D-Link
Building Networks for People

DAS-3626
Ethernet over VDSL Switch
Command Line Interface Guide

March 2015

Table of Contents

Chapter 1 Using Command Line Interface

The Switch can be managed through the Switch's serial port, Telnet, SNMP or the Web-based management agent. The Command Line Interface (CLI) can be used to configure and manage the Switch via the serial port or Telnet interfaces.

This manual provides a reference for all of the commands contained in the CLI. Every command will be introduced in terms of purpose, format, description, parameters, and examples. Configuration and management of the Switch via the Web-based management agent are discussed in the Web UI Reference Guide. For detailed information on installing hardware please also refer to the Hardware Installation Guide.

1-1 Accessing the Switch via the Serial Port

The Switch's serial port's default settings are as follows:

- 115200 baud
- no parity
- 8 data bits
- 1 stop bit

A computer running a terminal emulation program capable of emulating a VT-100 terminal and a serial port configured as above are then connected to the Switch's Console port via an included RS-232 to RJ-45 convertor cable.

With the serial port properly connected to a management computer, the following screen should be visible. If this screen does not appear, try pressing Ctrl+r to refresh the console screen.

```
                          DAS-3626 VDSL2 Switch
                          Command Line Interface

                        Firmware: Build 0.03.B028
          Copyright(C) 2011 D-Link Corporation. All rights reserved.
UserName:
```

There is no initial username or password. Just press the **Enter** key twice to display the CLI input cursor – **DAS-3626:admin#**. This is the command line where all commands are input.

1-2 Setting the Switch's IP Address

Each Switch must be assigned its own IP Address, which is used for communication with an SNMP network manager or other TCP/IP application (for example TFTP). The Switch's default IP address is 10.90.90.90. You can change the default Switch IP address to meet the specification of your networking address scheme.

The Switch is also assigned a unique MAC address by the factory. This MAC address cannot be changed, and can be found on the initial boot console screen – shown below.

```
  Boot Procedure                                          V1.00.009
-------------------------------------------------------------------------------

  Power On Self Test ....................................  100 %

  MAC Address   : 00-01-02-03-04-00
  H/W Version   : A1

  Please Wait, Loading V1.01.027 Runtime Image ..............  100 %
  UART init .................................................  100 %
  Starting runtime image
  Device Discovery .....................................      -  Boot
Procedure                                        V0.01.B009
-------------------------------------------------------------------------------

  Power On Self Test ....................................  100 %

  MAC Address   : D8-FE-E3-93-05-C0
  H/W Version   : A1G

  Please Wait, Loading V0.03.B028 Runtime Image .............  100 %
  UART init .................................................  100 %
  Starting runtime image
```

The Switch's MAC address can also be found in the Web management program on the Switch Information (Basic Settings) window on the Configuration menu.

The IP address for the Switch must be set before it can be managed with the Web-based manager.

Starting at the command line prompt, enter the commands **config ipif System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy**. Where the **x**'s represent the IP address to be assigned to the IP interface named **System** and the **y**'s represent the corresponding subnet mask.

Alternatively, you can enter **config ipif System ipaddress xxx.xxx.xxx.xxx/z**. Where the **x**'s represent the IP address to be assigned to the IP interface named **System** and the **z** represents the corresponding number of subnets in CIDR notation.

The IP interface named **System** on the Switch can be assigned an IP address and subnet mask which can then be used to connect a management station to the Switch's Telnet or Web-based management agent.

```
DAS-3626:admin#config ipif System ipaddress 10.1.2.3/255.0.0.0
Command: config ipif System ipaddress 10.1.2.3/8

Success.

DAS-3626:admin#
```

In the above example, the Switch was assigned an IP address of 10.24.22.100 with a subnet mask of 255.0.0.0. The system message **Success** indicates that the command was executed successfully. The Switch can now be configured and managed via Telnet, SNMP MIB browser and the CLI or via the Web-based management agent using the above IP address to connect to the Switch.

There are a number of helpful features included in the CLI. Entering the **?** command will display a list of all of the top-level commands.

```
DAS-3626:admin#?
Command: ?

Option                Description
--------------------------------------------------------------------------------
..                    go to parent directory
?                     Used to display all commands and specific command usage,
                      descriptions.
cable_diag            cable diagnostic
cfm
clear
config
create
debug                 Open IP-MAC Binding debug event or DHCP.
delete
disable
download
enable
login                 Used to log in a user to the switch's console.
logout                Used to log out a user from the switch's console.
no                    Close IP-MAC Binding debug event and DHCP.
ping                  Used to test the connectivity between network devices.
ping6                 Use ping6 command to test the IPv6 network connectivity
reboot                Used to restart the switch.
Reset
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

When entering a command without its required parameters, the CLI will prompt you with a **Next possible completions:** message.

```
DAS-3626:admin#config account
Command: config account
Next possible completions:

Option                Description
--------------------------------------------------------------------------------
<username>            The username is between 1 and 15 characters

DAS-3626:admin#
```

In this case, the command **config account** was entered with the parameter **<username>**. The CLI will then prompt to enter the **<username>** with the message, **Next possible completions:**. Every command in the CLI has this feature, and complex commands have several layers of parameter prompting.

In addition, after typing any given command plus one space, users can see all of the next possible sub-commands, in sequential order, by repeatedly pressing the **Tab** key.

To re-enter the previous command at the command prompt, press the up arrow cursor key. The previous command will appear at the command prompt.

```
DAS-3626:admin#config account
Command: config account
Next possible completions:

Option                Description
--------------------------------------------------------------------------------
<username>            The username is between 1 and 15 characters

DAS-3626:admin#config account
```

In the above example, the command **config account** was entered without the required parameter **<username>**, the CLI returned the **Next possible completions: <username>** prompt. The up arrow cursor control key was pressed to re-enter the previous command (**config account**) at the command prompt. Now the appropriate username can be entered and the **config account** command re-executed.

All commands in the CLI function in this way. In addition, the syntax of the help prompts are the same as presented in this manual – angle brackets < > indicate a numerical value or character string, braces { } indicate optional parameters or a choice of parameters, and brackets [ ] indicate required parameters.

If a command is entered that is unrecognized by the CLI, the top-level commands will be displayed under the **Available commands:** prompt.

```
DAS-3626:admin#the
Available commands:

Option                Description
--------------------------------------------------------------------------------
..                    go to parent directory
?                     Used to display all commands and specific command usage,
                      descriptions.
cable_diag            cable diagnostic
cfm
clear
config
create
debug                 Open IP-MAC Binding debug event or DHCP.
delete
disable
download
enable
login                 Used to log in a user to the switch's console.
logout                Used to log out a user from the switch's console.
no                    Close IP-MAC Binding debug event and DHCP.
ping                  Used to test the connectivity between network devices.
ping6                 Use ping6 command to test the IPv6 network connectivity
reboot                Used to restart the switch.
reset
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

The top-level commands consist of commands such as **show** or **config**. Most of these commands require one or more parameters to narrow the top-level command. This is equivalent to **show** what? or **config** what? Where the what? is the next parameter.

For example, entering the **show** command with no additional parameters, the CLI will then display all of the possible next parameters.

```
DAS-3626:admin#show
Command: show
Next possible completions:

Option                Description
--------------------------------------------------------------------------------
802.1p
access_profile        Used to display current access list table.
account               Used to display user accounts.
address_binding
alarm                 Used to display the config alarm or the status alarm.
arpentry              Used to display the ARP table.
asymmetric_vlan       Used to display the status of asymmetric VLAN
attack_log            Show attack log messages.
authen
authen_enable         Used to show a user-defined or default or all method
                      lists for promoting user's privilege to Admin level
authen_login          Used to show a user-defined or default or all method
                      lists of authentication methods for user login
authen_policy         Used to show that system access authentication policy is
                      enabled or disabled
auto_remote_download
auto_wifi_activate_code  Used to display auto wireless password.
bpdu-filter           Used to display BPDU filter.
bpdu_protection       Used to show BPDU Protection information.
bpdu_tunnel           Used to show BPDU Tunnel information.
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

In the above example, all of the possible next parameters for the **show** command are displayed. At the next command prompt, the up arrow was used to re-enter the **show** command, followed by the **account** parameter. The CLI then displays the user accounts configured on the Switch.

1-3 Command Syntax Symbols

Syntax	Description
angle brackets < >	Encloses a variable or value. Users must specify the variable or value. For example, in the syntax config command_history **<value 1-40>** users must enter how many entries for **<value 1-40>** when entering the command. DO NOT TYPE THE ANGLE BRACKETS.
square brackets [ ]	Encloses a required value or list of required arguments. Only one value or argument must be specified. For example, in the syntax create account **[admin | operator | user]** <username 15> users must specify either the admin-level or user-level account when entering the command. DO NOT TYPE THE SQUARE BRACKETS.
vertical bar |	Separates mutually exclusive items in a list, one of which must be entered. For example, in the syntax reset {[**config | system**]} {force_agree}

	users must specify either the community or trap receiver in the command. DO NOT TYPE THE VERTICAL BAR.
braces { }	Encloses an optional value or a list of optional arguments. One or more values or arguments can be specified. For example, in the syntax reset **{[config | system]} {force_agree}** users may choose configure or system in the command. DO NOT TYPE THE BRACES.
parentheses ( )	Indicates at least one or more of the values or arguments in the preceding syntax enclosed by braces must be specified. For example, in the syntax config bpdu_protection ports [<portlist> | all] {state [enable | disable] | mode [drop | block | shutdown]}**(1)** users have the option to specify hops or time or both of them. The "(1)" following the set of braces indicates at least one argument or value within the braces must be specified. DO NOT TYPE THE PARENTHESES.
ipif <ipif_name 12> metric <value 1-31>	**12** means the maximum length of the IP interface name. **1-31** means the legal range of the metric value.

1-4 Line Editing Keys

Keys	Description
Delete	Delete character under cursor and shift remainder of line to left.
Backspace	Delete character to left of cursor and shift remainder of line to left.
Insert	Toggle on and off. When toggled on, inserts text and shifts previous text to right.
Left Arrow	Move cursor to left.
Right Arrow	Move cursor to right
Tab	Help user to select appropriate token.
P	Display the previous page.
N or Space	Display the next page.
CTRL+C	Escape from displayed pages.
ESC	Escape from displayed pages.
Q	Escape from displayed pages.
R	refresh the displayed pages
a	Display the remaining pages. (The screen display will not pause again.)
Enter	Display the next line.

Keys	Description
Delete	Delete character under cursor and shift remainder of line to left.
Backspace	Delete character to left of cursor and shift remainder of line to left.
Insert	Toggle on and off. When toggled on, inserts text and shifts previous text to right.
Left Arrow	Move cursor to left.
Right Arrow	Move cursor to right
Tab	Help user to select appropriate token.
P	Display the previous page.
N or Space	Display the next page.
CTRL+C	Escape from displayed pages.
ESC	Escape from displayed pages.
Q	Escape from displayed pages.
R	refresh the displayed pages
a	Display the remaining pages. (The screen display will not pause again.)
Enter	Display the next line.

The screen display pauses when the show command output reaches the end of the page.

In the above example, all of the possible next parameters for the **show** command are displayed. At the next command prompt, the up arrow was used to re-enter the **show** command, followed by the **account** parameter. The CLI then displays the user accounts configured on the Switch.

Chapter 2 Basic Command List

show session
show serial_port
config serial_port {baud_rate [9600 | 19200 | 38400 | 115200] | auto_logout [never | 2_minutes | 5_minutes | 10_minutes | 15_minutes]}
enable clipaging
disable clipaging
login
logout
?
clear
show command_history
config command_history <value 1-40>
config greeting_message {default}
show greeting_message
config command_prompt [<string 16> | username | default]
config ports [<GE_portlist> | all] {medium_type [fiber | copper]} {speed [auto | 10_half | 10_full | 100_half | 100_full | 1000_full {[master | slave]}] | flow_control [enable | disable] | learning [enable | disable] | state [enable | disable] | mdix [auto | normal | cross] | [description <desc 1-32> | clear_description]}
show ports {<portlist>} {[description | err_disabled | details | media_type]}
create account [admin | operator | user] <username 15>
config account <username> <password>}
show account
delete account <username>
show switch
enable telnet {<tcp_port_number 1-65535>}
disable telnet
enable web {<tcp_port_number 1-65535>}
disable web
reboot {force_agree}
reset {[config |system [ww | south | north | central]]} {force_agree}
config firmware image_id <int 1-2> [delete | boot_up]
create ipif <ipif_name 12> {<network_address>} <vlan_name 32> {state [enable | disable]}
config ipif <ipif_name 12> [{ipaddress <network_address> | vlan <vlan_name 32> | state [enable | disable]} | ipv6 [ipv6address <ipv6networkaddr> | state [enable | disable]]]
delete ipif [<ipif_name 12> {ipv6address <ipv6networkaddr>} | all]
show ipif {<ipif_name 12>}
enable ipif_ipv6_link_local_auto [<ipif_name 12> | all]
disable ipif_ipv6_link_local_auto [<ipif_name 12> | all]
show ipif_ipv6_link_local_auto {<ipif_name 12>}

2-1 show session

Description

This command is used to display a list of currently users which are login to CLI sessions.

Format

show session

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable the password encryption:

```
DAS-3626:admin#show session
Command: show session

 ID   Live Time    From                                    Level User
 ---- ------------ --------------------------------------- ----- --------------
 *8   00:08:04.110 Serial Port                            admin Anonymous

Total Entries: 1

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

2-2 show serial_port

Description

This command is used to display the current serial port settings.

Format

show serial_port

Parameters

None.

Restrictions

None.

Example

To display the serial port setting:

```
DAS-3626:admin#show serial_port
Command: show serial_port

 Baud Rate     : 115200
 Data Bits     : 8
 Parity Bits   : None
 Stop Bits     : 1
 Auto-Logout   : 10 mins

DAS-3626:admin#
```

2-3 config serial_port

Description

This command is used to configure the serial bit rate that will be used to communicate with the management host and the auto logout time for idle connections.

Format

config serial_port {baud_rate [9600 | 19200 | 38400 | 115200] | auto_logout [never | 2_minutes | 5_minutes | 10_minutes | 15_minutes]}

Parameters

baud_rate - (Optional) Specifies the serial bit rate that will be used to communicate with the management host. The default baud rate is 115200. **9600** - Specifies the serial bit rate to be 9600. **19200** - Specifies the serial bit rate to be 19200. **38400** - Specifies the serial bit rate to be 38400. **115200** - Specifies the serial bit rate to be 115200.
auto_logout - (Optional) Specifies the auto logout time out setting: **never** - Specifies to never timeout. **2_minutes** - Specifies to auto logout when idle over 2 minutes. **5_minutes** - Specifies to auto logout when idle over 5 minutes. **10_minutes** - Specifies to auto logout when idle over 10 minutes. **15_minutes** - Specifies to auto logout when idle over 15 minutes.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure baud rate:

```
DAS-3626:admin#config serial_port baud_rate 115200
Command: config serial_port baud_rate 115200

Success.

DAS-3626:admin#
```

2-4 enable clipaging

Description

This command is used to enable the pausing of the screen display when the show command output reaches the end of the page. For those show commands that provide the display refresh function, the display will not be refreshed when clipaging is disabled. The default setting is enabled.

Format

enable clipaging

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable pausing of the screen display when show command output reaches the end of the page:

```
DAS-3626:admin# enable clipaging
Command: enable clipaging

Success.

DAS-3626:admin#
```

2-5 disable clipaging

Description

This command is used to disable the pausing of the screen display when the show command output reaches the end of the page. The default setting is enabled.

Format

disable clipaging

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable pausing of the screen display when show command output reaches the end of the page:

```
DAS-3626:admin# disable clipaging
Command: disable clipaging

Success.

DAS-3626:admin#
```

2-6 login

Description

This command is used to allow user login to the switch.

Format

login

Parameters

None.

Restrictions

None.

Example

To login the switch with a user name dlink:

```
DAS-3626:admin# login
Command: login

UserName:dlink
PassWord:****

DAS-3626:admin#
```

2-7 logout

Description

This command is used to logout when you are finished using the facility.

Format

logout

Parameters

None.

Restrictions

None.

Example

To logout current user:

```
DAS-3626:admin# logout
Command: logout


**********
* Logout *
**********

                        DGS-3120-24TC Gigabit Ethernet Switch
                             Command Line Interface

                           Firmware: Build 1.01.027
           Copyright(C) 2010 D-Link Corporation. All rights reserved.
UserName:
```

2-8 ?

Description

This command is used to display the usage description for all commands or the specific one.

Format

?

Parameters

None.

Restrictions

None.

Example

To get “ping” command usage, descriptions:

```
DAS-3626:admin#ping ?
Command: ping
Next possible completions:

Option                Description
------------------------------------------------------------------------------
<ipaddr>              the IP address of the entry.

DAS-3626:admin#
```

2-9 clear

Description

This command is used to clear screen.

Format

clear

Parameters

None.

Restrictions

None.

Example

To clear screen:

```
DAS-3626:admin# clear
Command: clear



DAS-3626:admin#
```

2-10 show command_history

Description

This command is used to display command history.

Format

show command_history

Parameters

None.

Restrictions

None.

Example

To display command history:

```
DAS-3626:admin#show command_history
Command: show command_history

? ping
login
show serial_port
show session
? config bpdu_protection ports
? reset
? create account
? create ipif
show
the
?

DAS-3626:admin#
```

2-11 config command_history

Description

This command is used to configure the number of commands that the switch can recall.

Format

config command_history <value 1-40>

Parameters

<value 1-40> - Enter the command history value that the switch can recall here. This value must be between 1 and 40.

Restrictions

None.

Example

To configure the number of command history:

```
DAS-3626:admin# config command_history 25
Command: config command_history 25

Success.

DAS-3626:admin#
```

2-12 config greeting_message

Description

This command is used to configure the greeting message (or banner).

Format

config greeting_message {default}

Parameters

default - (Optional) Specifies toreturn the greeting message (banner) to its original factory default entry.

Restrictions

Only Administrators and Operators can issue this command.

Example

To edit the banner:

```
DAS-3626:admin#config greeting_message
Command: config greeting_message

Greeting Messages Editor
================================================================================

                              DAS-3626 VDSL2 Switch
                             Command Line Interface

                            Firmware: Build 0.03.B028
          Copyright(C) 2011 D-Link Corporation. All rights reserved.
================================================================================
=

   <Function Key>                   <Control Key>
   Ctrl+C     Quit without save     left/right/
   Ctrl+W     Save and quit           up/down     Move cursor
                                    Ctrl+D        Delete line
                                    Ctrl+X        Erase all setting
                                    Ctrl+L        Reload original setting
--------------------------------------------------------------------------------
```

2-13 show greeting_message

Description

This command is used to display greeting message.

Format

show greeting_message

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To display greeting message:

```
DAS-3626:admin#show greeting_message
Command: show greeting_message

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

                              DAS-3626 VDSL2 Switch
                             Command Line Interface

                           Firmware: Build 0.03.B028
          Copyright(C) 2011 D-Link Corporation. All rights reserved.




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

DAS-3626:admin#
```

2-14 config command_prompt

Description

This command is used to modify the command prompt.

The current command prompt consists of four parts: “product name” + “:” + ”user level” + ”#” (e.g. “DAS-3626:admin#”). This command is used to modify the first part (1. “product name”) with a string consisting of a maximum of 16 characters, or to be replaced with the users’ login user name.

When users issue the “reset” command, the current command prompt will remain in tact. Yet, issuing the “reset system” will return the command prompt to its original factory default value.

Format

config command_prompt [<string 16> | username | default]

Parameters

<string 16> - Enter the new command prompt string of no more than 16 characters.
username - Enter this command to set the login username as the command prompt.
default - Enter this command to return the command prompt to its original factory default value.

Restrictions

Only Administrators and Operators can issue this command.

Example

To edit the command prompt:

```
DAS-3626:admin#config command_prompt Prompt#
Command: config command_prompt Prompt#

Success.

Prompt#:admin#
```

2-15 config ports

Description

This commands is used to configure the switch's port settings.

Format

config ports [<GE_portlist> | all] {medium_type [fiber | copper]} {speed [auto | 10_half | 10_full | 100_half | 100_full | 1000_full {[master | slave]}] | flow_control [enable | disable] | learning [enable | disable] | state [enable | disable] | mdix [auto | normal | cross] | [description <desc 1-32> | clear_description]}

Parameters

<GE_portlist> - Enter a list of ports used here.
all - Specifies that all the ports will be used for this configuration.
medium_type - (Optional) Specifies the medium type while the configure ports are combo ports **fiber** - Specifies that the medium type will be set to fiber. **copper** - Specifies that the medium type will be set to copper.
speed - (Optional) Specifies the port speed of the specified ports . **auto** - Specifies the port speed to auto negotiation. **10_half** - Specifies the port speed to 10_half. **10_full** - Specifies the port speed to 10_full. **100_half** - Specifies the port speed to 100_half. **100_full** - Specifies the port speed to 100_full._ **1000_full** - Specifies the port speed to 1000_full. While set port speed to 1000_full,user should specify master or slave mode for 1000 base TX interface, and leave the 1000_full without any master or slave setting for other interface.

master - Specifies that the port(s) will be set to master. **slave** - Specifies that the port(s) will be set to slave.
flow_control - (Optional) Specifies to turn on or turn off the flow control on one or more ports. **enable** - Specifies to turn on the flow control. **disable** - Specifies turn off the flow control.
learning - (Optional) Specifies to turn on or turn off MAC address learning on one or more ports. **enable** - Specifies that the learning option will be enabled. **disable** - Specifies that the learning option will be disabled.
state - (Optional) Specifies to enable or disable the specified port. If the specificed ports are in error-disabled status , configure their state to enable will recover these ports from disabled to enable state. **enable** - Specifies that the port state will be enabled. **disable** - Specifies that the port state will be disabled.
mdix - (Optional) Specifies the MDIX as auto, normal, and cross. If set to normal state, the port is in MDIX mode and can be connected to PC NIC using a straight cale. If set to cross state, the port is in mdi mode, and can be connected to a port (in mdix mode) on another switch thru a straight cabe. **auto** - Specifies that the MDIX mode for the port will be set to auto. **normal** - Specifies that the MDIX mode for the port will be set to normal. **cross** - Specifies that the MDIX mode for the port will be set to cross.
description - (Optional) Specifies the description of the port interface. **<desc 1-32>** - Enter the port interface description here. This value can be up to 32 characters long.
clear_description - (Optional) Specifies that the description field will be cleared.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the ports:

```
DAS-3626:admin#config ports all medium_type copper speed auto
Command: config ports all medium_type copper speed auto

Success.

DAS-3626:admin#
```

2-16 show ports

Description

This command is used to display the current configurations of a range of ports.

Format

show ports {<GE_portlist>} {[description | err_disabled | details | media_type]}

Parameters

<GE_portlist> - (Optional) Enter the list of ports to be configured here.
description - (Optional) Specifies to indicate if port description will be included in the display.
err_disabled - (Optional) Specifies to indicate if ports are disabled by some reasons will be

displayed.
details - (Optional) Specifies to display the port details.
media_type - (Optional) Specifies to display port transceiver type.

Restrictions

None.

Example

To display the port details:

```
DAS-3626:admin#show ports details
Command: show ports details

Port : 25
--------------------
Port Status                 : Link Down
Port Uptime                 : N/A
Description                 :
HardWare Type               : Gigabits Ethernet
MAC Address                 : D8-FE-E3-93-05-D9
Bandwidth                   : 1000000Kbit
Auto-Negotiation            : Enabled
Duplex Mode                 : Full Duplex
Flow Control                : Disabled
MDI                         : Auto
Module Type                 : None
Address Learning            : Enabled
Last Clear of Counter       : 5 hours 44 mins ago
BPDU Hardware Filtering Mode: Enabled
Queuing Strategy            : FIFO
TX Load                     :   0/100,          0 kbps,        0 packets/sec
RX Load                     :   0/100,          0 kbps,        0 packets/sec

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

2-17 create account

Description

This command is used to create user accounts. The username is between 1 and 15 characters, the password is between 0 and 15 characters. It is case sensitive. The number of account (include admin and user) is up to 8.

Format

create account [admin | operator | user] <username 15>

Parameters

admin - Specifies the name of the admin account.
operator - Specifies the name for a operator user account.
user - Specifies the name of the user account.

<username 15> - Enter the username used here. This name can be up to 15 characters long.

Restrictions

Only Administrators can issue this command.

Example

To create the admin-level user “dlink”:

```
DAS-3626:admin#create account admin dlink
Command: create account admin dlink

Enter a case-sensitive new password:*****
Enter the new password again for confirmation:*****
Success.

DAS-3626:admin#
```

To create the user-level user “Remote-Manager”:

```
DAS-3626:admin# create account user Remote-Manager
Command: create account user Remote-Manager

Success.

DAS-3626:admin#
```

2-18 config account

Description

This command is used to configure a user account.

When the password information is not specified in the command, the system will prompt the user to input the password interactively. For this case, the user can only input the plain text password.

If the password is present in the command, the user can select to input the password in the plain text form or in the encrypted form. The encryption algorithm is based on SHA-I.

Format

config account <username> <password>}

Parameters

<username> - Enter the user name for the account used here.
<password> - Enter the password for the user account. The length for of password in plain-text form and in encrypted form are different. For the plain-text form, passwords must have a minimum of 0 character and can have a maximum of 15 characters. For the encrypted form password, the length is fixed to 35 bytes long. The assword is case-sensitive.

Restrictions

Only Administrators can issue this command.

Example

To configure the user password of “dlink” account:

```
DAS-3626:admin#config account dlink
Command: config account dlink

Enter a old password:*****
Enter a case-sensitive new password:*****
Enter the new password again for confirmation:*****
Success.

DAS-3626:admin#
```

2-19 show account

Description

This command is used to display user accounts that have been created.

Format

show account

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To display the accounts that have been created:

```
DAS-3626:admin#show account
Command: show account

 Current Accounts:
 Username              Access Level
 ---------------       ------------
 admin                 Admin
 oper                  Operator
 user                  User

 Total Entries : 3

DAS-3626:admin#
```

2-20 delete account

Description

This command is used to delete an existing account.

Format

delete account <username>

Parameters

<username> - Enter the username to be deleted.

Restrictions

Only Administrators can issue this command.

Example

To delete the user account “System”:

```
DAS-3626:admin#delete account dlink
Command: delete account dlink

Are you sure to delete the last administrator account?(y/n)
Success.

DAS-3626:admin#
```

2-21 show switch

Description

This command is used to display the switch information.

Format

show switch

Parameters

None.

Restrictions

None.

Example

The following is an example for display of switch information.

```
DAS-3626:admin#show switch
Command: show switch

Device Type                 : DAS-3626 VDSL2 Switch
MAC Address                 : D8-FE-E3-93-05-C0
IP Address                  : 10.90.90.90 (Manual)
VLAN Name                   : default
Subnet Mask                 : 255.0.0.0
Default Gateway             : 0.0.0.0
Boot PROM Version           : Build 0.01.B009
Firmware Version            : Build 0.03.B028
Hardware Version            : A1G
Customer ID                 : World-Wide
Serial Number               : QT3O1D8001128
System Name                 :
System Location             :
System Uptime               : 0 days, 5 hours, 54 minutes, 28 seconds
System Contact              :
Spanning Tree               : Disabled
GVRP                        : Disabled
IGMP Snooping               : Disabled
MLD Snooping                : Disabled
VLAN Trunk                  : Disabled
TELNET                      : Enabled (TCP 23)
WEB                         : Enabled (TCP 80)
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

2-22 enable telnet

Description

This command is used to allow you to manage the switch via TELNET based management software.

Format

enable telnet {<tcp_port_number 1-65535>}

Parameters

<tcp_port_number 1-65535> - (Optional) Enter the TCP port number. TCP ports are numbered between 1 and 65535. The “well-known” TCP port for the TELNET protocol is 23.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable TELNET and configure port number:

```
DAS-3626:admin# enable telnet 23
Command: enable telnet 23

Success.

DAS-3626:admin#
```

2-23 disable telnet

Description

This command is used to disable the switch via TELNET based management software.

Format

disable telnet

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable TELNET:

```
DAS-3626:admin# disable telnet
Command: disable telnet

Success.

DAS-3626:admin#
```

2-24 enable web

Description

This command is used to allow you to manage the switch via HTTP based management software.

Format

enable web {<tcp_port_number 1-65535>}

Parameters

<tcp_port_number 1-65535> - (Optional) Enter the TCP port number. TCP ports are numbered between 1 and 65535. The “well-known” TCP port for the WEB protocol is 80.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable HTTP and configure port number:

```
DAS-3626:admin# enable web 80
Command: enable web 80

Success.

DAS-3626:admin#
```

2-25 disable web

Description

This command is used to disable the switch via HTTP based management software.

Format

disable web

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable HTTP:

```
DAS-3626:admin# disable web
Command: disable web

Success.

DAS-3626:admin#
```

2-26 reboot

Description

This command is used to restart the Switch.

Format

reboot {force_agree}

Parameters

force_agree - (Optional) Specifies to be executed immediatedly without further confirmation.

Restrictions

Only Administrators can issue this command.

Example

To reboot the switch:

```
DAS-3626:admin# reboot
Command: reboot

Are you sure to proceed with the system reboot?(y/n)
Please wait, the switch is rebooting…
```

2-27 reset

Description

This command is used to provide reset functions. The configuration setting will be reset to the default setting. For the “save system” command, the device will store the reset setting in the NVRAM and then reboot the system.

The configuration settings include enable/disable of clipaging, greeting message, and command prompt will also be reset by all the reset commands.

There is one exception, the “reset” command will not reset IP address configured on the system IPIF and the default gateway setting.

Format

reset {[config |system [ww | south | north | central]]} {force_agree}

Parameters

config - (Optional) Specifies to reset all parameters to default settings, but the Switch will not save nor reboot.
system - (Optional) Specifies to reset all parameters to default settings, and the Switch will save and reboot. **ww** - Specifies to use worldwide default settings. **south** - Specifies to use the default settings of southern area. **north** - Specifies to use the default settings of northern area. **central** - Specifies to use the default settings of central area.
force_agree - (Optional) Specifies be executed immediatedly without further confirmation.

Restrictions

Only Administrators can issue this command.

Example

To reset the switch:

```
DAS-3626:admin#reset system
Command: reset system

Are you sure you want to proceed with system reset?(y/t/n)
 y-(reset all include stacking configuration, save, reboot )
 t-(reset all exclude stacking configuration, save, reboot)
 n-(cancel command)y

Reboot & Load Factory Default Configuration...

Saving configurations and logs to NV-RAM...... Done.
Please wait, the switch is rebooting...
```

2-28 config firmware

Description

This command is used to select a firmware file as a boot up file or delete a specified firmware file. This command is required to be supported when multiple firmware images are supported.

Format

config firmware image_id <int 1-2> [delete | boot_up]

Parameters

image_id - Specifies the working section. The Switch can hold two firmware versions for the user to select from, which are specified by image ID. **<int 1-2>** - Enter the ID number of the firmware in the Switch's memory to be configured.
delete - Specifies to delete the specified firmware.
boot_up - Specifies the firmware as the boot up firmware.

Restrictions

Only Administrators can issue this command.

Example

To config image 1 as the boot up image:

```
DAS-3626:admin#config firmware image_id 1 boot_up
Command: config firmware image_id 1 boot_up

Success.

DAS-3626:admin#
```

2-29 create ipif

Description

This command is used to create an IP interface.

Format

create ipif <ipif_name 12> {<network_address>} <vlan_name 32> {state [enable | disable]}

Parameters

<ipif_name 12> - Enter the IP interface name here. This name can be up to 12 characters long.
<network_address> - (Optional) Enter the IPv4 networkaddress (xxx.xxx.xxx/xx). It specifies a host address and length of network mask.
<vlan_name 32> - Enter the VLAN name used here. This name can be up to 32 characters long.
state - (Optional) Specifies the state of the IP interface. **enable** - Specifies that the IP interface state will be enabled. **disable** - Specifies that the IP interface state will be disabled.

Restrictions

Only Administrators and Operators can issue this command.

Example

To create an IP interface:

```
DAS-3626:admin#create ipif Inter2 192.168.16.1/24 default state enable
Command: create ipif Inter2 192.168.16.1/24 default state enable

Success.

DAS-3626:admin#
```

2-30 config ipif

Description

This command is used to configure the IP interface.

Format

config ipif <ipif_name 12> [{ipaddress <network_address> | vlan <vlan_name 32> | state [enable | disable]} | ipv6 [ipv6address <ipv6networkaddr> | state [enable | disable]]]

Parameters

<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.
ipaddress - (Optional) Specifies to configure a network on an ipif. The address should specify a host address and length of network mask. Since an ipif can have only one IPv4 address, the new configured address will overwrite the original one.
<network_address> - Enter the network address used here.
vlan - (Optional) Specifies the name of the VLAN here.
<vlan_name 32> - Enter the VLAN name used here. This name can be up to 32 characters long.
state - (Optional) Specifies that the IPv4 interface state will be set to enabled or disabled.
enable - Specifies that the IPv4 interface state will be enabled.
disable - Specifies that the IPv4 interface state will be disabled.
ipv6 - Specifies that the IPv6 configuration will be done.
ipv6address - Specifies the IPv6 network address. The address should specify a host address and length of network prefix. There can be multiple V6 addresses defined on an interface. Thus, as a new address is defined, it is added on this ipif.
<ipv6networkaddr> - Enter the IPv6 address used here.
state - Specifies that the IPv6 interface state will be set to enabled or disabled.
enable - Specifies that the IPv6 interface sate will be enabled.
disable - Specifies that the IPv6 interface sate will be disabled.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure an interface's IPv4 network address:

```
DAS-3626:admin#config ipif System ipaddress 192.168.69.123/24 vlan default
Command: config ipif System ipaddress 192.168.69.123/24 vlan default

Success.

DAS-3626:admin#
```

2-31 delete ipif

Description

This command is used to delete an IP interface.

Format

delete ipif <ipif_name 12> {ipv6address <ipv6networkaddr>}

Parameters

<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.
ipv6address - (Optional) Specifies the IPv6 network address. The address should specify a host address and length of network prefix. There can be multiple V6 addresses defined on an interface.
<ipv6networkaddr> - Enter the IPv6 address used here.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete an IP interface:

```
DAS-3626:admin#delete ipif newone
Command: delete ipif newone

Success.

DAS-3626:admin#
```

2-32 show ipif

Description

This command is used to display an IP interface.

Format

show ipif {<ipif_name 12>}

Parameters

<ipif_name 12> - (Optional) Enter the IP interface name used here. This name can be up to 12 characters long.

Restrictions

None.

Example

To display an IP interface:

```
DAS-3626:admin#show ipif
Command: show ipif

IP Interface                : System
VLAN Name                   : default
Interface Admin State       : Enabled
Link Status                 : LinkDown
IPv4 Address                : 10.90.90.90/8 (Manual)
IPv4 State                  : Enabled
IPv6 State                  : Disabled

IP Interface                : outband
Interface Admin state       : Enabled
Link Status                 : LinkDown
IPv4 Address                : 192.168.1.10/24 (Manual)
IPv4 State                  : Enabled
IPv6 State                  : Disabled


Total Entries: 2

DAS-3626:admin#
```

2-33 enable ipif_ipv6_link_local_auto

Description

This command is used to enable the auto configuration of link local address when there are no IPv6 addresses explicitly configured. When an IPv6 address is explicitly configured, the link local address will be automatically configured, and the IPv6 processing will be started. When there is no IPv6 address explicitly configured, by default, link local address is not configured and the IPv6 processing will be disabled. By enable this automatic configuration, the link local address will be automatically configured and IPv6 processing will be started.

Format

enable ipif_ipv6_link_local_auto [<ipif_name 12> | all]

Parameters

<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.
all - Specifies that all the IP interfaces will be used.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable the IP interface for IPv6 link local automatic:

```
DAS-3626:admin#enable ipif_ipv6_link_local_auto newone
Command: enable ipif_ipv6_link_local_auto newone

Success.

DAS-3626:admin#
```

2-34 disable ipif_ipv6_link_local_auto

Description

This command is used to disable the auto configuration of link local address when no IPv6 address are configured.

Format

disable ipif_ipv6_link_local_auto [<ipif_name 12> | all]

Parameters

<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.
all - Specifies that all the IP interfaces will be used.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable the IP interface for IPv6 link local automatic:

```
DAS-3626:admin#disable ipif_ipv6_link_local_auto newone
Command: disable ipif_ipv6_link_local_auto newone

Success.

DAS-3626:admin#
```

2-35 show ipif_ipv6_link_local_auto

Description

This commands is used to display the link local address automatic configuration state.

Format

show ipif_ipv6_link_local_auto {<ipif_name 12>}

Parameters

<ipif_name 12> - (Optional) Enter the Ip interface name used here. This name can be up to 12 characters long.

Restrictions

Only Administrators and Operators can issue this command.

Example

T o display the link local address automatic configuration state.

```
DAS-3626:admin#show ipif_ipv6_link_local_auto
Command: show ipif_ipv6_link_local_auto

 IPIF: System          Automatic Link Local Address: Disabled

DAS-3626:admin#
```

Chapter 3 802.1Q VLAN Command List

create vlan <vlan_name 32> tag <vlanid 2-4094> {type [1q_vlan | private_vlan]} {advertisement}
create vlan vlanid <vidlist> {type [1q_vlan | private_vlan]} {advertisement}
delete vlan <vlan_name 32>
delete vlan vlanid <vidlist>
config vlan <vlan_name 32> {[add [tagged | untagged | forbidden] | delete] [<portlist> | bonding <bgroup_list>] | advertisement [enable | disable]}(1)
config vlan vlanid <vidlist> {[add [tagged | untagged | forbidden] | delete] [<portlist> | bonding <bgroup_list>] | advertisement [enable | disable] | name <vlan_name 32>}(1)
config port_vlan [<portlist> | bonding <bgroup_list> | all] {gvrp_state [enable | disable] | ingress_checking [enable | disable] | acceptable_frame [tagged_only | admit_all] | pvid <vlanid 1-4094>}(1)
show vlan {<vlan_name 32>}
show vlan ports {<portlist>}
show vlan vlanid <vidlist>
show vlan bonding <bgroup_list>
show port_vlan {<portlist>}
show port_vlan bonding <bgroup_list>
enable pvid auto_assign
disable pvid auto_assign
show pvid auto_assign
config gvrp [timer {join <value 100-100000> | leave <value 100-100000> | leaveall <value 100-100000> } | nni_bpdu_addr [dot1d | dot1ad]]
show gvrp
enable gvrp
disable gvrp
config private_vlan [<vlan_name 32> | vid <vlanid 1-4094>] [add [isolated | community] | remove] [<vlan_name 32> | vlanid <vidlist>]
show private_vlan {[<vlan_name 32> | vlanid<vidlist>]}

3-1 create vlan

Description

This command is used to create a VLAN on the switch. The VLAN ID must be always specified for creating a VLAN.

Format

create vlan <vlan_name 32> tag <vlanid 2-4094> {type [1q_vlan | private_vlan]} {advertisement}

Parameters

<vlan_name 32> - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
tag - Specifies the VLAN ID to be created. **<vlanid 2-4094>** - Enter the VLAN ID here. The VLAN ID value must be between 2 and 4094.
type - (Optional) Specifies the type of VLAN here. **1q_vlan** - Specifies that the type of VLAN used is based on the 802.1Q standard. **private_vlan** - Specifies that the private VLAN type will be used.
advertisement - (Optional) Specifies the VLAN as being able to be advertised out.

Restrictions

Only Administrators and Operators can issue this command.

Example

To create a VLAN with name “v2” and VLAN ID 2:

```
DAS-3626:admin# create vlan v2 tag 2 type 1q_vlan advertisement
Command: create vlan v2 tag 2 type 1q_vlan advertisement

Success.

DAS-3626:admin#
```

3-2 create vlan vlanid

Description

This command is used to create more than one VLANs at a time. A unique VLAN name (e.g. VLAN10) will be automatically assigned by the system. The automatic assignment of VLAN name is based on the following rule: “VLAN”+ID. For example, for VLAN ID 100, the VLAN name will be VLAN100. If this VLAN name is conflict with the name of an existing VLAN, then it will be renamed based on the following rule: “VLAN”+ID+”ALT”+ collision count. For example, if this conflict is the second collision, then the name will be VLAN100ALT2.

Format

create vlan vlanid <vidlist> {type [1q_vlan | private_vlan]} {advertisement}

Parameters

<vidlist> - Enter the VLAN ID list here.
type - (Optional) Specifies the type of VLAN to be created. **1q_vlan** - Specifies that the VLAN created will be a 1Q VLAN. **private_vlan** - Specifies that the private VLAN type will be used.
advertisement - (Optional) Specifies the VLAN as being able to be advertised out.

Restrictions

Only Administrators and Operators can issue this command.

Example

To create some VLANs using VLAN ID:

```
DAS-3626:admin# create vlan vlanid 10-30
Command: create vlan vlanid 10-30

Success.

DAS-3626:admin#
```

3-3 delete vlan

Description

This command is used to delete a previously configured VLAN by the name on the switch.

Format

delete vlan <vlan_name 32>

Parameters

<vlan_name 32> - Enter the VLAN name here. This name can be up to 32 characters long.

Restrictions

Only Administrators and Operators can issue this command.

Example

To remove a vlan v1:

```
DAS-3626:admin# delete vlan v1
Command: delete vlan v1

Success.

DAS-3626:admin#
```

3-4 delete vlan vlanid

Description

This command is used to delete one or a number of previously configured VLAN by VID list.

Format

delete vlan vlanid <vidlist>

Parameters

<vidlist> - Enter the VLAN ID list here.

Restrictions

Only Administrators and Operators can issue this command.

Example

To remove VLANs from 10-30:

```
DAS-3626:admin# delete vlan vlanid 10-30
Command: delete vlan vlanid 10-30

Success.

DAS-3626:admin#
```

3-5 config vlan

Description

This command is used to configure a VLAN based on the name.

Format

config vlan <vlan_name 32> {[add [tagged | untagged | forbidden] | delete] [<portlist> | bonding <bgroup_list>] | advertisement [enable | disable]}(1)

Parameters

<vlan_name 32> - Enter the VLAN name you want to add ports to. This name can be up to 32 characters long.
add - Specifies to add tagged, untagged or forbidden ports to the VLAN. **tagged** - Specifies the additional ports as tagged. **untagged** - Specifies the additional ports as untagged. **forbidden** - Specifies the additional ports as forbidden.
delete - Specifies to delete ports from the VLAN.
<portlist> - Enter the list of ports used for the configuration here.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
advertisement - Specifies the GVRP state of this VLAN. **enable** - Specifies to enable advertisement for this VLAN. **disable** - Specifies to disable advertisement for this VLAN.

Restrictions

Only Administrators and Operators can issue this command.

Example

To add port 4 to 8 as tagged ports to the VLAN v2:

```
DAS-3626:admin#config vlan v2 add tagged 4-8
Command: config vlan v2 add tagged 4-8

Success.

DAS-3626:admin#
```

3-6 config vlan vlanid

Description

This command is used to configure multiple VLANs at one time. But conflicts will be generated if you configure the name of multiple VLANs at one time.

Format

config vlan vlanid <vidlist> {[add [tagged | untagged | forbidden] | delete] [<portlist> | bonding <bgroup_list>] | advertisement [enable | disable] | name <vlan_name 32>}(1)

Parameters

<vidlist> - Enter a list of VLAN IDs to configure.
add - Specifies to add tagged, untagged or forbidden ports to the VLAN. **tagged** - Specifies the additional ports as tagged. **untagged** - Specifies the additional ports as untagged. **forbidden** - Specifies the additional ports as forbidden.
delete - Specifies to delete ports from the VLAN.
<portlist> - Enter the list of ports used for the configuration here.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
advertisement - Specifies the GVRP state of this VLAN. **enable** - Specifies to enable advertisement for this VLAN. **disable** - Specifies to disable advertisement for this VLAN.
name - Specifies the new name of the VLAN. **<vlan_name 32>** - Enter the VLAN name here. This name can be up to 32 characters long.

Restrictions

Only Administrators and Operators can issue this command.

Example

To add port 4 to 8 as tagged ports to the VLAN ID from 10-20:

```
DAS-3626:admin# config vlan vlanid 10-20 add tagged 4-8
Command: config vlan vlanid 10-20 add tagged 4-8

Success.

DAS-3626:admin#
```

3-7 config port_vlan

Description

This command is used to configure the ingress checking status, the sending and receiving GVRP information.

Format

config port_vlan [<portlist> | bonding <bgroup_list> | all] {gvrp_state [enable | disable] | ingress_checking [enable | disable] | acceptable_frame [tagged_only | admit_all] | pvid <vlanid 1-4094>}(1)

Parameters

<portlist> - Specifies a range of ports for which you want ingress checking. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 would specify switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 − in numerical order.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
all - Specifies that all the port will be used for this configuration.
gvrp_state - Specifies to enable or disable GVRP for the ports specified in the port list. **enable** - Specifies that GVRP for the specified ports will be enabled. **disable** - Specifies that GVRP for the specified ports will be disabled.
ingress_checking - Specifies to enable or disable ingress checking for the specified portlist. **enable** - Specifies that ingress checking will be enabled for the specified portlist. **disable** - Specifies that ingress checking will be disabled for the specified portlist.
acceptable_frame - Specifies the type of frame will be accepted by the port. **tagged_only** - Only tagged packets can be accepted by this port. **admit_all** - All packets can be accepted.
pvid - Specifies the PVID of the ports. **<vlanid 1-4094>** - Enter the VLAN ID here. The VLAN ID value must be between 1 and 4094.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable the ingress checking status, and the GVRP status of port 1 to 5:

```
DAS-3626:admin#config port_vlan 1-5 gvrp_state enable ingress_checking enable
Command: config port_vlan 1-5 gvrp_state enable ingress_checking enable

Success.

DAS-3626:admin#
```

3-8 show vlan

Description

This command is used to display the vlan information including of parameters setting and operational value.

Format

show vlan {<vlan_name 32>}

Parameters

<vlan_name 32> - (Optional) Enter the VLAN name here. The VLAN name can be up to 32 characters long.

Restrictions

None.

Example

To display VLAN settings:

```
DAS-3626:admin#show vlan
Command: show vlan


VLAN Trunk State        : Disabled
VLAN Trunk Member Ports :


VID             : 1               VLAN Name     : default
VLAN Type       : Static          Advertisement : Enabled
Member Ports    : 1-26
Static Ports    : 1-26
Current Tagged Ports  :
Current Untagged Ports: 1-26
Static Tagged Ports   :
Static Untagged Ports : 1-26
Forbidden Ports       :

Total Static VLAN Entries: 1
Total GVRP VLAN Entries: 0


DAS-3626:admin#
```

3-9 show vlan ports

Description

This command is used to display the vlan information per ports.

Format

show vlan ports {<portlist>}

Parameters

<portlist> - (Optional) Enter the list of ports that will be displayed here.

Restrictions

None.

Example

To display the VLAN configuration for port 6:

```
DAS-3626:admin#show vlan ports  6
Command: show vlan ports 6

 Port   VID   Untagged  Tagged  Dynamic  Forbidden
-----   ----  --------  ------  -------  ---------
 6      1       X         -       -        -

DAS-3626:admin#
```

3-10 show vlan vlanid

Description

This command is used to display the vlan information using the VLAN ID.

Format

show vlan vlanid <vidlist>

Parameters

<vidlist> - Enter the VLAN ID here.

Restrictions

None.

Example

To display the VLAN configuration for VLAN ID 1:

```
DAS-3626:admin#show vlan vlanid 1
Command: show vlan vlanid 1


VID             : 1               VLAN Name     : default
VLAN Type       : Static          Advertisement : Enabled
Member Ports    : 1-26
Static Ports    : 1-26
Current Tagged Ports  :
Current Untagged Ports: 1-26
Static Tagged Ports   :
Static Untagged Ports : 1-26
Forbidden Ports       :

 Total Entries : 1


DAS-3626:admin#
```

3-11 show vlan bonding

Description

This command is used to display the VLAN information of the specified VDSL bonding groups.

Format

show vlan bonding <bgroup_list>

Parameters

<bgroup_list> - Enter a list of VDSL bonding groups. The range is from 1 to 12.

Restrictions

None.

Example

To display the VLAN configuration for bonding group 1:

```
DAS-3626:admin#show vlan bonding 1
Command: show vlan bonding 1

 Port   VID   Untagged  Tagged  Dynamic  Forbidden
-----   ----  --------  ------  -------  ---------
 b1     1       -         X       -        -

DAS-3626:admin#
```

3-12 show port_vlan

Description

This command is used to display the ports' VLAN attributes on the Switch.

Format

show port_vlan {<portlist>}

Parameters

<portlist> - (Optional) Specifies a range of ports to be displayed.

Restrictions

None.

Example

To display 802.1Q port setting:

```
DAS-3626:admin#show port_vlan
Command: show port_vlan

Port     PVID  GVRP      Ingress Checking  Acceptable Frame Type
-------  ----  --------  ----------------  --------------------------
 1       1     Enabled   Enabled           All Frames
 2       1     Enabled   Enabled           All Frames
 3       1     Enabled   Enabled           All Frames
 4       1     Enabled   Enabled           All Frames
 5       1     Enabled   Enabled           All Frames
 6       1     Disabled  Enabled           All Frames
 7       1     Disabled  Enabled           All Frames
 8       1     Disabled  Enabled           All Frames
 9       1     Disabled  Enabled           All Frames
 10      1     Disabled  Enabled           All Frames
 11      1     Disabled  Enabled           All Frames
 12      1     Disabled  Enabled           All Frames
 13      1     Disabled  Enabled           All Frames
 14      1     Disabled  Enabled           All Frames
 15      1     Disabled  Enabled           All Frames
 16      1     Disabled  Enabled           All Frames
 17      1     Disabled  Enabled           All Frames
 18      1     Disabled  Enabled           All Frames
 19      1     Disabled  Enabled           All Frames
 20      1     Disabled  Enabled           All Frames
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

3-13 show port_vlan bonding

Description

This command is used to display the ports' VLAN attributes of the specified VDSL bonding groups on the Switch.

Format

show port_vlan bonding <bgroup_list>

Parameters

<bgroup_list> - Enter a list of VDSL bonding groups. The range is from 1 to 12.

Restrictions

None.

Example

To display the 802.1Q port setting of bonding group 1:

```
DAS-3626:admin#show port_vlan bonding 1
Command: show port_vlan bonding 1

Port     PVID  GVRP      Ingress Checking  Acceptable Frame Type
-------  ----  --------  ----------------  --------------------------
 b1      1     Disabled  Enabled           All Frames

 Total Entries : 1

DAS-3626:admin#
```

3-14 enable pvid auto_assign

Description

This command is used to enable the auto-assignment of PVID.

If "Auto-assign PVID" is enabled, PVID will be possibly changed by PVID or VLAN configuration. When user configures a port to VLAN X's untagged membership, this port's PVID will be updated with VLAN X. In the form of VLAN list command, PVID is updated with last item of VLAN list. When user removes a port from the untagged membership of the PVID's VLAN, the port's PVID will be assigned with "default VLAN".

Format

enable pvid auto_assign

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable the auto-assign PVID:

```
DAS-3626:admin# enable pvid auto_assign
Command: enable pvid auto_assign

Success.

DAS-3626:admin#
```

3-15 disable pvid auto_assign

Description

This command is used to disable auto assignment of PVID. This is the default.

Format

disable pvid auto_assign

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable the auto-assign PVID:

```
DAS-3626:admin# disable pvid auto_assign
Command: disable pvid auto_assign

Success.

DAS-3626:admin#
```

3-16 show pvid auto_assign

Description

This command is used to display the PVID auto-assignment state.

Format

show pvid auto_assign

Parameters

None.

Restrictions

None.

Example

To display PVID auto-assignment state:

```
DAS-3626:admin#show pvid auto_assign
Command: show pvid auto_assign

PVID Auto-assignment: Enabled

DAS-3626:admin#
```

3-17 config gvrp

Description

This command is used to configure the GVRP timer's value. The default value for Join time is 200 milliseconds; for Leave time is 600 milliseconds; for LeaveAll time is 10000 milliseconds.

Format

config gvrp [timer {join <value 100-100000> | leave <value 100-100000> | leaveall <value 100-100000> } | nni_bpdu_addr [dot1d | dot1ad]]

Parameters

timer - Specifies that the GVRP timer parameter will be configured.
- **join** - (Optional) Specifies the Join time will be set.
  - **<value 100-100000>** - Enter the join time used here. This value must be between 100 and 100000.
- **leave** - (Optional) Specifies the Leave time will be set.
  - **<value 100-100000>** - Enter the leave time used here. This value must be between 100 and 100000.
- **leaveall** - (Optional) Specifies the LeaveAll time will be set.
  - **<value 100-100000>** - Enter the leave all time used here. This value must be between 100 and 100000.

nni_bpdu_addr - Specifies to determine the BPDU protocol address for GVRP in service provide site. It can use 802.1d GVRP address, 802.1ad service provider GVRP address or a user defined multicast address. The range of the user defined address is 0180C2000000 - 0180C2FFFFFF.
- **dot1d** - Specifies that the NNI BPDU protocol address value will be set to Dot1d.
- **dot1ad** - Specifies that the NNI BPDU protocol address value will be set to Dot1ad.

Restrictions

Only Administrators and Operators can issue this command.

Example

To set the Join time to 200 milliseconds:

```
DAS-3626:admin# config gvrp timer join 200
Command: config gvrp timer join 200

Success.

DAS-3626:admin#
```

3-18 show gvrp

Description

This command is used to display the GVRP global setting.

Format

show gvrp

Parameters

None.

Restrictions

None.

Example

To display the global setting of GVRP:

```
DAS-3626:admin#show gvrp
Command: show gvrp

 Global GVRP   : Disabled
 Join Time     : 200 Milliseconds
 Leave Time    : 600 Milliseconds
 LeaveAll Time : 10000 Milliseconds
 NNI BPDU Address: dot1d

DAS-3626:admin#
```

3-19 enable gvrp

Description

This commands is used to enable the Generic VLAN Registration Protocol (GVRP).

Format

enable gvrp

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable the generic VLAN Registration Protocol (GVRP):

```
DAS-3626:admin# enable gvrp
Command: enable gvrp

Success.

DAS-3626:admin#
```

3-20 disable gvrp

Description

This command is used to disable the Generic VLAN Registration Protocol (GVRP).

Format

disable gvrp

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable the Generic VLAN Registration Protocol (GVRP):

```
DAS-3626:admin# disable gvrp
Command: disable gvrp

Success.

DAS-3626:admin#
```

3-21 config private_vlan

Description

This command is used to add or remove a secondary VLAN from a private VLAN.

Format

config private_vlan [<vlan_name 32> | vid <vlanid 1-4094>] [add [isolated | community] | remove] [<vlan_name 32> | vlanid <vidlist>]

Parameters

<vlan_name 32> - Enter the name of the private VLAN.
vid - Specifies the ID of the private VLAN. **<vlanid 1-4094>** - Enter the VLAN ID used here. This value must be between 1 and 4094.
add - Specifies that a secondary VLAN will be added to the private VLAN. **isolated** - Specifies the secondary VLAN as isolated VLAN. **community** - Specifies the secondary VLAN as community VLAN.
remove - Specifies that a secondary VLAN will be removed from the private VLAN.
<vlan_name 32> - Specifies the secondary VLAN name used. This name can be up to 32 characters long.
vlanid - A range of secondary VLAN to add or remove to the private VLAN. **<vidlist>** - Enter the secondary VLAN ID used here.

Restrictions

Only Administrators and Operators can issue this command.

Example

To associate secondary vlan to private vlan: v3

```
DAS-3626:admin#config private_vlan v3 add community v2
Command: config private_vlan v3 add community v2

Success.

DAS-3626:admin#
```

3-22 show private vlan

Description

This command is used to show the private VLAN information.

Format

show private_vlan {[<vlan_name 32> | vlanid<vidlist>]}

Parameters

<vlan_name 32> - (Optional) Specifies the name of the private VLAN or its secondary VLAN. This name can be up to 32 characters long.
vlanid - (Optional) Specifies the VLAN ID of the private VLAN or its secondary VLAN. **<vidlist>** - Enter the VLAN ID used here.

Restrictions

None.

Example

To display private VLAN settings:

```
DAS-3626:admin#show private_vlan
Command: show private_vlan

Primary VLAN    3
-----------------------------------------
 Promiscuous Ports   :
 Trunk Ports         :
 Community Ports     :                      Community VLAN   : 2


 Total Entries: 1


DAS-3626:admin#
```

Chapter 4 Access Authentication Control Command List

enable authen_policy
disable authen_policy
show authen_policy
create authen_login method_list_name <string 15>
config authen_login [default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local | none}
delete authen_login method_list_name <string 15>
show authen_login [default | method_list_name <string 15> | all]
create authen_enable method_list_name <string 15>
config authen_enable [default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local _enable | none}
delete authen_enable method_list_name <string 15>
show authen_enable [default | method_list_name <string 15> | all]
config authen application [console | telnet | ssh | http | all] [login | enable] [default | method_list_name <string 15>]
show authen application
create authen server_group <string 15>
config authen server_group [tacacs | xtacacs | tacacs+ | radius | <string 15>] [add | delete] server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]
delete authen server_group <string 15>
show authen server_group {<string 15>}
create authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit <int 1- 255>}
config authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+| radius] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit <int 1- 255>}
delete authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]
show authen server_host
config authen parameter response_timeout <int 0-255>
config authen parameter attempt <int 1-255>
show authen parameter
enable admin
config admin local_enable

4-1 enable authen_policy

Description

This command is used to enable system access authentication policy.

Enable system access authentication policy. When authentication is enabled, the device will adopt the login authentication method list to authenticate the user for login, and adopt the enable authentication method list to authenticate the enable password for promoting the user‘s privilege to Admin level.

Format

enable authen_policy

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To enable system access authentication policy:

```
DAS-3626:admin# enable authen_policy
Command: enable authen_policy

Success.

DAS-3626:admin#
```

4-2 disable authen_policy

Description

This command is used to disable system access authentication policy.

Disable system access authentication policy. When authentication is disabled, the device will adopt the local user account database to authenticate the user for login, and adopt the local enable password to authenticate the enable password for promoting the user‘s privilege to Admin level.

Format

disable authen_policy

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To disable system access authentication policy:

```
DAS-3626:admin# disable authen_policy
Command: disable authen_policy

Success.

