuid> [all|power|fan|cpu|temperature|register|present]	
alarm-mask onu-eth [all|link|fer|flr|ti]	
alarm-mask onu-pon <slot/port/onuid> [all|ber|fer|abnormal|aps|link]	

6 System log

6.1 Overview of system log

Log Module (Syslog) is mainly used to record the operation of the system and user behavior. Complete log module allows administrators to understand and monitor the system work and real-time recording system exception information. The system log information is from all the running modules, the log system to complete the collection, management, storage and display. Monitor log information can be displayed in the terminal; this approach is mainly used for debugging and viewing system status; also be stored to the log server, server, in this way for long-term operation of tracking systems and behavior of the user's command line

6.2 System log configuration

Configure at the configuration node:

Command	Specification
config syslog [enable|disable]	Open or close log service function
config syslog server [enable|disable]	Log module configured to save log information to the log server
config syslog server type [<name>|all] [enable|disable]	Whether a particular type of configuration information is

	saved to the log server
config syslog server lowest-level <0-7>	Configuration of a level above (including the level) of the information is saved to the log server
record command-line server [enable|disable]	The command line configuration is saved as a record to the log server
config syslog server [add|delete] <A.B.C.D> {[port] <1-65535>}*1 {[facility] <0-7>}*1	Add or delete the log server. port that is receiving log log server process on the service port number; facility that is the log information is saved to the log server file index number
config syslog monitor-screen [enable|disable]	Configure whether to log information output to all

	terminals
screen monitor undo screen monitor	Configured to open or close the log information output to the current terminal
monitor lowest-level <0-7>	Configuration in the current output of a level above the terminal log information (including the level).
monitor type [<typename>|all] [enable|disable]	Configuration in the current output terminal of a type of log information
monitor timestamp [none|time|datetime]	Configure the terminal output in the current time information
alarmlog-to-syslog [enable|disable]	Configure whether to save the alarm log information to the system log

show syslog configuration show syslog server configuration show monitor configuration show nvram syslog	View the system log configuration; View the contents of the current system log.

6.3 Configuration case

Step	Command	Explain
Step 1	GFA6700(config)#config syslog enable	Enable syslog server.
Step 2	GFA6700(config)#config syslog server enable	Save the configuration to enable the system log to the log server
Step 3	GFA6700(config)#config syslog server type all enable	Save the configuration to enable the system log to the log server
Step 4	GFA6700(config)#config syslog server lowest-level 5	Level 5 and above configuration information is saved to the server

Step 5	GFA6700(config)#record command-line server enable	Configuring the command line to log information to the server
Step 6	GFA6700(config)#config syslog server add 192.168.2.221 port 8808 facility 5	Add a Log Server
Step 7	GFA6700(config)#config syslog monitor-screen enable	Open the System Configuration log information output to the terminal
Step 8	GFA6700(config)#screen monitor	Allows the output to the terminal
Step 9	GFA6700(config)#monitor timestamp datetime	Output time information to the terminal
Step 10	GFA6700(config)#monitor lowest-level 5	Output level configuration information to more than 5-to-end
Step 11	GFA6700(config)#monitor type all enable	Configure the output of all types of information to the terminal

7 System monitoring and diagnostics

7.1 Detection network basic connectivity

ping command can be used to detect the basic network connectivity.

ping command sends Internet Control Message Protocol (CMP) request packet to an IP network equipment. If not received within the set time, the destination device response message, the output "REQUEST TIME OUT"; otherwise show the number of bytes response packet, packet sequence number, TTL, response time, while providing statistical information, including the transmission the number of packets, the number of response packets received, percentage of packets not responding, and response time minimum, maximum and average.

Ordinary users and administrators can use the ping command to the user

ping {[-t]}*1 {[-n] <1-65535>}*1 {[-l] <8-6400>}*1 {[-w] <1-255>}*1 {[-i] <1-255>}*1 {[-pattern] <user_pattern>}*1 {[-source] <A.B.C.D>}*1 <A.B.C.D>

Command	Explain
-i	The value of the specified TTL
-l	Specifies the size of ICMP message
-n	Specify how many were sent after the end of the ICMP PING request procedures. The default is 5

-pattern	Configuring ICMP messages can contain up to 16 user-defined number of 16 hexadecimal
-source	PING source IP address specified
-t	Configuration continuously PING, until by Ctrl + C to stop the program manually
-w	How much time to wait after the configuration response is that the destination did not receive barrier

7.2 Detected in the path of the destination message

Provide traceroute command is used to detect the road to the destination path between the data reported. Traceroute command sends Internet Control Message Protocol (ICMP) echo messages or UDP packets to IP network equipment. Only administrative users can use the traceroute command.

Command traceroute mode [udp | icmp] configure which packets to send.

Traceroute {[-saddr] <A.B.C.D>}*1 {[-firstttl] <1-30>}*1 {[-maxttl] <2-255>}*1 {[-port] <33434-65535>}*1 {[-count] <1-255>}*1 {[-waittime] <1-65535>}*1 <A.B.C.D>

Command	Explain
-count	Configuration did not jump the number of searches, the default is 3 times

-firstttl	Specifies the initial TTL message
-maxttl	Specifies the maximum message TTL. Search for the purpose specified IP equipment that is the maximum number of hops
-port	Specifies the UDP port number or ICMP sequence number
-saddr	Specifies the source IP address
-waittime	Specify the waiting time for each search

7.3 System running time

You can view the show start time command system run time.