DAS-3626:admin#
```

4-3 show authen_policy

Description

This command is used to display that system access authentication policy is enabled or disabled.

Format

show authen_policy

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To display system access authentication policy:

```
DAS-3626:admin# show authen_policy
Command: show authen_policy

Authentication Policy : Enabled

DAS-3626:admin#
```

4-4 create authen_login

Description

This command is used to create a user-defined method list of authentication methods for user login. The maximum supported number of the login method lists is 8.

Format

create authen_login method_list_name <string 15>

Parameters

<string 15> - Enter the user-defined method list name. This value can be up to 15 characters long.

Restrictions

Only Administrators can issue this command.

Example

To create a user-defined method list for user login:

```
DAS-3626:admin#create authen_login method_list_name login_list_1
Command: create authen_login method_list_name login_list_1

Success.

DAS-3626:admin#
```

4-5 config authen_login

Description

This command is used to configure a user-defined or default method list of authentication methods for user login. The sequence of methods will affect the altercation result. For example, if the sequence is tacacs+ first, then tacacs and local, when user trys to login, the authentication request will be sent to the first server host in tacacs+ built-in server group. If the first server host in tacacs+ group is missing, the authentication request will be sent to the second server host in tacacs+ group, and so on. If all server hosts in tacacs+ group are missing, the authentication request will be sent to the first server host in tacacs group…If all server hosts in tacacs group are missing, the local account database in the device is used to authenticate this user. When user logins the device successfully while using methods like tacacs/xtacacs/tacacs+/radius built-in or user-defined server groups or none, the “user” privilege level is assigned only. If user wants to get admin privilege level, user must use the “enable admin” command to promote his privilege level. But when local method is used, the privilege level will depend on this account privilege level stored in the local device.

Format

config authen_login [default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local | none}

Parameters

default - Specifies the default method list of authentication methods.

method_list_name - Specifies the user-defined method list of authentication methods.
- **<string 15>** - Enter the method list name here. This value can be up to 15 characters long.

method - Specifies the authentication method used.
- **tacacs** - (Optional) Specifies the authentication by the built-in server group “tacacs”.
- **xtacacs** - (Optional) Specifies the authentication by the built-in server group “xtacacs”.
- **tacacs+** - (Optional) Specifies the authentication by the built-in server group “tacacs+”.
- **radius** - (Optional) Specifies the authentication by the built-in server group “radius”.
- **server_group** - (Optional) Specifies the authentication by the user-defined server group.
  - **<string 15>** - Enter the server group value here. This value can be up 15 characters long.
- **local** - (Optional) Specifies the authentication by local user account database in device.
- **none** - (Optional) Specifies that there is no authentication.

Restrictions

Only Administrators can issue this command.

Example

To configure a user-defined method list for user login:

```
DAS-3626:admin#config authen_login method_list_name login_list_1 method tacacs+
tacacs local
Command: config authen_login method_list_name login_list_1 method tacacs+
tacacs Local

Success.

DAS-3626:admin#
```

4-6 delete authen_login

Description

This command is used to delete a user-defined method list of authentication methods for user login.

Format

delete authen_login method_list_name <string 15>

Parameters

<string 15> - Enter the user-defined method list name. This value can be up to 15 characters long.

Restrictions

Only Administrators can issue this command.

Example

To delete a user-defined method list for user login:

```
DAS-3626:admin# delete authen_login method_list_name login_list_1
Command: delete authen_login method_list_name login_list_1

Success.

DAS-3626:admin#
```

4-7 show authen_login

Description

This command is used to display the method list of authentication methods for user login.

Format

show authen_login [default | method_list_name <string 15> | all]

Parameters

default - Specifies to display default user-defined method list for user login.

method_list_name - Specifies to display the specific user-defined method list for user login. **<string 15>** - Enter the method list name here. This value can be up to 15 characters long.
all - Specifies to display all method lists for user login.

Restrictions

Only Administrators can issue this command.

Example

To display a user-defined method list for user login:

```
DAS-3626:admin# show authen_login method_list_name login_list_1
Command: show authen_login method_list_name login_list_1

Method List Name  Priority  Method Name      Comment
----------------  --------  ---------------  ------------------
login_list_1      1         tacacs+          Built-in Group
                  2         tacacs           Built-in Group
                  3         mix_1            User-defined Group
                  4         local            Keyword

DAS-3626:admin#
```

4-8 create authen_enable

Description

This command is used to create a user-defined method list of authentication methods for promoting user's privilege to Admin level.

Format

create authen_enable method_list_name <string 15>

Parameters

<string 15> - Enter the user-defined method list name. This value can be up to 15 characters long.

Restrictions

Only Administrators can issue this command.

Example

To create a user-defined method list for promoting user's privilege to Admin level:

```
DAS-3626:admin# create authen_enable method_list_name enable_list_1
Command: create authen_enable method_list_name enable_list_1

Success.

DAS-3626:admin#
```

4-9 config authen_enable

Description

This command is used to configure a user-defined or default method list of authentication methods for promoting user's privilege to Admin level. The sequence of methods will affect the authentication result. For example, if the sequence is tacacs+ first, then tacacs and local_enable, when user try to promote user's privilege to Admin level, the authentication request will be sent to the first server host in tacacs+ built-in server group. If the first server host in tacacs+ group is missing, the authentication request will be sent to the second server host in tacacs+ group, and so on. If all server hosts in tacacs+ group are missing, the authentication request will be sent to the first server host in tacacs group…If all server hosts in tacacs group are missing, the local enable password in the device is used to authenticate this user's password.

Format

config authen_enable [default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local _enable | none}

Parameters

default - Specifies the default method list of authentication methods.
method_list_name - Specifies the user-defined method list of authentication methods. **<string 15>** Enter the method list name here. This value can be up to 15 characters long.
method - Specifies the authentication method used. **tacacs** - (Optional) Specifies the authentication by the built-in server group "tacacs". **xtacacs** - (Optional) Specifies the authentication by the built-in server group "xtacacs". **tacacs+** - (Optional) Specifies the authentication by the built-in server group "tacacs+". **radius** - (Optional) Specifies the authentication by the built-in server group "radius". **server_group** - (Optional) Specifies the authentication by the user-defined server group. **<string 15>** - Enter the server group name here. This value can be up to 15 characters long. **local_enable** - (Optional) Specifies the authentication by local enable password in device. **none** - (Optional) Specifies that there is no authentication.

Restrictions

Only Administrators can issue this command.

Example

To configure a user-defined method list for promoting user's privilege to Admin level:

```
DAS-3626:admin# config authen_enable method_list_name enable_list_1 method
tacacs+ tacacs local_enable
Command: config authen_ enable method_list_name enable_list_1 method tacacs+
tacacs local_enable

Success.

DAS-3626:admin#
```

4-10 delete authen_enable

Description

This command is used to delete a user-defined method list of authentication methods for promoting user's privilege to Admin level.

Format

delete authen_enable method_list_name <string 15>

Parameters

<string 15> - Enter the user-defined method list name. This value can be up to 15 characters long.

Restrictions

Only Administrators can issue this command.

Example

To delete a user-defined method list for promoting user's privilege to Admin level:

```
DAS-3626:admin# delete authen_enable method_list_name enable_list_1
Command: delete authen_enable method_list_name enable_list_1

Success.

DAS-3626:admin#
```

4-11 show authen_enable

Description

This command is used to display the method list of authentication methods for promoting user's privilege to Admin level.

Format

show authen_enable [default | method_list_name <string 15> | all]

Parameters

default - Specifies to display default user-defined method list for promoting user's privilege to Admin level.
method_list_name - Specifies to display the specific user-defined method list for promoting user's privilege to Admin level. **<string 15>** - Enter the method list name here. This value can be up to 15 characters long.
all - Specifies to display all method lists for promoting user's privilege to Admin level.

Restrictions

Only Administrators can issue this command.

Example

To display all method lists for promoting user's privilege to Admin level:

```
DAS-3626:admin# show authen_enable method_list_name enable_list_1
Command: show authen_enable method_list_name enable_list_1

Method List Name  Priority  Method Name      Comment
----------------  --------  ---------------  ------------------
enable_list_1             1         tacacs+          Built-in Group
                          2         tacacs           Built-in Group
                          3         mix_1            User-defined Group
                          4         local            Keyword

Total Entries : 1

DAS-3626:admin#
```

4-12 config authen application

Description

This command is used to configure login or enable method list for all or the specified application.

Format

config authen application [console | telnet | ssh | http | all] [login | enable] [default | method_list_name <string 15>]

Parameters

console – Specifies to use console.
telnet - Specifies to use telnet.
ssh - Specifies to use SSH.
http - Specifies to use web.
all - Specifies to use console, telnet, SSH, and web.
login - Specifies to select the method list of authentication methods for user login.
enable - Specifies to select the method list of authentication methods for promoting user's privilege to Admin level.
default - Specifies the default method list.
method_list_name - Specifies the user-defined method list name.

<string> - Enter the method list name here. This value can be up to 15 characters long.

Restrictions

Only Administrators can issue this command.

Example

To configure the login method list for telnet:

```
DAS-3626:admin# config authen application telnet login method_list_name
login_list_1
Command: config authen application telnet login method_list_name login_list_1

Success.

DAS-3626:admin#
```

4-13 show authen application

Description

This command is used to display the login/enable method list for all applications.

Format

show authen application

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To display the login/enable method list for all applications:

```
DAS-3626:admin#show authen application
Command: show authen application

Application  Login Method List  Enable Method List
-----------  -----------------  ------------------
Console      default            default
Telnet       default            default
SSH          default            default
HTTP         default            default

DAS-3626:admin#
```

4-14 create authen server_group

Description

This command is used to create a user-defined authentication server group. The maximum supported number of server groups including built-in server groups is 8. Each group consists of 8 server hosts as maximum.

Format

create authen server_group <string 15>

Parameters

<string 15> - Enter the user-defined server group name. This value can be up to 15 characters long.

Restrictions

Only Administrators can issue this command.

Example

To create a user-defined authentication server group:

```
DAS-3626:admin# create authen server_group mix_1
Command: create authen server_group mix_1

Success.

DAS-3626:admin#
```

4-15 config authen server_group

Description

This command is used to add or remove an authentication server host to or from the specified server group. Built-in server group “tacacs”, “xtacacs”, “tacacs+”, “radius” accepts the server host with the same protocol only, but user-defined server group can accept server hosts with different protocols.

Format

config authen server_group [tacacs | xtacacs | tacacs+ | radius | <string 15>] [add | delete] server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]

Parameters

tacacs - Specifies to configure built-in server group “tacacs”.
xtacacs - Specifies to configure built-in server group “xtacacs”.
tacacs+ - Specifies to configure built-in server group “tacacs+”.
radius - Specifies to configure built-in server group “radius”.
<string 15> - Enter the server group name here. This value can be up to 15 characters long.

add - Specifies to add a server host to a server group.
delete - Specifies to remove a server host from a server group.
server_host - Specifies the server host's IP address. **<ipaddr>** - Enter the server host IP address here.
protocol - Specifies the authentication protocol used. **tacacs** - Specifies that the TACACS authentication protocol will be used. **xtacacs** - Specifies that the XTACACS authentication protocol will be used. **tacacs+** - Specifies that the TACACS+ authentication protocol will be used. **radius** - Specifies that the radius authentication protocol will be used.

Restrictions

Only Administrators can issue this command.

Example

To add an authentication server host to an server group:

```
DAS-3626:admin# config authen server_group mix_1 add server_host 10.1.1.222
protocoltacacs+
Command: config authen server_group mix_1 add server_host 10.1.1.222 protocol
tacacs+


Success.


DAS-3626:admin#
```

4-16 delete authen server_group

Description

This command is used to delete a user-defined authentication server group.

Format

delete authen server_group <string 15>

Parameters

<string 15> - Enter the user-defined server group name. This value can be up to 15 characters long.

Restrictions

Only Administrators can issue this command.

Example

To delete a user-defined authentication server group:

```
DAS-3626:admin# delete authen server_group mix_1
Command: delete authen server_group mix_1

Success.

DAS-3626:admin#
```

4-17 show authen server_group

Description

This command is used to display the authentication server groups.

Format

show authen server_group {<string 15>}

Parameters

<string 15> - (Optional) Enter the built-in or user-defined server group name. This value can be up to 15 characters long.

Restrictions

Only Administrators can issue this command.

Example

To display all authentication server groups:

```
DAS-3626:admin#show authen server_group
Command: show authen server_group

Group Name       IP Address       Protocol
---------------  ---------------  --------
mix_1            10.1.1.222       TACACS+
                 10.1.1.223       TACACS
radius           10.1.1.224       RADIUS
tacacs           10.1.1.225       TACACS
tacacs+          10.1.1.226       TACACS+
xtacacs          10.1.1.227       XTACACS

Total Entries : 5

DAS-3626:admin#
```

4-18 create authen server_host

Description

This command is used to create an authentication server host. When an authentication server host is created, IP address and protocol are the index. That means over 1 authentication protocol

services can be run on the same physical host. The maximum supported number of server hosts is 16.

Format

create authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit <int 1- 255>}

Parameters

<ipaddr> - Enter the server host IP address used here.
protocol - Specifies the host's authentication protocol. **tacacs** - Specifies the protocol as TACACS. **xtacacs** - Specifies the protocol as XTACACS. **tacacs+** - Specifies the protocol as TACACS+. **radius** - Specifies the protocol as RADIUS.
port - (Optional) Specifies the port number of authentication protocol for server host. The default value for TACACS/XTACACS/TACACS+ is 49. The default value for RADIUS is 1812. **<int 1-65535>** - Enter the authentication protocol port number here. This value must be between 1 and 65535.
key - (Optional) Specifies the key for TACACS+ and RADIUS authentication. If the value is null, no encryption will apply. This value is meaningless for TACACS and XTACACS. **<key_string 254>** - Enter the TACACS+ or the RADIUS key here. This key can be up to 254 characters long. **none** - Specifies to have no encryption for TACACS+ and RADIUS authentication. This value is meaningless for TACACS and XTACACS.
timeout - (Optional) Specifies the time in second for waiting server reply. Default value is 5 seconds. **<int 1-255>** - Enter the timeout value here. This value must be between 1 and 255 seconds.
retransmit - (Optional) Specifies the count for re-transmit. This value is meaningless for TACACS+. Default value is 2. **<int 1- 255>** - Enter the re-transmit value here. This value must be between 1 and 255.

Restrictions

Only Administrators can issue this command.

Example

To create a TACACS+ authentication server host, its listening port number is 15555 and timeout value is 10 seconds:

```
DAS-3626:admin# create authen server_host 10.1.1.222 protocol tacacs+ port
15555 timeout 10
Command: create authen server_host 10.1.1.222 protocol tacacs+ port 15555
timeout 10


Success.


DAS-3626:admin#
```

4-19 config authen server_host

Description

This command is used to configure an authentication server host.

Format

config authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit <int 1- 255>}

Parameters

<ipaddr> - Enter the server host IP address here.
protocol - Specifies the server host's authentication protocol. **tacacs** - Specifies the protocol as TACACS. **xtacacs** - Specifies the protocol as XTACACS. **tacacs+** - Specifies the protocol as TACACS+. **radius** - Specifies the protocol as RADIUS.
port - (Optional) Specifies the port number of authentication protocol for server host. Default value for TACACS/XTACACS/TACACS+ is 49. Default value for RADIUS is 1812. **<int 1-65535>** - Enter the port number here. This value must be between 1 and 65535.
key - (Optional) Specifies the key for TACACS+ and RADIUS authentication. If the value is null, no encryption will apply. This value is meaningless for TACACS and XTACACS. **<key_string 254>** - Enter the TACACS+ key here. This value can be up to 254 characters long. **none** - Specifies to have no encryption for TACACS+ and RADIUS authentication. This value is meaningless for TACACS and XTACACS.
timeout - (Optional) Specifies the time in second for waiting server reply. Default value is 5 seconds. **<int 1-255>** - Enter the timeout value here. This value must be between 1 and 255 seconds.
retransmit - (Optional) Specifies the count for re-transmit. This value is meaningless for TACACS+. Default value is 2. **<int 1- 255>** - Enter the re-transmit value here. This value must be between 1 and 255.

Restrictions

Only Administrators can issue this command.

Example

To configure a TACACS+ authentication server host's key value:

```
DAS-3626:admin# config authen server_host 10.1.1.222 protocol tacacs+ key "This
is a secret"
Command: config authen server_host 10.1.1.222 protocol tacacs+ key "This is a
se cret"

Success.

DAS-3626:admin#
```

4-20 delete authen server_host

Description

This command is used to delete an authentication server host.

Format

delete authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]

Parameters

<ipaddr> - Enter the server host IP address here.
protocol - Specifies the server host's authentication protocol. **tacacs** - Specifies the protocol as TACACS. **xtacacs** - Specifies the protocol as XTACACS. **tacacs+** - Specifies the protocol as TACACS+. **radius** - Specifies the protocol as RADIUS.

Restrictions

Only Administrators can issue this command.

Example

To delete an authentication server host:

```
DAS-3626:admin# delete authen server_host 10.1.1.222 protocol tacacs+
Command: delete authen server_host 10.1.1.222 protocol tacacs+

Success.

DAS-3626:admin#
```

4-21 show authen server_host

Description

This command is used to display the authentication server hosts.

Format

show authen server_host

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To display all authentication server hosts:

```
DAS-3626:admin# show authen server_host
Command: show authen server_host

IP Address       Protocol  Port   Timeout  Retransmit  Key
---------------  --------  -----  -------  ----------  ------------------------
-
10.1.1.222       TACACS+   15555  10       ------      This is a secret

Total Entries : 1

DAS-3626:admin#
```

4-22 config authen parameter response_timeout

Description

This command is used to configure the amount of time waiting or user input on console, telnet, SSH application.

Format

config authen parameter response_timeout <int 0-255>

Parameters

<int 0-255> - Enter the amount of time on console or telnet or SSH. This value must be between 0 and 255. 0 means there is no time out. Default value is 30 seconds.

Restrictions

Only Administrators can issue this command.

Example

To configure the amount of time waiting or user input to be 60 seconds:

```
DAS-3626:admin# config authen parameter response_timeout 60
Command: config authen parameter response_timeout 60

Success.

DAS-3626:admin#
```

4-23 config authen parameter attempt

Description

This command is used to configure the maximum attempts for user's trying to login or promote the privilege on console, telnet, SSH application.

Format

config authen parameter attempt <int 1-255>

Parameters

<int 1-255> - Enter the amount of attempts for user's trying to login or promote the privilege on console or telnet or SSH. This value must be between 1 and 255. Default value is 3.

Restrictions

Only Administrators can issue this command.

Example

To configure the maximum attempts for user's trying to login or promote the privilege to be 9:

```
DAS-3626:admin# config authen parameter attempt 9
Command: config authen parameter attempt 9

Success.

DAS-3626:admin#
```

4-24 show authen parameter

Description

This command is used to display the parameters of authentication.

Format

show authen parameter

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To display the parameters of authentication:

```
DAS-3626:admin#show authen parameter
Command: show authen parameter

Response Timeout : 60 seconds
User Attempts    : 9

DAS-3626:admin#
```

4-25 enable admin

Description

This command is used to enter the administrator level privilege. Promote the "user" privilege level to "admin" level. When the user enters this command, the authentication method tacacs, xtacacs, tacacs+, user-defined server groups, local_enable or none will be used to authenticate the user. Because TACACS, XTACACS and RADIUS don't support "enable" function in itself, if user wants to use either one of these 3 protocols to do enable authentication, user must create a special account on the server host first, which has a username "enable" and then configure its password as the enable password to support "enable" function.

This command can not be used when authentication policy is disabled.

Format

enable admin

Parameters

None.

Restrictions

None.

Example

To enable administrator lever privilege:

```
DGS-3120-24TC:puser# enable admin
Password:********

DAS-3626:admin#
```

4-26 config admin local_enable

Description

This command is used to configure the local enable password of administrator level privilege. When the user chooses the “local_enable” method to promote the privilege level, the enable password of local device is needed. When the password information is not specified in the command, the system will prompt the user to input the password interactively. For this case, the user can only input the plain text password. If the password is present in the command, the user

can select to input the password in the plain text form or in the encrypted form. The encryption algorithm is based on SHA-I.

Format

config admin local_enable

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To configure the administrator password:

```
DAS-3626:admin# config admin local_enable
Command: config admin local_ebable

Enter the old password:
Enter the case-sensitive new password:******
Enter the new password again for confirmation:******
Success.

DAS-3626:admin#
```

Chapter 5 Access Control List (ACL) Command List

create access_profile profile_id <value 1-8> profile_name <name 1-32> [ethernet {vlan {<hex 0x0-0x0fff>} | source_mac <macmask 000000000000-ffffffffffff> | destination_mac <macmask 000000000000-ffffffffffff> | 802.1p | ethernet_type} | ipv4 {vlan {<hex 0x0-0x0fff>} | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code} | igmp {type} | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}]} | packet_content_mask {offset_chunk_1 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_2 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_3 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_4 <value 0-31> <hex 0x0-0xffffffff>} | ipv6 {class | flowlabel | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask> | [tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | icmp {type | code}]}]
delete access_profile [profile_id <value 1-8> | profile_name <name 1-32> | all]
config access_profile [profile_id <value 1-8> | profile_name <name 1-32>] [add access_id [auto_assign | <value 1-256>] [ethernet {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] {mask <hex 0x0-0x0fff>} | source_mac <macaddr> {mask <macmask>} | destination_mac <macaddr> {mask <macmask>} | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff>} | ipv4 {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] {mask <hex 0x0-0x0fff>} | source_ip <ipaddr> {mask <netmask>} | destination_ip <ipaddr> {mask <netmask>} | dscp <value 0-63> | [icmp {type <value 0-255> | code <value 0-255>} | igmp {type <value 0-255>} | tcp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>} | flag [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | protocol_id <value 0-255> {user_define <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>}}]} | packet_content {offset_chunk_1 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>} | offset_chunk_2 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>} | offset_chunk_3 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>} | offset_chunk_4 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>}} | ipv6 {class <value 0-255> | flowlabel <hex 0x0-0xfffff> | source_ipv6 <ipv6addr> {mask<ipv6mask>} | destination_ipv6 <ipv6addr> {mask <ipv6mask>} | [tcp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex0x0-0xffff>}} | udp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | icmp {type <value 0-255> | code <value 0-255>}]}] [port [<portlist> | all] | vlan_based [vlan <vlan_name 32> | vlan_id <vlanid 1-4094>]] [permit {priority <value 0-7> {replace_priority} | [replace_dscp_with <value 0-63> | replace_tos_precedence_with <value 0-7>] | counter [enable | disable]} | mirror | deny] {time_range <range_name 32>} | delete access_id <value 1-256>]
show access_profile {[profile_id <value 1-8> | profile_name <name 1-32>]}
config flow_meter [profile_id <value 1-8> | profile_name <name 1-32>] access_id <value 1-256> [rate [<value 0-1048576>] {burst_size [<value 0-131072>]} rate_exceed [drop_packet | remark_dscp <value 0-63>] | tr_tcm cir <value 0-1048576> {cbs <value 0-131072>} pir <value 0-1048576> {pbs <value 0-131072>} {[color_blind | color_aware]} {conform [permit | replace_dscp <value 0-63>] {counter [enable | disable]}} exceed [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} violate [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} | sr_tcm cir <value 0-1048576> cbs <value 0-131072> ebs <value 0-131072> {[color_blind | color_aware]} {conform [permit | replace_dscp <value 0-63>] {counter [enable | disable]}} exceed [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} violate [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} | delete]
show flow_meter {[profile_id <value 1-8> | profile_name <name 1-32>] {access_id <value 1-256>}}

config time_range <range_name 32> [hours start_time <time hh:mm:ss> end_time <time hh:mm:ss> weekdays <daylist> | delete]
show time_range
show current_config access_profile

5-1 create access_profile profile_id

Description

This command is used to create access list rules.

Support for field selections can have additional limitations that are project dependent.

For example, for some hardware, it may be invalid to specify a class and source IPv6 address at the same time. The user will be prompted with these limitations.

Format

create access_profile profile_id <value 1-8> profile_name <name 1-32> [ethernet {vlan {<hex 0x0-0x0fff>} | source_mac <macmask 000000000000-ffffffffffff> | destination_mac <macmask 000000000000-ffffffffffff> | 802.1p | ethernet_type} | ipv4 {vlan {<hex 0x0-0x0fff>} | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code} | igmp {type} | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}]} | packet_content_mask {offset_chunk_1 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_2 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_3 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_4 <value 0-31> <hex 0x0-0xffffffff>} | ipv6 {class | flowlabel | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask> | [tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | icmp {type | code}]}]

Parameters

<value 1-8> - Enter the profile ID here. This value must be between 1 and 8.
profile_name - Specifies the name of the profile must be specified. The maximum length is 32 characters. **<name 1-32>** - Enter the profile name here.
ethernet - Specifies this is an ethernet mask. **vlan** - (Optional) Specifies a VLAN mask. Only the last 12 bits of the mask will be considered. **<hex 0x0-0x0fff>** - Enter the VLAN mask value here. **source_mac** - (Optional) Specifies the source MAC mask. **<macmask 000000000000-ffffffffffff>** - Enter the source MAC address used here. **destination_mac** - (Optional) Specifies the destination MAC mask. **<macmask 000000000000-ffffffffffff>** - Enter the destination MAC address used here. **802.1p** - (Optional) Specifies the 802.1p priority tag mask. **ethernet_type** - (Optional) Specifies the Ethernet type mask.
ipv4 - Specifies this is a IPv4 mask. **vlan** - (Optional) Specifies a VLAN mask. Only the last 12 bits of the mask will be considered. **<hex 0x0-0x0fff>** -Enter the VLAN mask value here. **source_ip_mask** - (Optional) Specifies a source IP address mask. **<netmask>** - Enter the source IP address mask here. **destination_ip_mask** - (Optional) Specifies a destination IP address mask. **<netmask>** - Enter the destination IP address mask here. **dscp** - (Optional) Specifies the DSCP mask.

icmp - (Optional) Specifies that the rule applies to ICMP traffic.
type - (Optional) Specifies the type of ICMP traffic.
code - (Optional) Specifies the code of ICMP traffic
igmp - (Optional) Specifies that the rule applies to IGMP traffic.
type - (Optional) Specifies the type of IGMP traffic.
tcp - (Optional) Specifies that the rule applies to TCP traffic.
src_port_mask - (Optional) Specifies the TCP source port mask.
<hex 0x0-0xffff> - Enter the TCP source port mask here.
dst_port_mask - (Optional) Specifies the TCP destination port mask.
<hex 0x0-0xffff> - Enter the TCP destination port mask here.
flag_mask - (Optional) Specifies the TCP flag field mask.
all - Specifies that all the flags will be used for the TCP mask.
urg - (Optional) Specifies that the TCP flag field will be set to 'urg'.
ack - (Optional) Specifies that the TCP flag field will be set to 'ack'.
psh - (Optional) Specifies that the TCP flag field will be set to 'psh'.
rst - (Optional) Specifies that the TCP flag field will be set to 'rst'.
syn - (Optional) Specifies that the TCP flag field will be set to 'syn'.
fin - (Optional) Specifies that the TCP flag field will be set to 'fin'.
udp - (Optional) Specifies that the rule applies to UDP traffic.
src_port_mask - Specifies the UDP source port mask.
<hex 0x0-0xffff> - Enter the UDP source port mask here.
dst_port_mask - Specifies the UDP destination port mask.
<hex 0x0-0xffff> - Enter the UDP destination port mask here.
protocol_id_mask - (Optional) Specifies that the rule applies to IP protocol ID traffic.
<0x0-0xff> - Enter the protocol ID mask here.
user_define_mask - (Optional) Specifies that the rule applies to the IP protocol ID, and that the mask option behind the IP header length is 20 bytes.
<hex 0x0-0xffffffff> - Enter a user-defined mask value here.

packet_content_mask - Specifies the packet content mask. Only one packet_content_mask profile can be created.
offset_chunk_1 - (Optional) Specifies that the offset chunk 1 will be used.
<value 0-31> - Enter the offset chunk 1 value here. This value must be between 0 and 31.
<hex 0x0-0xffffffff> - Enter the offset chunk 1 mask here.
offset_chunk_2 - (Optional) Specifies that the offset chunk 2 will be used.
<value 0-31> - Enter the offset chunk 2 value here. This value must be between 0 and 31.
<hex 0x0-0xffffffff> - Enter the offset chunk 2 mask here.
offset_chunk_3 - (Optional) Specifies that the offset chunk 3 will be used.
<value 0-31> - Enter the offset chunk 3 value here. This value must be between 0 and 31.
<hex 0x0-0xffffffff> - Enter the offset chunk 3 mask here.
offset_chunk_4 - (Optional) Specifies that the offset chunk 4 will be used.
<value 0-31> - Enter the offset chunk 4 value here. This value must be between 0 and 31.
<hex 0x0-0xffffffff> - Enter the offset chunk 4 mask here.

ipv6 - Specifies this is the IPv6 mask.
class - (Optional) Specifies the IPv6 class.
flowlabel - (Optional) Specifies the IPv6 flow label.
source_ipv6_mask - (Optional) Specifies an IPv6 source sub-mask.
<ipv6mask> - Enter the source IPv6 mask value here.
destination_ipv6_mask - (Optional) Specifies an IPv6 destination sub-mask.
<ipv6mask> -Enter the destination IPv6 mask value here.
tcp - (Optional) Specifies that the rule applies to TCP traffic.
src_port_mask - (Optional) Specifies an IPv6 Layer 4 TCP source port mask.
<hex 0x0-0xffff> - Enter the TCP source port mask value here.
des_port_mask - (Optional) Specifies an IPv6 Layer 4 TCP destination port mask.
<hex 0x0-0xffff> - Enter the TCP destination port mask value here.
udp - (Optional) Specifies that the rule applies to UDP traffic.
src_port_mask - (Optional) Specifies the UDP source port mask.
<hex 0x0-0xffff> - Enter the UDP source port mask value here.
dst_port_mask - (Optional) Specifies the UDP destination port mask.
<hex 0x0-0xffff> - Enter the UDP destination port mask value here.
icmp - (Optional) Specifies a mask for ICMP filtering.

type - (Optional) Specifies the inclusion of the ICMP type field in the mask.
code - (Optional) Specifies the inclusion of the ICMP code field in the mask.

Restrictions

Only Administrators and Operators can issue this command.

Example

To create an access profile:

```
DAS-3626:admin# create access_profile profile_id 1 profile_name t1 ethernet
vlan source_mac 00-00-00-00-00-01 destination_mac 00-00-00-00-00-02 802.1p
ethernet_type
Command: create access_profile profile_id 1 profile_name 1 ethernet vlan
source_mac 00-00-00-00-00-01 destination_mac 00-00-00-00-00-02 802.1p
ethernet_type

Success.

DAS-3626:admin# create access_profile profile_id 2 profile_name 2 ip vlan
source_ip_mask 20.0.0.0 destination_ip_mask 10.0.0.0 dscp icmp type code
Command: create access_profile profile_id 2 profile_name t2 ip vlan
source_ip_mask 20.0.0.0 destination_ip_mask 10.0.0.0 dscp icmp type code

Success.

DAS-3626:admin# create access_profile profile_id 4 profile_name 4
packet_content_mask offset_chunk_1 3 0xFFFF offset_chunk_2 5 0xFF00
offset_chunk_3 14 0xFFFF0000 offset_chunk_4 16 0xFF000000
Command: create access_profile profile_id 4 profile_name 4 packet_content_mask
offset_chunk_1 3 0xFFFF offset_chunk_2 5 0xFF00 offset_chunk_3 14 0xFFFF0000
offset_chunk_4 16 0xFF000000

Success.

DAS-3626:admin#
```

5-2 delete access_profile

Description

This command is used to delete access list profiles.

The delete access_profile command can only delete profiles that were created using the ACL module.

Format

delete access_profile [profile_id <value 1-8> | profile_name <name 1-32> | all]

Parameters

profile_id - Specifies the index of the access list profile.
<value 1-8> - Enter the profile ID value here. This value must be between 1 and 8.

profile_name - Specifies the name of the profile. The maximum length is 32 characters. **<name 1-32>** - Enter the profile name here. This value must be between 1 and 32.
all - Specifies that the whole access list profile will be deleted.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete the access list rule with a profile ID of 10:

```
DAS-3626:admin# delete access_profile profile_id 10
Command: delete access_profile profile_id 10

Success.

DAS-3626:admin#
```

5-3 config access_profile

Description

This command is used to configure an access list entry. The ACL mirror function works after the mirror has been enabled and the mirror port has been configured using the mirror command.

When applying an access rule to a target, the setting specified in the VLAN field will not take effect if the target is a VLAN.

Format

config access_profile [profile_id <value 1-8> | profile_name <name 1-32>] [add access_id [auto_assign | <value 1-256>] [ethernet {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] {mask <hex 0x0-0x0fff>} | source_mac <macaddr> {mask <macmask>} | destination_mac <macaddr> {mask <macmask>} | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff>} | ipv4 {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] {mask <hex 0x0-0x0fff>} | source_ip <ipaddr> {mask <netmask>} | destination_ip <ipaddr> {mask <netmask>} | dscp <value 0-63> | [icmp {type <value 0-255> | code <value 0-255>} | igmp {type <value 0-255>} | tcp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>} | flag [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | protocol_id <value 0-255> {user_define <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>}}]} | packet_content {offset_chunk_1 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>} | offset_chunk_2 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>} | offset_chunk_3 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>} | offset_chunk_4 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>}} | ipv6 {class <value 0-255> | flowlabel <hex 0x0-0xfffff> | source_ipv6 <ipv6addr> {mask<ipv6mask>} | destination_ipv6 <ipv6addr> {mask <ipv6mask>} | [tcp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex0x0-0xffff>}} | udp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | icmp {type <value 0-255> | code <value 0-255>}]}] [port [<portlist> | all] | vlan_based [vlan <vlan_name 32> | vlan_id <vlanid 1-4094>]] [permit {priority <value 0-7> {replace_priority} | [replace_dscp_with <value 0-63> | replace_tos_precedence_with <value

0-7>] | counter [enable | disable]} | mirror | deny] {time_range <range_name 32>} | delete access_id <value 1-256>]

Parameters

profile_id - Specifies the index of the access list profile.
- **<value 1-8>** - Enter the profile ID value here. This value must be between 1 and 8.

profile_name - Specifies the name of the profile.
- **<name 1-32>** - Enter the profile name here. This name can be up to 32 characters long.

add - Specifies a profile or a rule to be added.

access_id - Specifies the index of the access list entry. The value range is 1-256, but the supported maximum number of entries depends on the project. If the auto_assign option is selected, the access ID is automatically assigned, when adding multiple ports.
auto_assign - Specifies that the access ID will automatically be assigned.
- **<value 1-256>** - Enter the access ID used here. This value must be between 1 and 256.

ethernet - Specify to configure the ethernet access profile.
- **vlan** - (Optional) Specify the VLAN name.
  - **<vlan_name 32>** - Enter the name of the VLAN here. This name can be up to 32 characters long.
- **vlan_id** - (Optional) Specify the VLAN ID used.
  - **<vlanid 1-4094>** - Enter the VLAN ID used here. This value must be between 1 and 4094.
- **mask** - (Optional) Specify an additional mask parameter that can be configured.
  - **<hex 0x0-0x0fff>** - Enter the mask value here.
- **source_mac** - (Optional) Specify the source MAC address.
  - **<macaddr>** - Enter the source MAC address used for this configuration here.
  - **mask** - (Optional) Specify an additional mask parameter that can be configured.
    - **<macmask>** - Enter the source MAC mask used here.
- **destination_mac** - (Optional) Specify the destination MAC address.
  - **<macaddr>** - Enter the destination MAC address used for this configuration here.
  - **mask** - (Optional) Specify an additional mask parameter that can be configured.
    - **<macmask>** - Enter the destination MAC mask here.
- **802.1p** - (Optional) Specify the value of the 802.1p priority tag. The priority tag ranges from 1 to 7.
  - **<value 0-7>** - Enter the 802.1p priority tag value here.
- **ethernet_type** - (Optional) Specify the Ethernet type.
  - **<hex 0x0-0xffff>** - Enter the Ethernet type mask here.

ipv4 - Specify to configure the IP access profile.
- **vlan** - (Optional) Specify a VLAN name.
  - **<vlan_name 32>** - Enter the name of the VLAN here. This name can be up to 32 characters long.
- **vlan_id** - (Optional) Specify that VLAN ID used.
  - **<vlanid 1-4094>** - Enter the VLAN ID used here. This value must be between 1 and 4094.
- **mask** - (Optional) Specify an additional mask parameter that can be configured.
  - **<hex 0x0-0x0fff>** - Enter the mask value here.
- **source_ip** - (Optional) Specify an IP source address.
  - **<ipaddr>** - Enter the source IP address used for this configuration here.
  - **mask** - (Optional) Specify an additional mask parameter that can be configured.
    - **<netmask>** - Enter the source netmask used here.
- **destination_ip** - (Optional) Specify an IP destination address.
  - **<ipaddr>** - Enter the destination IP address used for this configuration here.
  - **mask** - (Optional) Specify an additional mask parameter that can be configured.
    - **<netmask>** - Enter the destination netmask used here.
- **dscp** - (Optional) Specify the value of DSCP. The DSCP value ranges from 0 to 63.
  - **<value>** - Enter the DSCP value here.
- **icmp** - (Optional) Specify to configure the ICMP parameters.
  - **type** - (Optional) Specify that the rule will apply to the ICMP Type traffic value.
    - **<value 0-255>** - Enter the ICMP type traffic value here. This value must be between 0 and 255.

code - Specify that the rule will apply to the ICMP Code traffic value.
<value 0-255> - Enter the ICMP code traffic value here. This value must be between 0 and 255.
igmp - (Optional) Specify to configure the IGMP parameters.
type - (Optional) Specify that the rule will apply to the IGMP Type traffic value.
<value 0-255> - Enter the IGMP type traffic value here. This value must be between 0 and 255.
tcp - (Optional) Specify to configure the TCP parameters.
src_port - (Optional) Specify that the rule will apply to a range of TCP source ports.
<value 0-65535> - Enter the TCP source port value here. This value must be between 0 and 65535.
mask - (Optional) Specify an additional mask parameter that can be configured.
<hex 0x0-0xffff> - Enter the source port mask here.
dst_port - (Optional) Specify that the rule will apply to a range of TCP destination ports.
<value 0-65535> - Enter the TCP destination port value here. This value must be between 0 and 65535.
mask - (Optional) Specify an additional mask parameter that can be configured.
<hex 0x0-0xffff> - Enter the destination port mask here.
flag - (Optional) Specify the TCP flag fields.
all - Specify that all the TCP flags will be used in this configuration.
urg - (Optional) Specify that the TCP flag field will be set to 'urg'.
ack - (Optional) Specify that the TCP flag field will be set to 'ack'.
psh - (Optional) Specify that the TCP flag field will be set to 'psh'.
rst - (Optional) Specify that the TCP flag field will be set to 'rst'.
syn - (Optional) Specify that the TCP flag field will be set to 'syn'.
fin - (Optional) Specify that the TCP flag field will be set to 'fin'.
udp - (Optional) Specify to configure the UDP parameters.
src_port - (Optional) Specify the UDP source port range.
<value 0-65535> - Enter the UDP source port value here. This value must be between 0 and 65535.
mask - (Optional) Specify an additional mask parameter that can be configured.
<hex 0x0-0xffff> - Enter the source port mask here.
dst_port - (Optional) Specify the UDP destination port range.
<value 0-65535> - Enter the UDP destination port value here. This value must be between 0 and 65535.
mask - (Optional) Specify an additional mask parameter that can be configured.
<hex 0x0-0xffff> - Enter the destination port mask here.
protocol_id - (Optional) Specify that the rule will apply to the value of IP protocol ID traffic.
<value 0-255> - Enter the protocol ID used here.
user_define - (Optional) Specify that the rule will apply to the IP protocol ID and that the mask options behind the IP header , which has a length of 20 bytes.
<hex 0x0-0xffffffff> - Enter the user-defined mask value here.
mask - (Optional) Specify an additional mask parameter that can be configured.
<hex 0x0-0xffffffff> - Enter the mask value here.

packet_content - A maximum of 11 offsets can be specified. Each offset defines 2 bytes of data which is identified as a single UDF field. The offset reference is also configurable. It can be defined to start at the end of the tag, the end of the ether type or the end of the IP header. To qualify the fields before the end of the tag, the destination address, source address, and the VLAN tags are also included
offset_chunk_1 – (Optional) Specify the value of the packet bytes to be matched. Offset chunk 1 will be used.
<hex 0x0-0xffffffff> - Enter the offset chunk 1 mask here.
offset_chunk_2 - (Optional) Specify the value of the packet bytes to be matched. Offset chunk 2 will be used.
<hex 0x0-0xffffffff> - Enter the offset chunk 2 mask here.
offset_chunk_3 - (Optional) Specify the value of the packet bytes to be matched. Offset chunk 3 will be used.
<hex 0x0-0xffffffff> - Enter the offset chunk 3 mask here.
offset_chunk_4 - (Optional) Specify the value of the packet bytes to be matched. Offset chunk 4 will be used.

<hex 0x0-0xffffffff> - Enter the offset chunk 4 mask here.

ipv6 - Specify that the rule applies to IPv6 fields.
- **class** - (Optional) Specify the value of the IPv6 class.
  - **<value 0-255>** - Enter the IPv6 class value here. This value must be between 0 and 255.
- **flowlabel** - (Optional) Specify the value of the IPv6 flow label.
  - **<hex 0x0-0xffff>** - Enter the IPv6 flow label mask used here.
- **source_ipv6** - (Optional) Specify the value of the IPv6 source address.
  - **<ipv6addr>** - Enter the source IPv6 address used for this configuration here.
  - **mask** - (Optional) Specify an additional mask parameter that can be configured.
    - **<ipv6mask>** - Enter the source IPv6 mask here.
- **destination_ipv6** - (Optional) Specify the value of the IPv6 destination address.
  - **<ipv6addr>** - Enter the destination IPv6 address used for this configuration here.
  - **mask** - (Optional) Specify an additional mask parameter that can be configured.
    - **<ipv6mask>** - Enter the destination IPv6 mask here.
- **tcp** - (Optional) Specify to configure the TCP parameters.
  - **src_port** - Specify the value of the IPv6 Layer 4 TCP source port.
    - **<value 0-65535>** - Enter the TCP source port value here. This value must be between 0 and 65535.
    - **mask** - (Optional) Specify an additional mask parameter that can be configured.
      - **<hex 0x0-0xffff>** - Enter the TCP source port mask value here.
  - **dst_port** - (Optional) Specify the value of the IPv6 Layer 4 TCP destination port.
    - **<value 0-65535>** - Enter the TCP destination port value here. This value must be between 0 and 65535.
    - **mask** - (Optional) Specify an additional mask parameter that can be configured.
      - **<hex 0x0-0xffff>** - Enter the TCP destination port mask value here.
- **udp** - (Optional) Specify to configure the UDP parameters.
  - **src_port** - Specify the value of the IPv6 Layer 4 UDP source port.
    - **<value 0-65535>** - Enter the UDP source port value here. This value must be between 0 and 65535.
    - **mask** - (Optional) Specify an additional mask parameter that can be configured.
      - **<hex 0x0-0xffff>** - Enter the UDP source port mask value here.
  - **dst_port** - Specify the value of the IPv6 Layer 4 UDP destination port.
    - **<value 0-65535>** - Enter the UDP destination port value here. This value must be between 0 and 65535.
    - **mask** - (Optional) Specify an additional mask parameter that can be configured.
      - **<hex 0x0-0xffff>** - Enter the UDP destination port mask value here.
- **icmp** - (Optional) Specify to configure the ICMP parameters used.
  - **type** - (Optional) Specify that the rule applies to the value of ICMP type traffic.
    - **<value 0-255>** - Enter the ICMP type traffic value here. This value must be between 0 and 255.
  - **code** - Specify that the rule applies to the value of ICMP code traffic.
    - **<value 0-255>** - Enter the ICMP code traffic value here. This value must be between 0 and 255.

port - Specify the port list used for this configuration.
- **<portlist>** - Enter a list of ports used for the configuration here.
- **all** - Specify that all the ports will be used for this configuration.

vlan_based - Specify that the rule will be VLAN based.
- **vlan** - Specify the VLAN name used for this configuration.
  - **<vlan_name>** - Enter the VLAN name used for this configuration here.
- **vlan_id** - Specify the VLAN ID used for this configuration.
  - **<vlanid 1-4094>** - Enter the VLAN ID used here. This value must be between 1 and 4094.

permit - Specify that packets matching the access rule are permitted by the Switch.
- **priority** - (Optional) Specify that the priority of the packet will change if the packet matches the access rule.
  - **<value 0-7>** - Enter the priority value here. This value must be between 0 and 7.
  - **replace_priority** - (Optional) Specify that the 802.1p priority of the outgoing packet will be replaced.
- **replace_dscp_with** - (Optional) Specify that the DSCP of the outgoing packet is changed with the new value. If using this action without an action priority, the packet will be sent to the default TC.

<value 0-63> - Enter the replace DSCP with value here. This value must be between 0 and 63. **replace_tos_precedence_with** - (Optional) Specify that the IP precedence of the outgoing packet is changed with the new value. If used without an action priority, the packet is sent to the default TC. **<value 0-7>** - Enter the replace ToS precedence with value here. This value must be between 0 and 7. **counter** - (Optional) Specify whether the ACL counter feature is enabled or disabled. This parameter is optional. The default option is disabled. If the rule is not bound with the flow_meter, all matching packets are counted. If the rule is bound with the flow_meter, then the "counter" is overridden. **enable** - Specify that the ACL counter feature will be enabled. **disable** - Specify that the ACL counter feature will be disabled.
mirror - Specify that packets matching the access rules are copied to the mirror port.
deny - Specify that packets matching the access rule are filtered by the Switch. **time_range** - (Optional) Specify the name of the time range entry. **<range_name 32>** - Enter the time range name here. This name can be up to 32 characters long.
delete access_id - Specify to delete the access ID. The value range is 1-256, but the supported maximum number of entries depends on the project. **<value 1-256>** - Enter the access ID used here. This value must be between 1 and 256.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure a rule entry for a packet content mask profile (option 3):

```
DAS-3626:admin#  config access_profile profile_id 5 add access_id auto_assign
packet_content offset5 0xF0 port all deny
Command: config access_profile profile_id 5 add access_id auto_assign
packet_content offset5 0xF0 port all deny


Success.


DAS-3626:admin#
```

5-4 show access_profile

Description

This command is used to display the current access list table.

Format

show access_profile {[profile_id <value 1-8> | profile_name <name 1-32>]}

Parameters

profile_id - (Optional) Specifies the index of the access list profile. **<value 1-6>** - Enter the profile ID used here. This value must be between 1 and 8.
profile_name - (Optional) Specifies the name of the profile. **<name 1-32>** - Enter the profile name used here. This name can be up to 32 characters long.

Restrictions

None.

Example

To display the current access list table:

```
DAS-3626:admin#show access_profile
Command: show access_profile

Access Profile Deny All status: Disabled
Access Profile Deny All port:

Access Profile Table

Total User Set Rule Entries : 3
================================================================================
=
Profile ID: 1     Profile name: Ethernet  Type: Ethernet

MASK on
    VLAN            : 0xFFF
    802.1p
--------------------------------------------------------------------------------
-
Access ID : 1    (auto assign)    Ports: 1

Match on
    VLAN ID         : 1
    802.1p          : 2

Action:
    Permit

CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

5-5 config flow_meter

Description

This command is used to configure the flow-based metering function. The metering function supports three modes: single rate two color, single rate three color, and two rate three color. The access rule must be created before the parameters of this function can be applied.

For the single rate two color mode, users may set the preferred bandwidth for this rule, in Kbps, and once the bandwidth has been exceeded, overflowing packets will either be dropped or have a drop precedence set, depending on the user configuration.

For single rate three color mode, users need to specify the committed rate, in Kbps, the committed burst size, and the excess burst size.

For the two rate three color mode, users need to specify the committed rate in Kbps, the committed burst size, the peak rate and the peak burst size.

There are two cases for mapping the color of a packet: Color-blind mode and Color-aware mode. In the Color-blind case, the determination for the packet's color is based on the metering result. In the Color-aware case, the determination for the packet's color is based on the metering result and the ingress DSCP.

When color-blind or color-aware is not specified, color-blind is the default mode.

The green color packet will be treated as the conforming action, the yellow color packet will be treated as the exceeding action, and the red color packet will be treated as the violating action.

The replace DSCP action can be performed on packets that conform (GREEN) and packets that do not conform (YELLOW and RED). If drop YELLOW/RED is selected, the action to replace the DSCP will not take effect.

Format

config flow_meter [profile_id <value 1-8> | profile_name <name 1-32>] access_id <value 1-256> [rate [<value 0-1048576>] {burst_size [<value 0-131072>]} rate_exceed [drop_packet | remark_dscp <value 0-63>] | tr_tcm cir <value 0-1048576> {cbs <value 0-131072>} pir <value 0-1048576> {pbs <value 0-131072>} {[color_blind | color_aware]} {conform [permit | replace_dscp <value 0-63>] {counter [enable | disable]}} exceed [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} violate [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} | sr_tcm cir <value 0-1048576> cbs <value 0-131072> ebs <value 0-131072> {[color_blind | color_aware]} {conform [permit | replace_dscp <value 0-63>] {counter [enable | disable]}} exceed [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} violate [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} | delete]

Parameters

profile_id - Specifies the profile ID. **<value 1-8>** - Enter the profile ID here. This value must be between 1 and 8.
profile_name - Specifies the name of the profile. The maximum length is 32 characters. **<name 1-32>** - Enter the profile name used here.
access_id - Specifies the access ID. **<value 1-256>** - Enter the access ID used here. This value must be between 1 and 256.
rate - Specifies the rate for single rate two color mode. Specifies the committed bandwidth in Kbps for the flow. The value m and n are determined by the project. **<value 0-1048576>** - Enter the rate for single rate two color mode here. This value must be between 0 and 1048576.
burst_size - (Optional) Specifies the burst size for the single rate two color mode. The unit is Kbytes. **<value 0-131072>** - Enter the burst size value here. This value must be between 0 and 131072.
rate_exceed - Specifies the action for packets that exceeds the committed rate in single rate, two color mode. **drop_packet** - Specifies to drop the packet immediately. **remark_dscp** - Specifies to mark the packet with a specified DSCP. The packet is set to have a high drop precedence. **<value 0-63>** - Enter the remark DSCP value here. This value must be between 0 and 63.
tr_tcm - Specifies the "two rate three color mode".
cir - Specifies the "Committed Information Rate". The unit is in Kbps. CIR should always be equal or less than PIR. **<value 0-1048576>** - Enter the commited information rate value here. This value must be between 0 and 1048576.
cbs - (Optional) Specifies the "Committed Burst Size". The unit is Kbytes. That is to say, 1 means

1Kbytes. This parameter is an optional parameter. The default value is 4*1024.
<value 0-1048576> - Enter the commited burst size value here. This value must be between 0 and 1048576.

pir - Specifies the “Peak Information Rate”. The unit is in Kbps. PIR should always be equal to or greater than CIR.
<value 0-1048576> - Enter the peak information rate value here. This value must be between 0 and 1048576.

pbs - (Optional) Specifies the “Peak Burst Size”. The unit is in Kbytes. This parameter is an optional parameter. The default value is 4*1024.
<value 0-131072> - Enter the peak burst size value here. This value must be between 0 and 131072.

color_blind - (Optional) Specifies the meter mode as color-blind. The default is color-blind mode.
color_aware - (Optional) Specifies the meter mode as color-aware. The final color of the packet is determined by the initial color of the packet and the metering result.

conform - (Optional) Specifies the action when a packet is mapped to the “green” color.
permit - Permits the packet.
replace_dscp - Specifies to change the DSCP of the packet.
<value 0-63> - Enter the replace DSCP value here. This value must be between 0 and 63.

counter - (Optional) Specifies the ACL counter. This is optional. The default is “disable”. The resource may be limited so that a counter cannot be turned on. Counters will be cleared when the function is disabled.
enable - Specifies that the ACL counter option will be enabled.
disable - Specifies that the ACL counter option will be disabled.

replace_dscp - (Optional) Specifies to change the DSCP of an un-conforming (yellow or red) packet.
<value 0-63> - Enter the replace DSCP value here. This value must be between 0 and 63.

exceed - Specifies the action when a packet is mapped to the “yellow” color.
permit - Specifies to permit the packet.
replace_dscp - Specifies to change the DSCP of the packet.
<value 0-63> - Enter the replace DSCP value here. This value must be between 0 and 63.
drop - Specifies to drop the packet.

counter - (Optional) Specifies the ACL counter. This is optional. The default is “disable”. The resource may be limited so that a counter cannot be turned on. Counters will be cleared when the function is disabled.
enable - Specifies that the ACL counter option will be enabled.
disable - Specifies that the ACL counter option will be disabled.

violate - Specifies the action when a packet is mapped to the “red” color.
permit - Specifies to permit the packet.
replace_dscp - Specifies to change the DSCP of the packet.
<value 0-63> - Enter the replace DSCP value here. This value must be between 0 and 63.
drop - Specifies to drop the packet.

counter - (Optional) Specifies the ACL counter. This is optional. The default is “disable”. The resource may be limited so that a counter cannot be turned on. Counters will be cleared when the function is disabled.
enable - Specifies that the ACL counter option will be enabled.
disable - Specifies that the ACL counter option will be disabled.

sr_tcm - Specifies “single rate three color mode”.

cir - Specifies the “Committed Information Rate”. The unit is Kbps.
<value 0-1048576> - Enter the comitted information rate value here. This value must be between 0 and 1048576.

cbs - Specifies the “Committed Burst Size” The unit is Kbytes.
<value 0-131072> - Enter the commited burst size value here. This value must be between 0 and 131072.

ebs - Specifies the “Excess Burst Size”. The unit is Kbytes.
<value 0-131072> - Enter the excess burst size value here. This value must be between 0 and 131072.

color_blind - (Optional) Specifies the meter mode as color-blind. The default is color-blind mode.
color_aware - (Optional) Specifies the meter mode as color-aware. The final color of the packet is determined by the initial color of the packet and the metering result.

conform - (Optional) Specifies the action when a packet is mapped to the “green” color. **permit** - Specifies to permit the packet. **replace_dscp** - Specifies to change the DSCP of the packet. **<value 0-63>** - Enter the replace DSCP value here. This value must be between 0 and 63.
counter - (Optional) Specifies the ACL counter. This is optional. The default is “disable”. The resource may be limited so that a counter cannot be turned on. Counters will be cleared when the function is disabled. **enable** - Specifies that the ACL counter option will be enabled. **disable** - Specifies that the ACL counter option will be disabled.
exceed - Specifies the action when a packet is mapped to the “yellow” color. **permit** - Specifies to permit the packet. **replace_dscp** - Specifies to change the DSCP of the packet. **<value 0-63>** - Enter the replace DSCP value here. This value must be between 0 and 63. **drop** - Specifies to drop the packet.
counter - (Optional) Specifies the ACL counter. This is optional. The default is “disable”. The resource may be limited so that a counter cannot be turned on. Counters will be cleared when the function is disabled. **enable** - Specifies that the ACL counter option will be enabled. **disable** - Specifies that the ACL counter option will be disabled.
violate - Specifies the action when a packet is mapped to the “red” color. **permit** - Specifies to permit the packet. **replace_dscp** - Specifies to change the DSCP of the packet. **<value 0-63>** - Enter the replace DSCP value here. This value must be between 0 and 63. **drop** - Specifies to drop the packet.
counter - (Optional) Specifies the ACL counter. This is optional. The default is “disable”. The resource may be limited so that a counter cannot be turned on. Counters will be cleared when the function is disabled. **enable** - Specifies that the ACL counter option will be enabled. **disable** - Specifies that the ACL counter option will be disabled.
delete - Specifies to delete the specified flow_meter.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure a “two rate, three color” flow meter:

```
DAS-3626:admin#config flow_meter profile_id 1 access_id 1 tr_tcm cir 1000 cbs
2000 pir 2000 pbs 2000 color_blind conform permit counter enable exceed permit
replace_dscp 60 counter enable violate drop
Command: config flow_meter profile_id 1 access_id 1 tr_tcm cir 1000 cbs 2000
pir 2000 pbs 2000 color_blind conform permit counter enable exceed permit
replace_dscp 60 counter enable violate drop


Success.
DAS-3626:admin#
```

5-6 show flow_meter

Description

This command is used to display the flow-based metering (ACL Flow Metering) configuration.

Format

show flow_meter {[profile_id <value 1-8> | profile_name <name 1-32>] {access_id <value 1-256>}}

Parameters

profile_id - (Optional) Specifies the profile ID. **<value 1-8>** - Enter the profile ID used here. This value must be between 1 and 8.
profile_name - (Optional) Specifies the name of the profile. The maximum length is 32 characters. **<name 1-32>** - Enter the profile name used here.
access_id - (Optional) Specifies the access ID. **<value 1-256>** - Enter the access ID used here. This value must be between 1 and 256.

Restrictions

None.

Example

To display the flow metering configuration:

```
DAS-3626:admin# show flow_meter
Command: show flow_meter

Flow Meter Information
------------------------------------------------------------------------------
Profile ID:1     Aceess ID:1     Mode : trTCM / ColorBlind
CIR(Kbps):1000     CBS(Kbyte):2000     PIR(Kbps):2000     PBS(Kbyte):2000
Action:
      Conform : Permit                         Counter: Enabled
       Exceed : Permit     Replace DSCP: 60    Counter: Enabled
      Violate : Drop                           Counter: Disabled
------------------------------------------------------------------------------
Total Entries: 1

DAS-3626:admin#
```

5-7 config time_range

Description

This command is used to configure a specific range of time to activate a function on the switch by specifying which time range in a day and which days in a week are covered in the time range. Note that the specified time range is based on the SNTP time or the configured time. If this time is not available, the time range will not be met.