GFA6700(config)#show start time

YYYY-MM-DD HH:MM:SS

Current system time:2010-09-01 17:02:34

Slot_no Mod_type Boot_time Running_time

1 GFA-GET 2010/09/01:14:36:55 -

3 GFA-SW 2010/09/01:14:36:30 0000:02:26:15

8 GFA-EPON 2010/09/01:14:38:16 -

11 GFA-PWU220 2010/09/01:14:36:55 -

7.4 View system resource usage

You can view the current command show system resource usage of system resources

GFA6700(config)#show system resource

System used memory 62207096 bytes.

Total system memory 93150680 bytes.

The percentage of Used memory: 66.7%.

User used memory 2635396 bytes.

Total user memory 33554432 bytes.

The percentage of Used memory: 7.8%.

The percentage of CPU: 6.9416%.

7.5 ARP Management

Address Resolution Protocol ARP provides a host MAC address and IP address mapping. EsayPath EPON will learn and maintain a mapping table for this mapping. If some of the specific host, do not want to EsayPath EPON way to get through the self-learning their address mapping, because such a huge network of learning may need to take some time, but also the risk of not learning, you can the way by hand for these hosts to establish a static address mapping table entry.

Command	Specification
arp agingtime [0|<20-360000>]	Configuring ARP table entry aging time
clear arp-cache [<slot/port>|<trunkname>]	Clear ARP table

show arp	View the current ARP table entry

8 Strong luminescene detection function of ONU

8.1 Function overview

EasyPath EPON supports strong luminescene (long luminous) detection function for the remote devices.When the remote devices appear the long luminous abnormal failures,reporting the alarm.This function should be used together with the optical power detection function,and the PON module should support the optical power detection.

8.2 Function configuration of strong luminescene detection

Command	Specification
optical-power [enable|disable]	Open or close the optical power detection function
optical-power interval <1-86400>	Configure the detection cycle of optical power detection
config onu-laser-always-on [enable|disable]	Configure the enable /disable of ONU strong luminescene detection

config onu-laser-always-on alarm-threshold [<threshold>|default]	Set the alarm thresholds of ONU strong luminescene ,the default is -35dBm
config onu-laser-always-on alarm-times [<1-20>|default]	Set the continuous detection times of strong luminous alarm confirmation,the default time is 3
config onu-laser-always-on alarm-clear-times [<1-20>|default]	Set the continuous detection times of strong luminous alarm elimination,the default time is 5
show onu-laser-always-on {[config|status]}*1	View the configuration of strong luminescene or the result of the detection

8.3 Configuration case

Step	Command	Specification

Step1	GFA6700(config)#optical-power enable	Enable the optical power detection function
Step2	GFA6700(config)#optical-power interval 15	Configure the detection cycle of optical power detection
Step3	GFA6700(config)#confi onu-laser-always-on enable	Enable the optical power detection function of ONU
Step4	GFA6700(config)#show onu-laser-always-on config onu laser always on is enable alarm threshold: -35 alarm times: 3 alarm clear times: 5	View the configuration of strong luminescene
Step5	GFA6700(config)#show onu-laser-always-on status onu 7/3/0 laser always on	View the result of the detection

Configure in accordance with the above steps,if there is strong luminous ONU , it will be deteced and report the alarm.Alarm format similar to the following:

2010-10-25, 16:26:01 onu7/3/0 laser always on:-14.5 dbm

9 Positioning the user location

9.1 Function overview

EasyPath EPON system supports the function that query the ONU

location according the user's MAC address or the user's PPOE account.In the current network, operators often encounter the network faults because the accessing of the broadband to the user PC, sometimes it wil cause the large area network paralysis.It will play a certain role for identifying the user's network location in the network managed by the operators to process this kind of faults timely.EasyPath EOPON system can specify the MAC location according to the MAC address or the user's PPOE account,and the specific can be positioned to the ONU level.Combined with our UniView DA network management platform,we can search and locate the position of the user(MAC address) in all the EasyPath EPON device network range which managed by the platform.Then we can fast locate the locations of fault users in a large range .

9.2 Function configuration

There are two ways of positioning in the positioning function of EasyPath EPON:One is according to the MAC address;the other is according to the PPOE account.

9.2.1 Positioning according to the MAC address

You can query the user's specific location under which switch which port which ONU.This function is default,no needs to configure and can be queried through the commands directly.

Command	Specification
trace-path mac-address <H.H.H>	Positioning according to the user's MAC address

9.2.2 Positioning according to the PPOE account

You can query the user's specific location under which switch which port which ONU according to the PPOE account in the EasyPath EPON system.

There are some requirements about the equipment in the positioning of user's account, it needs to bind the qos rules on the PON port, which can make the data stream of PPPOE image into the CPU, such as the case 2. And when establish a PPPOE connection, it must make sure it's the certificated PPPOE connection; otherwise it will not be recognized by the system .And each account can only correspond to five MAC addresses at the same time.

All the established tables can be eliminated only by deleting the user-id unless restarting the OLT equipment.