Format

config time_range <range_name 32> [hours start_time <time hh:mm:ss> end_time <time hh:mm:ss> weekdays <daylist> | delete]

Parameters

<range_name 32> - Enter the time range name used here. This name can be up to 32 characters long.
hours - Specifies the time of a day.
start_time - Specifies the starting time of a day.
<time hh:mm:ss> - Enter the starting time here. (24-hr time). For example, 19:00 means 7PM. 19 is also acceptable. The time specified in the start_time parameter must be smaller than the time specified in the end_time parameter.
end_time - Specifies the ending time of a day. (24-hr time)
<time hh:mm:ss> - Enter the ending time here. (24-hr time). For example, 19:00 means 7PM. 19 is also acceptable. The time specified in the start_time parameter must be smaller than the time specified in the end_time parameter.
weekdays - Specifies the list of days contained in the time range. Use a dash to define a period of days. Use a comma to separate specific days.
<daylist> - Enter the weekdays that will be included in this configuration here. For example, mon-fri (Monday to Friday). sun, mon, fri (Sunday, Monday and Friday)
delete - Specifies to delete a time range profile. When a time_range profile has been associated with ACL entries, deleting the time_range profile will fail.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure a time range named “1” that starts every Monday at 01:01:01am and ends at 02:02:02am:

```
DAS-3626:admin#config time_range 1 hours start_time 1:1:1 end_time 2:2:2
weekdays mon
Command: config time_range 1 hours start_time 1:1:1 end_time 2:2:2 weekdays mon

Success.

DAS-3626:admin#
```

5-8 show time_range

Description

This command is used to display the current time range settings.

Format

show time_range

Parameters

None.

Restrictions

None.

Example

To display the current time range settings:

```
DAS-3626:admin#show time_range
Command: show time_range

Time Range Information
------------------------
Range Name   :  1
Weekdays     :  Mon
Start Time   :  01:01:01
End Time     :  02:02:02

Total Entries :1

DAS-3626:admin#
```

5-9 show current_config access_profile

Description

This command is used to display the ACL part of the current configuration, when logged in with user level privileges.

The overall current configuration can be displayed by using the show config command, which is accessible with administrator level privileges.

Format

show current_config access_profile

Parameters

None.

Restrictions

None.

Example

To display the ACL part of the current configuration:

```
DAS-3626:admin# show current_config access_profile
Command: show current_config access_profile

#-----------------------------------------------------------------

# ACL

create access_profile ethernet vlan profile_id 1
config access_profile profile_id 1 add access_id 1 ethernet vlan default port 1
permit

create access_profile ip source_ip_mask 255.255.255.255 profile_id 2
config access_profile profile_id 2 add access_id 1 ip source_ip 10.10.10.10
port 2 deny



#-----------------------------------------------------------------

DAS-3626:admin#
```

Chapter 6 Address Resolution Protocol (ARP) Command List

create arpentry <ipaddr> <macaddr>
delete arpentry [<ipaddr> | all]
config arpentry <ipaddr> <macaddr>
config arp_aging time <minutes 0-65535>
clear arptable
show arpentry {ipif <ipif_name 12> | ipaddress <ipaddr> | static | mac_address <macaddr>}

6-1 create arpentry

Description

This command is used to enter a static ARP entry into the switch's ARP table.

Format

create arpentry <ipaddr> <macaddr>

Parameters

<ipaddr> - Enter the IP address of the end node or station.
<macaddr> - Enter the MAC address corresponding to the IP address above.

Restrictions

Only Administrators and Operators can issue this command.

Example

To create a static ARP entry for the IP address 10.48.74.121 and MAC address 00-50-BA-00-07-36:

```
DAS-3626:admin# create arpentry 10.48.74.121 00-50-BA-00-07-36
Command: create arpentry 10.48.74.121 00-50-BA-00-07-36

Success.

DAS-3626:admin#
```

6-2 delete arpentry

Description

This command is used to delete an ARP entry, by specifying either the IP address of the entry or all. Specifies 'all' clears the switch's ARP table.

Format

delete arpentry [<ipaddr> | all]

Parameters

<ipaddr> - Enter the IP address of the end node or station.
all - Specifies to delete all ARP entries.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete an entry of IP address 10.48.74.121 from the ARP table:

```
DAS-3626:admin# delete arpentry 10.48.74.121
Command: delete arpentry 10.48.74.121

Success.

DAS-3626:admin#
```

6-3 config arpentry

Description

This command is used to configure a static entry's MAC address in the ARP table. Specifies the IP address and MAC address of the entry.

Format

config arpentry <ipaddr> <macaddr>

Parameters

<ipaddr> - Enter the IP address of the end node or station.
<macaddr> - Enter the MAC address corresponding to the IP address above.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure a static ARP entry, whose IP address is 10.48.74.121, set its MAC address to 00-50-BA-00-07-37:

```
DAS-3626:admin# config arpentry 10.48.74.121 00-50-BA-00-07-37
Command: config arpentry 10.48.74.121 00-50-BA-00-07-37

Success.

DAS-3626:admin#
```

6-4 config arp_aging time

Description

This command is used to configure the maximum amount of time, in minutes, that a dynamic ARP entry can remain in the switch's ARP table, without being accessed, before it is dropped from the table.

Format

config arp_aging time <value 0-65535>

Parameters

<value 0-65535> - Enter the ARP age-out time in minutes. This value must be between 0 and 65535 minutes. The default is 20.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure ARP aging time to 30 minutes:

```
DAS-3626:admin# config arp_aging time 30
Command: config arp_aging time 30

Success.

DAS-3626:admin#
```

6-5 clear arptable

Description

This command is used to clear all the dynamic entries from ARP table.

Format

clear arptable

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To clear the ARP table:

```
DAS-3626:admin# clear arptable
Command: clear arptable

Success.

DAS-3626:admin#
```

6-6 show arpentry

Description

This command is used to display the ARP table. You can filter the display by IP address, MAC address, Interface name, or static entries.

Format

show arpentry {ipif <ipif_name 12> | ipaddress <ipaddr> | static}

Parameters

ipif - (Optional) Specifies the name of the IP interface the end node or station for which the ARP table entry was made, resides on. **<ipif_name 12>** - Enter the IP interface name here. This value can be up to 12 characters long.
ipaddress - (Optional) Specifies the IP address of the end node or station. **<ipaddr>** - Enter the IP address here.
static - (Optional) Specifies to display the static entries in the ARP table.

Restrictions

Only Administrators and Operators can issue this command.

Example

To display the ARP table:

```
DAS-3626:admin#  show arpentry
Command: show arpentry

ARP Aging Time : 20

Interface      IP Address       MAC Address        Type
-------------  ---------------  -----------------  ---------------
System         10.0.0.0         FF-FF-FF-FF-FF-FF  Local/Broadcast
System         10.1.1.1         00-02-03-04-05-06  Static
System         10.1.1.2         00-02-03-04-05-06  Dynamic
System         10.1.1.3         00-02-03-04-05-06  Static
System         10.90.90.90      00-01-02-03-04-00  Local
System         10.255.255.255   FF-FF-FF-FF-FF-FF  Local/Broadcast

Total Entries: 6

DAS-3626:admin#
```

Chapter 7 Asymmetric VLAN Command List

enable asymmetric_vlan
disable asymmetric_vlan
show asymmetric_vlan

7-1 enable asymmetric_vlan

Description

This command is used to enable the asymmetric VLAN function on the Switch.

Format

enable asymmetric_vlan

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable asymmetric VLANs:

```
DAS-3626:admin# enable asymmetric_vlan
Command: enable asymmetric_vlan

Success.

DAS-3626:admin#
```

7-2 disable asymmetric_vlan

Description

This command is used to disable the asymmetric VLAN function on the Switch.

Format

disable asymmetric_vlan

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable asymmetric VLANs:

```
DAS-3626:admin# disable asymmetric_vlan
Command: disable asymmetric_vlan

Success.

DAS-3626:admin#
```

7-3 show asymmetric_vlan

Description

This command is used to display the asymmetric VLAN state on the Switch.

Format

show asymmetric_vlan

Parameters

None.

Restrictions

None.

Example

To display the asymmetric VLAN state currently set on the Switch:

```
DAS-3626:admin# show asymmetric_vlan
Command: show asymmetric_vlan

Asymmetric VLAN: Enabled

DAS-3626:admin#
```

Chapter 8 BPDU Attack Protection Command List

config bpdu_protection bonding <bgroup_list> {state [enable | disable] | mode [drop | block | shutdown]}
config bpdu_protection ports [<portlist> | all] {state [enable | disable] | mode [drop | block | shutdown} (1)
config bpdu_protection recovery_timer [<sec 60-1000000> | infinite]
config bpdu_protection [trap | log] [none | attack_detected | attack_cleared | both]
enable bpdu_protection
disable bpdu_protection
show bpdu_protection {ports {<portlist>} | bonding <bgroup_list>}

8-1 config bpdu_protection bonding

Description

This command is used to configure the BPDP protection function for the VDSL bonding group on the Switch.

Format

config bpdu_protection bonding <bgroup_list> {state [enable | disable] | mode [drop | block | shutdown]}

Parameters

<bgroup_list> - Enter a list of VDSL bonding groups. The range is from 1 to 12.
state - Specifies the BPDU protection state. The default state is disable. **enable** - Specifies to enable BPDU protection. **disable** - Specifies to disable BPDU protection.
mode - Specifies the BPDU protection mode. The default mode is shutdown. **drop** - Specifies to drop all received BPDU packets when the bonding group enters under_attack state. **block** - Specifies to drop all packets (include BPDU and normal packets) when the bonding group enters under_attack state. **shutdown** - Specifies to shut down the bonding group when the bonding group enters under_attack state.

Restrictions

Only Administrators and Operators can issue this command.

Example

To set the admin state of BPDU protection function for the VDSL bonding group 2:

```
DAS-3626:admin#config bpdu_protection bonding 2 state enable
Command: config bpdu_protection bonding 2 state enable

Success.

DAS-3626:admin#
```

8-2 config bpdu_protection ports

Description

This command is used to configure the BPDP protection function for the ports on the Switch. In generally, there are two states in BPDU protection function. One is normal state, and another is under attack state. The under attack state have three modes: drop, block, and shutdown. A BPDU protection enabled port will enter under attack state when it receives one STP BPDU packet. And it will take action based on the configuration. Thus, BPDU protection can only be enabled on STP-disabled port.

BPDU protection has high priority than fbpdu setting configured by configure STP command in determination of BPDU handling. That is, when fbpbu is configured to forward STP BPDU but BPDU protection is enabled, then the port will not forward STP BPDU.

Format

config bpdu_protection ports [<portlist> | all] {state [enable | disable] | mode [drop | block | shutdown]}(1)

Parameters

<portlist> - Enter a range of ports to be configured.
all - Specifies that all the port will be configured.
state - Specifies the BPDU protection state. The default state is disable. **enable** - Specifies to enable BPDU protection. **disable** - Specifies to disable BPDU protection.
mode - Specifies the BPDU protection mode. The default mode is shutdown. **drop** - Specifies to drop all received BPDU packets when the port enters under_attack state. **block** - Specifies to drop all packets (include BPDU and normal packets) when the port enters under_attack state. **shutdown** - Specifies to shut down the port when the port enters under_attack state.

Restrictions

Only Administrators and Operators can issue this command.

Example

To set the port state enable and drop mode:

```
DAS-3626:admin# config bpdu_protection ports 1 state enable mode drop
Commands: config bpdu_protection ports 1 state enable mode drop

Success.

DAS-3626:admin#
```

8-3 config bpdu_protection recovery_interval

Description

This command is used to configure the auto-recovery timer. When a port enters the 'under attack' state, it can be disabled or blocked based on the configuration. To manually recover the port, the user needs to disable and re-enable the port.

Format

config bpdu_protection recovery_timer [<sec 60-1000000> | infinite]

Parameters

<sec 60 –1000000> - Enter the timer (in seconds) used by the Auto-Recovery mechanism to recover the port. The valid range is 60 to 1000000. The default value is 60.
infinite - Specifies the port will not be auto recovered.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the bpdu_protection recovery_timer to 120 seconds for the entire switch:

```
DAS-3626:admin# config bpdu_protection recovery_timer 120
Commands: config bpdu_protection recovery_timer 120

Success.

DAS-3626:admin#
```

8-4 config bpdu_protection

Description

This command is used to configure the BPDU protection trap or log state for the Switch.

Format

config bpdu_protection [trap | log] [none | attack_detected | attack_cleared | both]

Parameters

trap - Specifies the trap state.

log - Specifies the log state.
none - Specifies that neither attack_detected nor attack_cleared is trapped or logged.
attack_detected - Specifies that events will be logged or trapped when the BPDU attacks is detected.
attack_cleared - Specifies that events will be logged or trapped when the BPDU attacks is cleared.
both - Specifies that the events of attack_detected and attack_cleared shall be trapped or logged.

Restrictions

Only Administrators and Operators can issue this command.

Example

To config the BPDU protection trap state as both:

```
DAS-3626:admin# config bpdu_protection trap both
Commands: config bpdu_protection trap both

Success.

DAS-3626:admin#
```

8-5 enable bpdu_protection

Description

This command is used to enable BPDU protection function globally.

Format

enable bpdu_protection

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable BPDU protection function globally:

```
DAS-3626:admin# enable bpdu_protection
Commands: enable bpdu_protection

Success.

DAS-3626:admin#
```

8-6 disable bpdu_protection

Description

This command is used to disable BPDU protection function globally.

Format

disable bpdu_protection

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable BPDU protection function globally:

```
DAS-3626:admin# disable bpdu_protection
Commands: disable bpdu_protection

Success.

DAS-3626:admin#
```

8-7 show bpdu_protection

Description

This command is used to display BPDU protection global configuration or per port configuration and current status.

Format

show bpdu_protection {ports {<portlist>} | bonding <bgroup_list>}

Parameters

ports - (Optional) Specified a range of ports to be configured. **<portlist>** - (Optional) Enter the portlist here.
bonding - (Optional) Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.

Restrictions

None.

Example

To show the BPDU protection for the entire switch:

```
DAS-3626:admin#show bpdu_protection
Command: show bpdu_protection

 BPDU Protection Global Settings
 ---------------------------------------
 BPDU Protection Status         : Enabled
 BPDU Protection Recover Time   : 60 seconds
 BPDU Protection Trap Status    : None
 BPDU Protection Log Status     : Both


DAS-3626:admin#
```

To show the BPDU protection status ports 1-12:

```
DAS-3626:admin#show bpdu_protection ports 1-12
Command: show bpdu_protection ports 1-12

 Port  State        Mode       Status
------ -----------  ---------- ----------
 1     Enabled      Shutdown   Normal
 2     Enabled      Shutdown   Normal
 3     Enabled      Shutdown   Normal
 4     Enabled      Shutdown   Normal
 5     Enabled      Shutdown   Normal
 6     Enabled      Shutdown   Normal
 7     Enabled      Shutdown   Normal
 8     Enabled      Shutdown   Normal
 9     Enabled      Shutdown   Normal
 10    Enabled      Shutdown   Normal
 11    Enabled      Shutdown   Normal
 12    Enabled      Shutdown   Normal

DAS-3626:admin#
```

Chapter 9 Cable Diagnostics Command List

cable_diag ports [<GE_portlist> | all]

9-1 cable_diag ports

Description

This command is used to configure cable diagnostics on ports. For FE port, two pairs of cable will be diagnosed. For GE port, four pairs of cable will be diagnosed. The type of cable error can be open, short, or crosstalk.

Open means that the cable in the error pair does not have a connection at the specified position.

Short means that the cables in the error pair has a short problem at the specified position,

Crosstalk means that the cable in the error pair has a crosstalk problem at the specified position.

When a port is in link-up status, the test will obtain the distance of the cable. Since the status is link-up, the cable will not have the short or open problem. But the test may still detect the crosstalk problem.

When a port is in link-down status, the link-down may be caused by many factors.

1. When the port has a normal cable connection, but the remote partner is powered off, the cable diagnosis can still diagnose the health of the cable as if the remote partner is powered on.
2. When the port does not have any cable connection, the result of the test will indicate no cable.
3. The test will detect the type of error and the position where the error occurs.

Note that this test will consume a low number of packets. Since this test is for copper cable, the port with fiber cable will be skipped from the test. For combo port, the test will always be applied to the copper media only.

Format

cable_diag ports [<GE_portlist> | all]

Parameters

<GE_portlist> - Enter a list of ports used for the configuration here.
all - Specifies that all the ports will be used for this configuration.

Restrictions

Only Administrators and Operators can issue this command.

Example

To test the cable on port 25-26:

```
DAS-3626:admin#cable_diag ports 25-26
Command: cable_diag ports 25-26

Perform Cable Diagnostics ...

Port      Type      Link Status    Test Result                Cable Length (M)
------  ----------  -------------  -------------------------  -----------------
25      1000BASE-T  Link Down      No Cable                          -
26      1000BASE-T  Link Down      No Cable                          -


DAS-3626:admin#
```

Chapter 10 Configuration Command List

show config [current_config {<filter_expression>} | config_in_nvram <config_id 1-2> {<filter_expression>}] | information]
config configuration <config_id 1-2> [boot_up | active | delete]
save {[config <pathname 64> | log | all]}

10-1 show config

Description

This command is used to display the content of the current configuration, the configuration to be used in next boot, or the configuration file specified by the command.

Format

show config [current_config {<filter_expression>} | config_in_nvram <config_id 1-2> {<filter_expression>}] | information]

Parameters

current_config - Specifies to display the configurations entered without being saved in NVRAM. **<filter_expression>** - (Optional) Enter a filter string is enclosed by symbol ". Thus, the filter string itself cannot contain the " character. The filter string is case sensitive. This value can be up to 80 characters long.
config_in_nvram - Specifies to display the configurations entered and saved in NVRAM. **<config_id 1-2>** - Enter the configuration ID number. **<filter_expression>** - (Optional) Enter a filter string is enclosed by symbol ". Thus, the filter string itself cannot contain the " character. The filter string is case sensitive. This value can be up to 80 characters long.
information- Specifies to display the global information for the configuration settings.

Restrictions

Only Administrators can issue this command.

Example

The following example illustrates how the special filters 'modified' and .'effective' affect the configuration display:

```
DAS-3626:admin#show config information
Command: show config information

 ID          : 1(Boot up configuration)
 Version     : 0.03.B028
 Size        : 31130 Bytes
 Update Time: 2014/07/12 10:42:02
 From        : Local save
 User        : Guest(TELNET)
 Boot Up     : Yes


 ID          : 2
 Version     : 0.03.B028
 Size        : 49061 Bytes
 Update Time: 2013/08/13 17:06:44
 From        : Local save
 User        : Guest(Console)
 Boot Up     : No


Success.

DAS-3626:admin#
```

10-2 config configuration

Description

This command is used to select a configuration file as the next boot up configuration or to apply a specific configuration to the system. This command is required when multiple configuration files are supported.

Format

config configuration <config_id 1-2> [boot_up | active | delete]

Parameters

<config_id 1-2> - Enter a configuration ID.
boot_up - Specifies as a boot up file.
active - Specifies to apply the configuration.
delete - Specifies to remove the configuration file.

Restrictions

Only Administrators can issue this command.

Example

To configure the switch's configuration file as boot up:

```
DAS-3626:admin#config configuration 1 boot_up
Command: config configuration 1 boot_up

Success.

DAS-3626:admin#
```

10-3 save

Description

This command is used to save the current configuration to a file. This command is required to be supported regardless of whether file system is supported or whether multiple configuration files are supported. The configuration will only save to the master unit. For projects that support multiple configurations, the configuration ID or configuration file name can be specified. If the configuration ID or configuration file name is not specified, the next boot up configuration is implied.

Format

save {[config <config_id 1-2> | log | all]}

Parameters

config - Specifies to save the configuration to a file. **<config_id 1-2>** - (Optional) Enter a configuration ID here.
log - Specifies to save the log.
all - Specifies to save the configuration and the log.

Restrictions

Only Administrators and Operators can issue this command.

Example

To save the configuration:

```
DAS-3626:admin#save config c:/3120.cfg
Command: save config c:/3120.cfg

Saving all configurations to NV-RAM..... Done.

DAS-3626:admin#
```

Chapter 11 Connectivity Fault Management Command List

create cfm md <string 22> level <int 0-7>
config cfm md <string 22> {mip [none | auto | explicit] | sender_id [none | chassis | manage | chassis_manage]}
create cfm ma <string 22> md <string 22>
config cfm ma <string 22> md <string 22> {vlanid <vlanid 1-4094> | mip [none | auto | explicit | defer] | sender_id [none | chassis | manage | chassis_manage | defer] | ccm_interval [10ms | 100ms | 1sec | 10sec | 1min | 10min] | mepid_list [add | delete] <mepid_list>}
create cfm mep <string 32> mepid <int 1-8191> md <string 22> ma <string 22> direction [inward | outward] [port <port> | bonding_group < bgroup >]
config cfm mep [mepname <string 32> | mepid <int 1-8191> md <string 22> ma <string 22>] {state [enable | disable] | ccm [enable | disable] | pdu_priority <int 0-7> | fault_alarm [all | mac_status | remote_ccm | error_ccm | xcon_ccm | none] | alarm_time <centisecond 250 - 1000> | alarm_reset_time <centisecond 250-1000>}
delete cfm mep [mepname <string 32> | mepid <int 1-8191> md <string 22> ma <string 22>]
delete cfm ma <string 22> md <string 22>
delete cfm md <string 22>
enable cfm
disable cfm
config cfm [ports <portlist> | bonding < bgroup_list>] state [enable | disable]
show cfm ports <portlist>
show cfm bonding <bgroup_list>
show cfm {[md <string 22> {ma <string 22> {mepid <int 1-8191>}} | mepname <string 32>]}
show cfm fault {md <string 22> {ma <string 22>}}
show cfm port <port> {level <int 0-7> | direction [inward | outward] | vlanid <vlanid 1-4094>}
show cfm bonding_group <bgroup> {level <int 0-7> | direction [inward | outward] | vlanid <vlanid 1-4094>}
cfm loopback <macaddr> [mepname <string 32> | mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>]] {num <int 1-65535> | [length <int 0-1500> | pattern <string 1500>] | pdu_priority <int 0-7>}
show cfm loopback
cfm linktrace <macaddr> [mepname <string 32> | mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>]] {ttl <int 2-255> | pdu_priority <int 0-7>}
show cfm linktrace [mepname <string 32> | mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>]] {trans_id <uint>}
delete cfm linktrace {[md [<string 22> | md_index <uint 1-4294967295>] {ma [<string 22> | ma_index <uint 1-4294967295>] {mepid <int 1-8191>}} | mepname <string 32>]}
show cfm mipccm
show cfm remote_mep [mepname <string 32> | md <string 22> ma <string 22> mepid <int 1-8191>] remote_mepid <int 1-8191>
show cfm pkt_cnt {[[ports <portlist> | bonding < bgroup_list>] {[rx | tx]} | [rx | tx] | ccm]}
clear cfm pkt_cnt {[[ports <portlist> | bonding < bgroup_list>] {[rx | tx]} | [rx | tx] | ccm]}

11-1 create cfm md

Description

This command is used to create a maintenance domain.

Format

create cfm md <string 22> level <int 0-7>

Parameters

<string 22> - Enter the maintenance domain name here. This name can be up to 22 characters long.
level - Specifies the maintenance domain level. **<int 0-7>** - Enter the maintenance domain level here. This value must be between 0 and 7.

Restrictions

Only Administrators and Operators can issue this command.

Example

To create a maintenance domain called “op_domain” and assign a maintenance domain level of “2”:

```
DAS-3626:admin# create cfm md op_domain level 2
Command: create cfm md op_domain level 2

Success.

DAS-3626:admin#
```

11-2 config cfm md

Description

This command is used to configure the parameters of a maintenance domain. The creation of MIPs on an MA is useful to trace the link, MIP by MIP. It also allows the user to perform a loopback from an MEP to an MIP.

Format

config cfm md <string 22> {mip [none | auto | explicit] | sender_id [none | chassis | manage | chassis_manage]}

Parameters

<string 22> - Enter the maintenance domain name here. This name can be up to 22 characters long.
mip - (Optional) Specifies the control creations of MIPs. **none** - Specifies not to create MIPs. This is the default value. **auto** - Specifies that MIPs can always be created on any ports in this MD, if that port is not configured with an MEP of this MD. For the intermediate switch in an MA, the setting must be automatic in order for the MIPs to be created on this device. **explicit** - Specifies that MIPs can be created on any ports in this MD, only if the next existent lower level has an MEP configured on that port, and that port is not configured with an MEP of this MD.
sender_id - (Optional) Specifies the control transmission of the sender ID TLV. **none** - Specifies not to transmit the sender ID TLV. This is the default value.

chassis - Specifies to transmit the sender ID TLV with the chassis ID information.
manage - Specifies to transmit the sender ID TLV with the managed address information.
chassis_manage - Specifies to transmit sender ID TLV with chassis ID information and manage address information.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the maintenance domain called “op_domain” and specify the explicit option for creating MIPs:

```
DAS-3626:admin#config cfm md op_domain mip explicit
Command: config cfm md op_domain mip explicit

Success.

DAS-3626:admin#
```

11-3 create cfm ma

Description

This command is used to create a maintenance association. Different MAs in an MD must have different MA Names. Different MAs in different MDs may have the same MA Name.

Format

create cfm ma <string 22> md <string 22>

Parameters

<string 22> - Enter the maintenance association name here. This name can be up to 22 characters long.
md - Specifies the maintenance domain name.
<string 22> - Enter the maintenance domain name here. This name can be up to 22 characters long.

Restrictions

Only Administrators and Operators can issue this command.

Example

To create a maintenance association called “ma” and assign it to the maintenance domain “op_domain”:

```
DAS-3626:admin# create cfm ma op1 md op_domain
Command: create cfm ma op1 md op_domain

Success.

DAS-3626:admin#
```

11-4 config cfm ma

Description

This command is used to configure the parameters of a maintenance association. The MEP list specified for an MA can be located in different devices. MEPs must be created on the ports of these devices explicitly. An MEP will transmit a CCM packet periodically across the MA. The receiving MEP will verify these received CCM packets from the other MEPs against this MEP list for the configuration integrity check.

Format

config cfm ma <string 22> md <string 22> {vlanid <vlanid 1-4094> | mip [none | auto | explicit | defer] | sender_id [none | chassis | manage | chassis_manage | defer] | ccm_interval [10ms | 100ms | 1sec | 10sec | 1min | 10min] | mepid_list [add | delete] <mepid_list>}

Parameters

<string 22> - Enter the maintenance association name here. This name can be up to 22 characters long.
md - Specifies the maintenance domain name. **<string 22>** - Enter the maintenance domain name here. This name can be up to 22 characters long.
vlanid - (Optional) Specifies the VLAN Identifier. Different MAs must be associated with different VLANs. **<vlanid 1-4094>** - Enter the VLAN ID used here. This value must be between 1 and 4094.
mip - (Optional) Specifies the control creation of MIPs. **none** - Specifies not to create MIPs. **auto** - Specifies that MIPs can always be created on any ports in this MA, if that port is not configured with an MEP of that MA. **explicit** - Specifies that MIP can be created on any ports in this MA, only if the next existing lower level has an MEP configured on that port, and that port is not configured with an MEP of this MA. **defer** - Specifies to inherit the setting configured for the maintenance domain that this MA is associated with. This is the default value.
sender_id - (Optional) Specifies the control transmission of the sender ID TLV. **none** - Specifies not to transmit the sender ID TLV. This is the default value. **chassis** - Specifies to transmit the sender ID TLV with the chassis ID information. **manage** - Specifies to transmit the sender ID TLV with the manage address information. **chassis_manage** - Specifies to transmit the sender ID TLV with the chassis ID information and the manage address information. **defer** - Specifies to inherit the setting configured for the maintenance domain that this MA is associated with. This is the default value.
ccm_interval - (Optional) Specifies the CCM interval. **10ms** - Specifies that the CCM interval will be set to 10 milliseconds. Not recommended. **100ms** - Specifies that the CCM interval will be set to 100 milliseconds. Not recommended. **1sec** - Specifies that the CCM interval will be set to 1 second.

10sec - Specifies that the CCM interval will be set to 10 seconds. This is the default value. **1min** - Specifies that the CCM interval will be set to 1 minute. **10min** - Specifies that the CCM interval will be set to 10 minutes.
mepid_list - (Optional) Specifies the MEPIDs contained in the maintenance association. The range of the MEPID is 1-8191. **add** - Specifies to add MEPID(s). **delete** - Specifies to delete MEPID(s). By default, there is no MEPID in a newly created maintenance association. **<mepid_list>** - Enter the MEP ID list here.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure a CFM MA:

```
DAS-3626:admin# config cfm ma op1 md op_domain vlan 1 ccm_interval 1sec
Command: config cfm ma op1 md op_domain vlan 1 ccm_interval 1sec

Success.

DAS-3626:admin#
```

11-5 create cfm mep

Description

This command is used to create an MEP. Different MEPs in the same MA must have a different MEPID. MD name, MA name, and MEPID that together identify a MEP.

Different MEPs on the same device must have a different MEP name. Before creating an MEP, its MEPID should be configured in the MA's MEPID list.

Format

create cfm mep <string 32> mepid <int 1-8191> md <string 22> ma <string 22> direction [inward | outward] [port <port> | bonding_group < bgroup >]

Parameters

<string 32> - Enter the MEP name used here. It is unique among all MEPs configured on the device.This name can be up to 32 characters long.
mepid - Specifies the MEP ID. It should be configured in the MA's MEPID list. **<int 1-8191>** - Enter the MEP ID used here. This value must be between 1 and 8191.
md - Specifies the maintenance domain name. **<string 22>** - Enter the maintenance domain name used here. This name can be up to 22 characters long.
ma - Specifies the maintenance association name. **<string 22>** - Enter the maintenance association name used here. This name can be up to 22 characters long.
direction - Specifies the MEP direction. **inward** - Specifies the inward facing (up) MEP. **outward** - Specifies the outward facing (down) MEP.

port - Specifies the port number. This port should be a member of the MA's associated VLAN. **<port>** - Enter the port number used here.
bonding_group - Specifies a VDSL bonding group. **<bgroup>** - Enter a VDSL bonding group. The range is from 1 to 12.

Restrictions

Only Administrators and Operators can issue this command.

Example

To create a CFM MEP:

```
DAS-3626:admin# create cfm mep mep1 mepid 1 md op_domain ma op1 direction
inward port 2
Command: create cfm mep mep1 mepid 1 md op_domain ma op1 direction inward port
2


Success.


DAS-3626:admin#
```

11-6 config cfm mep

Description

This command is used to configure the parameters of an MEP.

An MEP may generate 5 types of Fault Alarms, as shown below by their priorities from high to low:

- Cross-connect CCM Received: priority 5
- Error CCM Received: priority 4
- Some Remote MEPs Down: priority 3
- Some Remote MEP MAC Status Errors: priority 2
- Some Remote MEP Defect Indications: priority 1

If multiple types of the fault occur on an MEP, only the fault with the highest priority will be alarmed.

Format

config cfm mep [mepname <string 32> | mepid <int 1-8191> md <string 22> ma <string 22>] {state [enable | disable] | ccm [enable | disable] | pdu_priority <int 0-7> | fault_alarm [all | mac_status | remote_ccm | error_ccm | xcon_ccm | none] | alarm_time <centisecond 250 - 1000> | alarm_reset_time <centisecond 250-1000>}

Parameters

mepname - Specifies the MEP name. **<string 32>** - Enter the MEP name used here. This name can be up to 32 characters long.
mepid - Specifies the MEP ID. **<int 1-8191>** - Enter the MEP ID used here. This value must be between 1 and 8191. **md** - Specifies the maintenance domain name. **<string 22>** - Enter the maintenance domain name used here. This name can be up to 22 characters long.

ma - Specifies the maintenance association name. **<string 22>** - Enter the maintenance association name used here. This name can be up to 22 characters long.
state - (Optional) Specifies the MEP administrative state. **enable** - Specifies that the MEP will be enabled. **disable** - Specifies that the MEP will be disabled. This is the default value.
ccm - (Optional) Specifies the CCM transmission state. **enable** - Specifies that the CCM transmission will be enabled. **disable** - Specifies that the CCM transmission will be disabled. This is the default value.
pdu_priority - (Optional) Specifies the 802.1p priority is set in the CCMs and the LTMs messages transmitted by the MEP. The default value is 7. **<int 0-7>** - Enter the PDU priority value here. This value must be between 0 and 7.
fault_alarm - (Optional) Specifies the control types of the fault alarms sent by the MEP. **all** - Specifies that All types of fault alarms will be sent. **mac_status** - Specifies that only the fault alarms whose priority is equal to or higher than "Some Remote MEP MAC Status Errors" are sent. **remote_ccm** - Specifies that only the fault alarms whose priority is equal to or higher than "Some Remote MEPs Down" are sent. **error_ccm** - Specifies that only the fault alarms whose priority is equal to or higher than "Error CCM Received" are sent. **xcon_ccm** - Specifies that only the fault alarms whose priority is equal to or higher than "Cross-connect CCM Received" are sent. **none** - Specifies that no fault alarm is sent. This is the default value.
alarm_time - (Optional) Specifies that a defect must exceed before the fault alarm can be sent. The unit is centisecond. The default value is 250. **<centisecond 250-1000>** - Enter the alarm time value here. This value must be between 250 and 1000 centiseconds.
alarm_reset_time - (Optional) Specifies the dormant duration time before a defect is triggered before the fault can be re-alarmed. The unit is centisecond, the range is 250-1000. The default value is 1000. **<centisecond 250-1000>** - Enter the alarm reset time value here. This value must be between 250 and 1000 centiseconds.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure a CFM MEP:

```
DAS-3626:admin# config cfm mep mepname mep1 state enable ccm enable
Command: config cfm mep mepname mep1 state enable ccm enable

Success.

DAS-3626:admin#
```

11-7 delete cfm mep

Description

This command is used to delete a previously created MEP.

Format

delete cfm mep [mepname <string 32> | mepid <int 1-8191> md <string 22> ma <string 22>]

Parameters

mepname - Specifies the MEP name. **<string 32>** - Enter the MEP name used here. This name can be up to 32 characters long.
mepid - Specifies the MEP ID. **<int 1-8191>** - Enter the MEP ID used here. This value must be between 1 and 8191. **md** - Specifies the maintenance domain name. **<string 22>** - Enter the maintenance domain name used here. This name can be up to 22 characters long. **ma** - Specifies the maintenance association name. **<string 22>** - Enter the maintenance association name used here. This name can be up to 22 characters long.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete a CFM MEP:

```
DAS-3626:admin# delete cfm mep mep1
Command: delete cfm mep mep1

Success.

DAS-3626:admin#
```

11-8 delete cfm ma

Description

This command is used to delete a created maintenance association. All MEPs created in the maintenance association will be deleted automatically.

Format

delete cfm ma <string 22> md <string 22>

Parameters

<string 22> - Enter the maintenance association name used here. This name can be up to 22 characters long.
md - Specifies the maintenance domain name. **<string 22>** - Enter the maintenance domain name used here. This name can be up to 22 characters long.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete a CFM MA:

```
DAS-3626:admin# delete cfm ma op1
Command: delete cfm ma op1

Success.

DAS-3626:admin#
```

11-9 delete cfm md

Description

This command is used to delete a previously created maintenance domain. All the MEPs and maintenance associations created in the maintenance domain will be deleted automatically.

Format

delete cfm md <string 22>

Parameters

<string 22> - Enter the maintenance domain name used here. This name can be up to 22 characters long.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete a CFM MD:

```
DAS-3626:admin# delete cfm domain op1
Command: delete cfm domain op1

Success.

DAS-3626:admin#
```

11-10 enable cfm

Description

This command is used to enable the CFM globally.

Format

enable cfm

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable the CFM globally:

```
DAS-3626:admin# enable cfm
Command: enable cfm

Success.

DAS-3626:admin#
```

11-11 disable cfm

Description

This command is used to disable the CFM globally.

Format

disable cfm

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable the CFM globally:

```
DAS-3626:admin# disable cfm
Command: disable cfm

Success.

DAS-3626:admin#
```

11-12 config cfm

Description

This command is used to enable or disable the CFM function on ports or bonding groups . By default, the CFM function is disabled.

If the CFM is disabled on a port:

1. MIPs are never created on that port.
2. MEPs can still be created on that port, and the configuration can be saved.
3. MEPs created on that port can never generate or process CFM PDUs. If the user issues a Loopback or Link trace test on those MEPs, it will prompt the user to inform them that the CFM function is disabled on that port.

Format

config cfm [ports <portlist> | bonding < bgroup_list>] state [enable | disable]

Parameters

ports - Specifies a list of ports to be configured. **<portlist>** - Enter the list of logical ports used for this configuration here.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
state - Specifies that the the CFM function will be enabled or disabled. **enable** - Specifies that the the CFM function will be enabled. **disable** - Specifies that the the CFM function will be disabled.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the CFM ports:

```
DAS-3626:admin#config cfm ports 3-6 state enable
Command: config cfm ports 3-6 state enable

Success.

DAS-3626:admin#
```

11-13 show cfm ports

Description

This command is used to show the CFM state of specified ports.

Format

show cfm ports <portlist>

Parameters

<portlist> - Enter the list of logical ports used for this configuration here.

Restrictions

None.

Example

To show the CFM ports:

```
DAS-3626:admin#show cfm ports 3-6
Command: show cfm ports 3-6

Port   State
-----  --------
3      Enabled
4      Enabled
5      Enabled
6      Enabled

DAS-3626:admin#
```

11-14 show cfm bonding

Description

This command is used to show the CFM state of specified bonding groups.

Format

show cfm bonding <bgroup_list>

Parameters

<bgroup_list> - Enter a list of VDSL bonding groups. The range is from 1 to 12.

Restrictions

None.

Example

To show the CFM state of bonding group 2:

```
DAS-3626:admin#show cfm bonding 2
Command: show cfm bonding 2

Port   State
-----  --------
b2     Enabled

DAS-3626:admin#
```

11-15 show cfm

Description

This command is used to show the CFM configuration.

Format

show cfm {[md <string 22> {ma <string 22> {mepid <int 1-8191>}} | mepname <string 32>]}

Parameters

md - (Optional) Specifies the maintenance domain name. **<string 22>** - Enter the maintenance domain name used here. This name can be up to 22 characters long. **ma** - (Optional) Specifies the maintenance association name. **<string 22>** - Enter the maintenance association name used here. This name can be up to 22 characters long. **mepid** - (Optional) Specifies the MEP ID. **<int 1-8191>** - Enter the MEP ID used here. This value must be between 1 and 8191.
mepname - (Optional) Specifies the MEP name. **<string 32>** - Enter the MEP name used here. This name can be up to 32 characters long.

Restrictions

None.

Example

To show the CFM configuration:

```
DAS-3626:admin#show cfm
Command: show cfm

CFM State: Enabled

MD Index    MD Name                 Level
----------  ----------------------  -----
1           op_domain               2

DAS-3626:admin#show cfm md op_domain
Command: show cfm md op_domain

MD Index    : 1
MD Name     : op_domain
MD Level    : 2
MIP Creation: Explicit
SenderID TLV: None

MA Index    MA Name                 VID
----------  ----------------------  ----
1           op1                     1

DAS-3626:admin#show cfm md op_domain ma op1
Command: show cfm md op_domain ma op1

MA Index    : 1
MA Name     : op1
MA VID      : 1
MIP Creation: Defer
CCM Interval: 1 second
SenderID TLV: Defer
MEPID List  :

MEPID  Direction  Port   Name         MAC Address
-----  ---------  -----  -----------  -----------------

DAS-3626:admin# show cfm mepname mep1
Command: show cfm mepname mep1

Name                : mep1
MEPID               : 1
Port                : 1
Direction           : inward
CFM Port State      : enabled
MAC Address         : XX-XX-XX-XX-XX-XX
MEP State           : enabled
CCM State           : enabled
PDU Priority        : 7
Fault Alarm         : mac_status
Alarm Time          : 2 second(s)
Alarm Reset Time    : 10 second(s)
Highest Fault       : Some Remote MEP Down
```

```
Out-of-Sequence CCMs: 0 received
Cross-connect CCMs  : 0 received
Error CCMs          : 0 received
Port Status CCMs    : 0 received
If Status CCMs      : 0 received
CCMs transmitted    : 1234
In-order LBRs       : 0 received
Out-of-order LBRs   : 0 received
Next LTM Trans ID   : 27
Unexpected LTRs     : 0 received
LBMs Transmitted    : 0

Remote
MEPID  MAC Address Status RDI PortSt IfSt    Detect Time
------ ----------- ------ --- ------- -------- -------------------
2      XX-..-XX-XX OK     Yes Blocked Up       2008-01-01 12:00:00
3      XX-..-XX-XX IDLE   No  No      No       2008-01-01 12:00:00
4      XX-..-XX-XX OK     No  Up      Down     2008-01-01 12:00:00
8      XX-..-XX-XX START  No  Up      Up       2008-01-01 12:00:00
12     XX-..-XX-XX FAILED No  Up      Up       2008-01-01 12:00:00
8      XX-..-XX-XX OK     No  Up      Up       2008-01-01 12:00:00

DAS-3626:admin#
```

11-16 show cfm fault

Description

This command is used to display all the fault conditions detected by the MEPs contained in the specified MA or MD. This display provides the overview of the fault status by MEPs.

Format

show cfm fault {md <string 22> {ma <string 22>}}

Parameters

md - (Optional) Specifies the maintenance domain name.
- **<string 22>** - Enter the maintenance domain name used here. This name can be up to 22 characters long.
- **ma** - (Optional) Specifies the maintenance association name.
  - **<string 22>** - Enter the maintenance association name used here. This name can be up to 22 characters long.

Restrictions

None.

Example

To show the CFM faults:

```
DAS-3626:admin# show cfm fault
Command: show cfm fault

MD Name     MA Name     MEPID  Status                AIS Status   LCK Status
----------- ----------- ----- ---------------------- ------------ ------------
op_domain   op1         1        Cross-connect CCM Received

DAS-3626:admin#
```

11-17 show cfm port

Description

This command is used to show MEPs and MIPs created on a port.

Format

show cfm port <port> {level <int 0-7> | direction [inward | outward] | vlanid <vlanid 1-4094>}

Parameters

<port> - Enter the port number used here.
level - (Optional) Specifies the MD Level. If not specified, all levels are shown. **<int 0-7>** - Enter the MD level value here. This value must be between 0 and 7.
direction - (Optional) Specifies the MEP direction. If not specified, both directions and the MIP are shown. **inward** - Specifies that the MEP direction will be inward facing. **outward** - Specifies that the MEP direction will be outward facing.
vlanid - (Optional) Specifies the VLAN identifier. If not specified, all VLANs are shown. **<vlanid 1-4094>** - Enter the VLAN ID used here. This value must be between 1 and 4094.

Restrictions

None.

Example

To show the MEPs and MIPs created on a port:

```
DAS-3626:admin#show cfm port 5
Command: show cfm port 5

MAC Address: D8-FE-E3-93-05-C5
MD Name      MA Name      MEPID  Level  Direction  VID
-----------  -----------  -----  -----  ---------  ----
op_domain    op1          1      2      inward     2
cust_domain  cust1        8      4      inward     2
serv_domain  serv2        MIP    3                 2

DAS-3626:admin#
```

11-18 show cfm bonding_group

Description

This command is used to show MEPs and MIPs created on a bonding group.

Format

show cfm bonding_group <bgroup> {level <int 0-7> | direction [inward | outward] | vlanid <vlanid 1-4094>}

Parameters

<bgroup> - Enter a VDSL bonding group. The range is from 1 to 12.
level - (Optional) Specifies the MD Level. If not specified, all levels are shown. **<int 0-7>** - Enter the MD level value here. This value must be between 0 and 7.
direction - (Optional) Specifies the MEP direction. If not specified, both directions and the MIP are shown. **inward** - Specifies that the MEP direction will be inward facing. **outward** - Specifies that the MEP direction will be outward facing.
vlanid - (Optional) Specifies the VLAN identifier. If not specified, all VLANs are shown. **<vlanid 1-4094>** - Enter the VLAN ID used here. This value must be between 1 and 4094.

Restrictions

None.

Example

To show the MEPs and MIPs created on a port:

```
DAS-3626:admin#show cfm bonding_group 2
Command: show cfm bonding_group 2

MAC Address: D8-FE-E3-93-05-C3
MD Name      MA Name      MEPID  Level  Direction  VID
-----------  -----------  -----  -----  ---------  ----
md1          ma2          2      7      In         1

DAS-3626:admin#
```

11-19 cfm loopback

Description

This command is used to start a CFM loopback test. You can press Ctrl+C to exit the loopback test. The MAC address represents the destination MEP or MIP that can be reached by this MAC address. The MEP represents the source MEP to initiate the loopback message.

Format

cfm loopback <macaddr> [mepname <string 32> | mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>]] {num <int 1-65535> | [length <int 0-1500> | pattern <string 1500>] | pdu_priority <int 0-7>}

Parameters

<macaddr> - Enter the destination MAC address here.
mepname - (Optional) Specifies the MEP name used. **<string 32>** - Enter the MEP name used here. This name can be up to 32 characters long.
mepid - (Optional) Specifies the MEP ID used. **<int 1-8191>** - Enter the MEP ID used here. This value must be between 1 and 8191.
md - (Optional) Specifies the maintenance domain name. **<string 22>** - Enter the maintenance domain name her. This name can be up to 22 characters long.
md_index - (Optional) Specifies the maintenance domain index. **<uint 1-4294967295>** - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.
ma - (Optional) Specifies the maintenance association name. **<string 22>** - Enter the maintenance association name her. This name can be up to 22 characters long.
ma_index - (Optional) Specifies the maintenance association index. **<uint 1-4294967295>** - Enter the maintenance association index value here. This value must be between 1 and 4294967295.
num - (Optional) Specifies number of LBMs to be sent. The default value is 4. **<int 1-65535>** - Enter the number of LBMs to be sent here. This value must be between 1 and 65535.
length - (Optional) Specifies the payload length of the LBM to be sent. The default is 0. **<int 0-1500>** - Enter the payload length here. This value must be between 0 and 1500.
pattern - (Optional) Specifies an arbitrary amount of data to be included in a Data TLV, along with an indication whether the Data TLV is to be included. **<string 1500>** - Enter the pattern used here. This value can be up to 1500 characters long.
pdu_priority - (Optional) Specifies the 802.1p priority to be set in the transmitted LBMs. If not specified, it uses the same priority as CCMs and LTMs sent by the MA. **<int 0-7>** - Enter the PDU priority value here. This value must be between 0 and 7.

Restrictions

Only Administrators and Operators can issue this command.

Example

To transmit a LBM:

```
DAS-3626:admin# cfm loopback 00-01-02-03-04-05 mep mep1
Command: cfm loopback 00-01-02-03-04-05 mep mep1

Request timed out.
Request timed out.
Reply from MPID 52: bytes=xxx time=xxxms
Request timed out.

CFM loopback statistics for 00-01-02-03-04-05:
    Packets: Sent=4, Received=1, Lost=3(75% loss).

DAS-3626:admin#
```

11-20 show cfm loopback

Description

This command is used to display the CFM loopback state.

Format

show cfm loopback

Parameters

None.

Restrictions

None.

Example

To show the CFM loopback state:

```
DAS-3626:admin#show cfm loopback
Command: show cfm loopback

CFM Loopback State: Enabled

DAS-3626:admin#
```

11-21 cfm linktrace

Description

This command is used to issue a CFM link track message.

Format

cfm linktrace <macaddr> [mepname <string 32> | mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>]] {ttl <int 2-255> | pdu_priority <int 0-7>}

Parameters

<macaddr> - Specifies the destination MAC address.
mepname - (Optional) Specifies the MEP name used. **<string 32>** - Enter the MEP name used here. This name can be up to 32 characters long.
mepid - (Optional) Specifies the MEP ID used. **<int 1-8191>** - Enter the MEP ID used here. This value must be between 1 and 8191.
md - (Optional) Specifies the maintenance domain name. **<string 22>** - Enter the maintenance domain name her. This name can be up to 22 characters long.
md_index - (Optional) Specifies the maintenance domain index. **<uint 1-4294967295>** - Enter the maintenance domain index value here. This value can be

between 1 and 4294967295.
ma - (Optional) Specifies the maintenance association name. **<string 22>** - Enter the maintenance association name her. This name can be up to 22 characters long.
ma_index - (Optional) Specifies the maintenance association index. **<uint 1-4294967295>** - Enter the maintenance association index value here. This value can be between 1 and 4294967295.
ttl - (Optional) Specifies the link trace message TTL value. The default value is 64. **<int 2-255>** - Enter the link trace message TTL value here. This value must be between 2 and 255.
pdu_priority - (Optional) Specifies the 802.1p priority to be set in the transmitted LTM. If not specified, it uses the same priority as CCMs sent by the MA. **<int 0-7>** - Enter the PDU priority value here. This value must be between 0 and 7.

Restrictions

Only Administrators and Operators can issue this command.

Example

To transmit an LTM:

```
DAS-3626:admin# cfm linktrace 00-01-02-03-04-05 mep mep1
Command: cfm linktrace 00-01-02-03-04-05 mep mep1

Transaction ID: 26
Success.

DAS-3626:admin#
```

11-22 show cfm linktrace

Description

This command is used to show the link trace responses. The maximum link trace responses a device can hold is 128.

Format

show cfm linktrace [mepname <string 32> | mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>]] {trans_id <uint>}

Parameters

mepname - (Optional) Specifies the MEP name used. **<string 32>** - Enter the MEP name used here. This name can be up to 32 characters long.
mepid - (Optional) Specifies the MEP ID used. **<int 1-8191>** - Enter the MEP ID used here. This value must be between 1 and 8191.
md - (Optional) Specifies the maintenance domain name. **<string 22>** - Enter the maintenance domain name her. This name can be up to 22 characters long.
md_index - (Optional) Specifies the maintenance domain index. **<uint 1-4294967295>** - Enter the maintenance domain index value here. This value must between 1 and 4294967295.
ma - (Optional) Specifies the maintenance association name.

<string 22> - Enter the maintenance association name her. This name can be up to 22 characters long.
ma_index - (Optional) Specifies the maintenance association index. **<uint 1-4294967295>** - Enter the maintenance association index value here. This value must between 1 and 4294967295.
trans_id - (Optional) Specifies the identifier of the transaction displayed. **<uint>** - Enter the transaction ID used here.

Restrictions

None.

Example

To show the link trace reply when the "all MPs reply LTRs" function is enabled:

```
DAS-3626:admin# show cfm linktrace mep mepname mep1 trans_id 26
Command: show cfm linktrace mep mepname mep1 trans_id 26

Transaction ID: 26
From MEP mep1 to 00-11-22-33-44-55
Start Time 2008-01-01 12:00:00


Hop  MEPID  MAC Address        Forwarded  Relay Action
---  -----  -----------------  ---------  ------------
1           00-22-33-44-55-66  Yes        FDB
2           00-33-44-55-66-77  Yes        MPDB
3           00-11-22-33-44-55  No         Hit

DAS-3626:admin#
```

To show the link trace reply when the "all MPs reply LTRs" function is disabled:

```
DAS-3626:admin# show cfm linktrace mep mep1 trans_id 26
Command: show cfm linktrace mep mep1 trans_id 26

Transaction ID: 26
From MEP mep1 to 00-11-22-33-44-55
Start Time 2008-01-01 12:00:00


Hop  MEPID  Ingress MAC Address  Egress MAC Address   Forwarded  Relay Action
---  -----  ------------------  ------------------  ---------  ------------
1    -      00-22-33-44-55-66   00-22-33-44-55-67   Yes        FDB
2    -      00-33-44-55-66-77   00-33-44-55-66-78   Yes        MPDB
3    X      00-44-55-66-77-88   00-11-22-33-44-55   No         Hit

DAS-3626:admin#
```

11-23 delete cfm linktrace

Description

This command is used to delete the stored link trace response data that have been initiated by the specified MEP.

Format

delete cfm linktrace {[md [<string 22> | md_index <uint 1-4294967295>] {ma [<string 22> | ma_index <uint 1-4294967295>] {mepid <int 1-8191>}} | mepname <string 32>]}

Parameters

md - (Optional) Specifies the maintenance domain name. **<string 22>** - Enter the maintenance domain name her. This name can be up to 22 characters long.
md_index - (Optional) Specifies the maintenance domain index. **<uint 1-4294967295>** - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.
ma - (Optional) Specifies the maintenance association name. **<string 22>** - Enter the maintenance association name her. This name can be up to 22 characters long.
ma_index - (Optional) Specifies the maintenance association index. **<uint 1-4294967295>** - Enter the maintenance association index value here. This value must be between 1 and 4294967295.
mepid - (Optional) Specifies the MEP ID used. **<int 1-8191>** - Enter the MEP ID used here. This value must be between 1 and 8191.
mepname - (Optional) Specifies the MEP name used. **<string 32>** - Enter the MEP name used here. This name can be up to 32 characters long.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete the CFM link trace reply:

```
DAS-3626:admin# delete cfm linktrace mep mep1
Command: delete cfm linktrace mep mep1

Success.

DAS-3626:admin#
```

11-24 show cfm mipccm

Description

This command is used to show the MIP CCM database entries. All entries in the MIP CCM database will be shown. A MIP CCM entry is similar to a FDB which keeps the forwarding port information of a MAC entry.

Format

show cfm mipccm

Parameters

None.

Restrictions

None.

Example

To show MIP CCM database entries:

```
DAS-3626:admin#show cfm mipccm
Command: show cfm mipccm

MA                      VID   MAC Address        Port
----------------------  ----  -----------------  -----
opma                    1     xx-xx-xx-xx-xx-xx  2
opma                    1     xx-xx-xx-xx-xx-xx  3

Total: 2

DAS-3626:admin#
```

11-25 show cfm remote_mep

Description

This command is used to show remote MEPs.

Format

show cfm remote_mep [mepname <string 32> | md <string 22> ma <string 22> mepid <int 1-8191>] remote_mepid <int 1-8191>

Parameters

mepname - Specifies the MEP name used. **<string 32>** - Enter the MEP name used here. This name can be up to 32 characters long.
md - Specifies the maintenance domain name. **<string 22>** - Enter the maintenance domain name her. This name can be up to 22 characters long. **ma** - Specifies the maintenance association name. **<string 22>** - Enter the maintenance association name her. This name can be up to 22 characters long. **mepid** - Specifies the MEP ID used. **<int 1-8191>** - Enter the MEP ID used here. This value must be between 1 and 8191.
remote_mepid - Specifies the Remote MEP ID used. **<int 1-8191>** - Enter the remote MEP ID used here. This value must be between 1 and 8191.

Restrictions

None.

Example

To show the CFM Remote MEP information:

```
DAS-3626:admin# show cfm remote_mep mepname mep1 remote_mepid 2
Command: show cfm remote_mep mepname mep1 remote_mepid 2

Remote MEPID             : 2
MAC Address              : 00-11-22-33-44-02
Status                   : OK
RDI                      : Yes
Port State               : Blocked
Interface Status         : Down
Last CCM Serial Number   : 1000
Sender Chassis ID        : 00-11-22-33-44-00
Sender Management Address: SNMP-UDP-IPv4 10.90.90.90:161
Detect Time              : 2008-01-01 12:00:00

DAS-3626:admin#
```

11-26 show cfm pkt_cnt

Description

This command is used to show the CFM packet's RX/TX counters.

Format

show cfm pkt_cnt {[[ports <portlist> | bonding < bgroup_list>] {[rx | tx]} | [rx | tx] | ccm]}

Parameters

ports - (Optional) Specifies the port counters to show. If not specified, all ports will be shown. **<portlist>** - Enter the list of ports used for this configuration here.
bonding - (Optional) Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
rx - (Optional) Specifies to display the RX counter.
tx - (Optional) Specifies to display the TX counter.
rx - (Optional) Specifies to display the RX counter.
tx - (Optional) Specifies to display the TX counter.
ccm - (Optional) Specifies the CCM RX counters.

Restrictions

None.

Example

To show the CFM packet's RX/TX counters:

```
DAS-3626:admin#show cfm pkt_cnt
Command: show cfm pkt_cnt

CFM RX Statistics
-------------------------------------------------------------------------------
Port  AllPkt   CCM      LBR      LBM      LTR      LTM      VidDrop  OpcoDrop
----- -------- -------- -------- -------- -------- -------- -------- --------
all   204      204      0        0        0        0        0        0
1     0        0        0        0        0        0        0        0
2     204      204      0        0        0        0        0        0
3     0        0        0        0        0        0        0        0
4     0        0        0        0        0        0        0        0
5     0        0        0        0        0        0        0        0
6     0        0        0        0        0        0        0        0
7     0        0        0        0        0        0        0        0
8     0        0        0        0        0        0        0        0
9     0        0        0        0        0        0        0        0
10    0        0        0        0        0        0        0        0
11    0        0        0        0        0        0        0        0
12    0        0        0        0        0        0        0        0

CFM TX Statistics
-----------------------------------------------------------
Port  AllPkt   CCM      LBR      LBM      LTR      LTM
----- -------- -------- -------- -------- -------- --------
all   3988     3984     0        0        0        4
1     0        0        0        0        0        0
2     204      204      0        0        0        4
3     578      578      0        0        0        0
4     578      578      0        0        0        0
5     578      578      0        0        0        0
6     578      578      0        0        0        0
7     578      578      0        0        0        0
8     578      578      0        0        0        0
9     578      578      0        0        0        0
10    578      578      0        0        0        0
11    578      578      0        0        0        0
12    578      578      0        0        0        0

DAS-3626:admin#
```

11-27 clear cfm pkt_cnt

Description

This command is used to clear the CFM packet's RX/TX counters.

Format

clear cfm pkt_cnt {[ports <portlist> | bonding < bgroup_list>] {[rx | tx]} | [rx | tx] | ccm]}

Parameters

ports - (Optional) Specifies the ports which require need the counters clearing. If not specified, all ports will be cleared. **<portlist>** - Enter the list of ports used for this configuration here.
bonding - (Optional) Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
rx - (Optional) Specifies to clear the RX counter.
tx - (Optional) Specifies to clear the TX counter.
rx - (Optional) Specifies to clear the RX counter.
tx - (Optional) Specifies to clear the TX counter. If not specified, both of them will be cleared.
ccm - (Optional) Specifies the CCM RX counters.