Commands about user account positioning:

Command	Specification
show trace-path history {[count]}*1	Check all account information of user
trace-path userid <userid>	Positioning according to the user's account
undo trace-path userid <userid>	Delete the established account tables of user

9.3 Configuration case

9.3.1 Case 1

Command	Specification
GFA6900(config)#trace-path mac-address 0000.0000.0102 1.OLT -- pon1/7 of GFA6900 2.PON1/7 -- onu1 named ONU-4FE	This command realizes the query through the user MAC address directly 1 Analysis in which PON port

3.ONU1/7/1 -- onu port eth1/4 4.ETH1/4 -- switch 000f.e906.ef39 Trace complete. GFA6900(config)	2 analysis which ONU of the PON port 3 Analysis the specific port of the ONU 4 Analysis the specific switch of the port The parsing is completed

9.3.2 Case 2

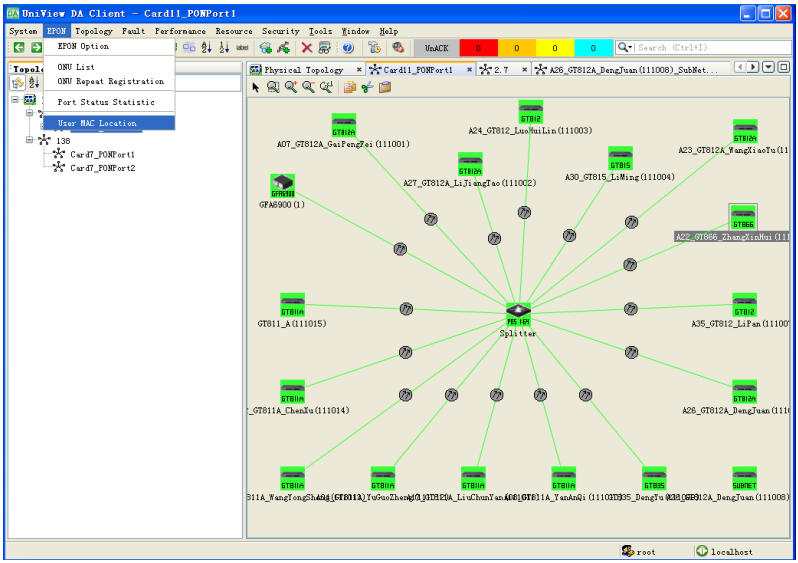
Step	Command	Specification
Step 1	GFA6900(config)#class-map 1 GFA6900(config-cmap)#match user-field 1 8864 ffff 13 GFA6900(config-cmap)#match user-field 2 c023 fdff 21 GFA6900(config-cmap)#exit GFA6900(config)#	Create class-map, matching offset
Step 2	GFA6900(config)#policy-map ingress 1 GFA6900(config-policymap)#match class-map 1 GFA6900(config-policymap-c)#set mirror port cpu GFA6900(config-policymap-c)#exit GFA6900(config-policymap)#exit GFA6900(config)#	Create policy-map,matching class-map,mirroring to the CPU
Step 3	GFA6900(config)#interface ethernet 1/7 GFA6900(if-pon1/7)#service-policy ingress 1	Bind the qos rules to the PON port

	GFA6900(if-pon1/7)#exit GFA6900(config)#	
Step 4	GFA6900(config)#show trace-path history user-id flag mac-addr port onu/port switch/port spirent resolved *0000.0002.0102 1/7 1/4 000f.e906.ef39/0 Total userid count=1 usermac resolved count=1,resolving count=0 GFA6900(config)#	Query the account information of user
Step 5	GFA6900(config)#trace-path userid spirent 1.OLT -- pon1/7 of GFA6900 2.PON1/7 -- onu1 named ONU-4FE 3.ONU1/7/1 -- onu port eth1/4 4.ETH1/4 -- switch 000f.e906.ef39 Trace complete. GFA6900(config)#	This command realizes the query through the user's account directly 1 Analysis in which PON port 2 analysis which ONU of the PON port 3 Analysis the specific port of the ONU 4 Analysis the specific switch of the port The parsing is completed

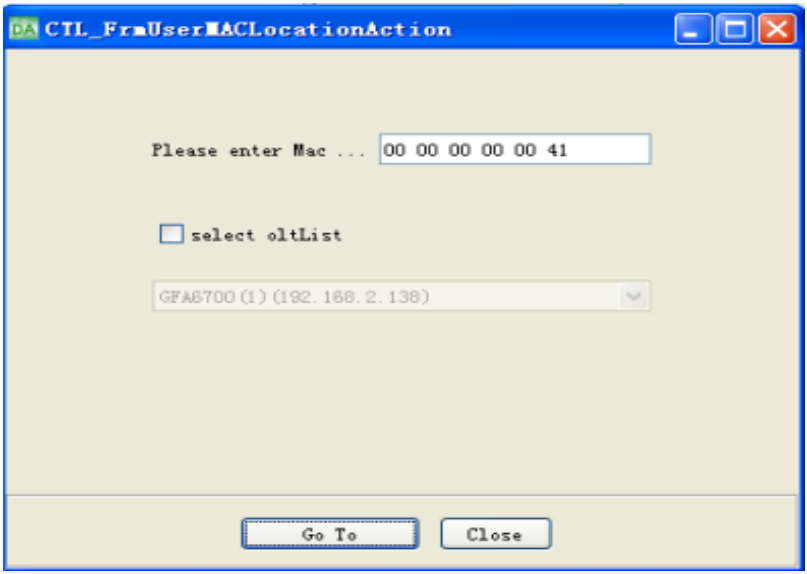
9.4 Function configuration （UniView DA Network Management platform）

The realize step that query the ONUONU location according to the user MAC address in the UniView DA network management are as follows:

Step1：Choose “User MAC Location”in the dropdown menu of EPON options

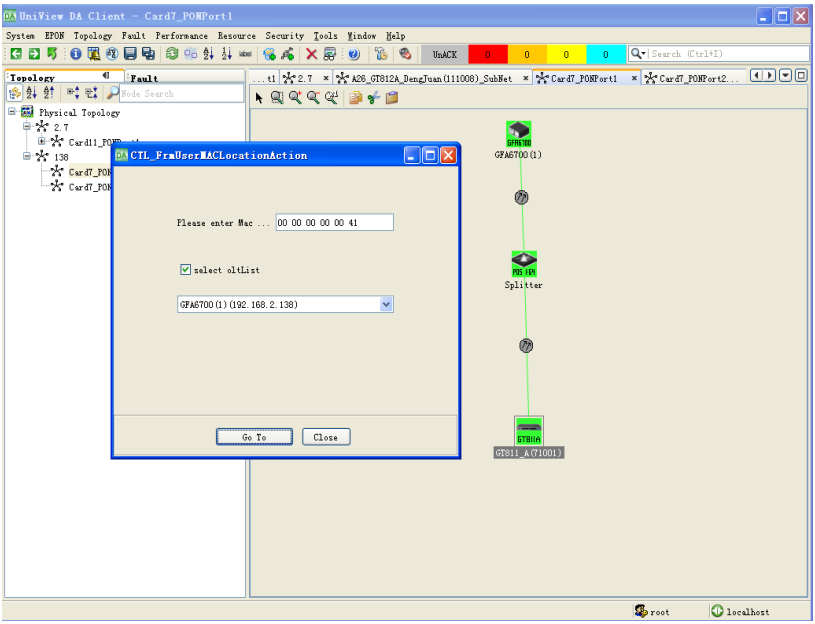


Step2:Enter the user MAC address in the pop-up dialog box.The methos for inputting the MAC address as shown below:

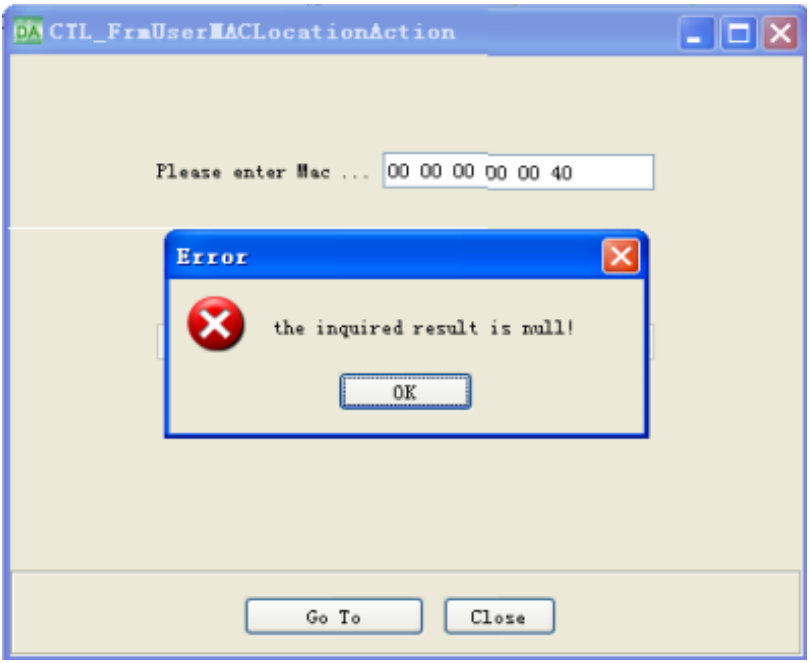


You can select the “select oltlist” if have known the user OLT,and choose the corresponding OLT in the drop-down box.If not selected,then search all the OLT which managed bythe whole UniView DA network plotform.Then click “Go To” to execute the lookup of the user MAC address.

Step3:If the system find the user MAC which ONU position,the mark the ONU,as show below:



If the system cant find the user MAC where the ONU position,then the network management gives the prompt,as show below:


CTL_FrmUserMACLocationAction
Please enter Mac ...
00 00 00 00 00 40
Error
the inquired result is null!
OK
Go To
Close

13 AAA authentication

1 Overview of AAA authentication

AAA is the abbreviation of Authentication, Authorization and Accounting.It provides a consistent configuration framework to authentication, authorization, and accounting the three security functions .Actually it's a management of network security.

This network security is mainly refers to the access control, including:

●Which users can access the network service

●What services can the users get who has the access light;

●How to account about the users who is using the network resource;

The AAA must provide authentication、authorization and accounting function for the above problems.

1.1 Authentication function

AAA supports the followingauthentication modes:

No authentication: Trust the users very much and don't take any legal inspection.It's not always using this way.

Local authentication:Configure the information of users(including the username、password and a variety of attributes of the local users) on the

device.The advantages of it are fast speed; reduce the cost of the operation, but the shortage is the amount of storage information limitated by the hardware of the device.

Remote authentication: Support the remote authentication through the RADIUS protocol or TACACS+ protocol.Device as a client to communicate with RADIUS server or TACACS+ server.For the RADIUS protocol, we can use standard or extended RADIUS protocol.

1.2 Authorization function

AAA supports the following authorization modes:

Direct authorization: Trust users very much and authenorize directly.

Local authorization: Authorize according to the related attributes which configured for the accounts of local users

Authorize after RADIUS authentication succeedly: The RADIUS authentication and the authorization are bound together, so we can't use the RADIUS to authorzize alone.

TACACS+ authorization：Authorize to the users by the TACACS server.

1.3 Accounting function

AAA supports the following accounting mode:

No accounting: Don't account to the users

Remote accounting: Supports accounting by the RADIUS server or

TACACS+ server.