Restrictions

Only Administrators and Operators can issue this command.

Example

To clear the CFM packet's RX/TX counters:

```
DAS-3626:admin# clear cfm pkt_cnt
Command: clear cfm pkt_cnt

Success.

DGS-3120-24TC: clear cfm pkt_cnt ccm
Command: show cfm pkt_cnt ccm

Success.

DAS-3626:admin#
```

Chapter 12 Debug Software Command List

debug address_binding [event | dhcp | all] state [enable | disable]
no debug address_binding

12-1 debug address_binding

Description

This command is used to start the IMPB debug when the IMPB module receives an ARP/IP packet or a DHCP packet.

Format

debug address_binding [event | dhcp | all] state [enable | disable]

Parameters

event - Specifies to print out the debug messages when IMPB module receives ARP/IP packets.
dhcp - Specifies to print out the debug messages when the IMPB module receives the DHCP packets.
all - Specifies to print out all debug messages.
state - Specifies to configure the IMPB debug state to be enabled or disabled. **enable** - Specifies that the state will be enabled. **disable** - Specifies that the state will be disabled.

Restrictions

Only Administrators can issue this command.

Example

To print out all debug IMPB messages:

```
DAS-3626:admin# debug address_binding all state enable
Command: debug address_binding all state enable

Success.

DAS-3626:admin#
```

12-2 no debug address_binding

Description

This command is used to stop the IMPB debug starting when the IMPB module receives an ARP/IP packet or a DHCP packet.

Format

no debug address_binding

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To stop IMPB debug: starting when the IMPB module receives an ARP/IP or DHCP packet:

```
DAS-3626:admin# no debug address_binding
Command: no debug address_binding

Success.

DAS-3626:admin#
```

Chapter 13 DHCP Relay Command List

config dhcp_relay {hops <int 1-16> | time <sec 0-65535>}
config dhcp_relay add ipif <ipif_name 12> <ipaddr>
config dhcp_relay add vlanid <vlan_id_list> <ipaddr>
config dhcp_relay delete ipif <ipif_name 12> <ipaddr>
config dhcp_relay delete vlanid <vlan_id_list> <ipaddr>
config dhcp_relay option_82 {state [enable | disable] | check [enable | disable] | policy [replace | drop | keep] | remote_id [default | user_define <desc 32>]}
enable dhcp_relay
disable dhcp_relay
show dhcp_relay {ipif <ipif_name 12>}

13-1 config dhcp_relay

Description

This command is used to configure the DHCP relay feature of the switch.

Format

config dhcp_relay {hops <int 1-16> | time <sec 0-65535>}

Parameters

hops - (Optional) Specifies the maximum number of relay hops that the DHCP/BOOTP packets can cross. The range is 1 to 16. The default value is 4. The DHCP packet will be dropped when the relay hop count in the received packet is equal to or greater than this setting. **<int 1-16>** - Enter the maximum number of relay hops here. This value must be between 1 and 16.
time - (Optional) Specifies the relay time. The time field in the DHCP packet must be equal to or greater than this setting to be relayed by the router. The default value is 0. **<sec 0-65535>** - Enter the relay time here. This value must be between 0 and 65535 seconds.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the DHCP relay hops and time parameters:

```
DAS-3626:admin# config dhcp_relay hops 4 time 2
Command: config dhcp_relay hops 4 time 2

Success.

DAS-3626:admin#
```

13-2 config dhcp_relay add ipif

Description

This command is used to configure add an IP destination address to the switch's DHCP relay table. Used to configure a DHCP server for relay of packets.

Format

config dhcp_relay add ipif <ipif_name 12> <ipaddr>

Parameters

<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.
<ipaddr> - Enter the DHCP/BOOTP server IP address.

Restrictions

Only Administrators and Operators can issue this command.

Example

To add a DHCP/BOOTP server to the relay table:

```
DAS-3626:admin# config dhcp_relay add ipif System 10.43.21.12
Command: config dhcp_relay add ipif System 10.43.21.12

Success.

DAS-3626:admin#
```

13-3 config dhcp_relay add vlanid

Description

This command is used to add an IP address as a destination to forward (relay) DHCP/BOOTP packets. If there is an IP interface in the VLAN and it has configured a DHCP server at the interface level, then the configuration at the interface level has higher priority. In this case, the DHCP server configured on the VLAN will not be used to forward the DHCP packets.

Format

config dhcp_relay add vlanid <vlan_id_list> <ipaddr>

Parameters

<vlan_id_list> - Enter the VLAN ID list used for this configuration here.
<ipaddr> - Enter the DHCP/BOOTP server IP address used here.

Restrictions

Only Administrators and Operators can issue this command.

Example

To add a DHCP/BOOTP server 10.43.21.12 to VLAN 1 to 10:

```
DAS-3626:admin# config dhcp_relay add vlanid 1-10 10.43.21.12
Command: config dhcp_relay add vlanid 1-10 10.43.21.12

Success.

DAS-3626:admin#
```

13-4 config dhcp_relay delete ipif

Description

This command is used to delete one of the IP destination addresses in the swith's relay table.

Format

config dhcp_relay delete ipif <ipif_name 12> <ipaddr>

Parameters

<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.
<ipaddr> - Enter the DHCP/BOOTP server IP address.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete a DHCP/BOOTP server to the relay table:

```
DAS-3626:admin# config dhcp_relay delete ipif System 10.43.21.12
Command: config dhcp_relay delete ipif System 10.43.21.12

Success.

DAS-3626:admin#
```

13-5 config dhcp_relay delete vlanid

Description

This command deletes an IP address as a destination to forward (relay) DHCP/BOOTP packets. If there is an IP interface in the VLAN and it has configured a DHCP server at the interface level, then the configuration at the interface level has higher priority. In this case, the DHCP server configured on the VLAN will not be used to forward the DHCP packets.

Format

config dhcp_relay delete vlanid <vlan_id_list> <ipaddr>

Parameters

<vlan_id_list> - Enter the VLAN ID list used for this configuration here.
<ipaddr> - Enter the DHCP/BOOTP server IP address used here.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete a DHCP/BOOTP server 10.43.21.12 from VLAN 2 and VLAN 3:

```
DAS-3626:admin# config dhcp_relay delete vlanid 2-3 10.43.21.12
Command: config dhcp_relay delete vlanid 2-3 10.43.21.12

Success.

DAS-3626:admin#
```

13-6 config dhcp_relay option_82

Description

This command is used to configure the processing of DHCP 82 option for the DHCP relay function.

Format

config dhcp_relay option_82 {state [enable | disable] | check [enable | disable] | policy [replace | drop | keep] | remote_id [default | user_define <desc 32>]}

Parameters

state - (Optional) Specifies to enable or disable the processing of DHCP 82 option for the DHCP relay function. The default setting is disabled. **enable** - Specifies that the option 82 processing will be enabled. When the state is enabled, the DHCP packet will be inserted with the option 82 field before being relayed to server. The DHCP packet will be processed based on the behaviour defined in check and policy setting. **disable** - Specifies that the option 82 processing will be disabled. When the state is disabled, the DHCP packet will be relayed directly to server without further check and processing on the packet.
check - (Optional) Specifies to enable or disable the checking. When the state is enabled, For packet come from client side, the packet should not have the option 82's field. If the packet has this option field, it will be dropped. The default setting is disabled. **enable** - Specifies that checking will be enabled. **disable** - Specifies that checking will be disabled.
policy - (Optional) Specifies the policy used. This option takes effect only when the check status is disabled. The default setting is set to 'replace'. **replace** - Replace the exiting option 82 field in the packet. The Switch will use it's own Option

82 value to replace the old Option 82 value in the packet. **drop** - Specifies to discard if the packet has the option 82 field. If the packet, that comes from the client side, contains and Option 82 value, then the packet will be dropped. If the packet, that comes from the client side doesn't contain an Option 82 value, then insert it's own Option 82 value into the packet. **keep** - Specifies to retain the existing option 82 field in the packet. If the packet, that comes from the client side, contains and Option 82 value, then keep the old Option 82 value. If the packet, that comes from the client side, doesn't contain an Option 82 value, then insert it's own Option 82 value into the packet.
remote_id - (Optional) Specifies the content in Remote ID suboption. **default** - Specifies to use switch's system MAC address as remote ID. **user_define** - Specifies to use user-defined string as remote ID. The space character is allowed in the string. **<desc 32>** - Enter the user defined description here. This value can be up to 32 characters long.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure dhcp_relay option 82:

```
DAS-3626:admin# config dhcp_relay option_82 state enable
Command: config dhcp_relay option_82 state enable

Success.

DAS-3626:admin# config dhcp_relay option_82 check disable
Command: config dhcp_relay option_82 check disable

Success.

DAS-3626:admin# config dhcp_relay option_82 policy replace
Command: config dhcp_relay option_82 policy replace

Success.

DAS-3626:admin# config dhcp_relay option_82 remote_id user_define “D-Link L2
Switch”
Command: config dhcp_relay option_82 remote_id user_define "D-Link L2 Switch"

Success.

DAS-3626:admin#
```

13-7 enable dhcp_relay

Description

This command is used to enable the DHCP relay function on the switch.

Format

enable dhcp_relay

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable the DHCP relay function.

```
DAS-3626:admin# enable dhcp_relay
Command: enable dhcp_relay

Success.

DAS-3626:admin#
```

13-8 disable dhcp_relay

Description

This command is used to disable the DHCP relay function on the switch.

Format

disable dhcp_relay

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable the DHCP relay function:

```
DAS-3626:admin# disable dhcp_relay
Command: disable dhcp_relay

Success.

DAS-3626:admin#
```

13-9 show dhcp_relay

Description

This command is used to display the current DHCP relay configuration. If no parameter is specified , the system will display all DHCP relay configuration.

Format

show dhcp_relay {ipif <ipif_name 12>}

Parameters

ipif - (Optional) Specifies the IP interface name.
<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.

Restrictions

None.

Example

To display DHCP relay configuration:

```
DAS-3626:admin#show dhcp_relay ipif System
Command: show dhcp_relay ipif System

DHCP/BOOTP Relay Status         : Disabled
DHCP/BOOTP Hops Count Limit     : 4
DHCP/BOOTP Relay Time Threshold : 0
DHCP Vendor Class Identifier Option 60 State: Disabled
DHCP Client Identifier Option 61 State: Disabled
DHCP Relay Agent Information Option 82 State  : Disabled
DHCP Relay Agent Information Option 82 Check  : Disabled
DHCP Relay Agent Information Option 82 Policy : Replace
DHCP Relay Agent Information Option 82 Remote ID : 00-01-02-03-04-00

Interface    Server 1        Server 2        Server 3        Server 4
------------ --------------- --------------- --------------- ---------------
System       10.90.90.100

DAS-3626:admin#
```

Chapter 14 Filter Database (FDB) Command List

create fdb <vlan_name 32> <macaddr> [port <port>| bonding_group <bgroup>	drop]
create fdb vlanid <vidlist> <macaddr> [port <port>| bonding_group <bgroup>	drop]
create multicast_fdb <vlan_name 32> <macaddr>
config multicast_fdb <vlan_name 32> <macaddr> [add | delete] <portlist>
config fdb aging_time <sec 10-1000000>
config multicast vlan_filtering_mode [vlanid <vidlist> | vlan <vlan_name 32> | all] [forward_all_groups | forward_unregistered_groups | filter_unregistered_groups]
delete fdb <vlan_name 32> <macaddr>
clear fdb [vlan <vlan_name 32> | port <port> | bonding_group <bgroup> | all]
show multicast_fdb {[vlan <vlan_name 32> | vlanid <vidlist>] | mac_address <macaddr>}
show fdb {[{port <port> | vlan <vlan_name 32> | mac_address <macaddr> | static} | aging_time | bonding_group <bgroup>]}
show multicast vlan_filtering_mode {[vlanid < vidlist> | vlan <vlan_name 32>]}

14-1 create fdb

Description

This command is used to create a static entry in the unicast MAC address forwarding table (database).

Format

create fdb <vlan_name 32> <macaddr> [port <port>| bonding_group <bgroup> | drop]

Parameters

<vlan_name 32> - Specifies a VLAN name associated with a MAC address. The maximum length of the VLAN name is 32 bytes.
<macaddr> - Enter the MAC address to be added to the static forwarding table.
port - Specifies the port number corresponding to the MAC destination address. The switch will always forward traffic to the specified device through this port. **<port>** - Enter the port number corresponding to the MAC destination address here.
bonding_group - Specifies a VDSL bonding group. **<bgroup>** - Enter a VDSL bonding group. The range is from 1 to 12.
drop - Specifies the action drop to be taken.

Restrictions

Only Administrators and Operators can issue this command.

Example

To create a unicast MAC forwarding entry:

```
DAS-3626:admin#create fdb default 00-00-00-00-01-02 port 5
Command: create fdb default 00-00-00-00-01-02 port 5

Success.

DAS-3626:admin#
```

To filter a unicast MAC:

```
DAS-3626:admin# create fdb default 00-00-00-00-01-02 drop
Command: create fdb default 00-00-00-00-01-02 drop

Success.

DAS-3626:admin#
```

14-2 create fdb vlanid

Description

This command is used to create a static entry in the unicast MAC address forwarding table (database).

Format

create fdb vlanid <vidlist> <macaddr> [port <port>| bonding_group <bgroup> | drop]

Parameters

<vidlist> - Specifies a VLAN ID associated with a MAC address.
<macaddr> - Enter the MAC address to be added to the static forwarding table.
port - Specifies the port number corresponding to the MAC destination address. The switch will always forward traffic to the specified device through this port. **<port>** - Enter the port number corresponding to the MAC destination address here.
bonding_group - Specifies a VDSL bonding group. **<bgroup>** - Enter a VDSL bonding group. The range is from 1 to 12.
drop - Specifies the action drop to be taken.

Restrictions

Only Administrators and Operators can issue this command.

Example

To create a unicast MAC forwarding entry:

```
DAS-3626:admin#create fdb vlanid 1 00-01-00-00-01-02 port 6
Command: create fdb vlanid 1 00-01-00-00-01-02 port 6

Success.

DAS-3626:admin#
```

To filter a unicast MAC:

```
DAS-3626:admin#create fdb vlanid 1 00-01-02-00-01-02 drop
Command: create fdb vlanid 1 00-01-02-00-01-02 drop

Success.

DAS-3626:admin#
```

14-3 create multicast_fdb

Description

This command is used to create a static entry in the multicast MAC address forwarding table (database).

Format

create multicast_fdb <vlan_name 32> <macaddr>

Parameters

<vlan_name 32> - Enter the name of the VLAN on which the MAC address resides. The maximum name length is 32.
<macaddr> - Enter the multicasts MAC address to be added to the static forwarding table.

Restrictions

Only Administrators and Operators can issue this command.

Example

To create a multicast MAC forwarding entry to the default VLAN:

```
DAS-3626:admin#create multicast_fdb default 01-00-5E-00-00-00
Command: create multicast_fdb default 01-00-5E-00-00-00

Success.

DAS-3626:admin#
```

14-4 config multicast_fdb

Description

This command is used to configure the switch’s multicast MAC address forwarding database.

Format

config multicast_fdb <vlan_name 32> <macaddr> [add | delete] <portlist>

Parameters

<vlan_name 32> - Enter the name of the VLAN on which the MAC address resides. The maximum name length is 32.
<macaddr> - Enter the MAC address that will be added or deleted to the forwarding table.
add - Specifies to add ports to the multicast forwarding table.
delete - Specifies to remove ports from the multicast forwarding table.
<portlist> - Enter a range of ports to be configured.

Restrictions

Only Administrators and Operators can issue this command.

Example

To add a multicast MAC forwarding entry to the default VLAN on port 1:1 to 1:5:

```
DAS-3626:admin#config multicast_fdb default 01-00-5E-00-00-00 add 1-5
Command: config multicast_fdb default 01-00-5E-00-00-00 add 1-5

Success.

DAS-3626:admin#
```

14-5 config fdb aging_time

Description

This command is used to configure the MAC address table aging time. The aging time affects the learning process of the Switch. Dynamic forwarding table entries, which are made up of the source MAC addresses and their associated port numbers, are deleted from the table if they are not accessed within the aging time. The aging time can be from 10 to 1000000 seconds with a default value of 300 seconds. A very long aging time can result in dynamic forwarding table entries that are out-of-date or no longer exist. This may cause incorrect packet forwarding decisions by the Switch. If the aging time is too short however, many entries may be aged out too soon. This will result in a high percentage of received packets whose source addresses cannot be found in the forwarding table, in which case the Switch will broadcast the packet to all ports, negating many of the benefits of having a switch.

Format

config fdb aging_time <sec 10-1000000>

Parameters

<sec 10-1000000> - Enter the FDB age out time must be between 10 to 1000000 seconds.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the MAC address table aging time to 600 seconds:

```
DAS-3626:admin# config fdb aging_time 600
Command: config fdb aging_time 600

Success.

DAS-3626:admin#
```

14-6 config multicast vlan_filtering_mode

Description

This command is used to configure the multicast packet filtering mode for VLANs.

The registered group will be forwarded to the range of ports in the multicast forwarding database.

Format

config multicast vlan_filtering_mode [vlanid <vidlist> | vlan <vlan_name 32> | all] [forward_all_groups | forward_unregistered_groups | filter_unregistered_groups]

Parameters

vlanid - Specifies a list of VLANs to be configured. **<vidlist>** - Enter the VLAN ID list here.
vlan - Specifies the name of the VLAN. The maximum name length is 32. **<vlan_name 32>** - Enter the VLAN name can be up to 32 characters long.
all - Specifies all configured VLANs.
forward_all_groups - Specifies that both the registered group and the unregistered group will be forwarded to all member ports of the specified VLAN where the multicast traffic comes in.
forward_unregistered_groups - Specifies that the unregistered group will be forwarded to all member ports of the VLAN where the multicast traffic comes in.
filter_unregistered_groups - Specifies that the unregistered group will be filtered.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the multicast packet filtering mode to filter all unregistered multicast groups for the VLAN 200 to 300:

```
DAS-3626:admin# config multicast vlan_filtering_mode vlanid 200-300
filter_unregistered_groups
Command: config multicast vlan_filtering_mode vlanid 200-300
filter_unregistered_groups

Success.

DAS-3626:admin#
```

14-7 delete fdb

Description

This command is used to delete a static entry from the forwarding database.

Format

delete fdb <vlan_name 32> <macaddr>

Parameters

<vlan_name 32> - Enter the name of the VLAN on which the MAC address resides. The maximum name length is 32.
<macaddr> - Enter the multicast MAC address to be deleted from the static forwarding table.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete a static FDB entry:

```
DAS-3626:admin# delete fdb default 00-00-00-00-01-02
Command: delete fdb default 00-00-00-00-01-02

Success.

DAS-3626:admin#
```

14-8 clear fdb

Description

This command is used to clear the switch's forwarding database for dynamically learned MAC addresses.

Format

clear fdb [vlan <vlan_name 32> | port <port> | bonding_group <bgroup> | all]

Parameters

vlan - Specifies the VLAN name. **<vlan_name 32>** - Enter the name of the VLAN on which the MAC address resides. The maximum name length is 32.
port - Specifies the port number. **<port>** - Enter the port number corresponding to the MAC destination address. The Switch will always forward traffic to the specified device through this port.
bonding_group - Specifies a VDSL bonding group. **<bgroup>** - Enter a VDSL bonding group. The range is from 1 to 12.
all - Specifies to clear all dynamic entries in the Switch's forwarding database.

Restrictions

Only Administrators and Operators can issue this command.

Example

To clear all FDB dynamic entries:

```
DAS-3626:admin# clear fdb all
Command: clear fdb all

Success.

DAS-3626:admin#
```

14-9 show multicast_fdb

Description

This command is used to display the multicast forwarding database of the Switch. If no parameter is specified, all multicast FDB entries will be displayed.

Format

show multicast_fdb {[vlan <vlan_name 32> | vlanid <vidlist>] | mac_address <macaddr>}

Parameters

vlan - (Optional) Specifies the name of the VLAN on which the MAC address resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - (Optional) Specifies to display the entries for the VLANs indicated by VID list. **<vidlist>** - Enter the VLAN ID list here.
mac_address - (Optional) Specifies a MAC address, for which FDB entries will be displayed. **<macaddr>** - Enter the MAC address here.

Restrictions

None.

Example

To display the multicast MAC address table:

```
DAS-3626:admin#show multicast_fdb
Command: show multicast_fdb

 VLAN Name      : default
 MAC Address    : 01-00-5E-00-00-00
 Egress Ports   : 1-5
 Mode           : Static

Total Entries: 1

DAS-3626:admin#
```

14-10 show fdb

Description

This command is used to display the current unicast MAC address forwarding database. If no parameter is specified, system will display the unicast address table.

Format

show fdb {[{port <port> | vlan <vlan_name 32> | mac_address <macaddr> | static} | aging_time | bonding_group <bgroup>]}

Parameters

port - (Optional) Specifies to display the entries for a specified port. <port> - Enter the port number here.
vlan - (Optional) Specifies to display the entries for a specific VLAN. The maximum name length is 32. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
mac_address - (Optional) Specifies to display a specific MAC address. **<macaddr>** - Enter the MAC address here.
static - (Optional) Specifies to display all permanent entries.
aging_time - (Optional) Specifies to display the unicast MAC address aging time.
bonding_group - (Optional) Specifies a VDSL bonding group. **<bgroup>** - Enter a VDSL bonding group. The range is from 1 to 12.

Restrictions

None.

Example

To display the FDB table:

```
DAS-3626:admin#show fdb
Command: show fdb

 Unicast MAC Address Aging Time  = 300

 VID  VLAN Name                         MAC Address       Port  Type
 ---- -------------------------------- ----------------- ----- ----------------
-
 1    default                           00-00-00-00-01-02 5     Permanent
 1    default                           00-01-00-00-01-02 6     Permanent
 1    default                           00-01-02-00-01-02 UNknown
 1    default                           D8-FE-E3-93-05-C0 CPU   Self

Total Entries: 4

DAS-3626:admin#
```

14-11 show multicast vlan_filtering_mode

Description

This command is used to show the multicast packet filtering mode for VLANs. If no parameter is specified, the device will show all multicast filtering settings in the device.

Note: A product supports the multicast VLAN filtering mode could not support the port filtering mode at the same time.

Format

show multicast vlan_filtering_mode {[vlanid < vidlist> | vlan <vlan_name 32>]}

Parameters

vlanid - (Optional) Specifies a list of VLANs to be configured. **<vidlist>** - Enter the VLAN ID list here.
vlan - (Optional) Specifies the name of the VLAN. The maximum name length is 32. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.

Restrictions

None.

Example

To show the multicast vlan_filtering_mode for VLANs:

```
DAS-3626:admin#show multicast vlan_filtering_mode
Command: show multicast vlan_filtering_mode

VLAN ID/VLAN Name                          Multicast Filter Mode
-----------------------------------------  ----------------------------
1   /default                               filter_unregistered_groups

DAS-3626:admin#
```

Chapter 15 IGMP Snooping Command List

The Internet Group Management Protocol (IGMP) is a L3 protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. IGMP snooping is the process of listening to IGMP network traffic. IGMP snooping, as implied by the name, is a feature that allows a layer 2 switch to "listen in" on the IGMP conversation between hosts and routers by processing the layer 3 IGMP packets sent in a multicast network.

When IGMP snooping is enabled in a switch it analyzes all IGMP packets between hosts connected to the Switch and multicast routers in the network. When a switch hears an IGMP report from a host for a given multicast group, the Switch adds the host's port number to the multicast list for that group. And, when the Switch hears an IGMP Leave, it removes the host's port from the table entry.

config igmp_snooping message priority <value 0-7>
config igmp_snooping message_limit [ports <portlist> | bonding <bgroup_list> | vlanid <vidlist>] [<value 1-1000> | no_limit]
show igmp_snooping message priority
show igmp_snooping message_limit [ports <portlist> | bonding <bgroup_list> | vlanid <vlanid_list>]
config igmp_snooping [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {state [enable | disable] | fast_leave [enable | disable] | report_suppression [enable | disable]}(1)
config igmp_snooping querier [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-7> | last_member_query_interval <sec 1-25> | state [enable | disable] | version <value 1-3>}(1)
config config router_ports [vlan <vlan_name 32> | vlanid <vlanid_list>] [add | delete] [<portlist> | bonding <bgroup_list>]
config router_ports_forbidden [vlan <vlan_name 32> | vlanid <vlanid_list>] [add | delete] [<portlist> | bonding <bgroup_list>]
enable igmp_snooping
disable igmp_snooping
create igmp_snooping static_group [vlan<vlan_name 32> | vlanid <vlanid_list>] <ipaddr>
delete igmp_snooping static_group [vlan<vlan_name 32> | vlanid <vlanid_list>] <ipaddr>
config igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr> [add | delete] [<portlist> | bonding <bgroup_list>]
show igmp_snooping static_group {[vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>}
show igmp_snooping {[vlan <vlan_name 32> | vlanid <vlanid_list>]}
show igmp_snooping group {[vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist> | bonding <bgroup_list>] {<ipaddr>}}
show igmp_snooping forwarding {[vlan <vlan_name 32> | vlanid <vlanid_list>]}
show router_ports [vlan <vlan_name 32> | vlanid <vlanid_list> | all] {[static | dynamic | forbidden]}
show igmp_snooping statistic counter [vlan <vlan_name> | vlanid <vlanid_list> | ports <portlist> | bonding <bgroup_list> | group <group> | per_port <portlist> per_vlan [vlan <vlan_name 32> | vlanid <vidlist>] | per_bonding <bgroup_list> per_vlan [vlan <vlan_name 32> | vlanid <vidlist>]]
clear igmp_snooping statistics counter [vlan <vlan_name> | vlanid <vlanid_list> | ports <portlist> | bonding <bgroup_list> | group <group> | per_port <portlist> per_vlan [vlan

<vlan_name 32> | vlanid <vidlist>] | per_bonding <bgroup_list> per_vlan [vlan <vlan_name 32> | vlanid <vidlist>]]

15-1 config igmp_snooping message priority

Description

This command is used to modify priority of IGMP snooping packet.

Format

config igmp_snooping message priority <value 0-7>

Parameters

<value 0-7> - Enter the priority of IGMP snooping packet. The value is between 0 and 7.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure priority of IGMP snooping message:

```
DAS-3626:admin#config igmp_snooping message priority 7
Command: config igmp_snooping message priority 7

Success.

DAS-3626:admin#
```

15-2 config igmp_snooping message_limit

Description

This command is used to configure rate limit of IGMP control packet.

Format

config igmp_snooping message_limit [ports <portlist> | bonding <bgroup_list> | vlanid <vidlist>] [<value 1-1000> | no_limit]

Parameters

ports - Specifies a list of ports to be configured for the rate limit of IGMP control packet. **<portlist>** - Enter a list of ports to be configured.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
vlanid - Specifies a list of VLAN IDs to be configure for the rate limit of IGMP control packet. **<vlanid_list>** - Enter the VLAN ID list here.
<value 1-1000> - Enter the message limitation value here. This value must be between 1 and

1000.
no_limit - Specifies that the rate limit of IGMP control packet is unlimited.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the rate limit of IGMP control packet:

```
DAS-3626:admin#config igmp_snooping message_limit ports 3 100
Command: config igmp_snooping message_limit ports 3 100

Success.

DAS-3626:admin#
```

15-3 show igmp_snooping message priority

Description

This command is used to display the priority of IGMP snooping packet.

Format

show igmp_snooping message priority

Parameters

None.

Restrictions

None.

Example

To display the priority of IGMP snooping packet:

```
DAS-3626:admin# show igmp_snooping message priority
Command: show igmp_snooping message priority

IGMP_SNOOP Message priority is 7 now

DAS-3626:admin#
```

15-4 show igmp_snooping message_limit

Description

This command is used to display the rate limit of IGMP control packet.

Format

show igmp_snooping message_limit [ports <portlist> | bonding <bgroup_list> | vlanid <vlanid_list>]

Parameters

ports - Specifies a list of ports to be displayed. **<portlist>** - Enter a list of ports to be displayed.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
vlanid - Specifies a list of VLANs to be displayed. **<vlanid_list>** - Enter the VLAN ID list here.

Restrictions

None.

Example

To display the message limitation:

```
DAS-3626:admin#show igmp_snooping message_limit ports 3
Command: show igmp_snooping message_limit ports 3

 Port      Message Limit
 --------  ---------------
 3         100

Total Entries: 1

DAS-3626:admin#
```

15-5 config igmp_snooping

Description

This command is used to configure IGMP snooping on the Switch.

Format

config igmp_snooping [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {state [enable | disable] | fast_leave [enable | disable] | report_suppression [enable | disable]}(1)

Parameters

vlan_name - Specifies the name of the VLAN for which IGMP snooping is to be configured. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specifies the VLAN ID for which IGMP snooping is to be configured. **<vlanid_list>** - Enter the VLAN ID here.
all - Specifies to use all configured VLANs.

state - Specifies to enable or disable IGMP snooping for the chosen VLAN. **enable** - Specifies to enable to enable IGMP snooping for the chosen VLAN. **disable** - Specifies to disable to disable IGMP snooping for the chosen VLAN.
fast_leave - Specifies to enable or disable the IGMP snooping fast leave function. **enable** - Specifies to enable to enable the IGMP snooping fast leave function. If enabled, the membership is immediately removed when the system receives the IGMP leave message. **disable** - Specifies to disable to disable the IGMP snooping fast leave function.
report_suppression - Specifies IGMP proxy reporting. If enabled, multiple IGMP reports or leave for a specific (S, G) will be integrated into one report only before sending to the router port. **enable** - Specifies to enable the proxy reporting. **disable** - Specifies to disable the proxy reporting.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure IGMP snooping:

```
DAS-3626:admin# config igmp_snooping vlan_name default state enable
Command: config igmp_snooping vlan_name default state enable

Success.

DAS-3626:admin#
```

15-6 config igmp_snooping querier

Description

This command is used to configure the time in seconds between general query transmissions, the maximum time in seconds to wait for reports from members, and the permitted packet loss that guarantees IGMP snooping.

Format

config igmp_snooping querier [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-7> | last_member_query_interval <sec 1-25> | state [enable | disable] | version <value 1-3>}(1)

Parameters

vlan_name - Specifies the name of the VLAN for which IGMP snooping querier is to be configured. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specifies the VLAN ID for which IGMP snooping querier is to be configured. **<vlanid_list>** - Enter the VLAN ID list here.
all - Specifies all VLANs for which IGMP snooping querier is to be configured.
query_interval - Specifies the amount of time in seconds between general query transmissions. The default setting is 125 seconds. **<sec 1-65535>** - Enter the query interval value here. This value must between 1 and 65535

seconds.
max_reponse_time - Specifies the maximum time in seconds to wait for reports from members. The default setting is 10 seconds. **<sec 1-25>** - Enter the maximum response time value here. This value must be between 1 and 25 seconds.
robustness_variable - Provides fine-tuning to allow for expected packet loss on a subnet. The value of the robustness variable is used in calculating the following IGMP message intervals: **<value 1-7>** - Enter the robustness variable value here. This value must be between 1 and 7. By default, the robustness variable is set to 2. You might want to increase this value if you expect a subnet to be loosely. • Group member interval—Amount of time that must pass before a multicast router decides there are no more members of a group on a network. This interval is calculated as follows: (robustness variable x query interval) + (1 x query response interval). • Other querier present interval—Amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the querier. This interval is calculated as follows: (robustness variable x query interval) + (0.5 x query response interval). • Last member query count—Number of group-specific queries sent before the router assumes there are no local members of a group. The default number is the value of the robustness variable.
last_member_query_interval - Specifies the maximum amount of time between group-specific query messages, including those sent in response to leave-group messages. You might lower this interval to reduce the amount of time it takes a router to detect the loss of the last member of a group. On receiving a leave message, the router will assume there are no local members on the interface if there are no reports received after the response time (which is last member query interval * robustness variable) **<sec 1-25>** - Enter the last member query interval value here. This value must be between 1 and 25 seconds.
state - Specifies the state of IGMP snooping querier. If the state is enabled, it allows the Switch to be selected as an IGMP Querier (sends IGMP query packets). It the state is disabled, then the Switch cannot play the role as a querier. Note that if the Layer 3 router connected to the Switch provide only the IGMP proxy function but does not provide the multicast routing function, then this state must be configured as disabled. Otherwise, if the Layer 3 router is not selected as the querier, it will not send the IGMP query packet. Since it will not send the multicast-routing protocol packet, the port will be timed out as a router port. **enable** - Specifies to enable to enable this state. **disable** - Specifies to disable to disable this state.
version - Specifies the version of IGMP packet that will be sent by this port. If an IGMP packet received by the interface has a version higher than the specified version, this packet will be dropped. **<value 1-3>** - Enter the version number here. This value must be between 1 and 3.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the IGMP snooping querier:

```
DAS-3626:admin# config igmp_snooping querier vlan_name default query_interval
125 state enable
Command: config igmp_snooping querier vlan_name default query_interval 125
state enable

Success.

DAS-3626:admin#
```

15-7 config router_ports

Description

This command is used to designate a range of ports as being connected to multicast-enabled routers. This will ensure that all packets with such a router as its destination will reach the multicast-enabled router, regardless of protocol, etc.

Format

config router_ports [vlan <vlan_name 32> | vlanid <vlanid_list>] [add | delete] [<portlist> | bonding <bgroup_list>]

Parameters

vlan - Specifies the name of the VLAN on which the router port resides. **<vlan_name 32>** - Enter the name of the VLAN.
vlanid - Specifies the ID of the VLAN on which the router port resides. **<vlanid_list>** - Enter the VLAN ID here.
add - Specifies to add the router ports.
delete - Specifies to delete the router ports.
<portlist> - Enter a range of ports to be configured.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.

Restrictions

Only Administrators and Operators can issue this command.

Example

To set up static router ports:

```
DAS-3626:admin#config router_ports vlan default add 1-10
Command: config router_ports vlan default add 1-10

Success.

DAS-3626:admin#
```

15-8 config router_ports_forbidden

Description

This command is used to designate a range of ports as being not connected to multicast-enabled routers. This ensures that the forbidden router port will not propagate routing packets out.

Format

config router_ports_forbidden [vlan <vlan_name 32> | vlanid <vlanid_list>] [add | delete] [<portlist> | bonding <bgroup_list>]

Parameters

vlan - Specifies the name of the VLAN on which the router port resides. **<vlan_name 32>** - Enter the name of the VLAN.
vlanid - Specifies the ID of the VLAN on which the router port resides. **<vlanid_list>** - Enter the VLAN ID list here.
add - Specifies to add the router ports.
delete - Specifies to delete the router ports.
<portlist> - Specifies a range of ports to be configured.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.

Restrictions

Only Administrators and Operators can issue this command.

Example

To set up port range 1-10 to forbidden router ports of default VLAN:

```
DAS-3626:admin#config router_ports_forbidden vlan default add 1-10
Command: config router_ports_forbidden vlan default add 1-10

Success.

DAS-3626:admin#
```

15-9 enable igmp_snooping

Description

This command is used to enable IGMP snooping on the Switch.

Format

enable igmp_snooping

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable IGMP snooping on the Switch:

```
DAS-3626:admin# enable igmp_snooping
Command: enable igmp_snooping

Success.

DAS-3626:admin#
```

15-10 disable igmp_snooping

Description

This command is used to disable IGMP snooping on the Switch. Disabling IGMP snooping allows all IGMP and IP multicast traffic to flood within a given IP interface. Note that disable igmp_snooping will also disable the forward multicast router only function.

Format

disable igmp_snooping

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable IGMP snooping on the Switch:

```
DAS-3626:admin# disable igmp_snooping
Command: disable igmp_snooping

Success.

DAS-3626:admin#
```

15-11 create igmp_snooping static_group

Description

This command is used to create an IGMP snooping static group. Member ports can be added to the static group. The static member and the dynamic member port form the member ports of a group.

The static group will only take effect when IGMP snooping is enabled on the VLAN. For those static member ports, the device needs to emulate the IGMP protocol operation to the querier, and forward the traffic destined to the multicast group to the member ports.

For a layer 3 device, the device is also responsible to route the packet destined for this specific group to static member ports.

The static member port will only affect V2 IGMP operation.

The Reserved IP multicast address 224.0.0.X must be excluded from the configured group.

The VLAN must be created first before a static group can be created.

Format

create igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>

Parameters

vlan - Specifies the name of the VLAN on which the static group resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specifies the ID of the VLAN on which the static group resides. **<vlanid_list>** - Enter the VLAN ID here.
<ipaddr> - Specifies the multicast group IP address.

Restrictions

Only Administrators and Operators can issue this command.

Example

To create an IGMP snooping static group for VLAN 1, group 239.1.1.1:

```
DAS-3626:admin# create igmp_snooping static_group vlan default 239.1.1.1
Command: create igmp_snooping static_group vlan default 239.1.1.1

Success.

DAS-3626:admin#
```

15-12 delete igmp_snooping static_group

Description

This command is used to delete an IGMP snooping multicast static group. The deletion of an IGMP snooping static group will not affect the IGMP snooping dynamic member ports for a group.

Format

delete igmp_snooping static_group [vlan<vlan_name 32> | vlanid <vlanid_list>] <ipaddr>

Parameters

vlan - Specifies the name of the VLAN on which the static group resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specifies the ID of the VLAN on which the static group resides. **<vlanid_list>** - Enter the VLAN ID list here.
<ipaddr> - Specifies the multicast group IP address.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete an IGMP snooping static group for VLAN 1, group 239.1.1.1:

```
DAS-3626:admin# delete igmp_snooping static_group vlan default 239.1.1.1
Command: delete igmp_snooping static_group vlan default 239.1.1.1

Success.

DAS-3626:admin#
```

15-13 config igmp_snooping static_group

Description

This command is used to configure IGMP snooping static group. When a port is configured as a static member port, the IGMP protocol will not operate on this port. For example, suppose that a port is a dynamic member port learned by IGMP. If this port is configured as a static member later, then the IGMP protocol will stop operating on this port. The IGMP protocol will resume once this port is removed from static member ports.

The static member port will only affect V2 IGMP operation.

Format

config igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr> [add | delete] [<portlist> | bonding <bgroup_list>]

Parameters

vlan - Specifies the name of the VLAN on which the static group resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specifies the ID of the VLAN on which the static group resides. **<vlanid_list>** - Enter the VLAN ID here.
<ipaddr> - Specifies the multicast group IP address (for Layer 3 switch).
add - Specifies to add the member ports.
delete - Specifies to delete the member ports.
<portlist> - Specifies a range of ports to be configured.
bonding - Specifies a list of VDSL bonding groups.

<bgroup_list> - Enter a list of VDSL bonding groups. The range is from 1 to 12.

Restrictions

Only Administrators and Operators can issue this command.

Example

To unset port range 9-10 from IGMP snooping static member ports for group 239.1.1.1 on default VLAN:

```
DAS-3626:admin#config igmp_snooping static_group vlan default 239.1.1.1 delete
9-10
Command: config igmp_snooping static_group vlan default 239.1.1.1 delete 9-10

Success.

DAS-3626:admin#
```

15-14 show igmp_snooping static_group

Description

This command is used to display the IGMP snooping multicast group static members.

Format

show igmp_snooping static_group {[vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>}

Parameters

vlan - Specifies the name of the VLAN on which the static group resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specifies the ID of the VLAN on which the static group resides. **<vlanid_list>** - Enter the VLAN ID here.
<ipaddr> - Specifies the multicast group IP address.

Restrictions

None.

Example

To display all the IGMP snooping static groups:

```
DAS-3626:admin#show igmp_snooping static_group
Command: show igmp_snooping static_group

VLAN ID/Name                          IP Address       Static Member Ports
------------------------------------  ---------------  ----------------------
1   /default                          239.1.1.1         9-10

 Total Entries : 1

DAS-3626:admin#
```

15-15 show igmp_snooping

Description

This command is used to display the current IGMP snooping configuration on the Switch. If the VLAN is not specified, the system will display all current IGMP snooping configurations.

Format

show igmp_snooping {[vlan <vlan_name 32> | vlanid <vlanid_list>]}

Parameters

vlan - (Optional) Specifies the name of the VLAN for which you want to view the IGMP snooping configuration. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - (Optional) Specifies the ID of the VLAN for which you want to view the IGMP snooping configuration. **<vlanid_list>** - Enter the VLAN ID list here.

Restrictions

None.

Example

To show IGMP snooping:

```
DAS-3626:admin#show igmp_snooping
Command: show igmp_snooping

 IGMP Snooping Global State              : Disabled

 VLAN Name                      : default
 Query Interval                 : 125
 Max Response Time              : 10
 Robustness Value               : 2
 Last Member Query Interval     : 1
 Querier State                  : Disabled
 Querier Role                   : Non-Querier
 Querier IP                     : 0.0.0.0
 Querier Expiry Time            : 0 secs
 State                          : Disabled
 Fast Leave                     : Disabled
 Message Limit                  : No Limitation
 Report Suppression             : Disabled
 Version                        : 2
 Version Translation            : Disabled

Total Entries: 1

DAS-3626:admin#
```

15-16 show igmp_snooping group

Description

This command is used to display the current IGMP snooping group configuration on the Switch.

Format

show igmp_snooping group {[vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist> | bonding <bgroup_list>] {<ipaddr>}}

Parameters

vlan - (Optional) Specifies the name of the VLAN for which you want to view IGMP snooping group information. If VLAN, ports and IP address are not specified, the system will display all current IGMP snooping group information. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - (Optional) Specifies the ID of the VLAN for which you want to view IGMP snooping group information. **<vlanid_list>** - Enter the VLAN ID list here.
ports - (Optional) Specifies a list of ports for which you want to view IGMP snooping group information. **<portlist>** - Enter the list of ports here.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
<ipaddr> - (Optional) Specifies the group IP address for which you want to view IGMP snooping group information.

Restrictions

None.

Example

To show IGMP snooping groups when IGMP v3 is supported:

```
DAS-3626:admin# show igmp_snooping group
Command: show igmp_snooping group

Source/Group                    : 10.0.0.1/225.0.0.1
 VLAN Name/VID                  : default/1
 Member Ports                   : 5
 UP Time                        : 6
 Expiry Time                    : 254
 Filter Mode                    : INCLUDE

 Source/Group                   : 10.0.0.10/225.0.0.1
 VLAN Name/VID                  : default/1
 Member Ports                   : 5
 UP Time                        : 6
 Expiry Time                    : 254
 Filter Mode                    : INCLUDE

 Source/Group                   : NULL/239.255.255.250
 VLAN Name/VID                  : default/1
 Member Ports                   : 5
 UP Time                        : 2
 Expiry Time                    : 258
 Filter Mode                    : EXCLUDE

 Total Entries: 3

DAS-3626:admin#
```

To show IGMP snooping groups when only IGMP v2 is supported: The third item is a data-driven learned entry. If the member port list is empty, the multicast packets will be forwarded to the router ports. If the router port list is empty, the packets will be dropped.

```
DAS-3626:admin# show igmp_snooping group
Command: show igmp_snooping group

Source/Group                   : NULL/226.0.0.1
 VLAN Name/VID                  : default/1
 Member Ports                   : 5
 UP Time                        : 10
 Expiry Time                    : 258
 Filter Mode                    : EXCLUDE

 Source/Group                   : NULL/226.0.0.2
 VLAN Name/VID                  : default/1
 Member Ports                   : 5
 UP Time                        : 9
 Expiry Time                    : 259
 Filter Mode                    : EXCLUDE

 Source/Group                   : NULL/226.0.0.3
 VLAN Name/VID                  : default/1
 Member Ports                   :
Router Ports        :
 UP Time                        : 1
 Expiry Time                    : 259
 Filter Mode                    : EXCLUDE

 Source/Group                   : NULL/239.255.255.250
 VLAN Name/VID                  : default/1
 Member Ports                   : 5
 UP Time                        : 1
 Expiry Time                    : 259
 Filter Mode                    : EXCLUDE

 Total Entries: 4

DAS-3626:admin#
```

15-17 show igmp_snooping forwarding

Description

This command is used to display the Switch's current IGMP snooping forwarding table. It provides an easy way for users to check the list of ports that the multicast group that comes from a specific sources will be forwarded to. The packet comes from the source VLAN. They will be forwarded to the forwarding VLAN. The IGMP snooping further restricts the forwarding ports. If no parameter is specified, the system will display all current IGMP snooping forwarding table entries of the Switch.

Format

show igmp_snooping forwarding {[vlan <vlan_name 32> | vlanid <vlanid_list>]}

Parameters

vlan - (Optional) Specifies the name of the VLAN for which you want to view IGMP snooping forwarding table information. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - (Optional) Specifies the ID of the VLAN for which you want to view IGMP snooping forwarding table information. **<vlanid_list>** - Enter the VLAN ID list here.

Restrictions

None.

Example

To show all IGMP snooping forwarding entries located on the Switch:

```
DAS-3626:admin# show igmp_snooping forwarding
Command: show igmp_snooping forwarding

VLAN Name      : default
Source IP      : 10.90.90.114
Multicast Group: 225.0.0.0
Port Member    : 2,7

VLAN Name      : default
Source IP      : 10.90.90.10
Multicast Group: 225.0.0.1
Port Member    : 2,5

VLAN Name      : default
Source IP      : 10.90.90.20
Multicast Group: 225.0.0.2
Port Member    : 2,8

Total Entries : 3

DAS-3626:admin#
```

15-18 show router_ports

Description

This command is used to display the currently configured router ports on the Switch. If no parameter is specified, the system will display all currently configured router ports on the Switch.

Format

show router_ports [vlan <vlan_name 32> | vlanid <vlanid_list> | all] {[static | dynamic | forbidden]}

Parameters

vlan - Specifies the name of the VLAN on which the router port resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specifies the ID of the VLAN on which the router port resides. **<vlanid_list>** - Enter the VLAN ID list here.
all - Specifies all VLANs on which the router port resides.
static - (Optional) Displays router ports that have been statically configured.
dynamic - (Optional) Displays router ports that have been dynamically configured.
forbidden - (Optional) Displays forbidden router ports that have been statically configured.

Restrictions

None.

Example

To display router ports:

```
DAS-3626:admin#show router_ports all
Command: show router_ports all


VLAN Name                : default
Static Router Port       : 1-10
Dynamic Router Port      :
Router IP                :
Forbidden Router Port    :

Total Entries: 1

DAS-3626:admin#
```

15-19 show igmp_snooping statistics counter

Description

This command is used to display the statistics counter for IGMP protocol packets that are received by the Switch since IGMP snooping was enabled.

Format

show igmp_snooping statistic counter [vlan <vlan_name> | vlanid <vlanid_list> | ports <portlist> | bonding <bgroup_list> | group <group> | per_port <portlist> per_vlan [vlan <vlan_name 32> | vlanid <vidlist>] | per_bonding <bgroup_list> per_vlan [vlan <vlan_name 32> | vlanid <vidlist>]]

Parameters

vlan - Specifies a VLAN to be displayed. **<vlan_name>** - Enter the VLAN name here.
vlanid - Specifies a list of VLANs to be displayed. **<vlanid_list>** - Enter the VLAN ID list here.

ports - Specifies a list of ports to be displayed. **<portlist>** - Enter the list of port to be displayed here.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
group - Specifies the group IP address for which you want to view IGMP snooping statistic counter information. **<group>** - Enter the group IP address.
per_port - Specifies a list of ports to be displayed. **<portlist>** - Enter the list of port to be displayed here. **per_vlan** - Specifies a VLAN to be displayed. **vlan** - Specifies the name of VLAN. **<vlan_name 32>** - Enter a VLAN name. **vlanid** - Specifies the VLAN ID. **<vidlist>** - Enter a VLAN ID.
per_bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12. **per_vlan** - Specifies a VLAN to be displayed. **vlan** - Specifies the name of VLAN. **<vlan_name 32>** - Enter a VLAN name. **vlanid** - Specifies the VLAN ID. **<vidlist>** - Enter a VLAN ID.

Restrictions

None.

Example

To display the IGMP snooping statistics counter:

```
DAS-3626:admin#  show igmp_snooping statistics counter vlanid 1
Command: show igmp_snooping statistics counter vlanid 1

VLAN Name             : Default
-----------------------------------------------
Group Number          : 10
Receive Statistics
      Query
IGMP v1 Query                   : 1
IGMP v2 Query                   : 1
IGMP v3 Query                   : 1
Total                           : 3
Dropped By Rate Limitation      : 1
Dropped By Multicast VLAN       : 1

  Report & Leave
IGMP v1 Report                  : 0
IGMP v2 Report                  : 10
IGMP v3 Report                  : 10
IGMP v2 Leave                   : 1
Total                           : 21
Dropped By Rate Limitation      : 0
Dropped By Max Group Limitation : 90
Dropped By Group Filter         : 0
Dropped By Multicast VLAN       : 1

Transmit Statistics
Query
IGMP v1 Query                   : 1
IGMP v2 Query                   : 1
IGMP v3 Query                   : 1
Total                           : 3
Report & Leave
IGMP v1 Report                  : 0
IGMP v2 Report                  : 10
IGMP v3 Report                  : 10
IGMP v2 Leave                   : 1
Total                           : 21

Total Entries : 1

DAS-3626:admin#
```

To display the IGMP snooping statistics counter for a port:

```
DAS-3626:admin#  show igmp_snooping statistics counter ports 1
Command: show igmp_snooping statistics counter ports 1

Port #1
-----------------------------------------------
Group Number                        : 10
Receive Statistics
     Query
IGMP v1 Query                       : 0
IGMP v2 Query                       : 0
IGMP v3 Query                       : 0
Total                               : 0
Dropped By Rate Limitation          : 0
Dropped By Multicast VLAN           : 0

Report & Leave
IGMP v1 Report                      : 0
IGMP v2 Report                      : 100
IGMP v3 Report                      : 0
IGMP v2 Leave                       : 0
Total                               : 100
Dropped By Rate Limitation          : 0
Dropped By Max Group Limitation     : 90
Dropped By Group Filter             : 0
Dropped By Multicast VLAN           : 0

Transmit Statistics
    Query
IGMP v1 Query                       : 0
IGMP v2 Query                       : 0
IGMP v3 Query                       : 0
Total                               : 0

Report & Leave
IGMP v1 Report                      : 0
IGMP v2 Report                      : 0
IGMP v3 Report                      : 0
IGMP v2 Leave                       : 0
Total                               : 0

Total Entries : 1

DAS-3626:admin#
```

15-20 clear igmp_snooping statistics counter

Description

This command is used to clear the IGMP snooping statistics counter.

Format

clear igmp_snooping statistics counter [vlan <vlan_name> | vlanid <vlanid_list> | ports <portlist> | bonding <bgroup_list> | group <group> | per_port <portlist> per_vlan [vlan <vlan_name 32> | vlanid <vidlist>] | per_bonding <bgroup_list> per_vlan [vlan <vlan_name 32> | vlanid <vidlist>]]

Parameters

vlan - Specifies a VLAN to be cleared. **<vlan_name>** - Enter the VLAN name here.
vlanid - Specifies a list of VLANs to be cleared. **<vlanid_list>** - Enter the VLAN ID list here.
ports - Specifies a list of ports to be cleared. **<portlist>** - Enter the list of port to be displayed here.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
group - Specifies group IP address to be cleared for IGMP snooping statistic counter information. **<group>** - Enter the group IP address.
per_port - Specifies a list of ports to be cleared. **<portlist>** - Enter the list of port to be cleared here. **per_vlan** - Specifies a VLAN to be cleared. **vlan** - Specifies the name of VLAN. **<vlan_name 32>** - Enter a VLAN name. **vlanid** - Specifies the VLAN ID. **<vidlist>** - Enter a VLAN ID.
per_bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12. **per_vlan** - Specifies a VLAN to be cleared. **vlan** - Specifies the name of VLAN. **<vlan_name 32>** - Enter a VLAN name. **vlanid** - Specifies the VLAN ID. **<vidlist>** - Enter a VLAN ID.

Restrictions

Only Administrators and Operators can issue this command.

Example

To clear the IGMP snooping statistics counter:

```
DAS-3626:admin#clear igmp_snooping statistic counter
Command: clear igmp_snooping statistic counter

Success.

DAS-3626:admin#
```

Chapter 16 IP-MAC-Port Binding (IMPB) Command List

config address_binding ip_mac ports [<portlist> | all] {arp_inspection [strict | loose | disable] | ip_inspection [enable | disable] | protocol [ipv4] | allow_zeroip [enable | disable] | forward_dhcppkt [enable | disable] | stop_learning_threshold <int 0-500>}
create address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports [<portlist> | all] | bonding <bgroup_list>}
delete address_binding [ip_mac [ipaddress <ipaddr> mac_address <macaddr> | all] | blocked [all | vlan_name <vlan_name> mac_address <macaddr>]]
config address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports [<portlist> | all] | bonding <bgroup_list>}
config address_binding ip_mac bonding <bgroup_list> {arp_inspection [strict | loose | disable] | ip_inspection [enable | disable] | protocol [ipv4] | allow_zeroip [enable | disable] | forward_dhcppkt [enable | disable] | stop_learning_threshold <int 0-500>}(1)
show address_binding [ip_mac [all | ipaddress <ipaddr> mac_address <macaddr>] | blocked [all | vlan_name <vlan_name> mac_address <macaddr>] | ports {<portlist>} | bonding <bgroup_list>]
enable address_binding dhcp_snoop
disable address_binding dhcp_snoop
clear address_binding dhcp_snoop binding_entry [ports [<portlist> | all] | bonding <bgroup_list>]
show address_binding dhcp_snoop {max_entry {ports <portlist> | bonding <bgroup_list>}}
show address_binding dhcp_snoop binding_entry {port <port> | bonding_group <bgroup>}
config address_binding dhcp_snoop max_entry [ports [<portlist> | all] | bonding <bgroup_list>] limit [<value 1-50> | no_limit]
enable address_binding trap_log
disable address_binding trap_log
config address_binding recover_learning [ports [<portlist> | all] | bonding <bgroup_list>]

16-1 config address_binding ip_mac ports

Description

This command is used to configure the state of IMPB on the switch for each port.

Format

config address_binding ip_mac ports [<portlist> | all] {arp_inspection [strict | loose | disable] | ip_inspection [enable | disable] | protocol [ipv4] | allow_zeroip [enable | disable] | forward_dhcppkt [enable | disable] | stop_learning_threshold <int 0-500>}

Parameters

<portlist> - Enter the list of ports used for this configuration here.
all - Specifies that all the ports will be used.
arp_inspection - (Optional) Specifies that the ARP inspection option will be configured. **strict** - Specifies that all packets are dropped by default until a legal ARP or IP packets are detected. **loose** - Specifies that all packets are forwarded by default until an illegal ARP or broadcast IP packets are detected. If not specified strict or loose, default is strict.

disable - Specifies to disable ARP inspection function. The default value is disabled.
ip_inspection - (Optional) Specifies that the IP inspection option will be configured. **enable** - Specifies to enable IP inspection function. The legal IP packets will be forward, while the illegal IP packets will be dropped. **disable** - Specifies to disable IP inspection function. The default value is disabled.
protocol - (Optional) Specifies the version used. **ipv4** - Specifies that only IPv4 packets will be checked.
allow_zeroip - (Optional) Specifies whether to allow ARP packets with a source IP address of 0.0.0.0. If the IP address 0.0.0.0 is not configured in the binding list and this setting is enabled, ARP packets with the source IP address of 0.0.0.0 will be allowed; If the IP address 0.0.0.0 is not configured in the binding list and this setting is disabled, ARP packets with the source IP address of 0.0.0.0 will not be allowed. This option does not affect the IMPB ACL Mode. **enable** - Specifies that the allow zero IP option will be enabled. **disable** - Specifies that the allow zero IP option will be disabled.
forward_dhcppkt - (Optional) Specifies to enable or disable the forward DHCP packets option. By default, DHCP packets with a broadcast DA will be flooded. When set to disabled, the broadcast DHCP packet received by the specified port will not be forwarded. This setting is effective when DHCP Snooping is enabled, in this case DHCP packets trapped by the CPU must be forwarded by the software. This setting controls the forwarding behavior in this situation. **enable** - Specifies that the forward DHCP packets option will be enabled. **disable** - Specifies that the forward DHCP packets option will be disabled.
stop_learning_threshold - (Optional) Specifies the stop learning threshold. When the number of blocked entries exceeds the threshold, the port will stop learning new addresses. Packets with a new address will be dropped. **<int 0-500>** - Enter the stop learning threshold value here. This value must be between 0 and 500.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable IMPB on port 1:

```
DAS-3626:admin#config address_binding ip_mac ports 1 arp_inspection strict
Command: config address_binding ip_mac ports 1 arp_inspection strict

Success.

DAS-3626:admin#
```

16-2 create address_binding ip_mac ipaddress

Description

This command is used to create an IMPB entry.

Format

create address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports [<portlist> | all] | bonding <bgroup_list>}

Parameters

ipaddress - Specifies the IP address used for the IMPB entry. **<ipaddr>** - Enter the IP address used here.
mac_address - Specifies the MAC address used for the IMPB entry. **<macaddr>** - Enter the MAC address used here.
ports - (Optional) Specifies the portlist the entry will apply to. If not specified, the settings will be applied to all ports. **<portlist>** - Enter a list of ports used for this configuration here. **all** - Specifies that all the ports will be included.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.

Restrictions

Only Administrators and Operators can issue this command.

Example

To create an IMPB entry:

```
DAS-3626:admin#create address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-
00-00-00-00-11
Command: create address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-
00-00-11

Success.

DAS-3626:admin#
```

16-3 delete address_binding

Description

This command is used to delete an IMPB entry or blocked entry.

Format

delete address_binding [ip_mac [ipaddress <ipaddr> mac_address <macaddr> | all] | blocked [all | vlan_name <vlan_name> mac_address <macaddr>]]

Parameters

ip_mac - Specifies the user created IMPB database. **ipaddress** - Specifies the learned IP address of the entry in the database. **<ipaddr>** - Enter the IP address used here. **mac_address** - Specifies the MAC address used for this configuration. **<macaddr>** - Enter the MAC address used here. **all** - Specifies that all the MAC address will be used.
blocked - Specifies the address database that the system has automatically learned and blocked. **all** - Specifies that all the entries will be used. **vlan_name** - Specifies the name of the VLAN to which the blocked MAC address belongs. **<vlan_name>** - Enter the VLAN name here. **mac_address** - Specifies the MAC address of the entry or the blocked MAC address. **<macaddr>** - Enter the MAC address used here.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete an IMPB entry:

```
DAS-3626:admin# delete address_binding ip_mac ipaddress 10.1.1.1 mac_address
00-00-00-00-00-11
Command: delete address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-
00-00-11

Success.

DAS-3626:admin#
```

To delete a blocked address:

```
DAS-3626:admin# delete address_binding blocked vlan_name v31 mac_address 00-00-
00-00-00-11
Command: delete address_binding blocked vlan_name v31 mac_address 00-00-00-00-
00-11

Success.

DAS-3626:admin#
```

16-4 config address_binding ip_mac ipaddress

Description

This command is used to update an IMPB entry.

Format

config address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports [<portlist> | all] | bonding <bgroup_list>}

Parameters

<ipaddr> - Enter the IP address used here.
mac_address - Specifies the MAC address of the entry being updated. **<macaddr>** - Enter the MAC address used here.
ports - (Optional) Specifies which ports are used for the IMPB entry being updated. If not specified, then it is applied to all ports. **<portlist>** - Enter the list of port used here. **all** - Specifies that all the ports will be used.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure an IMPB entry:

```
DAS-3626:admin# config address_binding ip_mac ipaddress 10.1.1.1 mac_address
00-00-00-00-00-11
Command: config address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-
00-00-11

Success.

DAS-3626:admin#
```

16-5 config address_binding ip_mac bonding

Description

This command is used to configure the state of IMPB on the Switch for each VDSL bonding group.

Format

config address_binding ip_mac bonding <bgroup_list> {arp_inspection [strict | loose | disable] | ip_inspection [enable | disable] | protocol [ipv4] | allow_zeroip [enable | disable] | forward_dhcppkt [enable | disable] | stop_learning_threshold <int 0-500>}(1)

Parameters

<bgroup_list> - Enter a list of VDSL bonding groups. The range is from 1 to 12.
arp_inspection - (Optional) Specifies that the ARP inspection option will be configured. **strict** - Specifies that all packets are dropped by default until a legal ARP or IP packets are detected. **loose** - Specifies that all packets are forwarded by default until an illegal ARP or broadcast IP packets are detected. If not specified strict or loose, default is strict. **disable** - Specifies to disable ARP inspection function. The default value is disabled.
ip_inspection - (Optional) Specifies that the IP inspection option will be configured. **enable** - Specifies to enable IP inspection function. The legal IP packets will be forward, while the illegal IP packets will be dropped. **disable** - Specifies to disable IP inspection function. The default value is disabled.
protocol - (Optional) Specifies the version used. **ipv4** - Specifies that only IPv4 packets will be checked.
allow_zeroip - (Optional) Specifies whether to allow ARP packets with a source IP address of 0.0.0.0. If the IP address 0.0.0.0 is not configured in the binding list and this setting is enabled, ARP packets with the source IP address of 0.0.0.0 will be allowed; If the IP address 0.0.0.0 is not configured in the binding list and this setting is disabled, ARP packets with the source IP address of 0.0.0.0 will not be allowed. This option does not affect the IMPB ACL Mode. **enable** - Specifies that the allow zero IP option will be enabled. **disable** - Specifies that the allow zero IP option will be disabled.
forward_dhcppkt - (Optional) Specifies to enable or disable the forward DHCP packets option. By default, DHCP packets with a broadcast DA will be flooded. When set to disabled, the broadcast DHCP packet received by the specified bonding group will not be forwarded. This setting is effective when DHCP Snooping is enabled, in this case DHCP packets trapped by the CPU must be forwarded by the software. This setting controls the forwarding behavior in

this situation.
enable - Specifies that the forward DHCP packets option will be enabled.
disable - Specifies that the forward DHCP packets option will be disabled.

stop_learning_threshold - (Optional) Specifies the stop learning threshold. When the number of blocked entries exceeds the threshold, the bonding group will stop learning new addresses. Packets with a new address will be dropped.
<int 0-500> - Enter the stop learning threshold value here. This value must be between 0 and 500.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the ARP inspection state of IMBP for VDSL bonding group 2 to disable:

```
DAS-3626:admin#config address_binding ip_mac bonding 2 arp_inspection disable
Command: config address_binding ip_mac bonding 2 arp_inspection disable

Success.

DAS-3626:admin#
```

16-6 show address_binding

Description

This command is used to display the IMPB entries, blocked MAC entries and port status.

Format

show address_binding [ip_mac [all | ipaddress <ipaddr> mac_address <macaddr>] | blocked [all | vlan_name <vlan_name> mac_address <macaddr>] | ports {<portlist>} | bonding <bgroup_list>]

Parameters

ip_mac -Specifies the user created IMPB database.
all - Specifies that all the IP addresses will be used.
ipaddress - Specifies the learned IP address of the entry in the database.
<ipaddr> - Enter the learned IP address here.
mac_address - Specifies the MAC address of the entry in the database.
<macaddr> - Enter the MAC address here.

blocked - Specifies the addresses in the database that the system has auto learned and blocked.
all - Specifies that all the MAC addresses will be used.
vlan_name - Specifies the name of the VLAN to which the blocked MAC address belongs.
<vlan_name> - Enter the VLAN name used here.
mac_address - Specifies the MAC address of the entry or the blocked MAC address.
<macaddr> - Enter the MAC address of the entry or the blocked MAC address.

ports - Specifies the ports for which the information is displayed. If not specified, all ports are displayed.
<portlist> - (Optional) Enter the list of ports used here.

bonding - Specifies a list of VDSL bonding groups.
<bgroup_list> - Enter a list of VDSL bonding groups. The range is from 1 to 12.

Restrictions

None.

Example

To show the IMPB global configuration:

```
DAS-3626:admin#show address_binding
Command: show address_binding

Trap/Log          : Disabled
DHCP Snoop        : Disabled

DAS-3626:admin#
```

To show the IMPB ports:

```
DAS-3626:admin#show address_binding ports
Command: show address_binding ports


 ARP: ARP Inspection   IP: IP Inspection

 Port   ARP      IP     Protocol Zero IP   DHCP Packet  Stop Learning
                                                       Threshold/Mode
 ----- -------- --------  ----- ---------  -----------  --------------
 1     Strict   Disabled  IPv4  Not Allow  Forward      500/Normal
 2     Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 3     Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 4     Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 5     Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 6     Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 7     Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 8     Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 9     Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 10    Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 11    Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 12    Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 13    Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 14    Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 15    Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
 16    Disabled Disabled  IPv4  Not Allow  Forward      500/Normal
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

To show IMPB entries:

```
DAS-3626:admin#show address_binding ip_mac all
Command: show address_binding ip_mac all

 M(Mode) - D:DHCP, S:Static ACL - A:Active I:Inactive

 IP Address                              MAC Address       M  ACL Ports
 --------------------------------------- ----------------- -- -- --------------
 10.1.1.1                                00-00-00-00-00-11 S  I  1-26

Total Entries : 1

DAS-3626:admin#
```

To show the IMPB entries that are blocked:

```
DAS-3626:admin#show address_binding blocked all
Command: show address_binding blocked all

 VID  VLAN Name                         MAC Address       Port
 ---- -------------------------------- ----------------- ----
 1     default                         00-01-02-03-29-38 7
 1     default                         00-0C-6E-5C-67-F4 7
 1     default                         00-0C-F8-20-90-01 7
 1     default                         00-0E-35-C7-FA-3F 7

Total entries : 4

DAS-3626:admin#
```

16-7 enable address_binding dhcp_snoop

Description

This command is used to enable DHCP snooping mode.

By default, DHCP snooping is disabled.

If a user enables DHCP Snooping mode, all ports which have IMPB disabled will become server ports. The switch will learn the IP addresses through server ports (by using DHCP Offer and DHCP ACK packets).

Note that the DHCP discover packet cannot be passed thru the user ports if the allow_zeroip function is disabled on the port.

The auto-learned IMPB entry will be mapped to a specific source port based on the MAC address learning function. This entry will be created as an IP-Inspection mode binding entry for this specific port. Each entry is associated with a lease time. When the lease time has expires, the expired entry will be removed from the port. The auto-learned binding entry can be moved from one port to another port if the DHCP snooping function has learned that the MAC address has moved to a different port.

If a situation occurs where a binding entry learned by DHCP snooping conflicts with a statically configured entry. The binding relation has conflicted. For example, if IP A is binded to MAC X with a static configuration and suppose that the binding entry learned by DHCP snooping is that IP A is

bound to MAC Y, and then it is conflict. When the DHCP snooping learned entry binds with the static configured entry, and the DHCP snooping learned entry will not be created.

In a situation where the same IMPB pair has been statically configured, the auto-learned entry will not be created. In a situation where the learned information is consistent with the statically configured entry the auto-learned entry will not be created. In a situation where the entry is statically configured in ARP mode the auto learned entry will not be created. In a situation where the entry is statically configured on one port and the entry is auto-learned on another port, the auto-learned entry will not be created.

Format

enable address_binding dhcp_snoop

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable DHCP IPv4 snooping mode:

```
DAS-3626:admin# enable address_binding dhcp_snoop
Command: enable address_binding dhcp_snoop

Success.

DAS-3626:admin#
```

16-8 disable address_binding dhcp_snoop

Description

This command is used to disable DHCP snooping mode. When the DHCP snooping function is disabled, all of the auto-learned binding entries will be removed.

Format

disable address_binding dhcp_snoop

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable DHCP IPv4 snooping mode:

```
DAS-3626:admin# disable address_binding dhcp_snoop
Command: disable address_binding dhcp_snoop

Success.

DAS-3626:admin#
```

16-9 clear address_binding dhcp_snoop binding_entry

Description

This command is used to clear the DHCP snooping entries learned for the specified ports.

Format

clear address_binding dhcp_snoop binding_entry [ports [<portlist> | all] | bonding <bgroup_list>]

Parameters

ports - Specifes a list of ports. **<portlist>** - Enter the list of ports to clear the DHCP snooping learned entries. **all** - Specifies all the ports to clear the DHCP snooping learned entries.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.

Restrictions

Only Administrators and Operators can issue this command.

Example

To clear DHCP IPv4 snooping entries on ports 1-3:

```
DAS-3626:admin# clear address_binding dhcp_snoop binding_entry ports 1-3
Command: clear address_binding dhcp_snoop binding_entry ports 1-3

Success.

DAS-3626:admin#
```

16-10 show address_binding dhcp_snoop

Description

This command is used to display the DHCP snooping configuration and learning database. If no parameter is specified, the command will display the enable/disable state.

Format

show address_binding dhcp_snoop {max_entry {ports <portlist> | bonding <bgroup_list>}}

Parameters

max_entry - (Optional) Specifies to show the maximum number of entries per port.
ports - (Optional) Specifies the ports used for this configuration.
<portlist> - Enter a list of ports used here.
bonding - (Optional) Specifies a list of VDSL bonding groups.
<bgroup_list> - Enter a list of VDSL bonding groups. The range is from 1 to 12.

Restrictions

None.

Example

To show the DHCP snooping state:

```
DAS-3626:admin#show address_binding dhcp_snoop
Command: show address_binding dhcp_snoop

DHCP Snoop(IPv4) : Enabled

DAS-3626:admin#
```

To display DHCP snooping maximun entry configuration:

```
DAS-3626:admin#show address_binding dhcp_snoop max_entry
Command: show address_binding dhcp_snoop max_entry

Port  Max Entry
----  ---------
1     No Limit
2     No Limit
3     No Limit
4     No Limit
5     No Limit
6     No Limit
7     No Limit
8     No Limit
9     No Limit
10    No Limit
11    No Limit
12    No Limit
13    No Limit
14    No Limit
15    No Limit
16    No Limit
17    No Limit
18    No Limit
19    No Limit
20    No Limit
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

16-11 show address_binding dhcp_snoop binding_entry

Description

This command is used to display the DHCP snooping binding entries.

Format

show address_binding dhcp_snoop binding_entry {port <port> | bonding_group <bgroup>}

Parameters

port - (Optional) Specifies the port used for this configuration. **<port>** - Enter the port number used here.
bonding_group - (Optional) Specifies a VDSL bonding group. **<bgroup>** - Enter a VDSL bonding group. The range is from 1 to 12.

Restrictions

None.

Example

To display the DHCP snooping binding entries:

```
DAS-3626:admin#show address_binding dhcp_snoop binding_entry
Command: show address_binding dhcp_snoop binding_entry

 S (Status) - A: Active, I: Inactive
 Time - Left Time (sec)

 IP Address                              MAC Address       S  LT(sec)    Port
 --------------------------------------- ----------------- -- ---------- -----
 10.62.58.35                             00-0B-5D-05-34-0B A  35964      1
 10.33.53.82                             00-20-c3-56-b2-ef I  2590       2

Total entries : 2

DAS-3626:admin#
```

16-12 config address_binding dhcp_snoop max_entry

Description

This command is used to specify the maximum number of entries that can be learned by a specified port.

Format

config address_binding dhcp_snoop max_entry [ports [<portlist> | all] | bonding <bgroup_list>] limit [<value 1-50> | no_limit]

Parameters

ports - Specifies the list of ports you would like to set the maximum number of entries that can be learned. **<portlist>** - Enter the list of ports used here. **all** - Specifies that all the ports will be used.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
limit - Specifies the maximum number. **<value 1-50>** - Enter the limit value here. This value must be between 1 and 50. **no_limit** - Specifies that the maximum number of learned entries is unlimited.

Restrictions

Only Administrators and Operators can issue this command.

Example

To set the maximum number of DHCP IPv4 snooping entries that ports 1–3 can learned to 10:

```
DAS-3626:admin#config address_binding dhcp_snoop max_entry ports 1-3 limit 10
Command: config address_binding dhcp_snoop max_entry ports 1-3 limit 10

Success.

DAS-3626:admin#
```

16-13 enable address_binding trap_log

Description

This command is used to send traps and logs when the IMPB module detects an illegal IP and MAC address.

Format

enable address_binding trap_log

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable the IMPB traps and logs:

```
DAS-3626:admin#enable address_binding trap_log
Command: enable address_binding trap_log

Success.

DAS-3626:admin#
```

16-14 disable address_binding trap_log

Description

This command is used to disable the IMPB traps and logs.

Format

disable address_binding trap_log

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable IMPB traps and logs:

```
DAS-3626:admin#disable address_binding trap_log
Command: disable address_binding trap_log

Success.

DAS-3626:admin#
```

16-15 config address_binding recover_learning ports

Description

This command is used to recover IMPB checking.

Format

config address_binding recover_learning [ports [<portlist> | all] | bonding <bgroup_list>]

Parameters

ports - Specifes a list of ports. **<portlist>** - Enter the list of port that need to recover the IMPB check. **all** - Specifies all the ports to recover the IMPB check.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.

Restrictions

Only Administrators and Operators can issue this command.

Example

To recover IMPB checking for ports 6 to 7:

```
DAS-3626:admin# config address_binding recover_learning ports 6-7
Command: config address_binding recover_learning ports 6-7

Success.

DAS-3626:admin#
```

Chapter 17 IPv6 Neighbor Discover Command List

create ipv6 neighbor_cache ipif <ipif_name 12> <ipv6addr> <macaddr>
delete ipv6 neighbor_cache ipif [<ipif_name 12> | all] [<ipv6addr> | static | dynamic | all]
show ipv6 neighbor_cache ipif [<ipif_name 12> | all] [ipv6address <ipv6addr> | static | dynamic | all]
config ipv6 nd ns ipif <ipif_name 12> **retrans_time** <millisecond 0-4294967295>
show ipv6 nd {ipif <ipif_name 12>}

17-1 create ipv6 neighbor_cache ipif

Description

This command is used to add a static neighbor on an IPv6 interface.

Format

create ipv6 neighbor_cache ipif <ipif_name 12> <ipv6addr> <macaddr>

Parameters

<ipif_name 12> - Enter the IPv6 interface name here. This name can be up to 12 characters long.
<ipv6addr> - Enter the address of the neighbor.
<macaddr> - Enter the MAC address of the neighbor.

Restrictions

Only Administrators and Operators can issue this command.

Example

Create a static neighbor cache entry:

```
DAS-3626:admin#create ipv6 neighbor_cache ipif System 3ffc::1 00:01:02:03:04:05
Command: create ipv6 neighbor_cache ipif System 3FFC::1 00-01-02-03-04-05

Success.

DAS-3626:admin#
```

17-2 delete ipv6 neighbor_cache ipif

Description

This command is used to delete a neighbor cache entry or static neighbor cache entries from the address cache or all address cache entries on this IP interface. Both static and dynamic entries can be deleted.

Format

delete ipv6 neighbor_cache ipif [<ipif_name 12> | all] [<ipv6addr> | static | dynamic | all]

Parameters

<ipif_name 12> - Enter the IPv6 interface name here. This name can be up to 12 characters long.
all - Specifies that all the interfaces will be used in this configuration.
<ipv6addr> - Enter the neighbor's address.
static - Specifies to delete the static entry.
dynamic - Specifies to delete the dynamic entries.
all - Specifies that all entries include static and dynamic entries will be deleted.

Restrictions

Only Administrators and Operators can issue this command.

Example

Delete a neighbor cache.entry on IP interface "System":

```
DAS-3626:admin# delete ipv6 neighbor_cache ipif System 3ffc::1
Command: delete ipv6 neighbor_cache ipif System 3FFC::1

Success.

DAS-3626:admin#
```

17-3 show ipv6 neighbor_cache ipif

Description

This command is used to display the neighbor cache entry for the specified interface. You can display a specific entry, all entries, or all static entries.

Format

show ipv6 neighbor_cache ipif [<ipif_name 12> | all] [ipv6address <ipv6addr> | static | dynamic | all]

Parameters

<ipif_name 12> - Enter the IPv6 interface name here. This name can be up to 12 characters long.
all - Specifies that all the interface will be displayed.
ipv6address - Enter the neighbor's address. **<ipv6addr>** - Enter the IPv6 address here.
static - Specifies to display the static neighbor cacheentry.
dynamic - Specifies to display the dynamic entries.
all - Specifies that all entries include static and dynamic entries will be displayed.

Restrictions

None.

Example

Show all neighbor cache entries of IP interface “System”:

```
DAS-3626:admin#show ipv6 neighbor_cache ipif System all
Command: show ipv6 neighbor_cache ipif System all

Neighbor                                 Link Layer Address Interface    State
---------------------------------------  ------------------ ------------ -----
3FFC::1                                  00-01-02-03-04-05  System       T

Total Entries: 1

State:
(I) means Incomplete state. (R) means Reachable state.
(S) means Stale state.      (D) means Delay state.
(P) means Probe state.      (T) means Static state.


DAS-3626:admin#
```

17-4 config ipv6 nd ns retrans_time ipif

Description

This command is used to configure the IPv6 ND neighbor solicitation retransmit time, which is between retransmissions of neighbor solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor.

Format

config ipv6 nd ns ipif <ipif_name 12> retrans_time <millisecond 0-4294967295>

Parameters

<ipif_name 12> - Enter the IPv6 interface name here. This name can be up to 12 characters long.
retrans_time - Specifies to neighbor solicitation’s re-transmit timer in millisecond. **<millisecond 0-4294967295>** - Enter the re-transmit timer value here. This value must be between 0 and 4294967295 milliseconds.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the retrans_time of IPv6 ND neighbor solicitation:

```
DAS-3626:admin#config ipv6 nd ns ipif System retrans_time 1000000
Command: config ipv6 nd ns ipif System retrans_time 1000000

Success.

DAS-3626:admin#
```

17-5 show ipv6 nd

Description

This command is used to display information regarding neighbor detection on the switch. If no IP interface is specified, it will show the IPv6 ND related configuration of all interfaces.

Format

show ipv6 nd {ipif <ipif_name 12>}

Parameters

ipif - (Optional) Specifies to the name of the interface. **<ipif_name 12>** - Enter the IP interface name here. This name can be up to 12 characters long.

Restrictions

Only Administrators and Operators can issue this command.

Example

To show IPv6 ND related configuration:

```
DAS-3626:admin#show ipv6 nd ipif System
Command: show ipv6 nd ipif System

Interface Name            : System
NS Retransmit Time        : 1000000 (ms)

DAS-3626:admin#
```

Chapter 18 IPv6 Route Command List

create ipv6route [default] [<ipif_name 12> <ipv6addr> |<ipv6addr>] {<metric 1-65535>} {[primary | backup]}
delete ipv6route [default] [<ipif_name 12> <ipv6addr> | <ipv6addr> | all]
show ipv6route

18-1 create ipv6route

Description

This command is used to create an IPv6 default route. If the next hop is a global address, it is not needed to indicate the interface name. If the next hop is a link local address, then the interface name must be specified.

Format

create ipv6route [default] [<ipif_name 12> <ipv6addr> |<ipv6addr>] {<metric 1-65535>} {[primary | backup]}

Parameters

default - Specifies the default route.
<ipif_name 12> - Enter the interface for the route. This name can be up to 12 characters long. **<ipv6addr>** - Enter the next hop address for this route.
<ipv6addr> - Enter the next hop address for this route.
<metric 1-65535> - (Optional) Enter the metric value here. The default setting is 1. This value must between 1 and 65535.
primary - (Optional) Specifies the route as the primary route to the destination.
backup - (Optional) Specifies the route as the backup route to the destination. The backup route can only be added when the primary route exists. If the route is not specified as the primary route or the backup route, then it will be auto-assigned by the system. The first created is the primary, the second created is the backup.

Restrictions

Only Administrators and Operators can issue this command.

Example

To create and IPv6 route:

```
DAS-3626:admin# create ipv6route default System 3FFC:: 1 primary
Command: create ipv6route default System 3FFC:: 1 primary

Success.

DAS-3626:admin#
```

18-2 delete ipv6route

Description

This command is used to delete an IPv6 static route. If the next hop is a global address, it is not needed to indicate the interface name. If the next hop is a link local address, then the interface name must be specified.

Format

delete ipv6route [default] [<ipif_name 12> <ipv6addr> | <ipv6addr> | all]

Parameters

default - Specifies the default route.
<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long. **<ipv6addr>** - Enter the next hop address for this route.
<ipv6addr> - Specifies the next hop address for the default route.
all - Specifies that all static created routes will be deleted.

Restrictions

Only Administrators and Operators can issue this command.

Example

Delete an IPv6 static route:

```
DAS-3626:admin# delete ipv6route default System 3FFC::
Command: delete ipv6route default System 3FFC::

Success.

DAS-3626:admin#
```

18-3 show ipv6route

Description

This command is used to display IPv6 routes.

Format

show ipv6route

Parameters

None.

Restrictions

None.

Example

Show all the IPv6 routes:

```
DAS-3626:admin#show ipv6route
Command: show ipv6route

IPv6 Prefix: ::/0                              Protocol: Static  Metric: 1
Next Hop   : 3001::254                         IPIF    : System
Backup     : Primary                           Status  : Inactive

Total Entries: 1

DAS-3626:admin#
```

Chapter 19 Jumbo Frame Command List

enable jumbo_frame
disable jumbo_frame
show jumbo_frame

19-1 enable jumbo_frame

Description

This command is used to configure the jumbo frame setting as enable.

Format

enable jumbo_frame

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable the Jumbo frame:

```
DAS-3626:admin#enable jumbo_frame
Command: enable jumbo_frame

The maximum size of jumbo frame is 13312 bytes.
Success.

DAS-3626:admin#
```

19-2 disable jumbo_frame

Description

This command is used to configure the jumbo frame setting as disable.

Format

disable jumbo_frame

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable the Jumbo frame:

```
DAS-3626:admin# disable jumbo_frame
Command: disable jumbo_frame

Success.

DAS-3626:admin#
```

19-3 show jumbo_frame

Description

This command is used to display the current configuration of jumbo frame.

Format

show jumbo_frame

Parameters

None.

Restrictions

None.

Example

To show the Jumbo frame:

```
DAS-3626:admin#show jumbo_frame
Command: show jumbo_frame

Jumbo Frame State  : Enabled
Maximum Jumbo Frame Size : 13312 Bytes


DAS-3626:admin#
```

Chapter 20 Link Aggregation Command List

create link_aggregation group_id <value 1> {type [lacp | static]}
delete link_aggregation group_id <value 1>
config link_aggregation group_id <value 1> {master_port <port> | ports <portlist> | state [enabled | disabled]}
config link_aggregation algorithm [mac_source | mac_destination | mac_source_dest | ip_source | ip_destination | ip_source_dest | l4_src_port | l4_dest_port | l4_src_dest_port]
show link_aggregation {group_id <value 1> | algorithm}
config lacp_port <portlist> mode [active | passive]
show lacp_port {<portlist>}

20-1 create link_aggregation group_id

Description

This command is used to create a link aggregation group on the switch.

Format

create link_aggregation group_id <value 1> {type [lacp | static]}

Parameters

<value 1> - Enter the group ID value here.
type - (Optional) Specifies the group type is belong to static or LACP. If type is not specified, the default is static type. **lacp** - Specifies to use LACP as the group type. **static** - Specifies to use static as the group type.

Restrictions

Only Administrators and Operators can issue this command.

Example

To create link aggregation group:

```
DAS-3626:admin# create link_aggregation group_id 1 type lacp
Command: create link_aggregation group_id 1 type lacp

Success.

DAS-3626:admin#
```

20-2 delete link_aggregation group_id

Description

This command is used to delete a previously configured link aggregation group.

Format

delete link_aggregation group_id <value 1>

Parameters

<value 1> - Enter the group ID value here.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete link aggregation group:

```
DAS-3626:admin# delete link_aggregation group_id 1
Command: delete link_aggregation group_id 1

Success.

DAS-3626:admin#
```

20-3 config link_aggregation group_id

Description

This command is used to configure a previously created link aggregation group.

Format

config link_aggregation group_id <value 1> {master_port <port> | ports <portlist> | state [enabled | disabled]}

Parameters

<value 1> - Enter the group ID value here.
master_port - (Optional) Specifies the master port ID. Specifies which port (by port number) of the link aggregation group will be the master port. All of the ports in a link aggregation group will share the port configuration with the master port. **<port>** - Enter the master port number here.
ports - (Optional) Specifies a range of ports that will belong to the link aggregation group. **<portlist>** - Enter the list of port used for the configuration here.
state - (Optional) Specifies to enable or disable the specified link aggregation group. If not specified, the group will keep the previous state, the default state is disabled. If configure LACP group, the ports' state machine will start. **enable** - Specifies to enable the specified link aggregation group. **disable** - Specifies to disable the specified link aggregation group.

Restrictions

Only Administrators and Operators can issue this command.

Example

To define a load-sharing group of ports, group-id 1, master port 25:

```
DAS-3626:admin#config link_aggregation group_id 1 master_port 25 ports 25-26
Command: config link_aggregation group_id 1 master_port 25 ports 25-26

Success.

DAS-3626:admin#
```

20-4 config link_aggregation algorithm

Description

This command is used to configure the part of the packet examined by the switch when selecting the egress port for transmitting load-sharing data. This feature is available using the address-based load-sharing algorithm, only.

Format

config link_aggregation algorithm [mac_source | mac_destination | mac_source_dest | ip_source | ip_destination | ip_source_dest | l4_src_port | l4_dest_port | l4_src_dest_port]

Parameters

mac_source - Specifies that the Switch should examine the MAC source address.
mac_destination - Specifies that the Switch should examine the MAC destination address.
mac_source_dest - Specifies that the Switch should examine the MAC source and destination address.
ip_source - Specifies that the Switch should examine the IP source address.
ip_destination - Specifies that the Switch should examine the IP destination address.
ip_source_dest - Specifies that the Switch should examine the IP source address and destination address.
l4_src_port - Specifies that the Switch should examine the TCP/UDP source port.
l4_dest_port - Specifies that the Switch should examine the TCP/UDP destination port.
l4_src_dest_port - Specifies that the Switch should examine the TCP/UDP source port and destination port.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure link aggregation algorithm for mac-source-dest:

```
DAS-3626:admin# config link_aggregation algorithm mac_source_dest
Command: config link_aggregation algorithm mac_source_dest

Success.

DAS-3626:admin#
```

20-5 show link_aggregation

Description

This command is used to display the current link aggregation configuration on the switch. If no parameter is specified, all link aggregation information will be displayed.

Format

show link_aggregation {group_id <value 1> | algorithm}

Parameters

group_id - (Optional) Specifies the group id. The group number identifies each of the groups. **<value 1>** - Enter the group ID value here.
algorithm - (Optional) Specifies to display the link aggregation by the algorithm in use.

Restrictions

None.

Example

To display link aggregation status:

```
DAS-3626:admin#show link_aggregation
Command: show link_aggregation

Link Aggregation Algorithm = MAC-Source

Group ID      : 1
Type          : LACP
Master Port   : 25
Member Port   : 25-26
Active Port   :
Status        : Enabled
Flooding Port :

Total Entries : 1

DAS-3626:admin#
```

20-6 config lacp_port

Description

This command is used to configure per-port LACP mode.

Format

config lacp_port <portlist> mode [active | passive]

Parameters

<portlist> - Enter the list of port used for the configuration here.
mode - Specifies the LACP mode used. **active** - Specifies to set the LACP mode as active. **passive** - Specifies to set the LACP mode as passive.

Restrictions

Only Administrators and Operators can issue this command.

Example

To config port LACP mode:

```
DAS-3626:admin#config lacp_port 25 mode active
Command: config lacp_port 25 mode active

Success.

DAS-3626:admin#
```

20-7 show lacp_port

Description

This command is used to display the current mode of LACP of the ports. If no parameter is specified, the system will display current LACP and all port status.

Format

show lacp_port {<portlist>}

Parameters

<portlist> - (Optional) Enter a list of ports to be displayed.

Restrictions

None.

Example

To show port lacp mode:

```
DAS-3626:admin#show lacp_port
Command: show lacp_port


 Port     Activity

 -----    --------
 25       Active
 26       Passive

DAS-3626:admin#
```

Chapter 21 Loop Back Detection (LBD) Command List

config loopdetect {recover_timer [<value 0> | <sec 60-1000000>] | interval <sec 1-32767>}
config loopdetect ports [<portlist> | all] state [enable | disable]
enable loopdetect
disable loopdetect
show loopdetect
show loopdetect ports {<portlist>}
config loopdetect trap [none | loop_detected | loop_cleared | both]
config loopdetect log state [enable | disable]

21-1 config loopdetect

Description

This command is used to setup the loop-back detection function (LBD) for the entire Switch.

Format

config loopdetect {recover_timer [<value 0> | <sec 60-1000000>] | interval <sec 1-32767>}

Parameters

recover_timer - (Optional) Specifies the time interval (in seconds) used by the Auto-Recovery mechanism to decide how long to check before determining that the loop status has gone. The default value for the recover timer is 60 seconds.
- **<value 0>** - Enter 0 for the time interval. 0 is a special value that the auto-recovery mechanism should be disabled. When the auto-recovery mechanism is disabled, a user would need to manually recover a disabled port.
- **<sec 60-1000000>** - Enter the recovery timer value here. This value must be between 60 and 1000000 seconds.

interval - (Optional) Specifies the time interval (in seconds) that the device will transmit all the CTP (Configuration Test Protocol) packets to detect a loop-back event. The default setting is 10 seconds.
- **<sec - 1-32767>** - Enter the time interval value here. This value must be between 1 and 32767 seconds.

Restrictions

Only Administrators and Operators can issue this command.

Example

To set the auto-recover time to 0, which disables the auto-recovery mechanism, the interval to 20 seconds:

```
DAS-3626:admin#config loopdetect recover_timer 0 interval 20
Command: config loopdetect recover_timer 0 interval 20

Success.

DAS-3626:admin#
```

21-2 config loopdetect ports

Description

This command is used to setup the loop-back detection function for the interfaces on the Switch.

Format

config loopdetect ports [<portlist> | all] state [enable | disable]

Parameters

<portlist> - Enter a list of ports that LBD will be configured on.
all - Specifies all ports in the system to be configured.
state - Specifies whether the LBD function should be enabled or disabled on the ports specified in the port list. The default state is disabled. **enable** - Specifies to enable the LBD function. **disable** - Specifies to disable the LBD function.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable the LBD function on ports 1-5:

```
DAS-3626:admin#config loopdetect ports 1-5 state enable
Command: config loopdetect ports 1-5 state enable

Success.

DAS-3626:admin#
```

21-3 enable loopdetect

Description

This command is used to enable the LBD function globally on the Switch. The default state is disabled.

Format

enable loopdetect

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable the LBD function globally:

```
DAS-3626:admin#enable loopdetect
Command: enable loopdetect

Success.

DAS-3626:admin#
```

21-4 disable loopdetect

Description

This command is used to disable the LBD function globally on the Switch.

Format

disable loopdetect

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable the LBD function globally:

```
DAS-3626:admin# disable loopdetect
Command: disable loopdetect

Success.

DAS-3626:admin#
```

21-5 show loopdetect

Description

This command is used to display the LBD global configuration.

Format

show loopdetect

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To show the LBD global settings:

```
DAS-3626:admin#show loopdetect
Command: show loopdetect

 LBD Global Settings
 ---------------------------
 Status         : Enabled
 Interval       : 20 sec
 Recover Time   : 0 sec
 Trap State     : None
 Log State      : Enabled

DAS-3626:admin#
```

21-6 show loopdetect ports

Description

This command is used to display the LBD per-port configuration. If no parameter is specified, the configuration for all ports will be displayed.

Format

show loopdetect ports {<portlist>}

Parameters

<portlist> - (Optional) Enter the list of port to be displayed.

Restrictions

None.

Example

To show the LBD settings on ports 1-9:

```
DAS-3626:admin#show loopdetect ports 1-9
Command: show loopdetect ports 1-9

Port   Loopdetect State  Loop Status  LoopDetected Time    LoopRecovered Time
------ ----------------- ------------ -------------------- -------------------
1      Enabled           Normal       -                    -
2      Enabled           Normal       -                    -
3      Enabled           Normal       -                    -
4      Enabled           Normal       -                    -
5      Enabled           Normal       -                    -
6      Disabled          Normal       -                    -
7      Disabled          Normal       -                    -
8      Disabled          Normal       -                    -
9      Disabled          Normal       -                    -



CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

21-7 config loopdetect trap

Description

This command is used to configure the trap modes for LBD.

Format

config loopdetect trap [none | loop_detected | loop_cleared | both]

Parameters

none - Specifies that there is no trap in the LBD function.
loop_detected - Specifies that the trap will only be sent when the loop condition is detected.
loop_cleared - Specifies that the trap will only be sent when the loop condition is cleared.
both - Specifies that the trap will either be sent when the loop condition is detected or cleared.

Restrictions

Only Administrators and Operators can issue this command.

Example

To specify that traps will be sent when the loop condition is detected or cleared:

```
DAS-3626:admin# config loopdetect trap both
Command: config loopdetect trap both

Success.

DAS-3626:admin#
```

21-8 config loopdetect log state

Description

This command is used to configure the log state for LBD. The default value is enabled.

Format

config loopdetect log state [enable | disable]

Parameters

enable - Specifies to enable the LBD log feature.
disable - Specifies to disable the LBD log feature. All LBD-related logs will not be recorded.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable the log state for LBD:

```
DAS-3626:admin# config loopdetect log state enable
Command: config loopdetect log state enable

Success.

DAS-3626:admin#
```

Chapter 22 MAC-based VLAN Command List

create mac_based_vlan mac_address <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]
delete mac_based_vlan {mac_address <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}
show mac_based_vlan {mac_address <macaddr> | [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}

22-1 create mac_based_vlan mac_address

Description

This command is used to create MAC-based VLAN entries. There is a global limitation of the maximum entries supported for the static MAC-based entry.

Format

create mac_based_vlan mac_address <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]

Parameters

<macaddr> - Enter the MAC address here.
vlan - Specifies the VLAN to be associated with the MAC address. **<vlan_name 32>** - Enter the VLAN name here. This name can be up to 32 characters long.
vlanid - Specifies the VLAN by VLAN ID. **<vlanid 1-4094>** - Enter the VLAN ID here. This value must be between 1 and 4094.

Restrictions

Only Administrators and Operators can issue this command.

Example

To create a static MAC-based VLAN entry:

```
DAS-3626:admin# create mac_based_vlan mac_address 00-11-22-33-44-55 vlanid 100
Command: create mac_based_vlan mac_address 00-11-22-33-44-55 vlanid 100

Success.

DAS-3626:admin#
```

22-2 delete mac_based_vlan

Description

This command is used to delete the static MAC-based VLAN entry. If no parameter is specified, ALL static configured entries will be removed.

Format

delete mac_based_vlan {mac_address <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}

Parameters

mac_address - (Optional) Specifies the MAC address used.
<macaddr> - Enter the MAC address used here.
vlan - Specifies the VLAN to be associated with the MAC address.
<vlan_name 32> - Enter the VLAN name here. This name can be up to 32 characters long.
vlanid - (Optional) Specifies the VLAN by VLAN ID.
<vlanid 1-4094> - Enter the VLAN ID here. This value must be between 1 and 4094.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete a static MAC-based VLAN entry:

```
DAS-3626:admin# delete mac_based_vlan mac_address 00-11-22-33-44-55 vlanid 100
Command: delete mac_based_vlan mac_address 00-11-22-33-44-55 vlanid 100

Success.

DAS-3626:admin#
```

22-3 show mac_based_vlan

Description

This command is used to display the static MAC-Based VLAN entry. If the MAC address and VLAN is not specified, all static entries will be displayed.

Format

show mac_based_vlan {mac_address <macaddr> | [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}

Parameters

mac_address - (Optional) Specifies the entry that you would like to display.
<macaddr> - Enter the MAC address used here.

vlan - (Optional) Specifies the VLAN that you would like to display. **<vlan_name 32>** - Enter the VLAN name here. This name can be up to 32 characters long.
vlanid - (Optional) Specifies the VLAN by VLAN ID. **<vlanid 1-4094>** - Enter the VLAN ID here. This value must be between 1 and 4094.

Restrictions

None.

Example

To display the MAC-based VLAN entry:

```
DAS-3626:admin#show mac_based_vlan
Command: show mac_based_vlan

 MAC Address         VLAN ID   Status      Type
 ------------------  --------  ----------  ------------------------------
 00-11-22-33-44-55   100       Active      Static

Total Entries : 1

DAS-3626:admin#
```

Chapter 23 MAC Spoofing Command List

config mac_spoof_detect port <portlist> state [enable | disable]
show mac_spoof_detect state

23-1 config mac_spoof_detect port

Description

This command is used to configure the MAC spoofing detect state on each port. When enabled, the port cannot move and its FDB entry will age out when the time expires.

Format

config mac_spoof_detect port <portlist> state [enable | disable]

Parameters

<portlist> - Enter a list of ports to be configured.
state - Specifies the MAC spoofing detect state. **enable** - Specifies to enable the MAC spoofing detect state. **disable** - Specifies to disable the MAC spoofing detect state.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable the the MAC spoofing detect state on port 1:

```
DAS-3626:admin#config mac_spoof_detect port 1 state enable
Command: config mac_spoof_detect port 1 state enable

Success.

DAS-3626:admin#
```

23-2 show mac_spoof_detect state

Description

This command is used to display the MAC spoofing detect state.

Format

show mac_spoof_detect state

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To display the MAC spoofing detect state:

```
DAS-3626:admin#show mac_spoof_detect state
Command: show mac_spoof_detect state

Port 1      : Enable
Port 2      : Disable
Port 3      : Disable
Port 4      : Disable
Port 5      : Disable
Port 6      : Disable
Port 7      : Disable
Port 8      : Disable
Port 9      : Disable
Port 10     : Disable
Port 11     : Disable
Port 12     : Disable
Port 13     : Disable
Port 14     : Disable
Port 15     : Disable
Port 16     : Disable
Port 17     : Disable
Port 18     : Disable
Port 19     : Disable
Port 20     : Disable
Port 21     : Disable
Port 22     : Disable
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

Chapter 24 Mirror Command List

config mirror port <port> {[add | delete] source ports <portlist> [rx | tx | both]}
enable mirror
disable mirror
show mirror

24-1 config mirror port

Description

This command is used to configure a mirror port, source port pair on the Switch. Traffic from any source port to a target port can be mirrored for real-time analysis. A logic analyzer or an RMON probe then can be attached to study the traffic crossing the source port in a completely unobtrusive manner. When mirroring port traffic, please note that the target port must be configured in the same VLAN and operates at the same speed as the source port. If the target port is operating at a lower speed, the source port will be forced to drop its operating speed to match that of the target port.

Format

config mirror port <port> {[add | delete] source ports <portlist> [rx | tx | both]}

Parameters

<port> - Enter the port number that will receive the packets duplicated at the mirror port.
add - (Optional) Specifies to add the mirror entry.
delete - (Optional) Specifies to delete the mirror entry.
source ports - (Optional) Specifies the port that will be mirrored. All packets entering and leaving the source port can be duplicated in the mirror port. **<portlist>** - Enter the list of port to be configured here.
rx - (Optional) Specifies to allow the mirroring packets received (flowing into) by the port or ports in the port list.
tx - (Optional) Specifies to allow the mirroring packets sent (flowing out of) by the port or ports in the port list.
both - (Optional) Specifies to mirror all the packets received or sent by the port or ports in the port list.

Restrictions

Only Administrators and Operators can issue this command.

Example

To add the mirroring ports:

```
DAS-3626:admin#config mirror port 3 add source ports 7-12 both
Command: config mirror port 3 add source ports 7-12 both

Success.

DAS-3626:admin#
```

24-2 enable mirror

Description

This command is used toenable the mirror function without having to modify the mirror session configuration.

Format

enable mirror

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable mirroring function:

```
DAS-3626:admin# enable mirror
Command: enable mirror

Success.

DAS-3626:admin#
```

24-3 disable mirror

Description

This command is used to disable the mirror function without having to modify the mirror session configuration.

Format

disable mirror

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable mirroring function:

```
DAS-3626:admin# disable mirror
Command: disable mirror

Success.

DAS-3626:admin#
```

24-4 show mirror

Description

This command is used to display the current mirror function state and mirror session configuration on the switch.

Format

show mirror

Parameters

None.

Restrictions

None.

Example

To display mirroring configuration:

```
DAS-3626:admin#show mirror
Command: show mirror

Current Settings
Mirror Status: Enabled
Target Port  : 3
Mirrored Port
           RX: 7-12
           TX: 7-12

DAS-3626:admin#
```

Chapter 25 MLD Snooping Command List

The Multicast Listener Discovery (MLD) is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol. MLDv1 is similar to IGMPv2 and MLDv2 similar to IGMPv3.

config mld_snooping message_limit [ports <portlist> | bonding <bgroup_list> | vlanid <vlanid_list>] [<value 1-1000> | no_limit]
show mld_snooping message_limit [ports <portlist> | bonding <bgroup_list> | vlanid <vlanid_list>]
config mld_snooping [vlan_name <vlan_name 32> | vlanid <vlanid_list> |all] {state [enable | disable] | fast_done [enable | disable] | report_suppression {state [enable | disable]}(1)
config mld_snooping querier [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-7> | last_listener_query_interval <sec 1-25> | state [enable | disable] | version <value 1-2>}(1)
config mld_snooping mrouter_ports [vlan <vlan_name 32> | vlanid <vlanid_list>] [add | delete] [<portlist> | bonding <bgroup_list>]
config mld_snooping mrouter_ports_forbidden [vlan <vlan_name 32> | vlanid <vlanid_list>] [add | delete] [<portlist> | bonding <bgroup_list>]
enable mld_snooping
disable mld_snooping
show mld_snooping {[vlan <vlan_name 32> | vlanid <vlanid_list>]}
show mld_snooping group {[vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist> | bonding <bgroup_list>] {<ipv6addr>}}
show mld_snooping forwarding {[vlan <vlan_name 32> | vlanid <vlanid_list>]}
show mld_snooping mrouter_ports [vlan <vlan_name 32> | vlanid <vlanid_list> | all] {[static | dynamic | forbidden]}
create mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr>
delete mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr>
config mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr> [add | delete] [<portlist> | bonding <bgroup_list>]
show mld_snooping static_group {[vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr>}
show mld_snooping statistic counter [vlan <vlan_name> | vlanid <vlanid_list> | ports <portlist> | bonding <bgroup_list> | group <ipv6group> | per_port <portlist> per_vlan [vlan <vlan_name 32> | vlanid <vidlist>] | per_bonding <bgroup_list> per_vlan [vlan <vlan_name 32> | vlanid <vidlist>]]
clear mld_snooping statistics counter [vlan <vlan_name> | vlanid <vlanid_list> | ports <portlist> | bonding <bgroup_list> | group <group> | per_port <portlist> per_vlan [vlan <vlan_name 32> | vlanid <vidlist>] | per_bonding <bgroup_list> per_vlan [vlan <vlan_name 32> | vlanid <vidlist>]]

25-1 config mld_snooping message_limit

Description

This command is used to configure the rate limit of MLD control packet.

Format

config mld_snooping message_limit [ports <portlist> | bonding <bgroup_list> | vlanid <vlanid_list>] [<value 1-1000> | no_limit]

Parameters

ports - Specifies a list of ports to be configured for the rate limit of MLD control packet. **<portlist>** - Enter a list of ports to be configured.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
vlanid - Specifies a list of VLAN IDs to be configure for the rate limit of MLD control packet. **<vlanid_list>** - Enter the VLAN ID list here.
<value 1-1000> - Enter the message limitation value here. This value must be between 1 and 1000.
no_limit - Specifies that the rate limit of IGMP control packet is unlimited.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the rate limit of MLD control packet:

```
DAS-3626:admin#config mld_snooping message_limit ports 3 100
Command: config mld_snooping message_limit ports 3 100

Success.

DAS-3626:admin#
```

25-2 show mld_snooping message_limit

Description

This command is used to display the rate limit of MLD control packet.

Format

show mld_snooping message_limit [ports <portlist> | bonding <bgroup_list> | vlanid <vlanid_list>]

Parameters

ports - Specifies a list of ports to be displayed. **<portlist>** - Enter a list of ports to be displayed.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
vlanid - Specifies a list of VLANs to be displayed. **<vlanid_list>** - Enter the VLAN ID list here.

Restrictions

None.

Example

To display the message limitation:

```
DAS-3626:admin#show mld_snooping message_limit ports 3
Command: show mld_snooping message_limit ports 3

 Port      Message Limit
 --------  ---------------
 b2        No Limit

Total Entries: 1

DAS-3626:admin#
```

25-3 config mld_snooping

Description

This command is used to configure MLD snooping on the Switch.

Format

config mld_snooping [vlan_name <vlan_name 32> | vlanid <vlanid_list> |all] {state [enable | disable] | fast_done [enable | disable] | report_suppression {state [enable | disable]}(1)

Parameters

vlan - Specifies the name of the VLAN for which MLD snooping is to be configured. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specifies the ID of the VLAN for which MLD snooping is to be configured. **<vlanid_list>** - Enter the VLAN ID list here.
all - Specifies all VLANs for which MLD snooping is to be configured.
state - Specifies to enable or disable MLD snooping for the chosen VLAN. **enable** - Specifies to enable MLD snooping for the chosen VLAN. **disable** - Specifies to disable MLD snooping for the chosen VLAN.
fast_done - Specifies to enable or disable MLD snooping fast_leave function. **enable** - Specifies to enable MLD snooping fast_leave function. If enable, the membership is immediately removed when the system receive the MLD leave message. **disable** - Specifies to disable MLD snooping fast_leave function.
report_suppression - Specifies MLD proxy reporting. **enable** - Specifies to enable the proxy reporting. **disable** - Specifies to disable the proxy reporting.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure MLD snooping:

```
DAS-3626:admin#config mld_snooping vlan default state enable
Command: config mld_snooping vlan default state enable

Success.

DAS-3626:admin#
```

25-4 config mld_snooping querier

Description

This command is used to configure the timer in seconds between general query transmissions, the maximum time in seconds to wait for reports from listeners, and the permitted packet loss that is guaranteed by MLD snooping.

Format

config mld_snooping querier [vlan <vlan_name 32> | vlanid <vlanid_list> | all] {query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-7> | last_listener_query_interval <sec 1-25> | state [enable | disable] | version <value 1-2>}(1)

Parameters

vlan - Specifies the name of the VLAN for which MLD snooping querier is to be configured.
<vlan_name 32> - Enter the VLAN name here. The VLAN name can be up to 32 characters long.

vlanid - Specifies the ID of the VLAN for which MLD snooping querier is to be configured.
<vlanid_list> - Enter the VLAN ID list here.

all - Specifies all VLANs for which MLD snooping querier is to be configured.

query_interval - Specifies the amount of time in seconds between general query transmissions. The default setting is 125 seconds.
<sec 1-65535> - Enter the query interval value here. This value must be between 1 and 65535 seconds.

max_reponse_time - Specifies the maximum time in seconds to wait for reports from listeners. The default setting is 10 seconds.
<sec 1-25> - Enter the maximum response time value here. This value must be between 1 and 25 seconds.

robustness_variable - Specifies to provide fine-tuning to allow for expected packet loss on a subnet. The value of the robustness variable is used in calculating the following MLD message intervals:
<value 1-7> - Enter the robustness variable value here. This value must be between 1 and 7.

- Group listener interval—Amount of time that must pass before a multicast router decides there are no more listeners of a group on a network. This interval is calculated as follows: (robustness variable * query interval) + (1 * query response interval).
- Other querier present interval—Amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the querier. This interval is calculated as follows: (robustness variable * query interval) + (0.5 * query response interval).
- Last listener query count—Number of group-specific queries sent before the router assumes there are no local listeners of a group. The default number is the value of the robustness variable.

- By default, the robustness variable is set to 2. You might want to increase this value if you expect a subnet to be loosely.

last_listener_query_interval - (Optional) Specifies the maximum amount of time between group-specific query messages, including those sent in response to done-group messages. You might lower this interval to reduce the amount of time it takes a router to detect the loss of the last listener of a group.
<sec 1-25> - Enter the last listener query interval value here. This value must be between 1 and 25 seconds.

state - (Optional) Specifies to allow the Switch to be specified as an MLD Querier (sends MLD query packets) or a Non-Querier (does not send MLD query packets). Set to enable or disable.
enable - Enter enable to enable the MLD querier state here.
disable - Enter disable to disable the MLD querier state here.

version - (Optional) Specifies the version of MLD packet that will be sent by this port. If a MLD packet received by the interface has a version higher than the specified version, this packet will be dropped.
<value 1-2> - Enter the version number value here. This value must be between 1 and 2.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the MLD snooping querier:

```
DAS-3626:admin#config mld_snooping querier vlan default query_interval 125
state enable
Command: config mld_snooping querier vlan default query_interval 125 state
enable

Success.

DAS-3626:admin#
```

25-5 config mld_snooping router_ports

Description

This command is used to designate a range of ports as being connected to multicast-enabled routers. This will ensure that all packets with such a router as its destination will reach the multicast-enabled router, regardless of protocol, etc.

Format

config mld_snooping mrouter_ports [vlan <vlan_name 32> | vlanid <vlanid_list>] [add | delete] [<portlist> | bonding <bgroup_list>]

Parameters

vlan - Specifies the name of the VLAN on which the router port resides.
<vlan_name 32> - Enter the VLAN name here. The VLAN name can be up to 32 characters long.

vlanid - Specifies the ID of the VLAN on which the router port resides.
<vlanid_list> - Enter the VLAN ID list here.

add - Specifies to add the router ports.
delete - Specifies to delete the router ports.
<portlist> - Enter a range of ports to be configured.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.

Restrictions

Only Administrators and Operators can issue this command.

Example

To set up static router ports:

```
DAS-3626:admin#config mld_snooping mrouter_ports vlan default add 1-10
Command: config mld_snooping mrouter_ports vlan default add 1-10

Success.

DAS-3626:admin#
```

25-6 config mld_snooping router_ports_forbidden

Description

This command is used to designate a range of ports as being not connected to multicast-enabled routers. This ensures that the forbidden router port will not propagate routing packets out.

Format

config mld_snooping mrouter_ports_forbidden [vlan <vlan_name 32> | vlanid <vlanid_list>] [add | delete] [<portlist> | bonding <bgroup_list>]

Parameters

vlan - Specifies the name of the VLAN on which the router port resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specifies the ID of the VLAN on which the router port resides. **<vlanid_list>** - Enter the VLAN ID list here.
add - Specifies to add the router ports.
delete - Specifies to delete the router ports.
<portlist> - Enter a range of ports to be configured.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.

Restrictions

Only Administrators and Operators can issue this command.

Example

To set up port range 1-10 to forbidden router ports of the default VLAN:

```
DAS-3626:admin#config mld_snooping mrouter_ports_forbidden vlan default add 1-
10
Command: config mld_snooping mrouter_ports_forbidden vlan default add 1-10

Success.

DAS-3626:admin#
```

25-7 enable mld_snooping

Description

This command is used to enable MLD snooping on the Switch.

Format

enable mld_snooping

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable MLD snooping on the Switch:

```
DAS-3626:admin# enable mld_snooping
Command: enable mld_snooping

Success.

DAS-3626:admin#
```

25-8 disable mld_snooping

Description

This command is used to disable MLD snooping on the Switch.

Format

disable mld_snooping

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable MLD snooping on the Switch:

```
DAS-3626:admin# disable mld_snooping
Command: disable mld_snooping

Success.

DAS-3626:admin#
```

25-9 show mld_snooping

Description

This command is used to display the current MLD snooping configuration on the Switch. If VLAN is not specified, the system will display all current MLD snooping configurations.

Format

show mld_snooping {[vlan <vlan_name 32> | vlanid <vlanid_list>]}

Parameters

vlan - (Optional) Specifies the name of the VLAN for which you want to view the IGMP snooping configuration. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - (Optional) Specifies the ID of the VLAN for which you want to view the IGMP snooping configuration. **<vlanid_list>** - Enter the VLAN ID list here.

Restrictions

None.

Example

To show MLD snooping:

```
DAS-3626:admin#show mld_snooping
Command: show mld_snooping

 MLD Snooping Global State               : Disabled

 VLAN Name                      : default
 Query Interval                 : 125
 Max Response Time              : 10
 Robustness Value               : 2
 Last Listener Query Interval   : 1
 Querier State                  : Enabled
 Querier Role                   : Non-Querier
 Querier IP                     : ::
 Querier Expiry Time            : 0 secs
 State                          : Enabled
 Fast Done                      : Disabled
 Message Limit                  : No Limitation
 Report Suppression             : Disabled
 Version                        : 1
 Translation                    : Disabled

Total Entries: 1


DAS-3626:admin#
```

25-10 show mld_snooping group

Description

This command is used to display the current MLD snooping group information on the Switch.

Format

show mld_snooping group {[vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist> | bonding <bgroup_list>] {<ipv6addr>}}

Parameters

vlan - (Optional) Specifies the name of the VLAN for which you want to view MLD snooping group information. If VLAN and ports and IP address are not specified, the system will display all current IGMP snooping group information. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - (Optional) Specifies the ID of the VLAN for which you want to view MLD snooping group information. **<vlanid_list>** - Enter the VLAN ID list here.
ports - (Optional) Specifies a list of ports for which you want to view MLD snooping group information. **<portlist>** - Enter the list of port here.
bonding - (Optional) Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
<ipv6addr> - (Optional) Specifies the group IPv6 address for which you want to view MLD

snooping group information.

Restrictions

None.

Example

To show an MLD snooping group when MLD v2 is supported:

```
DAS-3626:admin# show mld_snooping group
Command: show mld_snooping group

Source/Group        : 2001::1/FE1E::1
VLAN Name/VID       : default/1
Member Ports        : 1-2
UP Time             : 26
Expiry Time         : 258
Filter Mode         : INCLUDE

Source/Group        : 2002::2/FE1E::1
VLAN Name/VID:      : default/1
Member Ports        : 3
UP Time             : 29
Expiry Time         : 247
Filter Mode         : EXCLUDE

Source/Group        : NULL/FE1E::2
VLAN Name/VID       : default/1
Member Ports        : 4-5
UP Time             : 40
Expiry Time         : 205
Filter Mode         : EXCLUDE

Source/Group        : NULL/FF1E::5
VLAN Name/VID       : default/1
Reports             : 0
Member Ports        :
Router Ports        : 24
UP Time             : 100
Expiry Time         : 200
Filter Mode         : EXCLUDE

Total Entries : 4

DAS-3626:admin#
```

25-11 show mld_snooping forwarding

Description

This command is used to display the Switch's current MLD snooping forwarding table. It provides an easy way for users to check the list of ports that the multicast group that comes from specific

sources will be forwarded to. The packet comes from the source VLAN. They will be forwarded to the forwarding VLAN. The MLD snooping further restricts the forwarding ports. If no parameter is specified, the system will display all current MLD snooping forwarding table entries of the Switch.

Format

show mld_snooping forwarding {[vlan <vlan_name 32> | vlanid <vlanid_list>]}

Parameters

vlan - (Optional) Specifies the name of the VLAN for which you want to view MLD snooping forwarding table information. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - (Optional) Specifies the ID of the VLAN for which you want to view MLD snooping forwarding table information. **<vlanid_list>** - Enter the VLAN ID list here.

Restrictions

None.

Example

To show all MLD snooping forwarding entries located on the Switch.

```
DAS-3626:admin# show mld_snooping forwarding
Command: show mld_snooping forwarding

VLAN Name      : default
Source IP      : 2001::1
Multicast Group: FE1E::1
Port Member    : 2,7

VLAN Name      : default
Source IP      : 2001::2
Multicast Group: FF1E::1
Port Member    : 5

Total Entries : 2

DAS-3626:admin#
```

25-12 show mld_snooping mrouter_ports

Description

This command is used to display the currently configured router ports on the Switch.

Format

show mld_snooping mrouter_ports [vlan <vlan_name 32> | vlanid <vlanid_list> | all] {[static | dynamic | forbidden]}

Parameters

vlan - Specifies the name of the VLAN on which the router port resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specifies the ID of the VLAN on which the router port resides. **<vlanid_list>** - Enter the VLAN ID list here.
all - Specifies all VLANs on which the router port resides.
static - (Optional) Specifies to display router ports that have been statically configured.
dynamic - (Optional) Specifies to display router ports that have been dynamically configured.
forbidden - (Optional) Specifies to display forbidden router ports that have been statically configured.