Generally, AAA use the client /server structure;The client running on the managed resource side,the information of users are storaged centralized on the server.Therefore,the AAA framework has good expansibility and can realize the centralized management of users information easily.

1.4 Introduction of ISP Domain

ISP domain, i.e., ISP users group.A ISP domain is a user group formed by the users of a same ISP.In the username by the form of “userid@isp-name”,the “isp-name” after the “@” is the domain name of ISP domain.The access device use the “userid” as the user name for identity authentication and use the “isp-name” as the domain name.It can be different ISP users for the access from a same device Because the user attributes of ISP users(e.g. user name、password and service type/authority) are likely to be different from each other,it’s necessary to set the ISP domain to tell them apart.Inthe view of ISP domain,we can configure a set of separate ISP domain properties including the AAA strategy(use the RADIUS program and so on) for each ISP domain.

1.5 Radius Protocol

RADIUS (Remote Authentication Dia-In User Service) is a distributed; client/server structure information exchange protocol.It can protect the network from interference of unauthorized access.It's often used in a variety of network environment which require both high security and maintainthe remote user access.

1.5.1 The three parts of RADIUS server

Protocol: RFC 3865 and RFC 2866 based on the UDP/IP layer defines the format of RADIUS frame and message transmission mechanism, and also define the 1812 as the authentication port, 1813 as a charging port

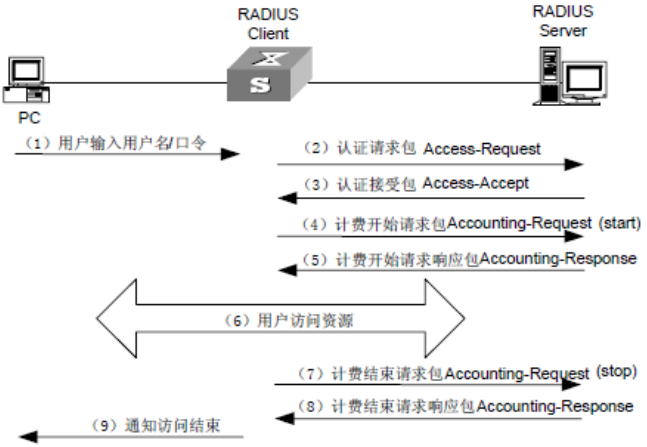
Server: The RADIUS server is running on the central computer or workstation, contains the relevant user authentication and network service access information

Client: It local in the dial-up access server side, and can spread over the whole network

1.5.2 The basic message interaction process of RADIUS

The RADIUS client (switch) and RADIUS server authenticate the interaction message by the shared key to enhance security.The RADIUS protocol merge the authentication and suthorization process, namely respone the authorization information in the message.The

process of interaction between user、switch and RADIUS server aa shown below:



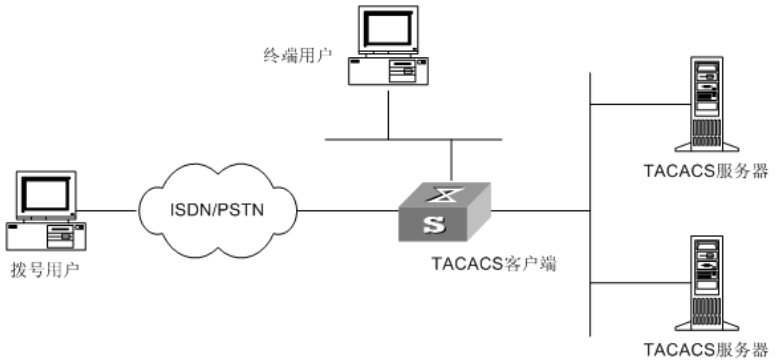
1.6 Introduction of TACACS+ protocol

In computer network, TACACS+ (Terminal Access Controller Access Control System Plus) is a protocol for the router、network access server and other connected computer devices to provides the access and control function by one or multiple centralized servers.TACACS+ provides independent authentication、authorization and accounting services.

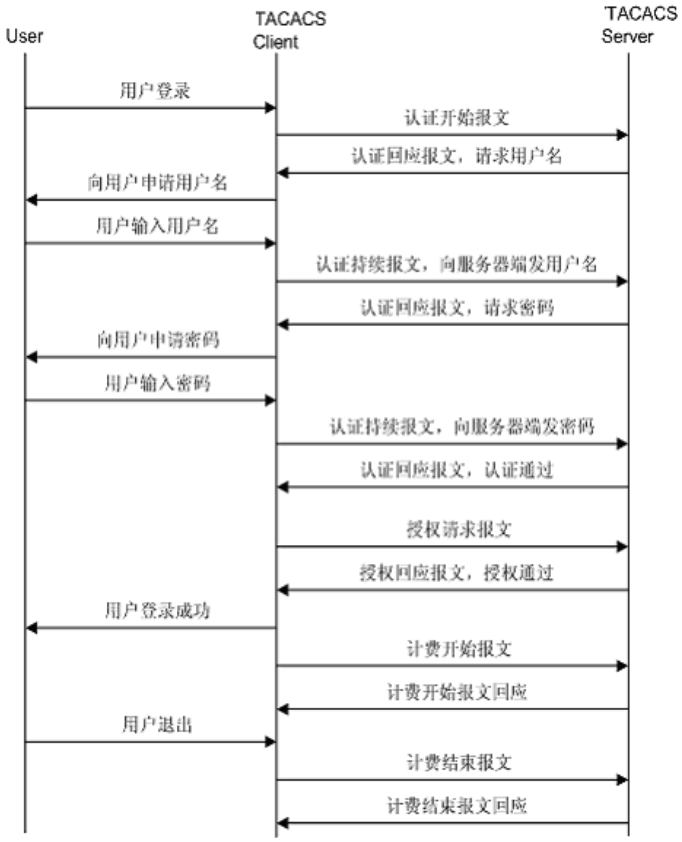
Although,theRADIUS intergrate the authentication and authorization function in the users configurations,it will separate the two operations.In addition,the differs is the TACACS+ use the transmission control protocol (TCP) and RADIUS use the user datagram protocol (UDP).Most administrators recommend the use of TACACS+，because the TCP is considered as the more reliable protocol.The extension of the TACACS+ protocol provides more anthentication request types and responsive codes for the initial protocol specification.

TACACS+ use the TCP pot 49, including three independent protocols, if it's required, it can be realized independently on the server.

The typical deployment scenarios of TACACS+ server as shown bellow:



Because the atacacs+ server are based on tcp,the message interactive rewuires high real tiem ,its specific prcess as shown bellows:



1.7 Realization distinction of RADIUS and TACACS+

Realziation distinction of RADIUS and TACACS+

TCP provides more advanced features than UDP.TCP is a reliable transfer service origente to the connection,but the UDP only provides the optimal transmission.So it requires the extra code to realize the mechanisms for the RADIUS ,such as retransmission、timeout etc,but all of these have inherent characteristics in the TCP.

Encryption mode

RADIUS only encrypte the password itself, and don't encrypte the other parts of the message,these are unspecified transmission.So this information can be captured by the third software.TACACS+ encrypte the whole data packet and only leave the the data in Baotou.There is a sign bit indicates the packet whether is encrypted in the data Baotou.The unencrypted packet is used for the debug,and general application is encrypted.So the encryption from the TACACS+ ensures the security of communication between client and server.

1.8 Features of EasyPath AAA authentication

OLT AAA authenticationfunction is designed according to the AAA frame configuration 、relevant configurations of domain 、relevant configurations of radius server and relevant configurations of TACACS+ server ,this four module design ,to design related functions and command sets.Design AAA authentication for OLT is mainly to realize the login users centralized management and centralized deployment to avoid the troubles from the add.delete users on the each OLT.

1.9 Configuration Commands

1.9.1 Configure AAA

Command	Specification
OLT(config)#config login-auth aaa_auth OLT(config)#config login-auth local	Configure AAA authentication for local or remote authentication; The default authentication is the local authentication,and

	it's effective for the username /password
OLT (config)#config aaa-authentication enable OLT (config)#config aaa-authentication disable	Configure the AAA authentication to enable or disable,the default is disable;
OLT (config)#config login-aaa time <1-600>	The client end will wait time after submitting the username and password when configure the AAA authentication,the default time is 30 seconds

1.9.2 Configure ISP domain

ISP domain, i.e., ISP users group.A ISP domain is a user group formed by the users of a same ISP.In the username by the form of "user_name@isp-name",the "isp-name" after the "@" is the domain name of ISP domain. The access device use the "use_name" as the user name for identity authentication and use the "isp-name" as the domain name.

Command	Specification
OLT (config)#create isp-domain <domain> OLT (config)#delete isp-domain <domain>	Create /Delete a ISP domain; The default domain can't be deleted;

	The rules of ISP domain:The first character can only be the capitals or the lowercase letters,and it can't contain the character except"A-Z","a-z","0-9",".",the length must less than 20 bytes.
OLT (config)#show isp-domain <domain> OLT (config)#show isp-domain	View the current ISP domain; The OLT can only contain 5 ISP domains most at the same time(include the default default domain)
OLT (config)#config isp-domain default username complete OLT (config)#config isp-domain default username incomplete	Configure whether input with the domain username when the inputing The default is complete ,it's need to input; Without the domain name,system caonsider it as the users of default domain
OLT (config)#config isp-domain default aaa-protocol radius OLT (config)#config isp-domain default aaa-protocol tacacs	Configure theusing of radius protocol and tacacs protocol in the default domain; The default using is the radius protocol in all

	domains;
OLT (config)#config isp-domain default authentication mode independent OLT (config)#config isp-domain default authentication mode primary-backup	Configure the authentication mode to independent or primary-backup in the default domain; Independent；only the first server is effective; Primary-backup:the primary-backup mode authentication,it will initiate the request when the local primary server does not give the response;l The default mode is the independent mode;
OLT (config)#config isp-domain default authentication add-server id 0 OLT (config)#config isp-domain default authentication delete-server id 0	Enable the configured radius server 0 in the default domain Delete radius server 0 in the default domain; Adding the smaller ID when add server,delete the larger ID when delete server;
OLT (config)#config isp-domain default tacc-authentication add-server id 0 OLT (config)#config isp-domain default tacc-authentication delete-server id 0	Enabel the configured tacacs+ server 0 in the default domain Delete tacacs+ server 0 in the default domain; Adding the smaller ID when

	add server,delete the larger ID when delete server;
OLT (config)#config isp-domain default authentication config-server id 0 type primary OLT (config)#config isp-domain default tacc-authenticate config-server-id 0 type primary	Set the server manually as the primary server which id is 0 in the default domain; The first added server is the primary server in the default