Restrictions

None.

Example

To display the mld_snooping router ports:

```
DAS-3626:admin#show mld_snooping mrouter_ports all
Command: show mld_snooping mrouter_ports all


VLAN Name                : default
Static Router Port       : 1-10
Dynamic Router Port      :
Router IP                : FE08::1
Forbidden Router Port    : 11

 Total Entries: 1


DAS-3626:admin#
```

25-13 create mld_snooping static_group

Description

This command is used to create an MLD snooping static group. Member ports can be added to the static group. The static member and the dynamic member ports form the member ports of a group.

The static group will only take effect when MLD snooping is enabled on the VLAN. For those static member ports, the device needs to emulate the MLD protocol operation to the querier, and forward the traffic destined to the multicast group to the member ports.

For a layer 3 device, the device is also responsible to route the packets destined for this specific group to static member ports.

The static member ports will only affect MLD V1 operation.

The Reserved IP multicast addresses FF0x::/16 must be excluded from the configured group.

The VLAN must be created first before a static group can be created.

Format

create mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr>

Parameters

vlan - Specifies the name of the VLAN on which the static group resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specifies the ID of the VLAN on which the static group resides. **<vlanid_list>** - Enter the VLAN ID list here.
<ipv6addr> - Enter the multicast group IPv6 address.

Restrictions

Only Administrators and Operators can issue this command.

Example

To create an MLD snooping static group for VLAN, named default; group FF1E::1:

```
DAS-3626:admin# create mld_snooping static_group vlan default FF1E::1
Command: create mld_snooping static_group vlan default FF1E::1

Success.

DAS-3626:admin#
```

25-14 delete mld_snooping static_group

Description

This command is used to delete a MLD Snooping multicast static group.

Format

delete mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr>

Parameters

vlan - Specifies the name of the VLAN on which the static group resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specifies the ID of the VLAN on which the static group resides. **<vlanid_list>** - Enter the VLAN ID list here.
<ipv6addr> - Enter the multicast group IP address.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete an MLD snooping static group for VLAN, named default; group FF1E::1:

```
DAS-3626:admin# delete mld_snooping static_group vlan default FF1E::1
Command: delete mld_snooping static_group vlan default FF1E::1

Success.

DAS-3626:admin#
```

25-15 config mld_snooping static_group

Description

This command is used to configure an MLD snooping multicast group static member port. When a port is configured as a static member port, the MLD protocol will not operate on this port. For example, suppose that a port is a dynamic member port learned by MLD. If this port is configured as a static member later, then the MLD protocol will stop operating on this port. The MLD protocol will resume once this port is removed from static member ports. The static member port will only affect MLD V1 operation.

Format

config mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr> [add | delete] [<portlist> | bonding <bgroup_list>]

Parameters

vlan - Specifies the name of the VLAN on which the static group resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specifies the ID of the VLAN on which the static group resides. **<vlanid_list>** - Enter the VLAN ID list here.
<ipv6addr> - Specifies the multicast group IPv6 address.
add - Specifies to add the member ports.
delete - Specifies to delete the member ports.
<portlist> - Specifies a range of ports to be configured.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.

Restrictions

Only Administrators and Operators can issue this command.

Example

To unset port range 9-10 from MLD snooping static member ports for group FF1E::1 on default VLAN:

```
DAS-3626:admin#config mld_snooping static_group vlan default FF1E::1 delete 9-
10
Command: config mld_snooping static_group vlan default FF1E::1 delete 9-10

Success.

DAS-3626:admin#
```

25-16 show mld_snooping static_group

Description

This command is used to display the MLD snooping multicast group static members.

Format

show mld_snooping static_group {[vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr>}

Parameters

vlan - (Optional) Specifies the name of the VLAN on which the static group resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - (Optional) Specifies the ID of the VLAN on which the static group resides. **<vlanid_list>** - Enter the VLAN ID list here.
<ipv6addr> - (Optional) Specifies the multicast group IPv6 address.

Restrictions

None.

Example

To display all the MLD snooping static groups:

```
DAS-3626:admin#show mld_snooping static_group
Command: show mld_snooping static_group

VLAN ID/Name                     IP Address                 Static Member Ports
------------------------------  -------------------------  ------------------
1   /default                    FF1E::1                    9-10

 Total Entries : 1


DAS-3626:admin#
```

25-17 show mld_snooping statistic counter

Description

This command is used to display the statistics counter for MLD protocol packets that are received by the Switch since MLD snooping was enabled.

Format

show mld_snooping statistic counter [vlan <vlan_name> | vlanid <vlanid_list> | ports <portlist> | bonding <bgroup_list> | group <ipv6group> | per_port <portlist> per_vlan [vlan <vlan_name 32> | vlanid <vidlist>] | per_bonding <bgroup_list> per_vlan [vlan <vlan_name 32> | vlanid <vidlist>]]

Parameters

vlan - Specifies a VLAN to be displayed. **<vlan_name>** - Enter the VLAN name here.
vlanid - Specifies a list of VLANs to be displayed. **<vlanid_list>** - Enter the VLAN ID list here.
ports - Specifies a list of ports to be displayed. **<portlist>** - Enter the list of port here.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
group - Specifies the group IPv6 address for which you want to view MLD snooping statistic counter information. **<ipv6group>** - Enter the group IP address.
per_port - Specifies a list of ports to be displayed. **<portlist>** - Enter the list of port to be displayed here. **per_vlan** - Specifies a VLAN to be displayed. **vlan** - Specifies the name of VLAN. **<vlan_name 32>** - Enter a VLAN name. **vlanid** - Specifies the VLAN ID. **<vidlist>** - Enter a VLAN ID.
per_bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12. **per_vlan** - Specifies a VLAN to be displayed. **vlan** - Specifies the name of VLAN. **<vlan_name 32>** - Enter a VLAN name. **vlanid** - Specifies the VLAN ID. **<vidlist>** - Enter a VLAN ID.

Restrictions

None.

Example

To show MLD snooping statistics counters:

```
DAS-3626:admin#show mld_snooping statistic counter vlan 1
Command: show mld_snooping statistic counter vlan 1

VLAN Name  : Default
-----------------------------------------------
  Total Groups          : 10
Receive Statistics
      Query
MLD v1 Query                    : 1
MLD v2 Query                    : 1
Total                           : 2
Dropped By Rate Limitation      : 1
Dropped By Multicast VLAN       : 1

  Report & Leave
MLD v1 Report                   : 0
MLD v2 Report                   : 10
MLD v1 Done                     : 1
Total                           : 11
Dropped By Rate Limitation      : 0
Dropped By Max Group Limitation : 90
Dropped By Group Filter         : 0
Dropped By Multicast VLAN       : 1

Transmit Statistics
Query
MLD v1 Query                    : 1
MLD v2 Query                    : 1
Total                           : 2
Report & Leave
MLD v1 Report                   : 0
MLD v2 Report                   : 10
MLD v1 Done                     : 1
Total                           : 11

Total Entries : 1

DAS-3626:admin#
```

25-18 clear mld_snooping statistic counter

Description

This command is used to clear MLD snooping statistics counters.

Format

clear mld_snooping statistics counter [vlan <vlan_name> | vlanid <vlanid_list> | ports <portlist> | bonding <bgroup_list> | group <ipv6group> | per_port <portlist> per_vlan [vlan <vlan_name 32> | vlanid <vidlist>] | per_bonding <bgroup_list> per_vlan [vlan <vlan_name 32> | vlanid <vidlist>]]

Parameters

vlan - Specifies a VLAN to be cleared. **<vlan_name>** - Enter the VLAN name here.
vlanid - Specifies a list of VLANs to be cleared. **<vlanid_list>** - Enter the VLAN ID list here.
ports - Specifies a list of ports to be cleared. **<portlist>** - Enter the list of port here.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
group - Specifies group IPv6 address for which you want to clear MLD snooping statistic counter information. **<ipv6addr>** - Enter the group IPV6 address.
per_port - Specifies a list of ports to be cleared. **<portlist>** - Enter the list of port to be cleared here. **per_vlan** - Specifies a VLAN to be cleared. **vlan** - Specifies the name of VLAN. **<vlan_name 32>** - Enter a VLAN name. **vlanid** - Specifies the VLAN ID. **<vidlist>** - Enter a VLAN ID.
per_bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12. **per_vlan** - Specifies a VLAN to be cleared. **vlan** - Specifies the name of VLAN. **<vlan_name 32>** - Enter a VLAN name. **vlanid** - Specifies the VLAN ID. **<vidlist>** - Enter a VLAN ID.

Restrictions

Only Administrators and Operators can issue this command.

Example

To clear MLD snooping statistics counter:

```
DAS-3626:admin# clear mld_snooping statistic counter
Command: clear mld_snooping statistic counter

Success.

DAS-3626:admin#
```

Chapter 26 Multicast Filter Command List

create mcast_filter_profile [ipv4 | ipv6] profile_id <value 1-60> profile_name <name 1-32>
config mcast_filter_profile [profile_id <value 1-60> | profile_name <name 1-32>] {profile_name <name 32> | [add | delete] <mcast_address_list>}(1)
config mcast_filter_profile ipv6 [profile_id <value 1-60> | profile_name <name 1-32>] {profile_name <name 1-32> | [add | delete] <mcastv6_address_list>}(1)
delete mcast_filter_profile [profile_id [<value 1-60> | all] | profile_name <name 1-32>] [ipv4 | ipv6]
show mcast_filter_profile [ipv4 | ipv6] {profile_id <value 1-60> | profile name <name 1-32>}
config limited_multicast_addr [ports <portlist> | bonding <bgroup_list> | vlanid <vlanid_list>] [ipv4 | ipv6] {[add | delete] [profile_id <value 1-60> | profile_name <name 1-32>] | access [permit | deny]}(1)
config max_mcast_group [ipv4 | ipv6] [ports <portlist> | bonding <bgroup_list> | vlanid <vlanid_list>] max_group [<value 1-256> | infinite]
show max_mcast_group [ipv4 | ipv6] [ports {<portlist>} | bonding <bgroup_list> | vlanid {<vlanid_list>}]
show limited_multicast_addr [ipv4 | ipv6] [ports {<portlist>} |bonding <bgroup_list> | vlanid {<vlanid_list>}]

26-1 create mcast_filter_profile

Description

This command is used to configure a multicast address profile. Multiple ranges of multicast addresses can be defined in the profile.

Format

create mcast_filter_profile [ipv4 | ipv6] profile_id <value 1-60> profile_name <name 1-32>

Parameters

ipv4 - Specifies to add an IPv4 multicast profile.
ipv6 - Specifies to add an IPv6 multicast profile.
profile_id - Specifies the ID of the profile. **<value 1-60>** - Enter the profile ID value here. This value must be between 1 and 60.
profile_name - Specifies to provide a meaningful description for the profile. **<name 32>** - Enter the profile name here. The profile name can be up to 32 characters long.

Restrictions

Only Administrators and Operators can issue this command.

Example

To create a IPv4 multicast address profile with a profile ID of 2 and a profile name of MOD:

```
DAS-3626:admin#create mcast_filter_profile ipv4 profile_id 2 profile_name MOD
Command: create mcast_filter_profile ipv4 profile_id 2 profile_name MOD

Success.

DAS-3626:admin#
```

26-2 config mcast_filter_profile

Description

This command is used to configure a range of multicast IP addresses to or from the profile.

Format

config mcast_filter_profile [profile_id <value 1-60> | profile_name <name 1-32>] {profile_name <name 32> | [add | delete] <mcast_address_list>}(1)

Parameters

profile_id - Specifies the ID of the profile. **<value 1-60>** - Enter the profile ID value here. This value must be between 1 and 60.
profile_name - Specifies to provide a meaningful description for the profile. **<name 1-32>** - Enter the profile name here. THe profile name can be up to 32 characters long.
profile_name - (Optional) Specifies provide a meaningful description for the profile. **<name 1-32>** - Enter the profile name here. THe profile name can be up to 32 characters long.
add - Specifies to add a multicast address.
delete - Specifies to delete a multicast address.
<mcast_address_list> - (Optional) Enter a list of the multicast addresses to be put in the profile. You can either specify a single multicast IP address or a range of multicast addresses using -.

Restrictions

Only Administrators and Operators can issue this command.

Example

To add the multicast address range 225.1.1.1 to 225.1.1.10 to the profile:

```
DAS-3626:admin#config mcast_filter_profile profile_id 2 add 225.1.1.1-
225.1.1.10
Command: config mcast_filter_profile profile_id 2 add 225.1.1.1-225.1.1.10

Success.

DAS-3626:admin#
```

26-3 config mcast_filter_profile ipv6

Description

This command is used to configure a range of IPv6 multicast addresses to the profile.

Format

config mcast_filter_profile ipv6 [profile_id <value 1-60> | profile_name <name 1-32>] {profile_name <name 1-32> | [add | delete] <mcastv6_address_list>}(1)

Parameters

profile_id - Specifies the ID of the profile. **<value 1-60>** - Enter the profile ID value here. This value must be between 1 and 60.
profile_name - Specifies to provide a meaningful description for the profile. **<name 1-32>** - Enter the profile name here. The profile name can be up to 32 characters long.
profile_name - Specifies to provide a meaningful description for the profile. **<name 1-32>** - Enter the profile name here. The profile name can be up to 32 characters long.
add - Specifies to add an IPv6 multicast address.
delete - Specifies to delete an IPv6 multicast address.
<mcastv6_address_list> - Enter a list of the IPv6 multicast addresses to put in the profile. You can either specify a single IPv6 multicast IP address or a range of IPv6 multicast addresses connected by '-'.

Restrictions

Only Administrators and Operators can issue this command.

Example

To add the IPv6 multicast address range FFF0E::100:0:0:20 – FFF0E::100:0:0:22 to profile ID 3:

```
DAS-3626:admin#config mcast_filter_profile ipv6 profile_id 3 add
FF0E::100:0:0:20-FF0E::100:0:0:22
Command: config mcast_filter_profile ipv6 profile_id 3 add FF0E::100:0:0:20-
FF0E::100:0:0:22

Success.

DAS-3626:admin#
```

26-4 delete mcast_filter_profile

Description

This command is used to delete a multicast address profile.

Format

delete mcast_filter_profile [profile_id [<value 1-60> | all] | profile_name <name 1-32>] [ipv4 | ipv6]

Parameters

profile_id - Specifies the ID of the profile. **<value 1-60>** - Enter the profile ID value here. This value must be between 1 and 60. **all** - Specifies that all multicast address profiles will be deleted.
profile_name - Specifies to the name of the profile.

<name 1-32> - Enter the profile name value here. The profile name can be up to 32 characters long.
ipv4 - Specifies to add an IPv4 multicast profile.
ipv6 - Specifies to add an IPv6 multicast profile.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete the multicast address profile with a profile ID of 3:

```
DAS-3626:admin# delete mcast_filter_profile profile_id 3
Command: delete mcast_filter_profile profile_id  3
Success.

DAS-3626:admin#
```

To delete the multicast address profile called MOD:

```
DAS-3626:admin# delete mcast_filter_profile profile_name MOD
Command: delete mcast_filter_profile profile_name MOD

Total entries: 2

DAS-3626:admin#
```

26-5 show mcast_filter_profile

Description

This command is used to display the defined multicast address profiles.

Format

show mcast_filter_profile [ipv4 | ipv6] {profile_id <value 1-60> | profile name <name 1-32>}

Parameters

ipv4 - Specifies to delete an IPv4 multicast profile.
ipv6 - Specifies to delete an IPv6 multicast profile.
profile_id - (Optional) Specifies the ID of the profile **<value 1-60>** - Enter the profile ID value here. This value must be between 1 and 60.
profile_name - (Optional) Specifies to display a profile based on the profile name. **<name 1-32>** - Enter the profile name here. The profile name can be up to 32 characters long.

Restrictions

None.

Example

To display the IPv4 multicast address profiles:

```
DAS-3626:admin#show mcast_filter_profile ipv4
Command: show mcast_filter_profile ipv4

Profile ID Name                            Multicast Addresses
---------- ------------------------------- -------------------------------
2          MOD                             225.1.1.1-225.1.1.10


Total Entries: 1


DAS-3626:admin#
```

26-6 config limited_multicast_addr

Description

This command is used to configure the multicast address filtering function on a port or VLAN. When there are no profiles specified with a port or VLAN, the limited function is not effective. When the function is configured on a port, it limits the multicast group operated by the IGMP or MLD snooping function. When this function is configured on a VLAN, the multicast group is limited to only operate the IGMP or MLD layer 3 functions.

Format

config limited_multicast_addr [ports <portlist> | bonding <bgroup_list> | vlanid <vlanid_list>] [ipv4 | ipv6] {[add | delete] [profile_id <value 1-60> | profile_name <name 1-32>] | access [permit | deny]}(1)

Parameters

ports - Specifies the range of ports to configure the multicast address filtering function. **<portslist>** - Enter the list of port to be configured here.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
vlanid - Specifies the VLAN ID of the VLAN that the multicast address filtering function will be configured on. **<vlanid_list>** - Enter the VLAN ID list here.
ipv4 - Specifies the IPv4 multicast profile.
ipv6 - Specifies the IPv6 multicast profile.
add - Specifies to add a multicast address profile to a port.
delete - Specifies to delete a multicast address profile to a port.
profile_id - Specifies a profile to be added to or deleted from the port. **<value 1-60>** - Enter the profile ID value here. This value must be between 1 and 60.
profile_name - Specifies the profile name used. **<name 1-32>** - Enter the profile name here. The profile name can be up to 32 characters long.
access - Specifies the access of packets matching the addresses defined in the profiles. **permit** - Specifies that packets matching the addresses defined in the profiles will be permitted. The default mode is permit. **deny** - Specifies that packets matching the addresses defined in the profiles will be denied.

Restrictions

Only Administrators and Operators can issue this command.

Example

To add multicast address profile 2 to ports 1-10:

```
DAS-3626:admin#config limited_multicast_addr ports 1-10 ipv4 add profile_id 2

Command: config limited_multicast_addr ports 1-10 ipv4 add profile_id 2

Success.

DAS-3626:admin#
```

26-7 config max_mcast_group

Description

This command is used to configure the maximum number of multicast groups that a port can join.

Format

config max_mcast_group [ipv4 | ipv6] [ports <portlist> | bonding <bgroup_list> | vlanid <vlanid_list>] max_group [<value 1-256> | infinite]

Parameters

ipv4 - Specifies that the maximum number of IPv4 learned addresses should be limited.
ipv6 - Specifies that the maximum number of IPv6 learned addresses should be limited.
ports - Specifies the range of ports to configure the max_mcast_group. **<portlist>** - Enter the list of ports to be configured here.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
vlanid - Specifies the VLAN ID to configure max_mcast_group. **<vlanid_list>** - Enter the VLAN ID list here.
max_group - Specifies the maximum number of multicast groups. **<value 1-256>** - Enter the maximum group value here. This value must be between 1 and 256. **infinite** - Specifies that the maximum group value will be set to infinite.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the maximum number of IPv4 multicast group that ports 1 and 3 can join to 100:

```
DAS-3626:admin#config max_mcast_group ipv4 ports 1,3 max_group 100
Command: config max_mcast_group ipv4 ports 1,3 max_group 100

Success.

DAS-3626:admin#
```

26-8 show max_mcast_group

Description

This command is used to display the maximum number of multicast groups that a port can join.

Format

show max_mcast_group [ipv4 | ipv6] [ports {<portlist>} | bonding <bgroup_list> | vlanid {<vlanid_list>}]

Parameters

ipv4 - Specifies to display the maximum number of IPv4 learned addresses.
ipv6 - Specifies to display the maximum number of IPv6 learned addresses.
ports - Specifies the range of ports for displaying information about the maximum number of multicast groups that the specified ports can join. **<portlist>** - (Optional) Enter the list of ports to be configured here.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
vlanid - Specifies the VLAN ID for displaying the maximum number of multicast groups. **<vlanid_list>** - (Optional) Enter the VLAN ID list here.

Restrictions

None.

Example

To display the maximum number of IPv4 multicast groups that ports 1 and 2 can join:

```
DAS-3626:admin#show max_mcast_group ipv4 ports 1-2
Command: show max_mcast_group ipv4 ports 1-2

Port      Max Multicast Group Number
------    ---------------------------
1         100
2         Infinite

Total Entries: 2


DAS-3626:admin#
```

To display the maximum number of multicast groups that VLANs 1 can join:

```
DAS-3626:admin#show max_mcast_group ipv4 vlanid 1
Command: show max_mcast_group ipv4 vlanid 1

VLAN      Max Multicast Group Number
------    --------------------------
1         Infinite

Total Entries: 1


DAS-3626:admin#
```

26-9 show limited_multicast_addr

Description

This command is used to display the multicast address range by port or by VLAN.

When the function is configured on a port, it limits the multicast groups operated by the IGMP or MLD snooping function and layer 3 functions. When the function is configured on a VLAN, it limits the multicast groups operated by the IGMP or MLD layer 3 functions.

Format

show limited_multicast_addr [ipv4 | ipv6] [ports {<portlist>} |bonding <bgroup_list> | vlanid {<vlanid_list>}]

Parameters

ipv4 - Specifies to display the IPv4 multicast profile associated with the port.
ipv6 - Specifies to display the IPv6 multicast profile associated with the port.
ports - Specifies the range of ports that require information displaying about the multicast address filtering function. **<portlist>** - (Optional) Enter the list of port to be configured here.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
vlanid - Specifies the VLAN ID of VLANs that require information displaying about the multicast address filtering function. **<vlanid_list>** - (Optional) Enter the VLAN ID list here.

Restrictions

None.

Example

To show the limited multicast address range on ports 1 and 3:

```
DAS-3626:admin#show limited_multicast_addr ipv4 ports 1,3
Command: show limited_multicast_addr ipv4 ports 1,3

Port    : 1
Access  : Deny

Profile ID Name                            Multicast Addresses
---------- ------------------------------- -------------------------------
2          MOD                             225.1.1.1-225.1.1.10


Port    : 3
Access  : Deny

Profile ID Name                            Multicast Addresses
---------- ------------------------------- -------------------------------
2          MOD                             225.1.1.1-225.1.1.10


DAS-3626:admin#
```

To show the limited multicast settings configured on VLAN 1:

```
DAS-3626:admin#show limited_multicast_addr ipv4 vlanid 1
Command: show limited_multicast_addr ipv4 vlanid 1

VLAN ID : 1
Access  : Deny

Profile ID Name                            Multicast Addresses
---------- ------------------------------- -------------------------------
2          MOD                             225.1.1.1-225.1.1.10



DAS-3626:admin#
```

Chapter 27 Multicast VLAN Command List

create [igmp_snooping | mld_snooping] multicast_vlan <vlan_name 32> <vlanid 2-4094>
config igmp_snooping multicast_vlan <vlan_name 32> {[add | delete] [member_port [<portlist> | bonding <bgroup_list>] | source_port [<portlist> | bonding <bgroup_list>] | tag_member_port [<portlist> | bonding <bgroup_list>] | state [enable | disable] | replace_source_ip {[<ipaddr> | none]} | replace_query_source_ip{[<ipaddr> | none]}}(1)
config mld_snooping multicast_vlan <vlan_name 32> {[add | delete] [member_port [<portlist> | bonding <bgroup_list>] | source_port [<portlist> | bonding <bgroup_list>] | tag_member_port [<portlist> | bonding <bgroup_list>] | state [enable | disable] | replace_source_ip {[<ipv6addr >|none]} | replace_query_source_ip {[<ipv6addr> | none]}}(1)
create [igmp_snooping | mld_snooping] multicast_vlan_group_profile <profile_name 1-32>
config igmp_snooping multicast_vlan_group_profile <profile_name 1-32> [add | delete] <mcast_address_list>
config mld_snooping multicast_vlan_group_profile <profile_name 1-32> [add | delete] <mcast_v6address_list>
delete [igmp_snooping | mld_snooping] multicast_vlan_group_profile [profile_name <profile_name 1-32> | all]
show [igmp_snooping | mld_snooping] multicast_vlan_group_profile {< profile_name 1-32>}
config [igmp_snooping | mld_snooping] multicast_vlan_group <vlan_name 32> [add | delete] profile_name <profile_name 1-32>
show [igmp_snooping | mld_snooping] multicast_vlan_group {<vlan_name 32>}
delete [igmp_snooping | mld_snooping] multicast_vlan <vlan_name 32>
enable [igmp_snooping | mld_snooping] multicast_vlan
disable [igmp_snooping | mld_snooping] multicast_vlan
config [igmp_snooping | mld_snooping] multicast_vlan forward_unmatched [enable | disable]
show [igmp_snooping | mld_snooping] multicast_vlan {<vlan_name 32>}

27-1 create [igmp_snooping | mld_snooping] multicast_vlan

Description

This command is used to create a multicast VLAN and implements relevant parameters as specified. More than one multicast VLANs can be configured.

Newly created IGMP snooping multicast VLANs must use a unique VLAN ID and name, i.e. they cannot use the VLAN ID or name of any existing 802.1q VLAN.

Also keep in mind the following conditions:

- Multicast VLANs cannot be configured or displayed using 802.1Q VLAN commands.
- An IP interface cannot be bound to a multicast VLAN.
- The multicast VLAN snooping function co-exists with the 802.1q VLAN snooping function.

Format

create [igmp_snooping | mld_snooping] multicast_vlan <vlan_name 32> <vlanid 2-4094>

Parameters

igmp_snooping - Specifies to configure VLAN for IGMP snooping.
mld_snooping - Specifies to configure VLAN for MLD snooping.
multicast_vlan - Specifies the name of the multicast VLAN to be created. Each multicast VLAN is given a name that can be up to 32 characters. **<vlan_name 32>** - Enter the VLAN here. The VLAN name can be up to 32 characters long. **<vlanid 2-4094>** - Enter the VLAN ID of the multicast VLAN to be created. This value must be between 2 and 4094.

Restrictions

Only Administrators and Operators can issue this command.

Example

To create an IGMP snooping multicast VLAN with the VLAN name mv1 and the VID 2:

```
DAS-3626:admin#create igmp_snooping multicast_vlan mv1 2
Command: create igmp_snooping multicast_vlan mv1 2

Success.

DAS-3626:admin#
```

27-2 config igmp_snooping multicast_vlan

Description

This command is used to add member ports and source ports to a list of multicast VLAN member ports. Member ports automatically become untagged members of the multicast VLAN and source ports automatically become tagged members of the multicast VLAN. However, member ports of one multicast VLAN are allowed to overlap with member ports on a different multicast VLAN.

A multicast VLAN must first be created using the create igmp_snooping multicast_vlan command before the multicast VLAN can be configured.

Format

config igmp_snooping multicast_vlan <vlan_name 32> {[add | delete] [member_port [<portlist> | bonding <bgroup_list>] | source_port [<portlist> | bonding <bgroup_list>] | tag_member_port [<portlist> | bonding <bgroup_list>] | state [enable | disable] | replace_source_ip {[<ipaddr> | none]} | replace_query_source_ip{[<ipaddr> | none]}}(1)

Parameters

<vlan_name 32> - Enter the name of the multicast VLAN here. The VLAN name can be up to 32 characters long.
add - Specifies that the entry will be added to the specified multicast VLAN.
delete - Specifies that the entry will be deleted to the specified multicast VLAN.
member_port - Specifies a member port or range of member ports to be added to the multicast VLAN. The specified range of ports will become untagged members of the multicast VLAN. **<portlist>** - Enter the list of port to be configured here. **bonding** - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.

source_port - Specifies a port or range of ports to be added to the multicast VLAN. **<portlist>** - Enter the list of port to be configured here. **bonding** - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
tag_member_port - Specifies the port or range of ports that will become tagged members of the multicast VLAN. **<portlist>** - Enter the list of port to be configured here. **bonding** - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
state - Specifies the multicast VLAN for a chosen VLAN to be enabled or disabled. **enable** - Specifies to enable the multicast VLAN for a chosen VLAN. **disable** - Specifies to disable the multicast VLAN for a chosen VLAN.
replace_source_ip - Specifies that before forwarding the report packet sent by the host, the source IP address in the join packet must be replaced by this IP address. If no parameter is psecified, the Switch specifies system IP address as replace source IP address. **<ipaddr>** - (Optional) Enter the replace source IP address here. **none** - (Optional) Specifies “0.0.0.0” as the replace source IP address.
replace_query_source_ip - Specifies that before forwarding the query packet sent by the router, the source IP address in the query packet must be replaced by this IP address. If no parameter is psecified, the Switch specifies system IP address as replace query source IP address. **<ipaddr>** - (Optional) Enter the replace source IP address here. **none** - (Optional) Specifies “0.0.0.0” as the replace query source IP address.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure an IGMP snooping multicast VLAN with the name “mv1”, make ports 1 and 3 members of the VLAN, and set the state to enable:

```
DAS-3626:admin#config igmp_snooping multicast_vlan mv1 add member_port 1,3
state enable
Command: config igmp_snooping multicast_vlan mv1 add member_port 1,3 state
enable

Success.

DAS-3626:admin#
```

27-3 config mld_snooping multicast_vlan

Description

This command is used to add member ports and source ports to a list of multicast VLAN member ports. Member ports automatically become untagged members of the multicast VLAN and source ports automatically become tagged members of the multicast VLAN. If the port list of an existing multicast VLAN is changed without specifying add or delete, the newly added port list replaces the existing port list. A member port list cannot overlap with a source port list of the same multicast VLAN. However, member ports of one multicast VLAN are allowed to overlap with member ports on a different multicast VLAN.

A multicast VLAN must first be created using the create mld_snooping multicast_vlan command before it can be configured.

Format

config mld_snooping multicast_vlan <vlan_name 32> {[add | delete] [member_port [<portlist> | bonding <bgroup_list>] | source_port [<portlist> | bonding <bgroup_list>] | tag_member_port [<portlist> | bonding <bgroup_list>] | state [enable | disable] | replace_source_ip {[<ipv6addr >|none]} | replace_query_source_ip {[<ipv6addr> | none]}}(1)

Parameters

<vlan_name 32> - Enter the name of the multicast VLAN. The VLAN name can be up to 32 characters long.
add - (Optional) Specifies to add member ports to the multicast VLAN.
delete - (Optional) Specifies to delete member ports to the multicast VLAN.
member_port - (Optional) Specifies a member port or range of member ports to be added to the multicast VLAN. The specified range of ports will become untagged members of the multicast VLAN. **<portlist>** - Enter the list of port to be configured here. **bonding** - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
source_port - (Optional) Specifies the port or range of ports to be added to the multicast VLAN. **<portlist>** - Enter the list of port to be configured here. **bonding** - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
tag_member_port - (Optional) Specifies the port or range of ports that will become tagged members of the multicast VLAN. **<portlist>** - Enter the list of port to be configured here. **bonding** - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
state - (Optional) Specifies the multicast VLAN for a chosen VLAN to be enabled or disabled. **enable** - Specifies to enable the multicast VLAN for a chosen VLAN. **disable** - Specifies to disable the multicast VLAN for a chosen VLAN.
replace_source_ip - Specifies that before forwarding the report packet sent by the host, the source IPv6 address in the join packet must be replaced by this IPv6 address. If no parameter is psecified, the Switch specifies system IPv6 address as replace source IPv6 address. **<ipv6addr>** - (Optional) Enter the replace source IPv6 address here. **none** - (Optional) Specifies "::" as the replace source IPv6 address.
replace_query_source_ip - Specifies that before forwarding the query packet sent by the router, the source IPv6 address in the query packet must be replaced by this IPv6 address. If no parameter is psecified, the Switch specifies system IPv6 address as replace query source IPv6 address. **<ipv6addr>** - (Optional) Enter the replace source IPv6 address here. **none** - (Optional) Specifies "::" as the replace query source IPv6 address.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure an MLD snooping multicast VLAN with the name "mv2", make ports 1 and 3 members of the VLAN, and set the state to enable:

```
DAS-3626:admin#config mld_snooping multicast_vlan mv2 add member_port 1,3 state
enable
Command: config mld_snooping multicast_vlan mv2 add member_port 1,3 state
enable

Success.

DAS-3626:admin#
```

27-4 create [igmp_snooping | mld_snooping] multicast_vlan_group_profile

Description

This command is used to create an IGMP or MLD snooping multicast group profile on the switch.

Format

create [igmp_snooping | mld_snooping] multicast_vlan_group_profile <profile_name 1-32>

Parameters

igmp_snooping - Specifies that an IGMP snooping profile will be created.
mld_snooping - Specifies that an MLD snooping profile will be created.
multicast_vlan_group_profile - Specifies the multicast VLAN profile name. The maximum length is 32 characters. **<profile_name 1-32>** - Enter the multicast VLAN group profile name here. The name can be up to 32 characters long.

Restrictions

Only Administrators and Operators can issue this command.

Example

To create an IGMP snooping multicast group profile with the name “test”:

```
DAS-3626:admin#create igmp_snooping multicast_vlan_group_profile test
Command: create igmp_snooping multicast_vlan_group_profile test

Success.

DAS-3626:admin#
```

27-5 config igmp_snooping multicast_vlan_group_profile

Description

This command is used to configure an IGMP snooping multicast group profile on the switch and add or delete multicast addresses for the profile.

Format

config igmp_snooping multicast_vlan_group_profile <profile_name 1-32> [add | delete] <mcast_address_list>

Parameters

<profile_name 1-32> - Enter the multicast VLAN group name here. This name can be up to 32 characters long.
add - Specifies to add a multicast address list to or from this multicast VLAN profile. The <mcast_address_list> can be a continuous single multicast address, such as 225.1.1.1, 225.1.1.3, 225.1.1.8, a multicast address range, such as 225.1.1.1-225.2.2.2, or both of types, such as 225.1.1.1, 225.1.1.18-225.1.1.20
delete - Specifies to delete a multicast address list to or from this multicast VLAN profile. The <mcast_address_list> can be a continuous single multicast addresses, such as 225.1.1.1, 225.1.1.3, 225.1.1.8, or a multicast address range, such as 225.1.1.1-225.2.2.2, or both types, such as 225.1.1.1, 225.1.1.18-225.1.1.20
<mcast_address_list> - Enter the multicast VLAN IP address here.

Restrictions

Only Administrators and Operators can issue this command.

Example

To add the single multicast address 225.1.1.1 and multicast range 225.1.1.10-225.1.1.20 to the IGMP snooping multicast VLAN profile named “test”:

```
DAS-3626:admin#config igmp_snooping multicast_vlan_group_profile test add
225.1.1.1, 225.1.1.10-225.1.1.20
Command: config igmp_snooping multicast_vlan_group_profile test add 225.1.1.1,
225.1.1.10-225.1.1.20

Success.

DAS-3626:admin#
```

27-6 config mld_snooping multicast_vlan_group_profile

Description

This command is used to configure an MLD snooping multicast group profile on the switch and add or delete multicast addresses for the profile.

Format

config mld_snooping multicast_vlan_group_profile <profile_name 1-32> [add | delete] <mcast_v6address_list>

Parameters

<profile_name 1-32> - Enter the multicast VLAN group profile name here. This name can be up to 32 characters long.
add - Specifies to add a multicast address list to or from this multicast VLAN profile. The

<mcast_v6address_list> can be a continuous single multicast addresses, such as FF1E::1, a multicast address range, such asFF1E::1-FF1E::2, or both of them, such as FF1E::1, FF1E::10-FF1E::20
delete - Specifies to delete multicast address list to or from this multicast VLAN profile. The <mcast_v6address_list> can be a continuous single multicast addresses, such as FF1E::1, a multicast address range, such as FF1E::1-FF1E::2, or both of them, such as FF1E::1, FF1E::10-FF1E::20
<mcast_v6address_list> - Enter the multicast VLAN IPv6 address here.

Restrictions

Only Administrators and Operators can issue this command.

Example

To add a multicast address or range to an MLD snooping multicast VLAN profile with name "mmv1":

```
DAS-3626:admin#config mld_snooping multicast_vlan_group_profile mmv1 add
FF1E::1, FF1E::10-FF1E::20
Command: config mld_snooping multicast_vlan_group_profile mmv1 add FF1E::1,
FF1E::10-FF1E::20

Success.

DAS-3626:admin#
```

27-7 delete [igmp_snooping | mld_snooping] multicast_vlan_group_profile

Description

This command is used to delete an IGMP snooping or MLD snooping multicast group profile on the switch. Specifies a profile name to delete it. Specifies all to remove all profiles along with the groups that belong to that profile.

Format

delete [igmp_snooping | mld_snooping] multicast_vlan_group_profile [profile_name <profile_name 1-32> | all]

Parameters

igmp_snooping - Specifies to delete an IGMP snooping group profile.
mld_snooping - Specifies to delete an MLD snooping group profile.
profile_name - Specifies the multicast VLAN profile name. **<profile_name 1-32>** - Enter the multicast VLAN profile name here. This name can be up to 32 characters long. **all** - Specifies to delete all the multicast VLAN profiles.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete an IGMP snooping multicast group profile with the name “MOD”:

```
DAS-3626:admin#delete igmp_snooping multicast_vlan_group_profile profile_name
MOD
Command: delete igmp_snooping multicast_vlan_group_profile profile_name MOD

Success.

DAS-3626:admin#
```

27-8 show [igmp_snooping | mld_snooping] multicast_vlan_group_profile

Description

This command is used to show the IGMP snooping or MLD snooping multicast group profiles.

Format

show [igmp_snooping | mld_snooping] multicast_vlan_group_profile {< profile_name 1-32>}

Parameters

igmp_snooping - Specifies that an IGMP snooping multicast group profile should be displayed.
mld_snooping - Specifies that an MLD snooping multicast group profile should be displayed.
multicast_vlan_group_profile - Specifies the profile name of the existing multicast VLAN profile that should be displayed. **<profile_name 1-32>** - (Optional) Enter the multicast VLAN group profile name here. The name can be up to 32 characters long.

Restrictions

None.

Example

To display all IGMP snooping multicast VLAN profiles:

```
DAS-3626:admin#show igmp_snooping multicast_vlan_group_profile
Command: show igmp_snooping multicast_vlan_group_profile

Profile Name                    Multicast Addresses
------------------------------- -------------------------------
test                            225.1.1.1
                                225.1.1.10-225.1.1.20


 Total Entries: 1


DAS-3626:admin#
```

27-9 config [igmp_snooping | mld_snooping] multicast_vlan_group

Description

This command is used to configure the multicast group learned with the specific multicast VLAN. The following two cases can be considered for examples:

Case 1- The multicast group is not configured, multicast VLANs do not have any member ports overlapping and the join packet received by the member port is learned on only the multicast VLAN that this port is a member of.

Case 2-,The join packet is learned with the multicast VLAN that contains the destination multicast group. If the destination multicast group of the join packet cannot be classified into any multicast VLAN to which this port belongs, then the join packet will be learned on the natural VLAN of the packet.

Note that a profile cannot overlap in different multicast VLANs. Multiple profiles can be added to a multicast VLAN.

Format

config [igmp_snooping | mld_snooping] multicast_vlan_group <vlan_name 32> [add | delete] profile_name <profile_name 1-32>

Parameters

igmp_snooping - Specifies IGMP snooping should be configured.
mld_snooping - Specifies MLD snooping should be configured.
multicast_vlan_group - Specifies the name of the multicast VLAN to be configured. Each multicast VLAN is given a name of up to 32 characters. **<vlan_name 32>** - Enter the multicast VLAN name here. The VLAN name can be up to 32 characters long.
add - Specifies to associate a profile to a multicast VLAN.
delete - Specifies to de-associate a profile from a multicast VLAN.
profile_name - Specifies the multicast VLAN profile name. **<profile_name 1-32>** - Enter the multicast VLAN profile name here. The name can be up to 32 characters long.

Restrictions

Only Administrators and Operators can issue this command.

Example

To add an IGMP snooping profile to a multicast VLAN group with the name “mv1”:

```
DAS-3626:admin#config igmp_snooping multicast_vlan_group mv1 add profile_name
test
Command: config igmp_snooping multicast_vlan_group mv1 add profile_name test

Success.

DAS-3626:admin#
```

27-10 show [igmp_snooping | mld_snooping] multicast_vlan_group

Description

This command is used to show an IGMP snooping or MLD snooping multicast VLAN group.

Format

show [igmp_snooping | mld_snooping] multicast_vlan_group {<vlan_name 32>}

Parameters

igmp_snooping - Specifies that IGMP snooping VLAN groups should be displayed.
mld_snooping - Specifies that MLD snooping VLAN groups should be displayed.
multicast_vlan_group - Specifies the the name of the multicast VLAN to be displayed. **<vlan_name 32>** - (Optional) Enter the VLAN name here. The VLAN name can be up to 32 characters long.

Restrictions

Only Administrators and Operators can issue this command.

Example

To show all IGMP snooping multicast VLAN groups setup on the switch:

```
DAS-3626:admin#show igmp_snooping multicast_vlan_group
Command: show igmp_snooping multicast_vlan_group


VLAN Name                       VLAN ID        Multicast Group Profiles
------------------------------  -------  --------------------------------
mv1                             2         test


DAS-3626:admin#
```

27-11 delete [igmp_snooping | mld_snooping] multicast_vlan

Description

This command is used to delete an IGMP or MLD snooping multicast VLAN.

Format

delete [igmp_snooping | mld_snooping] multicast_vlan <vlan_name 32>

Parameters

igmp_snooping - Specifies that an IGMP snooping multicast VLAN will be deleted.
mld_snooping - Specifies that an MLD snooping multicast VLAN will be deleted.
multicast_vlan - Specifies the name of the multicast VLAN to be deleted. **<vlan_name 32>** -Enter the VLAN name here. The VLAN name can be up to 32 characters long.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete an MLD snooping multicast VLAN called “v1”:

```
DAS-3626:admin#delete mld_snooping multicast_vlan v1
Command: delete mld_snooping multicast_vlan v1

Success.

DAS-3626:admin#
```

27-12 enable [igmp_snooping | mld_snooping] multicast_vlan

Description

This command is used to enable the status of the multicast VLAN function.

Format

enable [igmp_snooping | mld_snooping] multicast_vlan

Parameters

igmp_snooping - Specifies that IGMP snooping multicast VLAN is to be enabled.
mld_snooping - Specifies that MLD snooping multicast VLAN is to be enabled.

Restrictions

Only Administrators can issue this command.

Example

To enable the IGMP snooping multicast VLAN function globally:

```
DAS-3626:admin#enable igmp_snooping multicast_vlan
Command: enable igmp_snooping multicast_vlan

Success.

DAS-3626:admin#
```

27-13 disable [igmp_snooping | mld_snooping] multicast_vlan

Description

This command is used to disable the IGMP or MLD snooping multicast VLAN function. By default, the multicast VLAN is disabled.

Format

disable [igmp_snooping | mld_snooping] multicast_vlan

Parameters

igmp_snooping - Specifies that the IGMP snooping multicast VLAN function should be disabled.
mld_snooping - Specifies that the MLD snooping multicast VLAN function should be disabled.

Restrictions

Only Administrators can issue this command.

Example

To disable the MLD snooping multicast VLAN function:

```
DAS-3626:admin# disable mld_snooping multicast_vlan
Command: disable mld_snooping multicast_vlan

Success.

DAS-3626:admin#
```

27-14 config [igmp_snooping | mld_snooping] multicast_vlan forward_unmatched

Description

This command is used to configure the forwarding mode for multicast VLAN unmatched packets. When the switch receives an IGMP/MLD snooping packet, it will match the packet against the multicast profile to determine which multicast VLAN to associate with. If the packet does not match all profiles, the packet will be forwarded or dropped based on this setting.

By default, the packet will be dropped.

Format

config [igmp_snooping | mld_snooping] multicast_vlan forward_unmatched [enable | disable]

Parameters

igmp_snooping - Specifies that the IGMP snooping multicast VLAN function will be configured.
mld_snooping - Specifies that the MLD snooping multicast VLAN function will be configured.
multicast_vlan forward_unmatched - Specifies to enable or disable packet flooding on the multicast VLAN. **enable** - Specifies that the packet will be flooded on the VLAN. **disable** - Specifies that the packet will be dropped.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the forwarding mode for multicast VLAN unmatched packets：

```
DAS-3626:admin#config igmp_snooping multicast_vlan forward_unmatched enable
Command: config igmp_snooping multicast_vlan forward_unmatched enable

Success.

DAS-3626:admin#
```

27-15 show [igmp_snooping | mld_snooping] multicast_vlan

Description

This command is used to display information for a multicast VLAN.

Format

show [igmp_snooping | mld_snooping] multicast_vlan {<vlan_name 32>}

Parameters

igmp_snooping - Specifies that IGMP snooping multicast VLANs will be displayed.
mld_snooping - Specifies that MLD snooping multicast VLANs will be displayed.
multicast_vlan - Specifies the name of the multicast VLAN to be shown. **<vlan_name 32>** - (Optional) Enter the VLAN name here. The VLAN name can be up to 32 characters long.

Restrictions

None.

Example

To display all IGMP snooping multicast VLANs:

```
DAS-3626:admin#show igmp_snooping multicast_vlan
Command: show igmp_snooping multicast_vlan

IGMP Multicast VLAN Global State        : Enabled
IGMP Multicast VLAN Forward Unmatched   : Enabled

VLAN Name                       :mv1
VID                             :2

Member(Untagged) Ports          :1,3
Tagged Member Ports             :
Source Ports                    :
Status                          :Enabled
Replace Source IP               :10.90.90.90    (System IP)
Replace Query Source IP         :10.90.90.90    (System IP)


 Total Entries: 1


DAS-3626:admin#
```

Chapter 28 Multiple Spanning Tree Protocol (MSTP) Command List

show stp
show stp instance {<value 0-15>}
show stp ports {<portlist>}
show stp mst_config_id
create stp instance_id <value 1-4>
delete stp instance_id <value 1-4>
config stp instance_id <value 1-4> [add_vlan | remove_vlan] <vidlist>
config stp mst_config_id {revision_level <int 0-65535> | name <string>}
enable stp
disable stp
config stp version [mstp | rstp | stp]
config stp priority <value 0-61440> instance_id <value 0-4>
config stp {maxage <value 6-40> | maxhops <value 6-40> | hellotime <value 1-2> | forwarddelay <value 4-30> | txholdcount <value 1-10> | fbpdu [enable | disable] | nni_bpdu_addr [dot1d | dot1ad]}
config stp ports <portlist> {externalCost [auto | <value 1-200000000>] | hellotime <value 1-2> | migrate [yes | no] |edge [true | false | auto] | p2p [true | false | auto] | state [enable | disable] | restricted_role [true | false] | restricted_tcn [true | false] | fbpdu [enable | disable]}
config stp mst_ports <portlist> instance_id <value 0-4> {internalCost [auto | <value 1-200000000>] | priority <value 0-240>}

28-1 show stp

Description

This command is used to display the bridge parameters global settings.

Format

show stp

Parameters

None.

Restrictions

None.

Example

To show STP:

```
DAS-3626:admin#show stp
Command: show stp

 STP Bridge Global Settings
 ---------------------------
 STP Status          : Disabled
 STP Version         : RSTP
 Max Age             : 20
 Hello Time          : 2
 Forward Delay       : 15
 Max Hops            : 20
 TX Hold Count       : 6
 Forwarding BPDU     : Disabled
 NNI BPDU Address    : dot1d
 STP Port            : 1-26
 Forward BPDU Port   : 1-26

DAS-3626:admin#
```

28-2 show stp instance

Description

This command is used to display each instance parameters settings. Value means the instance ID, if there is no input of this value, all instance will be shown.

Format

show stp instance {<value 0-15>}

Parameters

<value 0-15> - (Optional) Enter the MSTP instance ID value here. This value must be between 0 and 15.

Restrictions

None.

Example

To show STP instance:

```
DAS-3626:admin#show stp instance
Command: show stp instance

 STP Instance Settings
 -------------------------
 Instance Type          : CIST
 Instance Status        : Disabled
 Instance Priority      : 32768(Bridge Priority : 32768, SYS ID Ext : 0 )


CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

28-3 show stp ports

Description

This command is used to display the port information includes parameters setting and operational value.

Format

show stp ports {<portlist>}

Parameters

<portlist> - (Optional) Enter a list of ports used for the configuration here.

Restrictions

None.

Example

To show STP ports:

```
DAS-3626:admin#show stp ports
Command: show stp ports

 STP Port Information
 ----------------------
 Port Index     : 1     , Hello Time: 2 /2 , Port STP : Enabled  ,
 External PathCost : Auto/200000   , Edge Port : False/No , P2P : Auto /Yes
 Port RestrictedRole : False,  Port RestrictedTCN : False
 Port Forward BPDU : Enabled
 MSTI   Designated Bridge   Internal PathCost  Prio  Status      Role
 -----  ------------------  -----------------  ----  ----------  ----------
 0      N/A                 200000             128   Disabled    Disabled


CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

28-4 show stp mst_config_id

Description

This command is used to display the MST configuration identification.

Format

show stp mst_config_id

Parameters

None.

Restrictions

None.

Example

show STP MST configuration ID:

```
DAS-3626:admin#show stp mst_config_id
Command: show stp mst_config_id

 Current MST Configuration Identification
 ---------------------------------------

 Configuration Name : D8:FE:E3:93:05:C0                Revision Level :0
 MSTI ID     VID List
 -------     ------------------------------------------------------------
    CIST     1-4094

DAS-3626:admin#
```

28-5 create stp instance_id

Description

This command is used to create an MST Instance without mapping the corresponding VLANs.

Format

create stp instance_id <value 1-4>

Parameters

<value 1-4> - Enter the MSTP instance ID here. This value must be between 1 and 4.

Restrictions

Only Administrators and Operators can issue this command.

Example

To create MSTP instance:

```
DAS-3626:admin#create stp instance_id 2
Command: create stp instance_id 2

 Warning:There is no VLAN mapping to this instance_id!
Success.

DAS-3626:admin#
```

28-6 delete stp instance_id

Description

This command is used to delete an MST Instance.

Format

delete stp instance_id <value 1-4>

Parameters

<value 1-4> - Enter the MSTP instance ID here. This value must be between 1 and 4.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete an MSTP instance:

```
DAS-3626:admin#delete stp instance_id 2
Command: delete stp instance_id 2

Success.

DAS-3626:admin#
```

28-7 config stp instance_id

Description

This command is used to map or remove the VLAN range of the specified MST instance for the existed MST instances.

Format

config stp instance_id <value 1-4> [add_vlan | remove_vlan] <vidlist>

Parameters

<value 1-4> - Enter the MSTP instance ID here. This value must be between 1 and 4.
add_vlan - Specifies to map the specified VLAN list to an existing MST instance.
remove_vlan - Specifies to delete the specified VLAN list from an existing MST instance.
<vidlist> - Enter a list of VLANs by VLAN ID.

Restrictions

Only Administrators and Operators can issue this command.

Example

To map a VLAN ID to an MSTP instance:

```
DAS-3626:admin#config stp instance_id 2 add_vlan 1-2
Command: config stp instance_id 2 add_vlan 1-2

Success.

DAS-3626:admin#
```

To remove a VLAN ID from an MSTP instance:

```
DAS-3626:admin#config stp instance_id 2 remove_vlan 2
Command: config stp instance_id 2 remove_vlan 2

Success.

DAS-3626:admin#
```

28-8 config stp mst_config_id

Description

This command is used to change the name or the revision level of the MST configuration identification.

Format

config stp mst_config_id {revision_level <int 0-65535> | name <string>}

Parameters

revision_level - (Optional) Specifies the same given name with different revision level also represents different MST regions. **<int 0-65535>** - Enter the revision level here. This value must be between 0 and 65535.
name - (Optional) Specifies the name given for a specific MST region. **<string>** - Enter the MST region name here.

Restrictions

Only Administrators and Operators can issue this command.

Example

To change the name and revision level of the MST configuration identification:

```
DAS-3626:admin#config stp mst_config_id revision_level 1 name block
Command: config stp mst_config_id revision_level 1 name block

Success.

DAS-3626:admin#
```

28-9 enable stp

Description

This command is used to enable STP globally.

Format

enable stp

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable STP:

```
DAS-3626:admin# enable stp
Command: enable stp

Success.

DAS-3626:admin#
```

28-10 disable stp

Description

This command is used to disable STP globally.

Format

disable stp

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable STP:

```
DAS-3626:admin# disable stp
Command: disable stp

Success.

DAS-3626:admin#
```

28-11 config stp version

Description

This command is used to configure the STP version.

Format

config stp version [mstp | rstp | stp]

Parameters

mstp - Specifies to use Multiple Spanning Tree Protocol.
rstp - Specifies to use Rapid Spanning Tree Protocol.
stp - Specifies to use Spanning Tree Protocol.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure STP version:

```
DAS-3626:admin#config stp version mstp
Command: config stp version mstp

Success.

DAS-3626:admin#
```

To config STP version with the same value of old configuration:

```
DAS-3626:admin#config stp version mstp
Command: config stp version mstp

 Configure value is the same with current value.
Success.

DAS-3626:admin#
```

28-12 config stp priority

Description

This command is used to configure the instance priority.

Format

config stp priority <value 0-61440> instance_id <value 0-4>

Parameters

<value 0-61440> - Enter the bridge priority value here. This value must be between 0 and 61440. This value must be divisible by 4096.
instance_id - Specifies the identifier to distinguish different STP instances. Instance 0 represents for default instance, CIST. **<value 0-4>** - Enter the STP instance ID here. This value must be between 0 and 15.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the STP instance ID:

```
DAS-3626:admin#config stp priority 61440 instance_id 0
Command: config stp priority 61440 instance_id 0

Success.

DAS-3626:admin#
```

28-13 config stp

Description

This command is used to configure the bridge parameters global settings.

Format

config stp {maxage <value 6-40> | maxhops <value 6-40> | hellotime <value 1-2> | forwarddelay <value 4-30> | txholdcount <value 1-10> | fbpdu [enable | disable] | nni_bpdu_addr [dot1d | dot1ad]}

Parameters

maxage - (Optional) Specifies to determine if a BPDU is valid. The default value is 20. **<value 6-40>** - Enter the maximum age value here. This value must be between 6-40.
maxhops - (Optional) Specifies to restrict the forwarded times of one BPDU. The default value is 20. **<value 6-40>** - Enter the maximum hops value here. This value must be between 6 and 40.
hello_time - (Optional) Specifies the time interval for sending configuration BPDUs by the Root Bridge. The default value is 2 seconds. This parameter is for STP and RSTP version. MSTP version uses per-port hellotime parameter. **<value 1-2>** - Enter the hello time value here. This value must be between 1 and 2.
forwarddelay - (Optional) Specifies the maximum delay time for one BPDU to be transmitted by a bridge and received from another bridge. The default value is 15. **<value 4-30>** - Enter the maximum delay time here. This value must be between 4 and 30.
txholdcount - (Optional) Specifies to restrict the numbers of BPDU transmitted in a time interval. **<value 1-10>** - Enter the transmitted BPDU restriction value here. This value must be between 1 and 10.
fbpdu - (Optional) Specifies to decide if the bridge will flood STP BPDU when STP functionality is disabled. **enable** - Specifies that the bridge will flood STP BPDU when STP functionality is disabled **disable** - Specifies that the bridge will not flood STP BPDU when STP functionality is disabled
nni_bpdu_addr - (Optional) Specifies to determine the BPDU protocol address for GVRP in service provide site. It can use 802.1d GVRP address, 802.1ad service provider GVRP address or an user defined mutilcast address. The range of the user defined address is 0180C2000000 - 0180C2FFFFFF. **dot1d** - Specifies that the NNI BPDU protocol address value will be set to Dot1d. **dot1ad** - Specifies that the NNI BPDU protocol address value will be set to Dot1ad.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure STP:

```
DAS-3626:admin#config stp maxage 25
Command: config stp maxage 25

Success.

DAS-3626:admin#
```

28-14 config stp ports

Description

This command is used to configure all the parameters of ports, except for Internal Path Cost and Port Priority.

Format

config stp ports <portlist> {externalCost [auto | <value 1-200000000>] | hellotime <value 1-2> | migrate [yes | no] | edge [true | false | auto] | p2p [true | false | auto] | state [enable | disable]| restricted_role [true | false] | restricted_tcn [true | false] | fbpdu [enable | disable]}

Parameters

<portlist> - Enter a list of ports used for the configuration here.
externalCost - (Optional) Specifies the path cost between MST regions from the transmitting Bridge to the CIST Root Bridge. It is only used at CIST level. **auto** - Specifies that the external cost value will be set to automatic. **<value 1-200000000>** - Enter the external cost value here. This value must be between 1 and 200000000.
hellotime - (Optional) Specifies the hello time of MSTP version. The default value is 2 . For STP and RSTP version, uses the per system hellotime parameter. **<value 1-2>** - Enter the hello time value here. This value must be between 1 and 2.
migrate - (Optional) Specifies the operation of management in order to specify the port to send MSTP BPDU for a delay time. **yes** - Specifies that the MSTP BPDU for a delay time will be sent. **no** - Specifies that the MSTP BPDU for a delay time will not be sent.
edge - (Optional) Specifies to decide if this port is connected to a LAN or a Bridged LAN. **true** - Specifies that the specified port(s) is edge. **false** - Specifies that the specified port(s) is not edge. **auto** – Specifies as auto mode. The bridge will delay for a period to become edge port if no bridge BPUD is received. The default is auto mode.
p2p - (Optional) Specifies to decide if this port is in Full-Duplex or Half-Duplex mode. **true** - Specifies that the port(s) is in Full-Duplex mode. **false** - Specifies that the port(s) is in Half-Duplex mode. **auto** - Specifies that the port(s) is in Full-Duplex and Half-Duplex mode.
state - (Optional) Specifies to decide if this port supports the STP functionality. **enable** - Specifies that STP functionality on the port(s) is enabled. **disable** - Specifies that STP functionality on the port(s) is disabled.
restricted_role - (Optional) Specifies to decide if this port not to be selected as Root Port. The default value is false. **true** - Specifies that the port can be specified as the root port. **false** - Specifies that the port can not be specified as the root port.
restricted_tcn - (Optional) Specifies to decide if this port not to propagate topology change. The default value is false. **true** - Specifies that the port can be set to propagate a topology change. **false** - Specifies that the port can not be set to propagate a topology change.
fbpdu - (Optional) Specifies to decide if this port will flood STP BPDU when STP functionality is disabled. When the state is set to enable, the received BPDU will be forwarded. When the state is set to disable, the received BPDU will be dropped. **enable** - Specifies that the port can be set to flood the STP BPDU when the STP functionality is disabled. **disable** - Specifies that the port can not be set to flood the STP BPDU when the STP functionality is disabled.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure STP ports:

```
DAS-3626:admin#config stp ports 1-10 externalCost auto
Command: config stp ports 1-10 externalCost auto

Success.

DAS-3626:admin#
```

28-15 config stp mst_ports

Description

This command is used to configure the ports management parameters.

Format

config stp mst_ports <portlist> instance_id <value 0-4> {internalCost [auto | <value 1-200000000>] | priority <value 0-240>}

Parameters

<portlist> - Enter a list of ports used only at CIST level for the configuration here.
instance_id - Specifies the instance ID used. **<value 0-4>** - Enter the instance ID used here. This value must be between 0 and 15.
internalCost - (Optional) Specifies the port path cost used in MSTP. **auto** - Specifies that the internal cost value will be set to auto. **<value 1-200000000>** - Enter the internal cost value here. This value must be between 1 and 200000000.
priority - (Optional) Specifies the port priority value. **<value 0-240>** - Enter the port priority value here. This value must be between 0 and 240.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure STP MST ports:

```
DAS-3626:admin#config stp mst_ports 1-10 instance_id 0 internalCost auto
Command: config stp mst_ports 1-10 instance_id 0 internalCost auto

Success.

DAS-3626:admin#
```

Chapter 29 Network Monitoring Command List

show packet ports <portlist>
show error ports <portlist>
show utilization [cpu | ports]
show utilization dram
show utilization flash
show utilization packet_buffer
clear counters {ports <portlist> | bonding <bgroup_list>}

29-1 show packet ports

Description

This command is used to display statistics about the packets sent and received by the switch.

Format

show packet ports <portlist>

Parameters

<portlist> - Enter a range of ports to be displayed.

Restrictions

None.

Example

To display the packets analysis for port 7:

```
DAS-3626:admin#show packet ports 7
Command: show packet ports 7

 Port Number : 7
 Frame Size/Type       Frame Counts                Frames/sec
 ---------------       ----------------------      -----------
 64                    0                           0
 65-127                0                           0
 128-255               0                           0
 256-511               0                           0
 512-1023              0                           0
 1024-1518             0                           0
 Unicast RX            0                           0
 Multicast RX          0                           0
 Broadcast RX          0                           0
 Unicast TX            0                           0
 Multicast TX          0                           0
 Broadcast TX          0                           0

 Frame Type            Total                       Total/sec
 ---------------       ----------------------      -----------
 RX Bytes              0                           0
 RX Frames             0                           0
 TX Bytes              0                           0
 TX Frames             0                           0
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

29-2 show error ports

Description

This command is used to display the error statistics for a range of ports.

Format

show errors ports <portlist>

Parameters

<portlist> - Ener a range of ports to be displayed.

Restrictions

None.

Example

To display the errors of the port 3:

```
DAS-3626:admin#show error ports 3
Command: show error ports 3


 Port Number : 3
                    RX Frames                                   TX Frames
                    ---------                                   ---------
 CRC Error          0                   Excessive Deferral    0
 Undersize          0                   CRC Error             0
 Oversize           0                   Late Collision        0
 Fragment           0                   Excessive Collision   0
 Jabber             0                   Single Collision      0
 Drop Pkts          0                   Collision             0
 Unknown Mcast Drop 0
 TrafficControl Drop 0
 Symbol Error       0
 ACL Meter Drop     0
 Ratelimit UDF Drop 0


CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

29-3 show utilization

Description

This command is used to display real-time CPU or port utilization statistics.

Format

show utilization [cpu | ports]

Parameters

cpu - Specifies to display information regarding the CPU.
ports - Specifies a range of ports to be displayed.

Restrictions

None.

Example

To display the ports utilization:

```
DAS-3626:admin#show utilization ports
Command: show utilization ports

Port TX(Byte/sec)   RX(Byte/sec)   Util Port TX(Byte/sec)   RX(Byte/sec)   Util
---- -------------- -------------- ---- ---- -------------- -------------- ----
1    0              0              0    21   0              0              0
2    0              0              0    22   0              0              0
3    0              0              0    23   0              0              0
4    0              0              0    24   0              0              0
5    0              0              0    25   0              63             1
6    0              0              0    26   0              0              0
7    0              0              0
8    0              0              0
9    0              0              0
10   0              0              0
11   0              0              0
12   0              0              0
13   0              0              0
14   0              0              0
15   0              0              0
16   0              0              0
17   0              0              0
18   0              0              0
19   0              0              0
20   0              0              0
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

To display the CPU utilization:

```
DAS-3626:admin#show utilization cpu
Command: show utilization cpu

CPU Utilization
-------------------------------------------------------------------------------
Five seconds -  18 %         One minute -  17 %         Five minutes -  17 %


CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

29-4 show utilization dram

Description

This command is used to display DRAM memory utilization.

Format

show utilization dram

Parameters

None.

Restrictions

None.

Example

To display DRAM utilization:

```
DAS-3626:admin#show utilization dram
Command: show utilization dram

DRAM utilization :
        Total DRAM      : 131072    KB
        Used DRAM       : 36640     KB
        Utilization     : 27 %



CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

29-5 show utilization flash

Description

This command is used to display the flash memory utilization.

Format

show utilization flash

Parameters

None.

Restrictions

None.

Example

To display FLASH utilization:

```
DAS-3626:admin#show utilization flash
Command: show utilization flash

Flash Memory Utilization :
        Total Flash     : 29618     KB
        Used Flash      : 13436     KB
        Utilization     : 45 %


CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

29-6 show utilization packet_buffer

Description

This command is used to display the utilization of current packet buffer.

Format

show utilization packet_buffer

Parameters

None.

Restrictions

None.

Example

To display the current packet buffer utilization:

```
DAS-3626:admin#show utilization packet_buffer
Command: show utilization packet_buffer

Packet Buffer Usage :  0 %


CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

29-7 clear counters

Description

This command is used to clear the switch's statistics counters. If no parameter is specified, system will display counters of all the ports.

Format

clear counters {ports <portlist> | bonding <bgroup_list>}

Parameters

ports - (Optional) Specifies a range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then highest switch number, and the highest port number of the range (also separeted by a colon) are specified. The beginning and end of the port list range are seperated by a dash. **<portlist>** - Enter a list of ports used for the configuration here.
bonding - (Optional) Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.

Restrictions

Only Administrators and Operators can issue this command.

Example

To clear the switch's statistics counters:

```
DAS-3626:admin#clear counters ports 7-9
Command: clear counters ports 7-9

Success.

DAS-3626:admin#
```

Chapter 30 Peripherals Command List

show device_status

30-1 show device_status

Description

This command is used to display the current status of power(s) and fan(s) on the system.

Format

show device_status

Parameters

None.

Restrictions

None.

Example

To show device status:

```
AS-3626:admin#show device_status
Command: show device_status

AC Power       :    Active
DC Power       :    Empty
 FAN TRAY INSERT

  FAN     RPM     Max     Min    Threshold(Hi/Lo)   Status   errCount
-------------------------------------------------------------------
   1      3276    3308    3096     3500 / 1100      Normal     0
   2      3308    3341    3096     3500 / 1100      Normal     0

 Sensor    deg C    Max   Min    Threshold(Hi/Lo)   Status   errCount
-------------------------------------------------------------------
   T1       42      42     28       95  / 0         Normal     0
   T2       39      39     29       83  / 0         Normal     0
   T3       41      41     28       93  / 0         Normal     0

DAS-3626:admin#
```

Chapter 31 Ping Command List

ping <ipaddr> {times <value 1-255> | timeout <sec 1-99> | size <value32-1500>}
ping6 <ipv6addr> {times <value 1-255> | size <value 1-6000> | timeout <sec 1-10>}

31-1 ping

Description

This command is used to send Internet Control Message Protocol (ICMP) echo messages to a remote IP address. The remote IP address will then “echo” or return the message. This is used to confirm connectivity between the switch and the remote device.

Format

ping <ipaddr> {times <value 1-255> | timeout <sec 1-99> | size <value32-1500>}

Parameters

<ipaddr> - Specifies the IP address of the host.
times - (Optional) Specifies the number of individual ICMP echo messages to be sent. The maximum value is 255. Press the "CTRL+C” to break the ping test. **<value 1-255>** - Enter the number of individual ICMP echo messages to be sent here. This value must be between 1 and 255.
timeout - (Optional) Specifies the time-out period while waiting for a response from the remote device. A value of 1 to 99 seconds can be specified. The default is 1 second. **<sec 1-99>** - Enter the time-out period here. This value must be between 1 and 99 seconds.
size - (Optional) Specifies size of the test packet. **<value32-1500>** - Enter the size of the test packet here. This value must be between 32 and 1500.

Restrictions

None.

Example

To send ICMP echo message to “10.51.17.1” for 4 times:

```
DAS-3626:admin# ping 10.51.17.1 times 4
Command: ping 10.51.17.1 times 4

Reply from 10.51.17.1, time<10ms
Reply from 10.51.17.1, time<10ms
Reply from 10.51.17.1, time<10ms
Reply from 10.51.17.1, time<10ms

Ping Statistics for 10.51.17.1
Packets: Sent =4, Received =4, Lost =0

DAS-3626:admin#
```

31-2 ping6

Description

This command is used to send IPv6 Internet Control Message Protocol (ICMP) echo messages to a remote IPv6 address. The remote IPv6 address will then “echo” or return the message. This is used to confirm the IPv6 connectivity between the switch and the remote device.

Format

ping6 <ipv6addr> {times <value 1-255> | size <value 1-6000> | timeout <sec 1-10>}

Parameters

<ipv6addr> - Enter the IPv6 address here.
times - (Optional) Specifies the number of individual ICMP echo messages to be sent. The maximum value is 255. Press the "CTRL+C” to break the ping test. **<value 1-255>** - Enter the number of individual ICMP echo messages to be sent here. This value must be between 1 and 255.
size - (Optional) Specifies size of the test packet. **<value 1-6000>** - Enter the size of the test packet here. This value must be between 1 and 6000.
timeout - (Optional) Specifies the time-out period while waiting for a response from the remote device. The default is 1 second. **<sec 1-10>** - Enter the time-out period here. This value must be between 1 and 10 seconds.

Restrictions

None.

Example

To send ICMP echo message to “3000::1” for 4 times:

```
DAS-3626:admin# ping6 3000::1 times 4
Command: ping6 3000::1 times 4

Reply from 3000::1, bytes=200, time<10ms
Reply from 3000::1, bytes=200, time<10ms
Reply from 3000::1, bytes=200, time<10ms
Reply from 3000::1, bytes=200, time<10ms

Ping Statistics for 3000::1
Packets: Sent =4, Received =4, Lost =0

DAS-3626:admin#
```

Chapter 32 Port Security Command List

config port_security bonding <bgroup_list> {admin_state [enable | disable] | max_learning_addr <max_lock_no 1-2048> | lock_address_mode [Permanent | DeleteOnTimeout | DeleteOnReset]}(1)
config port_security ports <portlist> {admin_state [enable | disable] | max_learning_addr <max_lock_no 1-2048> | lock_address_mode [Permanent | DeleteOnTimeout | DeleteOnReset]}(1)
config port_security vlan [<vlan_name 32> | vlanid <vidlist>] max_learning_addr <max_lock_no 1-512> {admin_state [enable | disable]}
delete port_security_entry vlan_name <vlan_name 32> mac_address <macaddr> [port <port> | bonding_group <bgroup>]
clear port_security_entry {port <portlist> | bonding <bgroup_list>}
show port_security {ports <portlist> | bonding <bgroup_list>}
show port_security_vlan {<vlan_name 32> | vlanid <vidlist>}
enable port_security trap_log
disable port_security trap_log

32-1 config port_security bonding

Description

This command is used to configure the admin state, the maximum number of addresses that can be learnt and the lock address mode for each VDSL bonding group.

Format

config port_security bonding <bgroup_list> {admin_state [enable | disable] | max_learning_addr <max_lock_no 1-2048> | lock_address_mode [Permanent | DeleteOnTimeout | DeleteOnReset]}(1)

Parameters

<bgroup_list> - Enter a list of VDSL bonding groups. The range is from 1 to 12.
admin_state - Specifies the state of the port security function for the VDSL bonding group. **enable** - Specifies to enable the port security function. **disable** - Specifies to disable the port security function. This is the default.
max_learning_addr - Specifies the maximum number of port security entries that can be learned for the VDSL bonding group. If the setting is smaller than the number of current learned entries of the VDSL bonding group, the command will be rejected. The default value is 32. **<max_lock_no 1-2048>** - Enter the maximum number of port security entries that can be learned here. This value must be between 1 and 2048.
lock_address_mode - Specifies the lock address mode. The default mode is deleteonreset. **Permanent** - The address will never be deleted unless the user removes it manually, the VLAN of the entry is removed, the port is removed from the VLAN, or port security is disabled on the port where the address resides. **DeleteOnTimeout** - Specifies that this entry will be removed if the entry is idle for the specified aging time. **DeleteOnReset** - Specifies that this address will be removed if the Switch is reset or rebooted. Events that cause permanent entries to be deleted also apply to the deleteonreset entries.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the bonding group security setting so that the maximum number of port security entries is restricted to 10, and the lock_address mode is set to permanent on bonding group 1:

```
DAS-3626:admin# config port_security bonding 1 admin_state enable
max_learning_addr 10 lock_address_mode Permanent
Command: config port_security bonding 1 admin_state enable max_learning_addr 10
lock_address_mode Permanent


Success.



DAS-3626:admin#
```

32-2 config port_security ports

Description

This command is used to configure the admin state, the maximum number of addresses that can be learnt and the lock address mode.

There are three levels that limit the number of learned entries; a port, a VLAN, and a bonding group. If any limitation is exceeded, the new entry will be discarded.

Format

config port_security ports <portlist> {admin_state [enable | disable] | max_learning_addr <max_lock_no 1-2048> | lock_address_mode [Permanent | DeleteOnTimeout | DeleteOnReset]}(1)

Parameters

<portlist> - Enter the list of port used for this configuration here.
admin_state - Specifies the state of the port security function on the port. **enable** - Specifies to enable the port security function on the port. **disable** - Specifies to disable the port security function on the port. By default, the setting is disabled.
max_learning_addr - Specifies the maximum number of port security entries that can be learned on this port. If the setting is smaller than the number of current learned entries on the port, the command will be rejected. The default value is 32. **<max_lock_no 1-2048>** - Enter the maximum number of port security entries that can be learned here. This value must be between 1 and 2048.
lock_address_mode - Specifies the lock address mode. The default mode is deleteonreset. **Permanent** - The address will never be deleted unless the user removes it manually, the VLAN of the entry is removed, the port is removed from the VLAN, or port security is disabled on the port where the address resides. **DeleteOnTimeout** - Specifies that this entry will be removed if the entry is idle for the specified aging time. **DeleteOnReset** - Specifies that this address will be removed if the Switch is reset or rebooted. Events that cause permanent entries to be deleted also apply to the deleteonreset entries.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the port-based port security setting so that the maximum number of port security entries is restricted to 10, and the lock_address mode is set to permanent on port 6:

```
DAS-3626:admin#config port_security ports 6 admin_state enable
max_learning_addr 10 lock_address_mode Permanent
Command: config port_security ports 6 admin_state enable max_learning_addr 10
lock_address_mode Permanent

Success.

DAS-3626:admin#
```

32-3 config port_security vlan

Description

This command is used to configure the maximum number of port security entries that can be learned on a specific VLAN.

There are three levels that limit the number of learned entries; a port, a VLAN, and a bonding group. If any limitation is exceeded, the new entry will be discarded.

Format

config port_security vlan [<vlan_name 32> | vlanid <vidlist>] max_learning_addr <max_lock_no 1-512> {admin_state [enable | disable]}

Parameters

<vlan_name 32> - Enter the VLAN name here. This name can be up to 32 characters long.
vlanid - Specifies a list of VLANs by VLAN ID. **<vidlist>** - Enter the VLAN ID list here.
max_learning_addr - Specifies the maximum number of port security entries that can be learned by this VLAN. If the setting is lower than the number of current learned entries on the VLAN, the command will be rejected. **<max_lock_no 1-512>** - Enter the maximum number of port security entries that can be learned here. This value must be between 1 and 512.
admin_state - Specifies the state of the port security function on the VLAN. **enable** - Specifies to enable the port security function. **disable** - Specifies to disable the port security function. By default, the setting is disabled.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the maximum number of VLAN-based port security entries on VLAN 1 to be 64:

```
DAS-3626:admin# config port_security vlan vlanid 1 max_learning_addr 64
admin_state enable
Command: config port_security vlan vlanid 1 max_learning_addr 64 admin_state
enable

 Cannot enable as it is Port Security by port enabled!

DAS-3626:admin#
```

32-4 delete port_security_entry vlan_name

Description

This command is used to delete a port security entry.

Format

delete port_security_entry vlan_name <vlan_name 32> mac_address <macaddr> [port <port> | bonding_group <bgroup>]

Parameters

<vlan_name 32> - Enter the VLAN name here. This name can be up to 32 characters long.
mac_address - Specifies the MAC address of the entry. **<macaddr>** - Enter the MAC address used here.
port - Specifies a port to be deleted. **<port>** - Enter a port to be deleted.
bonding_group - Specifies a VDSL bonding group. **<bgroup>** - Enter a VDSL bonding group. The range is from 1 to 12.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete the port security entry with a MAC address of 00-00-00-00-00-01 on VLAN 1:

```
DAS-3626:admin#delete port_security_entry vlan_name default mac_address 00-00-
00-00-00-01 port 6
Command: delete port_security_entry vlan_name default mac_address 00-00-00-00-
00-01 port 6

Success.

DAS-3626:admin#
```

32-5 clear port_security_entry

Description

This command is used to clear the MAC entries learned by the port security function.

Format

clear port_security_entry {port <portlist> | bonding <bgroup_list>}

Parameters

port - (Optional) Specifies the range of ports to be configured. **<portlist>** - Enter the port security entries learned on the specified port will be cleared.
bonding - (Optional) Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.

Restrictions

Only Administrators and Operators can issue this command.

Example

To clear the port security entries on port 6:

```
DAS-3626:admin# clear port_security_entry ports 6
Command: clear port_security_entry ports 6

Success.

DAS-3626:admin#
```

32-6 show port_security

Description

This command is used to display the port security related information, including state, maximum learned addresses and lock address mode on a port and/or a bonding group.

If both ports and bonding groups are specified, configurations matching any of these parameters will be displayed.

Format

show port_security {ports <portlist> | bonding <bgroup_list>}

Parameters

ports - (Optional) Specifies the range of ports that will show their configuration. **<portlist>** - Enter the list of port used for this configuration here.
bonding - (Optional) Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.

Restrictions

None.

Example

To display the global configuration of port security:

```
DAS-3626:admin#show port_security
Command: show port_security

Port_security Trap/Log : Enabled

 Port    Admin State  Max. Learning Addr.  Lock Address Mode
 -----   -----------  -------------------  -----------------
 b1      Enabled              10           Permanent
 b2      Disabled             64           DeleteOnTimeout
 b3      Disabled             64           DeleteOnTimeout
 b4      Disabled             64           DeleteOnTimeout
 b5      Disabled             64           DeleteOnTimeout
 b6      Disabled             64           DeleteOnTimeout
 b7      Disabled             64           DeleteOnTimeout
 b8      Disabled             64           DeleteOnTimeout
 b9      Disabled             64           DeleteOnTimeout
 b10     Disabled             64           DeleteOnTimeout
 b11     Disabled             64           DeleteOnTimeout
 b12     Disabled             64           DeleteOnTimeout
 25      Disabled             1024         DeleteOnTimeout
 26      Disabled             1024         DeleteOnTimeout

DAS-3626:admin#
```

32-7 show port_security_vlan

Description

This command is used to display the port security related information, including state, maximum learned addresses and lock address mode on the specified VLANs.

Format

show port_security_vlan {<vlan_name 32> | vlanid <vidlist>}

Parameters

<vlan_name 32> - (Optional) Enter the VLAN name here. This name can be up to 32 characters long.
vlanid - (Optional) Specifies a list of VLAN ID to be displayed. **<vidlist>** - Enter the VLAN ID list here.

Restrictions

None.

Example

To display the vlan configuration of port security:

```
DAS-3626:admin# show port_security_vlan vlanid 1
Command: show port_security_vlan vlanid 1

 VID  VLAN Name                        Admin State  Max. Learning Addr.
 ---- -------------------------------- ------------ -------------------
 1    default                          Disabled     64

DAS-3626:admin#
```

32-8 enable port_security trap_log

Description

This command is used to enable the port security trap/log. When the port security trap is enabled, if there is a new MAC address that violates the pre-defined port security configuration, a trap will be sent out with the MAC address, port and other relevant information being logged.

Format

enable port_security trap_log

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable the port security trap and save the log:

```
DAS-3626:admin#enable port_security trap_log
Command: enable port_security trap_log

Success.

DAS-3626:admin#
```

32-9 disable port_security trap_log

Description

This command is used to disable the port security trap/log. If the port security trap is disabled, no trap will be sent out for a MAC violation.

Format

disable port_security trap_log

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable the port security trap/log:

```
DAS-3626:admin# disable port_security trap_log
Command: disable port_security trap_log

Success.

DAS-3626:admin#
```

Chapter 33 Protocol VLAN Command List

create dot1v_protocol_group group_id <id> {group_name <name 32>}
config dot1v_protocol_group [group_id <id> | group_name <name 32>] [add protocol [ethernet_2 | ieee802.3_snap | ieee802.3_llc] <protocol_value> | delete protocol [ethernet_2 | ieee802.3_snap | ieee802.3_llc] <protocol_value>]
delete dot1v_protocol_group [group_id <id> | group_name <name 32> | all]
show dot1v_protocol_group {[group_id <id> | group_name <name 32>]}
config port dot1v [ports [<portlist> | all] | bonding <bgroup_list>] [add protocol_group [group_id <id> | group_name <name 32>] [vlan <vlan_name 32> | vlanid <id>] {priority <value 0-7>} | delete protocol_group [group_id <id> | all]]
show port dot1v {ports <portlist>}

33-1 create dot1v_protocol_group

Description

This command is used to create a protocol group for protocol VLAN function.

Format

create dot1v_protocol_group group_id < id> {group_name <name 32>}

Parameters

<id> - Enter the group ID which is used to identify a set of protocols. The range is from 1 to 16.
group_name - (Optional) Specifies the name of the protocol group. The maximum length is 32 chars. If group name is not specified, the group name will be automatically generated in accordance with ProtocolGroup+group_id. For example, the auto-generated name for group id 2 is ProtocolGroup2. If the auto-generated name is in conflict with an existing group, an alternative name will be used in accordance with ProtocolGroup+group_id+ALT+num. The value for num starts with 1. If it is still in conflict, then previous number will be used instead. **<name 32>** - Enter the group name here. This name can be up to 32 characters long.

Restrictions

Only Administrators and Operators can issue this command.

Example

To create a protocol group:

```
DAS-3626:admin#create dot1v_protocol_group group_id 10 group_name General_Group
Command: create dot1v_protocol_group group_id 10 group_name General_Group

Success.

DAS-3626:admin#
```

33-2 config dot1v_protocol_group add protocol

Description

This command is used to add a protocol to a protocol group. The selection of a protocol can be a pre-defined protocol type or a user defined protocol.

Format

config dot1v_protocol_group [group_id <id> | group_name <name 32>] [add protocol [ethernet_2 | ieee802.3_snap | ieee802.3_llc] <protocol_value> | delete protocol [ethernet_2 | ieee802.3_snap | ieee802.3_llc] <protocol_value>]

Parameters

group_id - Specifies the ID of the protocol group which is used to identify a set of protocols. **<id>** - Enter the group ID used here. The range is from 1 to 16.
group_name - Specifies the name of the protocol group. **<name 32>** - Enter the group name here. This name can be up to 32 characters long.
add protocol - Specifies that the protocol will be added to the specified group. **ethernet_2** - Specifies that the Ethernet 2 protocol will be used. **ieee802.3_snap** - Specifies that the IEEE 802.3 Snap protocol will be used. **ieee802.3_llc** - Specifies that the IEEE 802.3 LLC protocol will be used. **<protocol_value>** - Enter the protocol value here.
delete protocol - Specifies that the protocol will be removed from the specified group. **ethernet_2** - Specifies that the Ethernet 2 protocol will be used. **ieee802.3_snap** - Specifies that the IEEE 802.3 Snap protocol will be used. **ieee802.3_llc** - Specifies that the IEEE 802.3 LLC protocol will be used. **<protocol_value>** - Enter the protocol value here.

Restrictions

Only Administrators and Operators can issue this command.

Example

To add a protocol ipv6 to protocol group 100:

```
DAS-3626:admin#config dot1v_protocol_group group_id 10 add protocol ethernet_2
86DD
Command: config dot1v_protocol_group group_id 10 add protocol ethernet_2 86DD

Success.

DAS-3626:admin#
```

33-3 delete dot1v_protocol_group

Description

This command is used to delete a protocol group.

Format

delete dot1v_protocol_group [group_id <id> | group_name <name 32> | all]

Parameters

group_id - Specifies the group ID to be deleted. **<id>** - Enter the group ID used here. The range is from 1 to 16.
group_name - Specifies the name of the group to be deleted. **<name 32>** - Enter the group name here. This name can be up to 32 characters long.
all - Specifies that all the protocol group will be deleted.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete protocol group 8:

```
DAS-3626:admin#delete dot1v_protocol_group group_id 8
Command: delete dot1v_protocol_group group_id 8

Success.

DAS-3626:admin#
```

33-4 show dot1v_protocol_group

Description

This command is used to display the protocols defined in a protocol group. If no parameter is specified, all the configured protocol groups will be displayed.

Format

show dot1v_protocol_group {[group_id <id> | group_name <name 32>]}

Parameters

group_id - (Optional) Specifies the ID of the group to be displayed. **<id>** - Enter the group ID used here. The range is from 1 to 16.
group_name - (Optional) Specifies the name of the protocol group to be displayed. **<name 32>** - Enter the group name here. This name can be up to 32 characters long.

Restrictions

None.

Example

To display the protocol group ID 10:

```
DAS-3626:admin#show dot1v_protocol_group group_id 10
Command: show dot1v_protocol_group group_id 10

Protocol Group ID Protocol Group Name              Frame Type     Protocol
Value
----------------- -------------------------------- -------------- -------------
-
10                General_Group                    EthernetII     86DD

Total Entries: 1

DAS-3626:admin#
```

33-5 config port dot1v

Description

This command is used to assign the VLAN for untagged packets ingress from the port list based on the protocol group configured. This assignment can be removed by using the delete protocol_group option.

When priority is not specified in the command, the port default prority will be the priority for those untagged packets classified by the protocol vlan.

Format

config port dot1v [ports [<portlist> | all] | bonding <bgroup_list>] [add protocol_group [group_id <id> | group_name <name 32>] [vlan <vlan_name 32> | vlanid <id>] {priority <value 0-7>} | delete protocol_group [group_id <id> | all]]

Parameters

ports - Specifies a list of ports to be configured. **<portlist>** - Enter a list of ports used for the configuration here. **all** - Specifies that all the ports will be used for this configuration.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
add protocol_group - Specifies that the group specified will be added. **group_id** - Specifies the group ID of the protocol group. **<id>** - Enter the group ID used here. **group_name** - Specifies the name of the protocol group. **<name 32>** - Enter the name of the group used here. This name can be up to 32 characters long. **vlan** - The VLAN that is to be associated with this protocol group on this port. **<vlan_name 32>** - Enter the name of the VLAN here. This name can be up to 32 characters long. **vlanid** - Specifies the VLAN ID. **<id>** - Enter the VLAN ID used here. **priority** - (Optional) Specifies the priority to be associated with the packet which has been classified to the specified VLAN by the protocol. **<value 0-7>** - Enter the priority value here. This value must be between 0 and 7.
delete protocol_group - Specifies that the group specified will be deleted. **group_id** - Specifies the group ID of the protocol group. **<id>** - Enter the group ID used here. **all** - Specifies that all the groups will be deleted.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the group ID 10 on port 3 to be associated with VLAN, default:

```
DAS-3626:admin#config port dot1v ports 3 add protocol_group group_id 10 vlan
default
Command: config port dot1v ports 3 add protocol_group group_id 10 vlan default


Success.


DAS-3626:admin#
```

33-6 show port dot1v

Description

This command is used to display the VLAN to be associated with untagged packet ingressed from a port based on the protocol group. If no parameter is specified, information for all ports will be displayed.

Format

show port dot1v {ports <portlist>}

Parameters

ports - (Optional) Specifies a range of ports to be displayed. **<portlist>** - Enter a list of ports used for the configuration here.

Restrictions

None.

Example

The example display the protocol VLAN information for port 3:

```
DAS-3626:admin#show port dot1v ports 3
Command: show port dot1v ports 3

 Port: 3
 Group ID Group Name           VID  VLAN Name                        Prio
 -------- -------------------- ---- -------------------------------- ----
 10       General_Group        1    default                          -


Total Entries: 1

DAS-3626:admin#
```

Chapter 34 QinQ Command List

enable qinq
disable qinq
config qinq inner_tpid <hex 0x1 - 0xffff>
config qinq [ports [<portlist> | all] | bonding <bgroup_list>] {role [uni | nni] | missdrop [enable | disable] | outer_tpid <hex 0x1 - 0xffff> | add_inner_tag [<hex 0x1 - 0xffff> | disable]}
show qinq
show qinq inner_tpid
show qinq ports {<portlist>}
show qinq bonding <bgroup_list>
create vlan_translation [ports [<portlist> | all] | bonding <bgroup_list>] [add cvid <vidlist> | replace cvid <vlanid 1-4094>] svid <vlanid 1-4094> {priority <priority 0-7>}
delete vlan_translation [ports [<portlist> | all] | bonding <bgroup_list>] {cvid <vidlist>}
show vlan_translation {[ports <portlist> | bonding <bgroup_list> |cvid <vidlist>]}

34-1 enable qinq

Description

This command is used to enable QinQ. When QinQ is enabled, all network port roles will be NNI ports and outer TPID will be set to 0x88A8; all existing static VLANs will run as S-VLAN; all dynamic learned L2 address will be cleared; all dynamic registered VLAN entries will be cleared; and GVRP will be disabled.

To run GVRP on the switch, the administrator should enable GVRP manually. In QinQ mode, GVRP protocol will employ reserve address 01-80-C2-00-00-0D.

Format

enable qinq

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable QinQ:

```
DAS-3626:admin# enable qinq
Command: enable qinq

Success.

DAS-3626:admin#
```

34-2 disable qinq

Description

This command is used to disable the QinQ. When QinQ is disabled, all dynamic learned L2 addresses will be cleared, all dynamic registered VLAN entries will be cleared, and GVRP will be disabled.

To run GVRP on the switch, the administrator should enable GVRP manually.

Format

disable qinq

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable QinQ:

```
DAS-3626:admin# disable qinq
Command: disable qinq

Success.

DAS-3626:admin#
```

34-3 config qinq inner_tpid

Description

The command is used to configure the inner TPID of the system. The inner TPID is used to decide if the ingress packet is c-tagged. Inner tag TPID is per system configurable.

Format

config qinq inner_tpid <hex 0x1 - 0xffff>

Parameters

<hex 0x1-0xffff> - Enter the inner-TPID of the system here.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the inner TPID in the system to 0x9100:

```
DAS-3626:admin# config qinq inner_tpid 0x9100
Command: config qinq inner_tpid 0x9100

Success.

DAS-3626:admin#
```

34-4 config qinq

Description

This command is used to configure the QinQ port's parameters.

Format

config qinq [ports [<portlist> | all] | bonding <bgroup_list>] {role [uni | nni] | missdrop [enable | disable] | outer_tpid <hex 0x1 - 0xffff> | add_inner_tag [<hex 0x1 - 0xffff> | disable]}

Parameters

ports - Specifies a list of ports to be configured. **<portlist>** - Enter a list of ports used for the configuration here. **all** - Specifies that all the ports will be used for this configuration.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
role - (Optional) Specifies the port role in QinQ mode. **uni** - Specifies that the port is connecting to the customer network. **nni** - Specifies that the port is connecting to the service provider network.
missdrop - (Optional) Specifies the state of the miss drop of ports option. **enable** - Specifies that the miss drop of ports option will be enabled. **disable** - Specifies that the miss drop of ports option will be disabled.
outer_tpid - (Optional) Specifies the outer-TPID of a port. **<hex 0x1 - 0xffff>** - Enter the outer-TPID value used here.
add_inner_tag - (Optional) Specifies to add an inner tag for ingress untagged packets. If set, the inner tag will be added for the ingress untagged packets and therefore the packets that egress to the NNI port will be double tagged. If disable, only the s-tag will be added for ingress untagged packets. **<hex 0x1 - 0xffff>** - Enter the inner tag value used here. **disable** - Specifies that the add inner tag option will be disabled.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure port list 1-4 as NNI port and set the TPID to 0x88A8:

```
DAS-3626:admin#config qinq ports 1-4 role nni outer_tpid 0x88A8
Command: config qinq ports 1-4 role nni outer_tpid 0x88A8

Success.

DAS-3626:admin#
```

34-5 show qinq

Description

This command is used to display the global QinQ status.

Format

show qinq

Parameters

None.

Restrictions

None.

Example

To display the global QinQ status:

```
DAS-3626:admin#show qinq
Command: show qinq

 QinQ Status : Enabled

DAS-3626:admin#
```

34-6 show qinq inner_tpid

Description

This command is used to display the inner-TPID of a system.

Format

show qinq inner_tpid

Parameters

None.

Restrictions

None.

Example

To display the inner-TPID of a system:

```
DAS-3626:admin# show qinq inner_tpid
Command: show qinq inner_tpid

 Inner TPID: 0x9100


DAS-3626:admin#
```

34-7 show qinq ports

Description

This command is used to display the QinQ configuration of the ports.

Format

show qinq ports {<portlist>}

Parameters

<portlist> - (Optional) Enter the list of ports to be displayed here.

Restrictions

None.

Example

To show the QinQ mode for ports 1-2:

```
DAS-3626:admin#show qinq ports 1-2
Command: show qinq ports 1-2

Port ID:    1
------------------------------------------------------------
  Role:                     NNI
  Miss Drop:                Disabled
  Outer Tpid:               0x88a8
  Use Inner Priority:       Disabled
  Add Inner Tag:            Disabled

Port ID:    2
------------------------------------------------------------
  Role:                     NNI
  Miss Drop:                Disabled
  Outer Tpid:               0x88a8
  Use Inner Priority:       Disabled
  Add Inner Tag:            Disabled

DAS-3626:admin#
```

34-8 show qinq bonding

Description

This command is used to display the QinQ configuration of the bonding group.

Format

show qinq bonding <bgroup_list>

Parameters

<bgroup_list> - Enter a list of VDSL bonding groups. The range is from 1 to 12.

Restrictions

None.

Example

To show the QinQ mode for bonding group 1:

```
DAS-3626:admin# show qinq bonding 1
Command: show qinq bonding 1


Port ID:    b1
------------------------------------------------------------
  Role:                     NNI
  Miss Drop:                Disabled
  Outer Tpid:               0x8100
  Use Inner Priority:       Disabled
  Add Inner Tag:            Disabled

DAS-3626:admin#
```

34-9 create vlan_translation ports

Description

This command is used to create a VLAN translation rule. This setting will not be effective when the QinQ mode is disabled.

This configuration is only effective for a UNI port. At UNI port, the ingress C-VLAN tagged packets will be translated to S-VLAN tagged packets by adding or replacing according the configured rule. The S-VLAN Tag of egress packets at this port will be recovered to C-VLAN Tag or stripped.

Format

create vlan_translation [ports [<portlist> | all] | bonding <bgroup_list>] [add cvid <vidlist> | replace cvid <vlanid 1-4094>] svid <vlanid 1-4094> {priority <priority 0-7>}

Parameters

ports - Specifies a list of ports to be created. **<portlist>** - Enter a list of ports used here. **all** - Specifies that all the ports to be used here.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
add - Specifies to add an S-Tag to the packet. **cvid** - Specifies the customer VLAN ID used. **<vidlist>** - Enter the customer VLAN ID used here.
replace - Specifies to replace the C-Tag with the S-Tag. **cvid** - Specifies the customer VLAN ID used. **<vlanid 1-4094>** - Enter the customer VLAN ID used here.
svid - Specifies the service provider VLAN ID used. **<vlanid 1-4094>** - Enter the service provider VLAN ID used here.
priority - (Optional) Specifies to assign an 802.1p priority to the S-Tag. If the priority is not specified, a 802.1p priority of the S-Tag will be assigned by default. **<priority 0-7>** - Enter the 802.1p S-Tag priority value here. This value must be between 0 and 7.

Restrictions

Only Administrators and Operators can issue this command.

Example

To replace the C-Tag in which the CVID is 20, with the S-Tag and the S-VID is 200 at UNI Port 1:

```
DAS-3626:admin#create vlan_translation ports 1 replace cvid 20 svid 200
Command: create vlan_translation ports 1 replace cvid 20 svid 200

Success.

DAS-3626:admin#
```

34-10 delete vlan_translation ports

Description

This command is used to delete translation relationships between the C-VLAN and the S-VLAN.

Format

delete vlan_translation [ports [<portlist> | all] | bonding <bgroup_list>] {cvid <vidlist>}

Parameters

ports - Specifies a list of ports to be deleted. **<portlist>** - Enter a list of ports used here. **all** - Specifies that all the ports to be used here.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
cvid - (Optional) Specifies the rules for the specified CVIDs. If the CVID is not specified, all rules configured for the port will be deleted. **<vidlist>** - Enter the CVID value here.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete a VLAN translation rule on ports 1-4:

```
DAS-3626:admin#delete vlan_translation ports 1-4
Command: delete vlan_translation ports 1-4

Success.

DAS-3626:admin#
```

34-11 show vlan_translation

Description

This command is used to display the existing C-VLAN-based VLAN translation rules.

Format

show vlan_translation {[ports <portlist> | bonding <bgroup_list> |cvid <vidlist>]}

Parameters

ports - (Optional) Specifies a list of ports to be displayed. **<portlist>** - Enter the list of ports to be displayed here.
bonding - (Optional) Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
cvid - (Optional) Specifies the rules for the specified CVIDs. **<vidlist>** - Enter the CVID value used here.

Restrictions

None.

Example

To show C-VLANs based on VLAN translation rules in the system:

```
DAS-3626:admin#show vlan_translation
Command: show vlan_translation

Port    CVID       SPVID      Action    Priority
-----   --------   --------   -------   ---------
1       1          1          Add       -
2       1          1          Add       -
3       1          1          Add       -
4       1          1          Add       -

 Total Entries: 4


DAS-3626:admin#
```

Chapter 35 Quality of Service (QoS) Command List

config scheduling <class_id 0-7> { max_packet <value 1-255>}
config scheduling_mechanism [strict | wrr]
show scheduling
show scheduling_mechanism
config 802.1p user_priority <priority 0-7> <class_id 0-7>
show 802.1p user_priority
config 802.1p default_priority [<portlist> | all | bonding <bgroup_list>] <priority 0-7>
show 802.1p default_priority {<portlist> | bonding <bgroup_list>}
config dscp trust [<portlist> | bonding <bgroup_list> | all] state [enable | disable]
show dscp trust [<portlist> | bonding <bgroup_list> | all]
config dscp map dscp_priority <dscp 0-63> to <priority 0-7>
show dscp map {<portlist>} [dscp_priority | dscp_dscp] {dscp <dscp_list>}

35-1 config scheduling

Description

This command is used to configure the traffic scheduling mechanism for each CoS queue.

Format

config scheduling <class_id 0-7> { max_packet <value 1-255>}

Parameters

<class_id 0-7> - Enter the hardware priority. The hardware priority queues are identified by number from 0 to 7 with the 0 queue being the lowest priority.
max_packet - Specifies to use weighted fair algorithm to handle packets in priority queues. Each queue will operate based on its setting of max_packet. **<value 1-255>** - Enter the value between 1 and 255.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the weight of priority 1 to 20:

```
DAS-3626:admin# onfig scheduling 1 max_packet 20
Command: config scheduling 1 max_packet 20

Success.

DAS-3626:admin#
```

35-2 config scheduling_mechanism

Description

This command is used to configure the traffic scheduling mechanism for each CoS queue.

Format

config scheduling_mechanism [strict | wrr]

Parameters

strict - All queues operate in strict mode.
wrr - Each queue operates based on its setting.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the traffic scheduling mechanism for each CoS queue:

```
DAS-3626:admin# config scheduling_mechanism strict
Command: config scheduling_mechanism strict

Success.

DAS-3626:admin#
```

35-3 show scheduling

Description

This command is used to display the current traffic scheduling parameters.

Format

show scheduling

Parameters

None.

Restrictions

None.

Example

To display the traffic scheduling parameters:

```
DAS-3626:admin#show scheduling
Command: show scheduling


QOS Output Scheduling

Class ID  Max. Packets
--------  -------------
Class-0   1
Class-1   20
Class-2   3
Class-3   4
Class-4   5
Class-5   6
Class-6   7
Class-7   8


DAS-3626:admin#
```

35-4 show scheduling_mechanism

Description

This command is used to show the traffic scheduling mechanism.

Format

show scheduling_mechanism

Parameters

None.

Restrictions

None.

Example

To show scheduling mechanism:

```
DAS-3626:admin#show scheduling_mechanism
Command: show scheduling_mechanism

QOS scheduling_mechanism
Class ID  Mechanism
--------  -----------
Class-0   Strict
Class-1   Strict
Class-2   Strict
Class-3   Strict
Class-4   Strict
Class-5   Strict
Class-6   Strict
Class-7   Strict


DAS-3626:admin#
```

35-5 config 802.1p user_priority

Description

This command is used to map the 802.1p user priority of an incoming packet to one of the eight hardware queues available on the switch.

Format

config 802.1p user_priority <priority 0-7> <class_id 0-7>

Parameters

<priority 0-7> - The 802.1p user priority you want to associate with the <class_id> (the number of the hardware queue) with.
<class_id 0-7> - The number of the switch's hardware priority queue. The switch has 8 hardware priority queues available. They are numbered between 0 (the lowest priority) and 7 (the highest priority).

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the 802.1p user priority:

```
DAS-3626:admin#config 802.1p user_priority 1 3
Command: config 802.1p user_priority 1 3

Success.

DAS-3626:admin#
```

35-6 show 802.1p user_priority

Description

This command is used to display 802.1p user priority for ports.

Format

show 802.1p user_priority

Parameters

None.

Restrictions

None.

Example

To display the 802.1p user priority:

```
DAS-3626:admin#show 802.1p user_priority
Command: show 802.1p user_priority


QOS Class of Traffic

Priority-0  ->  <Class-0>
Priority-1  ->  <Class-3>
Priority-2  ->  <Class-2>
Priority-3  ->  <Class-3>
Priority-4  ->  <Class-4>
Priority-5  ->  <Class-5>
Priority-6  ->  <Class-6>
Priority-7  ->  <Class-7>


DAS-3626:admin#
```

35-7 config 802.1p default_priority

Description

Ths command is used to configure the 802.1p default priority settings on the switch. If an untagged packet is received by the switch, the priority configured with this command will be written to the packet's priority field.

Format

config 802.1p default_priority [<portlist> | all | bonding <bgroup_list>] <priority 0-7>

Parameters

<portlist> - Enter a range of ports for which the default priority is to be configured.
all - Specifies that the command apply to all ports on the switch.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
<priority 0-7> - The priority value (0 to 7) assigned to untagged packets received by the switch or a range of ports on the switch.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the 802.1p default priority settings on the switch:

```
DAS-3626:admin#config 802.1p default_priority all 5
Command: config 802.1p default_priority all 5

Success.

DAS-3626:admin#
```

35-8 show 802.1p default_priority

Description

This command is used to display the current configured default priority settings on the switch.

The default priority can also be assigned by the RADIUS server through the authentication process. The authentication with the RADIUS sever can be per port or port user. For per port authentication, the priority assigned by RADIUS server will be the effective port default priority. For per user authentication, the priority assigned by RADIUS will not be the effective port default priority whereas it will become the priority associated with MAC address. Note that only devices supporting MAC-based VLAN can provide per user authentication. If no parameter is specified, all ports for 802.1p default priority will be displayed.

Format

show 802.1p default_priority {<portlist> | bonding <bgroup_list>}

Parameters

<portlist> - (Optional) Specified a range of ports to be displayed.
bonding - (Optional) Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.

Restrictions

None.

Example

To display 802.1p default priority:

```
DAS-3626:admin#show 802.1p default_priority 1-10
Command: show 802.1p default_priority 1-10

 Port   Priority
 -----  --------
 1      5
 2      5
 3      5
 4      5
 5      5
 6      5
 7      5
 8      5
 9      5
 10     5

DAS-3626:admin#
```

35-9 config dscp trust

Description

This command is used to configure the state of DSCP trust per port. When DSCP is not trusted, 802.1p is trusted.

Format

config dscp trust [<portlist> | bonding <bgroup_list> | all] state [enable | disable]

Parameters

<portlist> - Enter the list of port used for this configuration here.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
all - Specifies that the command apply to all ports on the switch.
state - Enable or disable to trust DSCP. By default, DSCP trust is disabled. **enable** - Specifies that the DSCP trust state will be enabled. **disable** - Specifies that the DSCP trust state will be disabled.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable DSCP trust on ports 1-8:

```
DAS-3626:admin#config dscp trust 1-8 state enable
Command: config dscp trust 1-8 state enable

Success.

DAS-3626:admin#
```

35-10 show dscp trust

Description

This command is used to display DSCP trust state for the specified ports on the switch.

Format

show dscp trust [<portlist> | bonding <bgroup_list> | all]

Parameters

<portlist> - (Optional) A range of ports to display.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
all - Specifies that the command apply to all ports on the switch.

Restrictions

None.

Example

To display DSCP trust status on ports 1-8:

```
DAS-3626:admin#show dscp trust ports 1-8
Command: show dscp trust ports 1-8

Port DSCP-Trust
---- ----------
1    Enabled
2    Enabled
3    Enabled
4    Enabled
5    Enabled
6    Enabled
7    Enabled
8    Enabled

DAS-3626:admin#
```

35-11 config dscp map dscp_priority

Description

This command is used to determine the priority of the packet (which will be then used to determine the scheduling queue) when the port is in DSCP trust state.

The DSCP mapping will take effect at the same time when IP packet ingress from a DSCP-trusted port.

Format

config dscp map dscp_priority <dscp 0-63> to <priority 0-7>

Parameters

<dscp 0-63> - Enter a list of DSCP value to be mapped to a specific priority.
to - Specifies that the above or following parameter will be mapped to the previously mentioned parameter. **<priority 0-7>** - Specifies the result priority of mapping.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the mapping of the DSCP priority to priority 1:

```
DAS-3626:admin#config dscp map dscp_priority 1 to 1
Command: config dscp map dscp_priority 1 to 1

Success.

DAS-3626:admin#
```

35-12 show dscp map dscp_priority

Description

This command is used to display the DSCP value to be mapped to a specific priority.

Format

show dscp map dscp_priority

Parameters

None.

Restrictions

None.

Example

To display the DSCP value to be mapped to a specific priority:

```
DAS-3626:admin#show dscp map dscp_priotity
Command: show dscp map dscp_priotity

DSCP    Priority
------  --------
0       0
1       1
2       0
3       0
4       0
5       0
6       0
7       0
8       1
9       1
10      1
11      1
12      1
13      1
14      1
15      1
16      2
17      2
18      2
19      2
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

Chapter 36 Remote Switched Port ANalyzer (RSPAN) Command List

enable rspan
disable rspan
create rspan vlan [vlan_name <vlan_name> | vlan_id <value 1-4094>]
delete rspan vlan [vlan_name <vlan_name> | vlan_id <value 1-4094>]
config rspan vlan [vlan_name <vlan_name> | vlan_id <vlanid 1-4094>] [redirect [add | delete] ports <portlist> | source {[add | delete] ports <portlist> [rx | tx | both]}]
show rspan {[vlan_name <vlan_name> | vlan_id <vlanid 1-4094>]}

36-1 enable rspan

Description

This command is used to enable the RSPAN function. The purpose of the RSPAN function is to mirror packets to a remote switch.

A packet travels from the switch where the monitored packet is received, passing through the intermediate switch, and then to the switch where the sniffer is attached. The first switch is also named the source switch.

To make the RSPAN function work, the RSPAN VLAN source setting must be configured on the source switch. For the intermediate and the last switch, the RSPAN VLAN redirect setting must be configured.

Note: RSPAN VLAN mirroring will only work when RSPAN is enabled (when one RSPAN VLAN has been configured with a source port).

The RSPAN redirect function will work when RSPAN is enabled and at least one RSPAN VLAN has been configured with redirect ports.

Format

enable rspan

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure RSPAN state to enable:

```
DAS-3626:admin# enable rspan
Command: enable rspan

Success.

DAS-3626:admin#
```

36-2 disable rspan

Description

This command is used to disable the RSPAN function.

Format

disable rspan

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure RSPAN state to disabled:

```
DAS-3626:admin# disable rspan
Command: disable rspan

Success.

DAS-3626:admin#
```

36-3 create rspan vlan

Description

This command is used to create the RSPAN VLAN. Up to 16 RSPAN VLANs can be created.

Format

create rspan vlan [vlan_name <vlan_name> | vlan_id <value 1-4094>]

Parameters

vlan_name - Specifies the RSPAN VLAN by VLAN name. **<vlan_name>** - Enter the VLAN name here.	
vlan_id - Specifies the RSPAN VLAN by VLAN ID. **<value 1-4094>** - Enter the VLAN ID here. This value must be between 1 and 4094.	

Restrictions

Only Administrators and Operators can issue this command.

Example

To create an RSPAN VLAN entry by VLAN name “v2”:

```
DAS-3626:admin#create rspan vlan vlan_name v2
Command: create rspan vlan vlan_name v2

Success.

DAS-3626:admin#
```

36-4 delete rspan vlan

Description

This command is used to delete RSPAN VLANs.

Format

delete rspan vlan [vlan_name <vlan_name> | vlan_id <value 1-4094>]

Parameters

vlan_name - Specifies to delete an RSPAN VLAN by VLAN name.	
	<vlan_name> - Enter the VLAN name here.
vlan_id - Specifies to delete an RSPAN VLAN by VLAN ID.	
	<value 1-4094> - Enter the VLAN ID here. This value must be between 1 and 4094.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete an RSPAN VLAN entry by VLAN name “v2”:

```
DAS-3626:admin#delete rspan vlan vlan_name v2
Command: delete rspan vlan vlan_name v2

Success.

DAS-3626:admin#
```

36-5 config rspan vlan

Description

This command is used to configure the source setting for the RSPAN VLAN on the source switch or configures the redirect port on the intermediate switch and destination switch..

Format

config rspan vlan [vlan_name <vlan_name> | vlan_id <vlanid 1-4094>] [redirect [add | delete] ports <portlist> | source {[add | delete] ports <portlist> [rx | tx | both]}]

Parameters

vlan_name - Specifies the RSPAN VLAN by VLAN name. **<vlan_name>** - Enter the VLAN name here.
vlan_id - Specifies the RSPAN VLAN by VLAN ID. **<value 1-4094>** - Enter the VLAN ID here. This value must be between 1 and 4094.
redirect - Specifies output portlist for the RSPAN VLAN packets. If the redirect port is a Link Aggregation port, there will perform the Link Aggregation behavior for RSPAN packets. **add** - Specifies to add output ports for the RSPAN VLAN packets. **delete** - Specifies to delete output ports for the RSPAN VLAN packets. **ports** - Specifies the output ports for the RSPAN VLAN packets. **<portlist>** - Enter the list of ports that will be used for this configuration here.
source - Specifies the source ports. If the ports are not specified by this command, the source of RSPAN will come from the source specified by the mirror command or the flow-based source specified by an ACL. If no parameter is specified for source, it deletes the configured source parameters. **add** - (Optional) Specifies to add source ports. **delete** - (Optional) Specifies to delete source ports. **ports** - (Optional) Specifies the source portlist to add to or delete from the RSPAN source. **<portlist>** - Enter the list of ports that will be used for this configuration here. **rx** - (Optional) Specifies to only monitor ingress packets. **tx** - (Optional) Specifies to only monitor egress packets. **both** - (Optional) Specifies to monitor both ingress and egress packets.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure an RSPAN source entry without source target port:

```
DAS-3626:admin#config rspan vlan vlan_name v2 source add ports 2-5 rx
Command: config rspan vlan vlan_name v2 source add ports 2-5 rx

Success.

DAS-3626:admin#
```

36-6 show rspan

Description

This command is used to display the RSPAN configuration.

Format

show rspan {[vlan_name <vlan_name> | vlan_id <vlanid 1-4094>]}

Parameters

vlan_name - (Optional) Specifies the RSPAN VLAN by VLAN name **<vlan_name>** - Enter the VLAN name here.
vlan_id - (Optional) Specifies the RSPAN VLAN by VLAN ID. **<value 1-4094>** - Enter the VLAN ID here. This value must be between 1 and 4094.

Restrictions

None.

Example

To display the RSPAN configuration:

```
DAS-3626:admin#show rspan
Command: show rspan

RSPAN   : Disabled

RSPAN VLAN ID  : 2
--------------------
  Source Port
      RX            : 2-5
      TX            :

Total RSPAN VLAN :1


DAS-3626:admin#
```

Chapter 37 Safeguard Engine Command List

config safeguard_engine {state [enable | disable] | utilization {rising <value 20-100> | falling <value 20-100>} | trap_log [enable | disable] | mode [strict | fuzzy]}
show safeguard_engine

37-1 config safeguard_engine

Description

This command is used to configure the CPU protection control for the system.

Format

config safeguard_engine {state [enable | disable] | utilization {rising <value 20-100> | falling <value 20-100>} | trap_log [enable | disable] | mode [strict | fuzzy]}

Parameters

state - (Optional) Specifies the CPU protection state to enable or disable. **enable** - Specifies that CPU protection will be enabled. **disable** - Specifies that CPU protection will be enabled.
utilization - (Optional) Specifies the CPU protection threshold. **rising** - Specifies the utilization rising threshold , the range is between 20%-100% , if the CPU utilization is over the rising threshold, the switch enters exhausted mode. **<value 20-100>** - Enter the utilization rising value here. This value must be between 20 and 100. **falling** - Specifies the utilization falling threshold , the range is between 20%-100% , if the CPU utilization is lower than the falling threshold, the switch enters normal mode. **<value 20-100>** - Enter the utilization falling value here. This value must be between 20 and 100.
trap_log - (Optional) Specifies the state of CPU protection related trap/log mechanism to enable or disable. If set to enable, trap and log will be active while cpu protection current mode changed.If set to disable, current mode change will not trigger trap and log events. **enable** - Specifies that the CPU protection trap or log mechanism will be enabled. **disable** - Specifies that the CPU protection trap or log mechanism will be disabled.
mode - (Optional) Specifies the controlling method of broadcast traffic. **strict** - Specifies to strct mode. The Switch will stop receiving all ‘ARP not to me’ packets (the protocol address of target in ARP packet is the Switch itself). That means no matter what reasons cause the high CPU utilization (may not caused by ARP storm), the Switch reluctantly processes any ’ARP not to me’ packets in exhausted mode. **fuzzy** - Specifies to fuzzy mode. The Switch will adjust the bandwidth dynamically depend on some reasonable algorithm.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure CPU protection:

```
DAS-3626:admin#config safeguard_engine state enable utilization rising 50
falling 30 trap_log enable
Command: config safeguard_engine state enable utilization rising 50 falling 30
trap_log enable

Success.

DAS-3626:admin#
```

37-2 show safeguard_engine

Description

This command is used to show safeguard engine information.

Format

show safeguard_engine

Parameters

None.

Restrictions

None.

Example

To show safeguard_engine information:

```
DAS-3626:admin#show safeguard_engine
Command: show safeguard_engine



Safeguard Engine State          :  Enabled
Safeguard Engine Current Status :  Normal Mode
==================================================
CPU Utilization Information:
Rising Threshold  :  50%
Falling Threshold :  30%
Trap/Log State    :  Enabled
Mode              :  Fuzzy

DAS-3626:admin#
```

Note: Safeguard engine current status has two modes: exhausted and normal mode.

Chapter 38 Secure Shell (SSH) Command List

config ssh algorithm [3DES | AES128 | AES192 | AES256 | arcfour | blowfish | cast128 | twofish128 | twofish192 | twofish256 | MD5| SHA1 | RSA | DSA] [enable | disable]
show ssh algorithm
config ssh authmode [password | publickey | hostbased] [enable | disable]
show ssh authmode
config ssh user <username 15> authmode [hostbased [hostname <domain_name 32> | hostname_IP <domain_name 32> [<ipaddr> | <ipv6addr>]] | password | publickey]
show ssh user authmode
config ssh server {maxsession <int 1-8> | contimeout <sec 120-600> | authfail <int 2-20> | rekey [10min | 30min | 60min | never] | port <tcp_port_number 1-65535>}
enable ssh
disable ssh
show ssh server

38-1 config ssh algorithm

Description

This command is used to configure SSH service algorithm.