1.9.3 Configure RADIU Protocol

Command	Specification
OLT(config)#radius authentication enable OLT (config)#radius authentication disable	Enable/Disable radius protocol; Disable is default; This setting is effective in the global,affect all domains;
OLT (config)#radius authentication add-server id 0 server-ip 192.168.2.244 client-ip 192.168.2.130 udp-port 1234	Server id:The range of id is 0~4 for adding server,add from the smalle id; Server-ip：Specify the ip address of radius server Client-ip：ip address of OLT Udp-port：The using port number of radius server，the default

	number is 1812；
OLT (config)#radius authentication delete-server id 0	Delete the radius server whose id is 0 Deletion should be in accordance with ID order from big to small order
OLT (config)#radius authentication server-switch enable OLT (config)#radius authentication server-switch disable	Configure switch of radius server on/off; The default is off; This configuration is effective in the global,affect all domains;
OLT (config)#radius authentication config-server id 0 status active	Configure active state of ID 0 radius server The state of the new add server is active in the default; This command is mainly usie in the priticular case of artificial intervention;
OLT(config)#radius authentication config-server id 0 shared-secret greenway	Configure the shared key to greenway1for communicate with the id 0 radius server The default shared key

	is greenway； The premise is the shared key must be consistent for the normal communication between the client and the server!
OLT(config)#radius authentication config-server id 0 max-retransmit-count 5 OLT(config)#radius authentication config-server id 0 retransmit-interval 5	The time is 5 of configuration of the radius protocol retransmission interval/retransmission ; Tdefault time is 3

1.9.4 Configure TACACS+ Protocol

Command	Specification
OLT (config)#tacc authentication enable OLT (config)#tacc authentication disable	Enable/Disable tacacs+ protocol; Disable is default; This setting is effective in the global,affect all domains;
OLT (config)#tacc authentication add-server id 0 server-ip 192.168.2.244 client-ip 192.168.2.130 share-key greenway1	Server id:The range of id is 0~4 for adding server,add from the smalle id; Server-ip：Specify the ip address of radius server Client-ip：ip address of

	OLT Share-key：The default shared key is greenway ， the configuration of OLT and tacacs+ server is consistent； Authentication port : the default authentication port is tcp 49 of tacacs+ server
OLT (config)#tacc authentication delete-server id 0	Delete the tacacs+ server whose id is 0 Deletion should be in accordance with ID order from big to small order
OLT (config)#tacc authentication server-switch enable OLT (config)#tacc authentication server-switch disable	Configure switch of tacacs+ server on/off; The default is off; This configuration is effective in the global,affect all domains;
OLT (config)#tacc authentication config-server id 0 status active OLT (config)#tacc authentication config-server id 0 status inactive	Configure active state of ID 0 tacacs+ server The state of the new add server is active in the default; This command is

	mainly usie in the priticular case of artificial intervention;
OLT (config)#tacc authentication config-server id 0 share-key greenway1	Configure the shared key to greenway1for communicate with the id 0 tacacs+ server The default shared key is greenway； The premise is the shared key must be consistent for the normal communication between the client and the server!
OLT (config)#config tacc re-transmit period 5 OLT (config)#config tacc re-transmit max-num 5	The time is 5 of configuration of the tacacs+ protocol retransmission interval/retransmission ; Tdefault time is 3

1.10 Configuration case

1.10.1 Case 1

Case description

For the OLT remote access users (TELNET) through the RADIUS server authentication application configuration

Configuration steps

Step	Command	Specification

Step1	OLT(config)#config aaa-authentication enable	Configure AAA authentication enable
Step2	OLT (config)#config login-auth aaa_auth	Configure the AAA authentication mode to remote authentication mode
Step3	OLT (config)#radius authentication enable	Configure radius authentication function enable
Step4	OLT (config)#radius authentication add-server id 0 server-ip 192.168.2.244 client-ip 192.168.2.130	Configure the ip address of radius server 、 radius client ； This step ignore the configuration of udp port ,i.e. use the 1812 default port,and must ensure the server terminal use this port ；
Step5	OLT(config)#radius authentication config-server id 0 shared-secret greenway1	Configure the shared key of the communication between the client and the server; The premise is the shared key must be consistent for

		the success between the client and the server!
Step6	OLT(config)#config isp-domain default authentication add-server id 0	Enable the configuration item of server id 0 in the default domain
Step7	OLT(config)#config isp-domain default aaa-protocol radius	Enable radius authentication in the default domain
Step8	OLT(config)#show radius RADIUS AUTH: [Enable] ID STATE SERVER-IP SERVER-PORT CLIENT-IP SECRET -- ----- --------- ---------- --------- ------ 0 ACTIVE 192.168.2.244 1812 192.168.2.130 greenway1 ID RETRANSMIT-INTERVAL MAX-RETRANSMIT-COUNT ------- ------------------------ ------------------------ 0 3 3 OLT (config)#	View radius related configuration

Step9	OLT (config)#show isp-domain default ========== ========== ========== Domain Id : 0 AAA Protocol : RADIUS Domain Name : default Authenticate Mode : independent Radius Authentication: Enabled User Name : complete Tacc+ Authentication: Disabled Radius Auth Server Info: ID TYPE STATE SERVER-IP SERVER-PORT CLIENT-IP SECRET -- ---- ----- --------- ---------- --------- ------ 0 PRIMARY ACTIVE 192.168.2.244 1812 192.168.2.130 greenway1 TACACS+ Auth Server Info: ID TYPE STATE SERVER-IP SERVER-PORT SECRET ---------- ----------	View the relevant configurations of default domain

	OLT (config)0023	

1.10.2 Case 2

Case description

For the OLT remote access users (TELNET) through the TACACS+ server authentication application configuration

Configuration steps

Step	Command	Specification
Step	OLT(config)#config aaa-authentication enable	Configure AAA authentication enable
Step2	OLT (config)#config login-auth aaa_auth	Configure the AAA authentication mode to remote authentication mode
STEP3	OLT (config)#tacc authentication enable	Configure TACACS+ authentication function enable
Step4	OLT (config)#tacc authentication add-server id 0 server-ip 192.168.2.244 client-ip 192.168.2.130	Configure ip address of tacacs+ server 、tacacs+ client ip
Step5	OLT(config)#tacc authentication config-server id 0 shared-secret greenway1	Configure the shared key of the communication between the client and the server;

		The premise is the shared key must be consistent for the success between the client and the server!
Step6	OLT(config)#config isp-domain default tacc-authentication add-server id 0	Enable the configuration item of server id 0 in the default domain
Step7	OLT(config)#config isp-domain default aaa-protocol tacacs	Enable tacacs+ authentication in the default domain
Step8	OLT (config)#show tacc ========== ========== ========== ====== TACC authentication enabled ---------- ---------- id server-status server-ip client-ip tcp-port share-key ---------- ---------- 0 Active 192.168.2.244 192.168.2.130 49 greenway1 ---------- ----------	View tacacs+ related configuration

	---------- ---------- TACC re-transmit configuration ========== ========== ========== ====== max retransmit number: 3 retransmit period: 3(seconds) ---------- ---------- OLT (config)#	
Step8	OLT (config)# show isp-domain default ========== ========== ========== Domain Id : 0 AAA Protocol : tacacs Domain Name : default Authenticate Mode : independent Radius Authentication: disabled User Name : complete Tacc+ Authentication: Enabled Radius Auth Server Info: ID TYPE STATE SERVER-IP SERVER-PORT CLIENT-IP SECRET	View the relevant configurations of default domain

	-- ---- ----- --------- ---------- --------- ------ TACACS+ Auth Server Info: ID TYPE STATE SERVER-IP SERVER-PORT SECRET ---------- 0 PRIMARY ACTIVE 192.168.2.244 49 greenway1 OLT (config)#	

1.10.3 Case 3

Case Description

For the OLT remote access users (TELNET) through the double servers to realize the primary-backup redundancy redius authentication;

Configuration steps

Step	Command	Specification
Step1	OLT(config)#config aaa-authentication enable	Configure AAA authentication enable
Step2	OLT (config)#config login-auth aaa_auth	Configure the AAA authentication mode to remote authentication

		mode
Step3	OLT (config)#radius authentication enable	Configure radius authentication function enable
Step4	OLT (config)#radius authentication add-server id 0 server-ip 192.168.2.244 client-ip 192.168.2.130 GFA6900(config)#radius authentication add-server id 1 server-ip 192.168.2.99 client-ip 192.168.2.130	Configure ip address of tacacs+ server and tacacs+ client ip
Step5	OLT(config)#radius authentication config-server id 0 shared-secret greenway1 OLT(config)#radius authentication config-server id 1 shared-secret greenway1	Configure the shared key of the communication between the client and the server; The premise is the shared key must be consistent for the success between the client and the server!
Stp6	OLT(config)#radius authentication server-switch enable	Enable the toggle switch of the radius server and tacacs+ server
Step7	OLT(config)#config isp-domain default authentication mode primary-backup	Enable primary-backup server mode in the two domains

		respectively
Step8	OLT(config)#config isp-domain default authentication add-server id 0 GFA6900(config)#config isp-domain default authentication add-server id 1	Enable the configuration item of server id 0 in the default domain
Step9	OLT(config)#config isp-domain default aaa-protocol radius	Enable radius authentication in the default domain
Step10	OLT(config)#show radius RADIUS AUTH: [Enable] ID STATE SERVER-IP SERVER-PORT CLIENT-IP SECRET -- ----- --------- ---------- --------- ------ 0 ACTIVE 192.168.2.244 1812 192.168.2.130 greenway1 1 ACTIVE 192.168.2.99 1812 192.168.2.130 greenway1 ID RETRANSMIT-INTERVAL MAX-RETRANSMIT-COUNT ------- ------------------------	View relevant configurations of radius

	------------------------ 0 3 3 1 3 3 OLT(config)#	
Step11	OLT(config)#show isp-domain default ========== ========== ========== Domain Id : 0 AAA Protocol : RADIUS Domain Name : default Authenticate Mode : Primary-Backup Radius Authentication: Enabled User Name : Incomplete Tacc+ Authentication: Enabled Radius Auth Server Info: ID TYPE STATE SERVER-IP SERVER-PORT CLIENT-IP SECRET -- ---- ----- ---------- ---------- ------ 0 PRIMARY ACTIVE 192.168.2.244 1812 192.168.2.130 greenway1 1 BACKUP ACTIVE 192.168.2.99 1812 192.168.2.130 greenway1	View the related configurations of default domain

	TACACS+ Auth Server Info: ID TYPE STATE SERVER-IP SERVER-PORT SECRET ---------- ---------- OLT (config)#	

Compaion of ring network and expert of star network

北京格林伟迪科技有限公司
GW DELIGHT TECHNOLOGY CO., LTD.

GW DELIGHT TECHNOLOGY CO., LTD
Address: No.28, Shangdi Xilu, Haidian District, Beijing
Post Code：100085
Telephone：(86-10) 62961077
Fax：(86-10) 82899881
Website：www.gwdelight.com
E-mail：gwdelight@gwdelight.com