Format

config ssh algorithm [3DES | AES128 | AES192 | AES256 | arcfour | blowfish | cast128 | twofish128 | twofish192 | twofish256 | MD5| SHA1 | RSA | DSA] [enable | disable]

Parameters

3DES - Specifies the SSH algorithim as 3DES. The "3DES" cipher is three-key triple-DES (encrypt-decrypt-encrypt), where the first 8 bytes of the key are used for the first encryption, the next 8 bytes for the decryption, and the following 8 bytes for the final encryption.
AES (128,192,256) - Specifies the SSH algorithim as Advanced Encryption Standard.
arcfour - Specifies the SSH algorithim as RC4. RC4 (also known as ARC4 or ARCFOUR meaning Alleged RC4) is the most widely-used software stream cipher.
blowfish - Specifies the SSH algorithim as Blowfish is a keyed, symmetric block cipher.
cast128 - Specifies the SSH algorithim as CAST-128. CAST-128 is a 12- or 16-round feistel network with a 64-bit block size and a key size of between 40 to 128 bits.
twofish (128,192,256) - Specifies the SSH algorithim as twofish. Twofish has a 128-bit block size, a key size ranging from 128 to 256 bits.
MD5 - Specifies the SSH algorithim as Message-Digest Algorithm 5.
SHA1 - Specifies the SSH algorithim as Secure Hash Algorithm.
RSA - Specifies the SSH algorithim as RSA. RSA encryption algorithm is a non-symmetric encryption algorithm.
DSS - Specifies the SSH algorithim as Digital Signature Standard.
enable - Specifies to enable the algorithm.
disable - Specifies to disable the algorithm.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable SSH server public key algorithm:

```
DAS-3626:admin#config ssh algorithm 3DES enable
Command: config ssh algorithm 3DES enable

Success.

DAS-3626:admin#
```

38-2 show ssh algorithm

Description

This command is used to display the SSH service algorithm.

Format

show ssh algorithm

Parameters

None.

Restrictions

None.

Example

To show server algorithm:

```
DAS-3626:admin#show ssh algorithm
Command: show ssh algorithm

Encryption Algorithm
--------------------------
3DES       : Enabled
AES128     : Enabled
AES192     : Enabled
AES256     : Enabled
Arcfour    : Enabled
Blowfish   : Enabled
Cast128    : Enabled
Twofish128 : Enabled
Twofish192 : Enabled
Twofish256 : Enabled

Data Integrity Algorithm
--------------------------
MD5        : Enabled
SHA1       : Enabled

Public Key Algorithm
--------------------------
RSA        : Enabled
DSA        : Enabled
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

38-3 config ssh authmode

Description

This command is used to configure user authentication method for SSH.

Format

config ssh authmode [password | publickey | hostbased] [enable | disable]

Parameters

password - Specifies user authentication method as password.
publickey - Specifies user authentication method as public key.
hostbased - Specifies user authentication method as host-based.
enable - Specifies to enable user authentication method.
disable - Specifies to disable user authentication method.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure user authentication method:

```
DAS-3626:admin# config ssh authmode publickey enable
Command: config ssh authmode publickey enable

Success.

DAS-3626:admin#
```

38-4 show ssh authmode

Description

This command is used to display the user authentication method.

Format

show ssh authmode

Parameters

None.

Restrictions

None.

Example

To show user authentication method:

```
DAS-3626:admin#show ssh authmode
Command: show ssh authmode

The SSH Authentication Method:
Password    : Enabled
Public Key  : Enabled
Host-based  : Enabled


DAS-3626:admin#
```

38-5 config ssh user

Description

This command is used to configure the user information for SSH configuration.

Format

config ssh user <username 15> authmode [hostbased [hostname <domain_name 32> | hostname_IP <domain_name 32> [<ipaddr> | <ipv6addr>]] | password | publickey]

Parameters

<username 15> - Enter the user name used here. This name can be up to 15 characters long.
authmode - Specifies the authentication method. **hostbased** - Specifies user authentication method as host-based. **hostname** - Specifies host domain name. **<domain_name 32>** - Enter the domain name here. This name can be up to 32 characters long. **hostname_IP** - Specifies host domain name and IP address. **<domain_name 32>** - Specifies host name if configuring Host-based method. **<ipaddr>** - Specifies host IP address if configuring Host-based method. **<ipv6addr>** - Specifies host IPv6 address if configuring Host-based method. **password** - Specifies user authentication method. **publickey** - Specifies user authentication method.

Restrictions

Only Administrators can issue this command.

Example

To update user “test” authentication method:

```
DAS-3626:admin# config ssh user test authmode publickey
Command: config ssh user test authmode publickey

Success.

DAS-3626:admin#
```

38-6 show ssh user

Description

This command is used to display the SSH user information.

Format

show ssh user authmode

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To show user information about SSH configuration:

```
DAS-3626:admin# show ssh user authmode
Command: show ssh user authmode

Current Accounts
Username          AuthMode             HostName            HostIP
------------  -------------        ------------      -------------
test              Public Key
alpha             Host-based           alpha-local        172.18.61.180
beta              Host-based           beta-local          3000::105
Total Entries : 3

DAS-3626:admin#
```

38-7 config ssh server

Description

This command configures the SSH server general information.

Format

config ssh server {maxsession <int 1-8> | contimeout <sec 120-600> | authfail <int 2-20> | rekey [10min | 30min | 60min | never]}

Parameters

maxsession - (Optional) Specifies SSH server maximum session at the same time, maximum 8 sessions. **<int 1-8>** - Enter the maximum session value here. This value must be between 1 and 8.
contimeout - (Optional) Specifies SSH server connection time-out, in the unit of second. **<sec 120-600>** - Enter the connection time-out value here. This value must be between 120 and 600 seconds.
authfail - (Optional) Specifies user maximum fail attempts. **<int 2-20>** - Enter the user maximum fail attempts value here. This value must be between 2 and 20.
rekey - (Optional) Specifies time to re-generate session key. There are 10 minutes, 30 minutes, 60 minutes and never for the selection, which the never means do NOT re- generate session key **10min** - Specifies that the re-generate session key time will be 10 minutes. **30min** - Specifies that the re-generate session key time will be 30 minutes. **60min** - Specifies that the re-generate session key time will be 60 minutes. **never** - Specifies that the re-generate session key time will be set to never.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure SSH server maximum session number is 3:

```
DAS-3626:admin# config ssh server maxsession 3
Command: config ssh server maxsession 3

Success.

DAS-3626:admin#
```

38-8 enable ssh

Description

This command is used to enable SSH server services. When enabling SSH, Telnet will be disabled.

Format

enable ssh

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable SSH server:

```
DAS-3626:admin# enable ssh
Command: enable ssh

Success.

DAS-3626:admin#
```

38-9 disable ssh

Description

This command is used to disable SSH server services.

Format

disable ssh

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable the SSH server services:

```
DAS-3626:admin#disable ssh
Command: disable ssh

Success.

DAS-3626:admin#
```

38-10 show ssh server

Description

This command is used to display the SSH server general information.

Format

show ssh server

Parameters

None.

Restrictions

None.

Example

To show SSH server:

```
DAS-3626:admin#show ssh server
Command: show ssh server

The SSH Server Configuration
Maximum Session              : 3
Connection Timeout           : 120
Authentication Fail Attempts : 2
Rekey Timeout                : Never
TCP Port Number              : 22


DAS-3626:admin#
```

Chapter 39 Secure Sockets Layer (SSL) Command List

download ssl certificate <ipaddr> certfilename <path_filename 64> keyfilename <path_filename 64>
enable ssl {ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5}}
disable ssl {ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5}}
show ssl {certificate}
show ssl cachetimeout
config ssl cachetimeout <value 60-86400>

39-1 download ssl certificate

Description

This command is used to download the certificate to the device according to the certificate level. The user can download the specified certificate to the device which must, according to desired key exchange algorithm. For RSA key exchange, the user must download RSA type certificate and for DHS_DSS is using the DSA certificate for key exchange.

Format

download ssl certificate <ipaddr> certfilename <path_filename 64> keyfilename <path_filename 64>

Parameters

<ipaddr> - Enter the TFTP server IP address used for this configuration here.
certfilename - Specifies the desired certificate file name. **<path_filename 64>** - Enter the certificate file path respect to TFTP server root path, and input characters max to 64 octets.
keyfilename - Specifies the private key file name which accompany with the certificate. **<path_filename 64>** - Enter the private key file path respect to TFTP server root path, and input characters max to 64 octets.

Restrictions

Only Administrators can issue this command.

Example

To download certificate from TFTP server:

```
DAS-3626:admin# download ssl certificate 10.55.47.1 certfilename cert.der
keyfilename pkey.der
Command: download ssl certificate 10.55.47.1 certfilename cert.der keyfilename
pkey.der

Success.

DAS-3626:admin#
```

39-2 enable ssl

Description

This command is used to enable SSL feature which means enable SSLv3 and TLSv1. For each ciphersuites, user must specify it by this command.

Format

enable ssl {ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5}}

Parameters

ciphersuite - (Optional) Specifies the cipher suite combination used for this configuration.
- **RSA_with_RC4_128_MD5** - (Optional) Specifies RSA key exchange with RC4 128 bits encryption and MD5 hash.
- **RSA_with_3DES_EDE_CBC_SHA** - (Optional) Specifies RSA key exchange with 3DES_EDE_CBC encryption and SHA hash.
- **DHE_DSS_with_3DES_EDE_CBC_SHA** - (Optional) Specifies DH key exchange with 3DES_EDE_CBC encryption and SHA hash.
- **RSA_EXPORT_with_RC4_40_MD5** - (Optional) Specifies RSA_EXPORT key exchange with RC4 40 bits encryption and MD5 hash.

Restrictions

Only Administrators can issue this command.

Example

To enable the SSL ciphersuite for RSA_with_RC4_128_MD5:

```
DAS-3626:admin# enable ssl ciphersuite RSA_with_RC4_128_MD5
Command: enable ssl ciphersuite RSA_with_RC4_128_MD5

Success.

DAS-3626:admin#
```

To enable SSL:

```
DAS-3626:admin# enable ssl
Command: enable ssl

Success.

DAS-3626:admin#
```

Note: Web will be disabled when SSL is enabled.

39-3 disable ssl

Description

This command is used to disable SSL feature and for each ciphersuites status user must specified it by this command.

Format

disable ssl {ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5}}

Parameters

ciphersuite - (Optional) Specifies the cipher suite combination used for this configuration.
- **RSA_with_RC4_128_MD5** - (Optional) Specifies RSA key exchange with RC4 128 bits encryption and MD5 hash.
- **RSA_with_3DES_EDE_CBC_SHA** - (Optional) Specifies RSA key exchange with 3DES_EDE_CBC encryption and SHA hash.
- **DHE_DSS_with_3DES_EDE_CBC_SHA** - (Optional) Specifies DH key exchange with 3DES_EDE_CBC encryption and SHA hash.
- **RSA_EXPORT_with_RC4_40_MD5** - (Optional) Specifies RSA_EXPORT key exchange with RC4 40 bits encryption and MD5 hash.

Restrictions

Only Administrators can issue this command.

Example

To disable SSL ciphersuite for RSA_with_RC4_128_MD5:

```
DAS-3626:admin# disable ssl ciphersuite RSA_with_RC4_128_MD5
Command: disable ssl ciphersuite RSA_with_RC4_128_MD5

Success.

DAS-3626:admin#
```

To disable SSL:

```
DAS-3626:admin# disable ssl
Command: disable ssl

Success.

DAS-3626:admin#
```

39-4 show ssl

Description

This command is used to display the certificate status. User must download specified certificate type according to desired key exchange algorithm. The options may be no certificate, RSA type or DSA type certificate

Format

show ssl {certificate}

Parameters

certificate - (Optional) Specifies that the SSL certificate will be displayed.

Restrictions

None.

Example

To show SSL:

```
DAS-3626:admin#show ssl
Command: show ssl

 SSL Status                                    Enabled

 RSA_WITH_RC4_128_MD5                          Enabled
 RSA_WITH_3DES_EDE_CBC_SHA                     Enabled
 DHE_DSS_WITH_3DES_EDE_CBC_SHA                 Enabled
 RSA_EXPORT_WITH_RC4_40_MD5                    Enabled

DAS-3626:admin#
```

To show certificate:

```
DAS-3626:admin# show ssl certificate
Command: show ssl certificate

Loaded with RSA Certificate!

DAS-3626:admin#
```

39-5 show ssl cachetimeout

Description

This command is used to display cache timeout value which is designed for dlktimer library to remove the session id after expired. In order to support the resume session feature, the SSL library keep the session id in web server, and invoking the dlktimer library to remove this session id by cache timeout value.

Format

show ssl cachetimeout

Parameters

None.

Restrictions

None.

Example

To show SSL cache timeout:

```
DAS-3626:admin# show ssl cachetimeout
Commands: show ssl cachetimeout

Cache timeout is 600 seconds

DAS-3626:admin#
```

39-6 config ssl cachetimeout

Description

This command is used to configure cache timeout value which is designed for dlktimer library to remove the session id after expired. In order to support the resume session feature, the SSL library keep the session id in web server, and invoking the dlktimer library to remove this session id by cache timeout value. The unit of argument's value is second and it's boundary is between 60 (1 minute) and 86400 (24 hours). Default value is 600 seconds.

Format

config ssl cachetimeout <value 60-86400>

Parameters

<value 60-86400> - Enter the SSL cache timeout value here. This value must be between 60 and 86400.

Restrictions

None.

Example

To configure the SSL cache timeout value to 60:

```
DAS-3626:admin# config ssl cachetimeout 60
Commands: config ssl cachetimeout 60

Success.

DAS-3626:admin#
```

Chapter 40 Simple Network Management Protocol (SNMP) Command List

create snmp community <community_string 32> view <view_name 32> [read_only | read_write]
delete snmp community <community_string 32>
show snmp community {<community_string 32>}
create snmp user <user_name 32> <groupname 32> {encrypted [by_password auth [md5 <auth_password 8-16> | sha <auth_password 8-20>] priv [none | des <priv_password 8-16>] | by_key auth [md5 <auth_key 32-32> | sha <auth_key 40-40>] priv [none | des <priv_key 32-32>]]}
delete snmp user <username 32>
show snmp user
create snmp group <groupname 32> [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]] {read_view <view_name 32> | write_view <view_name 32> | notify_view <view_name 32>}
delete snmp group <groupname 32>
show snmp groups
create snmp view <view_name 32> <oid> view_type [included | excluded]
delete snmp view <view_name 32> [all | <oid>]
show snmp view {<view_name 32>}
create snmp [host <ipaddr> | v6host <ipv6addr>] [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]] <auth_string 32>
delete snmp [host <ipaddr> | v6host <ipv6addr>]
show snmp host {<ipaddr>}
show snmp v6host {<ipv6addr>}
config snmp engineID <snmp_engineID 10-64>
show snmp engineID
enable snmp
disable snmp
config snmp system_name {<sw_name>}
config snmp system_location {<sw_location>}
config snmp system_contact {<sw_contact>}
enable snmp traps
disable snmp traps
enable snmp authenticate_traps
disable snmp authenticate_traps
show snmp traps {linkchange_traps {ports <portlist>}}
show snmp trap_group
show snmp trap_group_for_host {<ipaddr>}
show snmp trap_group_for_v6host {<ipv6addr>}

40-1 create snmp community

Description

This command is used to create an SNMP community string.

Use an SNMP community string to define the relationship between the SNMP manager and the agent. The community string acts like a password to permit access to the agent on the switch. You can specify one or more of the following characteristics associated with the string:

An access list of IP addresses of the SNMP managers that are permitted to use the community string to gain access to the agent.

A MIB view, which defines the subset of all MIB objects accessible to the given community.

Read and write or read-only permission for the MIB objects accessible to the community.

Format

create snmp community <community_string 32> [read_only | read_write]

Parameters

<community_string> - Enter the alphanumeric community string of up to 32 characters used to authentication of users wanting access to the switch's SNMP agent.
read_only - Specifies to allow the user using the above community string to have read only access to the switch's SNMP agent.
read_write - Specifies to allow the user using the above community string to have read and write access to the switch's SNMP agent. The default read only community string is public. The default read write community string is private.

Restrictions

Only Administrators can issue this command.

Example

To create a read-only level SNMP community "System":

```
DAS-3626:admin#create snmp community System read_only
Command: create snmp community System read_only

Success.

DAS-3626:admin#
```

40-2 delete snmp community

Description

This command is used to delete an SNMP community string.

Format

delete snmp community <community_string 32>

Parameters

<community_string 32> - Enter the community string value here. This value can be up to 32 characters long.

Restrictions

Only Administrators can issue this command.

Example

To delete a SNMP community “System”:

```
DAS-3626:admin#delete snmp community System
Command: delete snmp community System

Success.

DAS-3626:admin#
```

40-3 show snmp community

Description

This command is used to display the community string configurations. If no parameter is specified, all community string information will be displayed.

Format

show snmp community <community_string 32>

Parameters

<community_string 32> - (Optional) Enter the Community string.

Restrictions

None.

Example

To display SNMP community:

```
DAS-3626:admin#show snmp community
Command: show snmp community

SNMP Community Table
Community Name                   View Name                        Access
Right
--------------------------------  --------------------------------  -----------
private                          CommunityView                    read_write
public                           CommunityView                    read_only

Total Entries: 2

DAS-3626:admin#
```

40-4 create snmp user

Description

This command is used to create a new user to an SNMP group originated by this command.

Format

create snmp user <user_name 32> <groupname 32> {encrypted [by_password auth [md5 <auth_password 8-16> | sha <auth_password 8-20>] priv [none | des <priv_password 8-16>] | by_key auth [md5 <auth_key 32-32> | sha <auth_key 40-40>] priv [none | des <priv_key 32-32>]]}

Parameters

<user_name 32> - Enter the name of the user on the host that connects to the agent. The range is 1 to 32.

<groupname 32> - Enter the name of the group to which the user is associated. The range is 1 to 32.

encrypted - (Optional) Specifies whether the password appears in encrypted format.
- **by_password** - Specifies input password for authentication and privacy.
  - **auth** - Specifies an authentication level setting session. The options are md5 and sha.
    - **md5** - Specifies the HMAC-MD5-96 authentication level.
      - **<auth_password 8-16>** - Enter the MD5 authentication password here. This value must be between 8 and 16 characters.
    - **sha** - Specifies the HMAC-SHA-96 authentication level.
      - **<auth_password 8-20>** - Enter the SHA authentication password here. This value must be between 8 and 20 characters.
  - **priv** - Specifies a privacy key used by DES, it is hex string type.
    - **none** - Specifies that no encryption will be used for the privacy key.
    - **des** - Specifies that the DES encryption will be used for the privacy key.
      - **<priv_password 8-16>** - Enter the DES password value here. This value must be between 8 and 16 characters long.
- **by_key** - Specifies input key for authentication and privacy.
  - **auth** - Specifies an authentication string used by MD5 or SHA1.
    - **md5** - Specifies an authentication key used by MD5, it is hex string type.
      - **<auth_key 32-32>** - Enter the MD5 authentication key here. This value must be 32 characters long.
    - **sha** - Specifies an authentication key used by SHA1, it is hex string type.
      - **<auth_key 40-40>** - Enter the SHA authentication key here. This value must be 32 characters long.
  - **priv** - Specifies a privacy key used by DES, it is hex string type.
    - **none** - Specifies that no encryption will be used for the privacy key.
    - **des** - Specifies that the DES encryption will be used for the privacy key.
      - **<priv_key 32-32>** - Enter the DES privacy key here. This value must be 32 characters long.

Restrictions

Only Administrators can issue this command.

Example

To create a SNMP user “user123” with group “group123”:

```
DAS-3626:admin#create snmp user user123 group123 encrypted by_password auth md5
12345678 priv des 12345678
Command: create snmp user user123 group123 encrypted by_password auth md5
12345678 priv des 12345678

Success.

DAS-3626:admin#
```

40-5 delete snmp user

Description

This command is used to remove a user from an SNMP group and delete the associated group in SNMP group.

Format

delete snmp user <username 32>

Parameters

<username 32> - Enter the name of the user on the host that connects to the agent. The range is 1 to 32.

Restrictions

Only Administrators can issue this command.

Example

To delete a SNMP user “user123”:

```
DAS-3626:admin# delete snmp user user123
Command: delete snmp user user123

Success.

DAS-3626:admin#
```

40-6 show snmp user

Description

This command is used to display information on each SNMP username in the group username table.

Format

show snmp user

Parameters

None.

Restrictions

None.

Example

To show SNMP user:

```
DAS-3626:admin#show snmp user
Command: show snmp user

Username                         Group Name                       VerAuthPriv
-------------------------------  -------------------------------  -----------
initial                          initial                          V3 NoneNone
user123                          group123                         V3 MD5 DES

Total Entries: 2

DAS-3626:admin#
```

40-7 create snmp group

Description

This command is used to create a new SNMP group, or a table that maps SNMP users to SNMP views.

Format

create snmp group <groupname 32> [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]] {read_view <view_name 32> | write_view <view_name 32> | notify_view <view_name 32>}

Parameters

<groupname 32> - Enter the group name here. This name can be up to 32 characters long.
v1 - Specifies the least secure of the possible security models.
v2c - Specifies the second least secure of the possible security models.
v3 - Specifies the most secure of the possible. **noauth_nopriv** - Specifies to support neither packet authentication nor encrypting. **auth_nopriv** - Specifies to support packet authentication. **auth_priv** - Specifies to support packet authentication and encrypting.
read_view - (Optional) Specifies that the view name would be read. **<view_name 32>** - Enter the read view name here. This name can be up to 32 characters long.
write_view - (Optional) Specifies that the view name would be write. **<view_name 32>** - Enter the wite view name here. This name can be up to 32 characters long.
notify_view - (Optional) Specifies that the view name would be notify. **<view_name 32>** - Enter the notify view name here. This name can be up to 32 characters long.

Restrictions

Only Administrators can issue this command.

Example

To create SNMP group “group123”:

```
DAS-3626:admin#create snmp group group123 v2c write_view v2
Command: create snmp group group123 v2c write_view v2

Success.

DAS-3626:admin#
```

40-8 delete snmp group

Description

This command is used to remove a SNMP group.

Format

delete snmp group <groupname 32>

Parameters

<groupname 32> - Enter the name of the group will be deleted.

Restrictions

Only Administrators can issue this command.

Example

To delete SNMP group “group123”:

```
DAS-3626:admin# delete snmp group group123
Command: delete snmp group group123

Success.

DAS-3626:admin#
```

40-9 show snmp groups

Description

This command is used to display the names of groups on the switch and the security model, level, the status of the different views.

Format

show snmp groups

Parameters

None.

Restrictions

None.

Example

To show SNMP groups:

```
DAS-3626:admin#show snmp groups
Command: show snmp groups

Vacm Access Table Settings

Group    Name    : public
ReadView Name    : CommunityView
WriteView Name   :
Notify View Name : CommunityView
Securiy Model    : SNMPv1
Securiy Level    : NoAuthNoPriv

Group    Name    : public
ReadView Name    : CommunityView
WriteView Name   :
Notify View Name : CommunityView
Securiy Model    : SNMPv2
Securiy Level    : NoAuthNoPriv

Group    Name    : initial
ReadView Name    : restricted
WriteView Name   :
Notify View Name : restricted
Securiy Model    : SNMPv3
Securiy Level    : NoAuthNoPriv
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

40-10 create snmp view

Description

This command is used to assign views to community strings to limit which MIB objects an SNMP manager can access.

Format

create snmp view <view_name 32> <oid> view_type [included | excluded]

Parameters

<view_name 32> - Enter the view name here. The name can be up to 32 characters long.
<oid> - Enter the Object-Identified tree, MIB tree.
view_type - Specifies the access type of the MIB tree in this view. **included** - Specifies to include for this view. **excluded** - Specifies to exclude for this view.

Restrictions

Only Administrators can issue this command.

Example

To create SNMP view “view123”:

```
DAS-3626:admin#create snmp view view123 1.3.6 view_type included
Command: create snmp view view123 1.3.6 view_type included

Success.

DAS-3626:admin#
```

40-11 delete snmp view

Description

This command is used to remove a view record.

Format

delete snmp view <view_name 32> [all | <oid>]

Parameters

<view_name 32> - Enter the view name here. The name can be up to 32 characters long.
all - Specifies that all view records will be removed.**<**
<oid> - Enter the Object-Identified tree, MIB tree.

Restrictions

Only Administrators can issue this command.

Example

To delete SNMP view “view123”:

```
DAS-3626:admin# delete snmp view view123 all
Command: delete snmp view view123 all

Success.

DAS-3626:admin#
```

40-12 show snmp view

Description

This command is used to display the SNMP view record.

Format

show snmp view {<view_name 32>}

Parameters

<view_name 32> - (Optional) Enter the view name here. The name can be up to 32 characters long.

Restrictions

None.

Example

To show SNMP view:

```
DAS-3626:admin#show snmp view
Command: show snmp view

Vacm View Table Settings
View Name                       Subtree                          View Type
------------------------------  -------------------------------  ---------
-
view123                         1.3.6                            Included
restricted                      1.3.6.1.2.1.1                    Included
restricted                      1.3.6.1.2.1.11                   Included
restricted                      1.3.6.1.6.3.10.2.1               Included
restricted                      1.3.6.1.6.3.11.2.1               Included
restricted                      1.3.6.1.6.3.15.1.1               Included
CommunityView                   1                                Included
CommunityView                   1.3.6.1.6.3                      Excluded
CommunityView                   1.3.6.1.6.3.1                    Included

Total Entries: 9

DAS-3626:admin#
```

40-13 create snmp

Description

This command is used to create a recipient of an SNMP trap operation.

Format

create snmp [host <ipaddr> | v6host <ipv6addr>] [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]] <auth_string 32>

Parameters

host - Specifies the recipient for which the traps are targeted. **<ipaddr>** - The IP address of the recipient for which the traps are targeted.
v6host - Specifies the IPv6 host address to which the trap packet will be sent. **<ipv6addr>** - Enter the IPv6 address of the recipient for which the traps are targeted.
v1 - Specifies he least secure of the possible security models.
v2c - Specifies he second least secure of the possible security models.
v3 - Specifies he most secure of the possible. **noauth_nopriv** - Specifies to support neither packet authentication nor encrypting. **auth_nopriv** - Specifies to support packet authentication. **auth_priv** - Specifies support packet authentication and encrypting.
<auth_string 32> - Enter the authentication string. If the v1 or v2 is specified, the auth_string presents the community string, and it must be one of the entries in community table. If the v3 is specified, the auth_string presents the user name, and it must be one of the entries in the user table.

Restrictions

Only Administrators can issue this command.

Example

To create SNMP host “10.0.0.1” with community string “public”:

```
DAS-3626:admin# create snmp host 10.0.0.1 v1 public
Command: create snmp host 10.0.0.1 v1 public

Success.

DAS-3626:admin#
```

40-14 delete snmp

Description

This command is used to delete a recipient of an SNMP trap operation.

Format

delete snmp [host <ipaddr> | v6host <ipv6addr>]

Parameters

host - Specifies the IP address of the recipient for which the traps are targeted. **<ipaddr>** - Enter the IP address used for the configuration here.
v6host - Specifies the IPv6 address of the recipient for which the traps are targeted. **<ipv6addr>** - Enter the IPv6 address used for the configuration here.

Restrictions

Only Administrators can issue this command.

Example

To delete SNMP host “10.0.0.1”:

```
DAS-3626:admin# delete snmp host 10.0.0.1
Command: delete snmp host 10.0.0.1

Success.

DAS-3626:admin#
```

40-15 show snmp host

Description

This command is used to display the recipient for which the traps are targeted. If no parameter is specified, all SNMP hosts will be displayed.

Format

show snmp host {<ipaddr>}

Parameters

<ipaddr> - (Optional) Enter the IP address used for the configuration here.

Restrictions

None.

Example

To show SNMP host:

```
DAS-3626:admin#show snmp host
Command: show snmp host

SNMP Status: Enabled

SNMP Host Table
Host IP Address  SNMP Version     Community Name / SNMPv3 User Name
---------------  ---------------  ---------------------------------
10.0.0.1         V1               public

Total Entries: 1

DAS-3626:admin#
```

40-16 show snmp v6host

Description

This command is used to display the recipient for which the traps are targeted. If no parameter is specified, all SNMP hosts will be displayed.

Format

show snmp v6host {<ipv6addr>}

Parameters

v6host - (Optional) Specifies the IPv6 host address.
<ipv6addr> - Enter the IPv6 address used for the configuration here.

Restrictions

None.

Example

To show SNMP host:

```
DAS-3626:admin#show snmp v6host
Command: show snmp v6host

SNMP Status: Enabled

SNMP Host Table
-----------------------------------------------------------------
Host IPv6 Address : 3FFE::2
SNMP Version      : V1
Community Name/SNMPv3 User Name : public

Total Entries: 1

DAS-3626:admin#
```

40-17 config snmp engineID

Description

This command is used to configure a identifier for the SNMP engine on the switch.

Format

config snmp engineID <snmp_engineID 10-64>

Parameters

<snmp_engineID 10-64> - Enter the SNMP engine ID here. . It is octet string type. It accepts the hex number directly. This value must be between 10 and 64.

Restrictions

Only Administrators can issue this command.

Example

To configure SNMP engine ID to “1023457890”:

```
DAS-3626:admin# config snmp engineID 1023457890
Command: config snmp engineID 1023457890

Success.

DAS-3626:admin#
```

40-18 show snmp engineID

Description

This command is used to display the identification of the SNMP engine on the switch. The default value is suggested in RFC2271. The very first bit is 1, and the first four octets are set to the binary equivalent of the agent’s SNMP management private enterprise number as assigned by IANA,

D_Link is 171. The fifth octet is 03 to indicates the rest is the MAC address of this device. The 6th –11th octets is MAC address.

Format

show snmp engineID

Parameters

None.

Restrictions

None.

Example

To show SNMP engine ID:

```
DAS-3626:admin# show snmp engineID
Command: show snmp engineID

SNMP Engine ID : 1023457890

DAS-3626:admin#
```

40-19 enable snmp

Description

This command is used to enable the SNMP function.

Format

enable snmp

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable SNMP:

```
DAS-3626:admin# enable snmp
Command: enable snmp

Success.

DAS-3626:admin#
```

40-20 disable snmp

Description

This command is used to disable the SNMP function.

Format

disable snmp

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable SNMP:

```
DAS-3626:admin# disable snmp
Command: disable snmp

Success.

DAS-3626:admin#
```

40-21 config snmp system_name

Description

This command is used to configure the name for the switch.

Format

config snmp system_name {<sw_name>}

Parameters

<sw_name> - (Optional) Enter the system name used here. A maximum of 128 characters is allowed.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the switch name for “DAS-3626 Switch”:

```
DAS-3626:admin#config snmp system_name DAS-3626 Switch
Command: config snmp system_name DAS-3626 Switch

Success.

DAS-3626:admin#
```

40-22 config snmp system_location

Description

This command is used to enter a description of the location of the switch.

Format

config snmp system_location {<sw_location>}

Parameters

<sw_location> - (Optional) Enter the system location string here. A maximum of 128 characters is allowed.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the switch location for “HQ 5F”:

```
DAS-3626:admin# config snmp system_location HQ 5F
Command: config snmp system_location HQ 5F

Success.

DAS-3626:admin#
```

40-23 config snmp system_contact

Description

This command is used to enter the name of a contact person who is responsible for the switch.

Format

config snmp system_contact {<sw_contact>}

Parameters

<sw_contact> - (Optional) Enter the system contact string here. A maximum of 128 characters is allowed.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the switch contact to “MIS Department II”:

```
DAS-3626:admin#config snmp system_contact MIS Department II
Command: config snmp system_contact MIS Department II

Success.

DAS-3626:admin#
```

40-24 enable snmp traps

Description

This command is used to enable SNMP trap support.

Format

enable snmp traps

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable SNMP trap support:

```
DAS-3626:admin# enable snmp traps
Command: enable snmp traps

Success.

DAS-3626:admin#
```

40-25 disable snmp traps

Description

This command is used to disable SNMP trap support on the switch.

Format

disable snmp traps

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To prevent SNMP traps from being sent from the switch:

```
DAS-3626:admin# disable snmp traps
Command: disable snmp traps

Success.

DAS-3626:admin#
```

40-26 enable snmp authenticate_traps

Description

This command is used to enable SNMP authentication failure trap support.

Format

enable snmp authenticate_traps

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable SNMP authentication trap support:

```
DAS-3626:admin# enable snmp authenticate_traps
Command: enable snmp authenticate_traps

Success.

DAS-3626:admin#
```

40-27 disable snmp authenticate_traps

Description

This command is used to disable SNMP authentication failure trap support.

Format

disable snmp authenticate_traps

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable SNMP authentication trap support:

```
DAS-3626:admin# disable snmp authenticate_traps
Command: disable snmp authenticate_traps

Success.

DAS-3626:admin#
```

40-28 show snmp traps

Description

This command is used to display the snmp trap sending status.

Format

show snmp traps {linkchange_traps {ports <portlist>}}

Parameters

linkchange_traps - (Optional) Specifies that the SNMP trap sending status will be displayed.
ports - (Optional) Specifies the ports for the display. **<portlist>** - Enter the list of ports used for the display here.

Restrictions

None.

Example

To display the SNMP trap status:

```
DAS-3626:admin#show snmp traps
Command: show snmp traps

SNMP Traps         : Enabled
Authenticate Trap  : Enabled

DAS-3626:admin#
```

40-29 show snmp trap_group

Description

This command is used to display SNMP trap group information.

Format

show snmp trap_group

Parameters

None.

Restrictions

None.

Example

To show snmp trap_group information:

```
DAS-3626:admin#show snmp trap_group
Command: show snmp trap_group

Id    Group
----  ----------------
1     Authentication
2     Equipment
3     Interface
4     System
5     VDSL

DAS-3626:admin#
```

40-30 show trap_group_for_host

Description

This command is used to display SNMP host trap group table.

Format

show snmp trap_group_for_host {<ipaddr>}

Parameters

<ipaddr> - (Optional) Enter the IP address of the trap host.

Restrictions

None.

Example

To show SNMP host trap group table:

```
DAS-3626:admin#show snmp trap_group_for_host
Command: show snmp trap_group_for_host

SNMP Host Trap Group Table
-----------------------------------------------------------------
Host IP Address   : 172.19.17.228
Trap Group        : Authentication Equipment Interface System VDSL

Host IP Address   : 172.19.17.251
Trap Group        : Authentication Equipment Interface System VDSL

Total Entries: 2

DAS-3626:admin#
```

40-31 show trap_group_for_v6host

Description

This command is used to display SNMP IPv6 host trap group table.

Format

show snmp trap_group_for_v6host {<ipv6addr>}

Parameters

<ipv6addr> - (Optional) Enter the IPv6 address of the trap host.

Restrictions

None.

Example

To show SNMP IPv6 host trap group table:

```
DAS-3626:admin# show snmp trap_group_for_v6host
Command: show snmp trap_group_for_v6host

SNMP Host Trap Group Table
------------------------------------------------------------------
Host IPv6 Address : 2001:470:24:3C3:2935:A8AC:CCFF:70F7
Trap Group        : Authentication Equipment Interface System VDSL

Total Entries: 1

DAS-3626:admin#
```

Chapter 41 System Log Command List

clear log
show log {[index <value_list> | severity {module <module_list>} {emergency | alert | critical | error | warning | notice | informational | debug | <level_list 0-7>} | module<module_list>]}
enable syslog
disable syslog
show syslog
config syslog host <index 1-4> | all] {severity [emergency | alert | critical | error | warning | notice | informational | debug | <level 0-7>] | udp_port <udp_port_number> | state [enable | disable]}
create syslog host <index 1-4> ipaddress [<ipaddr> |<ipv6addr>] {severity [emergency | alert | critical | error | warning | notice | informational | debug | <level 0-7>] | udp_port <udp_port_number> | state [enable | disable]}
delete syslog host [<index 1-4> | all]
show syslog host {<index 1-4>}
config log_save_timing [time_interval <min 1-65535> | on_demand | log_trigger]
show log_save_timing
show attack_log {index <value_list>}
clear attack_log

41-1 clear log

Description

This command is used to clear the switch's history log.

Format

clear log

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To clear the switch's history log:

```
DAS-3626:admin# clear log
Command: clear log

Success.

DAS-3626:admin#
```

41-2 show log

Description

This command is used to display the switch's history log. If no parameter is specified, all history log entries will be displayed.

Format

show log {[index <value_list> | severity {emergency | alert | critical | error | warning | notice | informational | debug | <level_list 0-7>}]}

Parameters

index - (Optional) Specifies to display the history log between the log number of X and Y. For example, showing log index 1-5 will display the history log from 1 to 5. **<value_list>** - Enter the index value here.
severity - (Optional) Specifies the severity level used. **emergency** - (Optional) Specifies the severity level to 0. **alert** - (Optional) Specifies the severity level to to 1. **critical** - (Optional) Specifies the severity level to 2. **error** - (Optional) Specifies the severity level to 3. **warning** - (Optional) Specifies the severity level to 4. **notice** - (Optional) Specifies the severity level to 5. **informational** - (Optional) Specifies the severity level to 6. **debug** - (Optional) Specifies the severity level to 7. **<level_list 0-7>** - (Optional) Specifies a list of severity level which is to be displayed. If there is more than one severity level, please separate them by comma. The level number is from 0 to 7.

Restrictions

None.

Example

To display the Switch's history log:

```
DAS-3626:admin#show log index 1-3
Command: show log index 1-3

Index Date       Time     Level   Log Text
----- ---------- -------- ------- --------------------------------------------

3     2014-08-03 04:52:37 CRIT(2) System started up
2     2014-08-03 04:52:37 ERRO(3) System has reset without management command
1     2014-08-03 04:52:37 CRIT(2) System cold start

DAS-3626:admin#
```

41-3 enable syslog

Description

This command is used to enable the sending of syslog messages.

Format

enable syslog

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable the sending of syslog messages:

```
DAS-3626:admin# enable syslog
Command: enable syslog

Success.

DAS-3626:admin#
```

41-4 disable syslog

Description

This command is used to disable the sending of syslog messages.

Format

disable syslog

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable the sending of syslog messages:

```
DAS-3626:admin# disable syslog
Command: disable syslog

Success.

DAS-3626:admin#
```

41-5 show syslog

Description

This command is used to display the syslog protocol global state.

Format

show syslog

Parameters

None.

Restrictions

None.

Example

To display the syslog protocol global state:

```
DAS-3626:admin#show syslog
Command: show syslog

Syslog Global State: Enabled

DAS-3626:admin#
```

41-6 config syslog host

Description

This command is used to configure the syslog host configurations. The user can choose and report a specific level of messages to a specific host. When the user chooses a specific level for a specific host, messages which are at that severity level or higher will be reported to the specified host.

Format

config syslog host [<index 1-4> | all] {severity [emergency | alert | critical | error | warning | notice | informational | debug | <level 0-7>] | udp_port <udp_port_number> | state [enable | disable]}

Parameters

<index 1-4> - Enter the host index value here.
all - Specifies that all the host indexes will be used.
severity - (Optional) Specifies the severity level. **emergency** - Specifies the severity level to 0. **alert** - Specifies the severity level to 1. **critical** - Specifies the severity level to 2. **error** - Specifies the severity level to 3. **warning** - Specifies the severity level to 4. **notice** - Specifies the severity level to 5. **informational** - Specifies the severity level to 6. **debug** - Specifies the severity level to 7. **<level 0-7>** - Enter the severity level value here. This value must be between 0 and 7.
udp_port - (Optional) Specifies the UDP port number. **<udp_port_number>** - Enter the UDP port number used here.
state - (Optional) Specifies the syslog protocol is used for the transmission of event notification messages across networks to a host. The option enables or disables the host to receive such messages. **enable** - Specifies that the host to receive such messages will be enabled. **disable** - Specifies that the host to receive such messages will be disabled.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the syslog host configuration:

```
DAS-3626:admin#config syslog host all severity debug state enable
Command: config syslog host all severity debug state enable

Success.

DAS-3626:admin#
```

41-7 create syslog host

Description

This command is used to create a new syslog host. The user can choose and report specific levels of messages to a specific host. When the user chooses a specific level for a specific host, messages which are at that severity level or higher will be reported to that host.

Format

create syslog host <index 1-4> ipaddress [<ipaddr> |<ipv6addr>] {severity [emergency | alert | critical | error | warning | notice | informational | debug | <level 0-7>] | udp_port <udp_port_number> | state [enable | disable]}

Parameters

<index 1-4> - Enter the host index value here.
all - Specifies that all the host indexes will be used.

severity - (Optional) Specifies the severity level. **emergency** - Specifies the severity level to 0. **alert** - Specifies the severity level to 1. **critical** - Specifies the severity level to 2. **error** - Specifies the severity level to 3. **warning** - Specifies the severity level to 4. **notice** - Specifies the severity level to 5. **informational** - Specifies the severity level to 6. **debug** - Specifies the severity level to 7. **<level 0-7>** - Enter the severity level value here. This value must be between 0 and 7.
udp_port - (Optional) Specifies the UDP port number. **<udp_port_number>** - Enter the UDP port number used here.
state - (Optional) Specifies the syslog protocol is used for the transmission of event notification messages across networks to a host. The option enables or disables the host to receive such messages. **enable** - Specifies that the host to receive such messages will be enabled. **disable** - Specifies that the host to receive such messages will be disabled.

Restrictions

Only Administrators and Operators can issue this command.

Example

Adds a new syslog host:

```
DAS-3626:admin#create syslog host 1 ipaddress 10.90.90.1 severity all state
enable
Command: create syslog host 1 ipaddress 10.90.90.1 severity all state enable

Success.

DAS-3626:admin#
```

41-8 delete syslog host

Description

This command is used to delete the syslog host(s).

Format

delete syslog host [<index 1-4> | all]

Parameters

<index 1-4> - Enter the host index value here.
all - Specifies that all the host indexes will be used.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete the specific syslog host:

```
DAS-3626:admin#delete syslog host 1
Command: delete syslog host 1

Success.

DAS-3626:admin#
```

41-9 show syslog host

Description

This command is used to display the syslog host configurations. If no parameter is specified, all hosts will be displayed.

Format

show syslog host {<index 1-4>}

Parameters

<index 1-4> - (Optional) Enter the host index value here.

Restrictions

None.

Example

To show the syslog host information:

```
DAS-3626:admin#show syslog host
Command: show syslog host

Syslog Global State: Enabled

Host Id  Host IP Address  Severity          UDP Port  Status
-------  ---------------  ----------------  --------  --------
1        10.90.90.1       All               514       Enabled

Total Entries : 1

DAS-3626:admin#
```

41-10 config log_save_timing

Description

This command is used to set the method for saving the log.

Format

config log_save_timing [time_interval <min 1-65535> | on_demand | log_trigger]

Parameters

time_interval - Specifies to save log to flash every xxx minutes. (If no new log events occur in this period, don't save.) **<min 1-65535>** - Enter the time interval value here. This value must be between 1 and 65535 minutes.
on_demand - Specifies to save log to flash whenever the user enters the "save log" or "save all" command. The default setting is on_demand.
log_trigger - Specifies to save log to flash whenever a new log event arrives.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the method for saving a log as on demand:

```
DAS-3626:admin# config log_save_timing on_demand
Command: config log_save_timing on_demand

Success.

DAS-3626:admin#
```

41-11 show log_save_timing

Description

This command is used to show the method for saving the log.

Format

show log_save_timing

Parameters

None.

Restrictions

None.

Example

To show the timing method used for saving the log:

```
DAS-3626:admin#show log_save_timing
Command: show log_save_timing

Saving Log Method: On_demand

DAS-3626:admin#
```

41-12 show attack_log

Description

This command is used to display the attack log messages. The attack log message refers to log messages driven by modules such as DOS and the IP-MAC-port binding module. This type of log message may generate a large amount of messages and quickly cause the system to run out of system log storage. Therefore, for this type of log messages only the first log that is generated each minute can be stored in the system log, with the rest of them being stored in a separate table named attack log. If no parameter is specified, all entries in the attack log will be displayed.

Format

show attack_log {index <value_list>}

Parameters

index - (Optional) Specifies the list of index numbers of the entries that need to be displayed. For example, show attack_log index 1-5 will display the attack log messages from 1 to 5. **<value_list>** - Enter the index numbers of the entries that needs to be displayed here.

Restrictions

None.

Example

To show dangerous messages on the master:

```
DAS-3626:admin#  show attack_log index 1
Command: show attack_log index 1

Index   Date       Time      Level     Log Text
----- ---------- -------- -------- ----------------------------------------
--
1      2008-10-17 15:00:14 CRIT(2)   Land attack is blocked from (IP:
10.72.24.1
                                          Port: 7)

DAS-3626:admin#
```

41-13 clear attack_log

Description

This command is used to clear the attack log.

Format

clear attack_log

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To clear the master's attack log:

```
DAS-3626:admin# clear attack_log
Command: clear attack_log

Success.

DAS-3626:admin#
```

Chapter 42 System Severity Command List

config system_severity [trap | log | all] [emergency | alert| critical | error | warning | notice | information | debug | <level 0-7>]
show system_severity

42-1 config system_severity

Description

This command is used to configure the severity level control for the system.

When the user chooses a specific level to log or trap, messages at that severity level or more will be logged or trapped to SNMP managers.

Format

config system_severity [trap | log | all] [emergency | alert| critical | error | warning | notice | information | debug | <level 0-7>]

Parameters

trap - Specifies the severity level control for traps.
log - Specifies the severity level control for the log.
all - Specifies the severity level control for traps and the log.
emergency - Specifies the severity level to 0.
alert - Specifies the severity level to 1.
critical - Specifies the severity level to 2.
error - Specifies the severity level to 3.
warning - Specifies the severity level to 4.
notice - Specifies the severity level to 5.
information - Specifies the severity level to 6.
debug - Specifies the severity level to 7.
<level 0-7> - Enter the severity level here. This value must be between 0 and 7.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure severity level control as information level for trap:

```
DAS-3626:admin# config system_severity trap information
Command: config system_severity trap information

Success.

DAS-3626:admin#
```

42-2 show system_severity

Description

This command is used to display the severity level controls for the system.

Format

show system_severity

Parameters

None.

Restrictions

None.

Example

To show severity level control for system:

```
DAS-3626:admin#show system_severity
Command: show system_severity

System Severity Trap : information(6)
System Severity Log : information(6)

DAS-3626:admin#
```

Chapter 43 TFTP Client Command List

download [firmware_fromTFTP [<ipaddr> | <ipv6addr>] <path_filename 64> image_id <int 1-2> | cfg_fromTFTP [<ipaddr> | <ipv6addr>] <path_filename 64> <config_id 1-2>]
upload [cfg_toTFTP [<ipaddr> | <ipv6addr>] <path_filename 64> <config_id 1-2> | log_toTFTP [<ipaddr> | <ipv6addr>] <path_filename 64> | attack_log_toTFTP [<ipaddr> | <ipv6addr>] <path_filename 64> | firmware_toTFTP [<ipaddr> | <ipv6addr>] <path_filename 64>]

43-1 download

Description

This command is used to download the firmware image and configuration from TFTP server.

Format

download [firmware_fromTFTP [<ipaddr> | <ipv6addr>] <path_filename 64> image_id <int 1-2> | cfg_fromTFTP [<ipaddr> | <ipv6addr>] <path_filename 64> <config_id 1-2>]

Parameters

firmware_fromTFTP - Specifies to download firmware from a TFTP server. **<ipaddr>** - Enter the IP address of the TFTP server. **<ipv6addr>** - Enter the IPv6 address of the TFTP server. **<path_filename 64>** - Enter the source file path name here. This name can be up to 64 characters long. **image_id** - Specifies to download one of the two firmware files. **<int 1-2>** - Enter the image ID.
cfg_fromTFTP - Specifies to download a configuration file from a TFTP server. **<ipaddr>** - Enter the IP address of the TFTP server. **<ipv6addr>** - Enter the IPv6 address of the TFTP server. **<path_filename 64>** - Enter the pathname specifies the pathname on the TFTP server. It can be a relative pathname or an absolute pathname. This name can be up to 64 characters long. **<config_id 1-2>** - Specifies to download one of the two configuration files.

Restrictions

Only Administrators can issue this command.

Example

To download firmware from TFTP:

```
DAS-3626:admin# download firmware_fromTFTP 10.77.93.5 firmware.had
Command: download firmware_fromTFTP 10.77.93.5 firmware.had

 Connecting to server.................. Done.
 Download firmware..................... Done.  Do not power off!
 Please wait, programming flash......... Done.

DAS-3626:admin#
```

To download configuration from TFTP:

```
DAS-3626:admin# download cfg_fromTFTP 10.77.93.5 config
Command: download cfg_fromTFTP 10.77.93.5 config

 Connecting to server.................. Done.
 Download configuration................ Done.

DAS-3626:admin#
```

43-2 upload

Description

This command is used to upload firmware and configuration from device to TFTP server.

Format

upload [cfg_toTFTP [<ipaddr> | <ipv6addr>] <path_filename 64> <config_id 1-2> | log_toTFTP [<ipaddr> | <ipv6addr>] <path_filename 64> | attack_log_toTFTP [<ipaddr> | <ipv6addr>] <path_filename 64> | firmware_toTFTP [<ipaddr> | <ipv6addr>] <path_filename 64>]

Parameters

cfg_toTFTP - Specifies that the configuration file will be uploaded to the TFTP server. **<ipaddr>** - Enter the IP address of the TFTP server. **<ipv6addr>** - Enter the IPv6 address of the TFTP server. **<path_filename 64>** - Enter the pathname specifies the pathname on the TFTP server. It can be a relative pathname or an absolute pathname. This name can be up to 64 characters long. **<config_id 1-2>** - Specifies to upload one of the two configuration files.
log_toTFTP - Specifies to upload a log file from device to TFTP server. **<ipaddr>** - The IP address of the TFTP server. **<ipv6addr>** - The IPv6 address of the TFTP server. **<path_filename 64>** - Enter the pathname on the TFTP server. It can be a relative pathname or an absolute pathname. This name can be up to 64 characters long.
attack_log_toTFTP – Specifies that the attack log will be uploaded to the TFTP server. **<ipaddr>** - Enter the IP address of the TFTP server. **<ipv6addr>** - Enter the IPv6 address of the TFTP server. **<path_filename 64>** - Enter the path name on the TFTP server to hold the attack log. This name can be up to 64 characters long.
firmware_toTFTP – Specifies that the firmware file will be uploaded to the TFTP server. **<ipaddr>** - Enter the IP address of the TFTP server. **<ipv6addr>** - Enter the IPv6 address of the TFTP server.

<path_filename 64> - Enter the pathname specifies the pathname on the TFTP server. It can be a relative pathname or an absolute pathname. This name can be up to 64 characters long.

Restrictions

Only Administrators and Operators can issue this command.

Example

To upload firmware from a file system device to a TFTP server:

```
DAS-3626:admin# upload firmware_toTFTP 10.77.93.5 firmware.had
Command: upload firmware_toTFTP 10.77.93.5 firmware.had

 Connecting to server.................. Done.
 Upload firmware....................... Done.

DAS-3626:admin#
```

To upload configuration to TFTP:

```
DAS-3626:admin#upload cfg_toTFTP 10.77.93.5 config
Command: upload cfg_toTFTP 10.77.93.5 config

 Connecting to server.................. Done.
 Upload configuration.................. Done.

DAS-3626:admin#
```

In upload log to TFTP:

```
DAS-3626:admin#upload log_toTFTP 10.77.93.5 log_file
Command: upload log_toTFTP 10.77.93.5 log_file

 Connecting to server.................. Done.
 Upload log............................ Done.

DAS-3626:admin#
```

To upload the dangerous log:

```
DAS-3626:admin# upload attack_log_toTFTP 10.77.93.5 attack_log_file
Command: upload attack_log_toTFTP 10.77.93.5 attack_log_file

Success.

DAS-3626:admin#
```

Chapter 44 Time and SNTP Command List

config sntp {primary <ipaddr> | secondary <ipaddr> | poll-interval <int 30-99999>}
config sntp IPv6 {primary <ipv6addr> | secondary <ipv6addr> | poll-interval <int 30-99999>}
show sntp
enable sntp
disable sntp
config time <date ddmthyyyy> <time hh:mm:ss>
config time_zone {operator [+ | -] | hour <gmt_hour 0-13> | min <minute 0-59>}
config dst [disable | repeating {s_week <start_week 1-4,last> | s_day <start_day sun-sat> | s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_week <end_week 1-4,last> | e_day <end_day sun-sat> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]} | annual {s_date <start_date 1-31> | s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_date <end_date 1-31> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]}]
show time

44-1 config sntp

Description

This command is used to change SNTP configurations.

Format

config sntp {primary <ipaddr> | secondary <ipaddr> | poll-interval <int 30-99999>}

Parameters

primary - (Optional) Specifies the SNTP primary server IP address. **<ipaddr>** - Enter the IP address used for this configuration here.
secondary - (Optional) Specifies the SNTP secondary server IP address. **<ipaddr>** - Enter the IP address used for this configuration here.
poll-interval - (Optional) Specifies the polling interval range seconds. **<int 30-99999>** - Enter the polling interval range here. This value must be between 30 and 99999 seconds.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure SNTP:

```
DAS-3626:admin#config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-interval 30
Command: config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-interval 30

Success.

DAS-3626:admin#
```

44-2 config sntp ipv6server

Description

This command is used to configure the SNTP IPv6 configuration.

Note: If both SNTP IPv4 and IPv6 servers are configured, the SNTP IPv4 server has higher priority, the Switch's time syncs with the IPv4 server's time first.

Format

config sntp IPv6 {primary <ipv6addr> | secondary <ipv6addr> | poll-interval <int 30-99999>}

Parameters

primary - (Optional) Specifies the SNTP primary server IPv6 address. **<ipv6addr>** - Enter the IP address used for this configuration here.
secondary - (Optional) Specifies the SNTP secondary server IPv6 address. **<ipv6addr>** - Enter the IP address used for this configuration here.
poll-interval - (Optional) Specifies the polling interval range seconds. **<int 30-99999>** - Enter the polling interval range here. This value must be between 30 and 99999 seconds.

Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

Example

To configure SNTP:

```
DAS-3626:admin#config sntp IPv6 primary 1000::1 secondary 1000::2 poll-interval
40
Command: config sntp IPv6 primary 1000::1 secondary 1000::2 poll-interval 40

Success.

DAS-3626:admin#
```

44-3 show sntp

Description

This command is used to display SNTP current time source and configuration.

Format

show sntp

Parameters

None.

Restrictions

None.

Example

To show SNTP:

```
DAS-3626:admin#show sntp
Command: show sntp

     Current Time Source   : System Clock
     SNTP                  : Disabled
     IPv4 SNTP Primary Server   : 10.1.1.1
     IPv4 SNTP Secondary Server : 10.1.1.2
     IPv6 SNTP Primary Server   : 1000::1
     IPv6 SNTP Secondary Server : 1000::2
     SNTP Poll Interval    : 40 sec

DAS-3626:admin#
```

44-4 enable sntp

Description

This command is used to turn on SNTP support.

Format

enable sntp

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable SNTP:

```
DAS-3626:admin# enable sntp
Command: enable sntp

Success.

DAS-3626:admin#
```

44-5 disable sntp

Description

This command is used to turn off SNTP support.

Format

disable sntp

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable SNTP:

```
DAS-3626:admin# disable sntp
Command: disable sntp

Success.

DAS-3626:admin#
```

44-6 config time

Description

This command is used to configure time and date settings of the device.

Format

config time <date ddmthyyyy> <time hh:mm:ss>

Parameters

<date ddmthyyyy> - Specifies the system clock date. An example would look like this: '30jun2010'.
<time hh:mm:ss> - Specifies the system clock time. An example would look like this: '12:00:00'.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure time:

```
DAS-3626:admin# config time 30jun2014 16:30:30
Command: config time 30jun2014 16:30:30

Success.

DAS-3626:admin#
```

44-7 config time_zone

Description

This command is used to configure time zone of the device.

Format

config time_zone {operator [+ | -] | hour <gmt_hour 0-13> | min <minute 0-59>}

Parameters

operator - (Optional) Specifies the operator of time zone. **[+ | -]** - Specifies that time should be added or subtracted to or from the GMT.
hour - (Optional) Specifies the hour of time zone. **<gmt_hour 0-13>** - Enter the hour value of the time zone here. This value must be between 0 and 13.
min - (Optional) Specifies the minute of time zone. **<minute 0-59>** - Enter the minute value of the time zone here. This value must be between 0 and 59.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure time_zone:

```
DAS-3626:admin# config time_zone operator + hour 2 min 30
Command: config time_zone operator + hour 2 min 30

Success.

DAS-3626:admin#
```

44-8 config dst

Description

This command is used to configure Daylight Saving Time of the device.

Format

config dst [disable | repeating {s_week <start_week 1-4,last> | s_day <start_day sun-sat> | s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_week <end_week 1-4,last> | e_day <end_day sun-sat> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]} | annual {s_date <start_date 1-31> | s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_date <end_date 1-31> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]}]

Parameters

disable - Specifies to disable the Daylight Saving Time of the switch.

repeating - Specifies to set the Daylight Saving Time to repeating mode.
- **s_week, e_week** - (Optional) Specifies to configure the start /end week number of Daylight Saving Time.
  - **<start_week 1-4, last>** - Enter the starting week number of Daylight Saving Time here. This value must be between 1 and 4.
  - **<end_week 1-4, last>** - Enter the ending week number of Daylight Saving Time here. This value must be between 1 and 4.
- **s_day, e_day** - (Optional) Specifies to configure the start /end day number of Daylight Saving Time.
  - **<start_day sun-sat>** - Enter the starting day value of Daylight Saving Time here. This value must either be sun, mon, tue, wed, thu, fri or sat.
  - **<end_day sun-sat>** - Enter the ending day value of Daylight Saving Time here. This value must either be sun, mon, tue, wed, thu, fri or sat.
- **s_mth, e_mth** - (Optional) Specifies to configure the start /end month number of Daylight Saving Time.
  - **<start_mth 1-12>** - Enter the starting month number of Daylight Saving Time here. This value must be between 1 and 12.
  - **<end_mth 1-12>** - Enter the ending month number of Daylight Saving Time here. This value must be between 1 and 12.
- **s_time, e_time** - (Optional) Specifies to configure the start /end time of Daylight Saving Time.
  - **<start_time hh:mm>** - Enter the starting time of Daylight Saving Time here. This value must be in the hh:mm format.
  - **<end_time hh:mm>** - Enter the starting time of Daylight Saving Time here. This value must be in the hh:mm format.
- **offset** - (Optional) Specifies the number of minutes to add or to subtract during summertime. The ranges of offset are 30, 60, 90,120. The default value is 60.
  - **30** - Specifies that the offset range will 30 minutes.
  - **60** - Specifies that the offset range will 60 minutes.
  - **90** - Specifies that the offset range will 90 minutes.
  - **120** - Specifies that the offset range will 120 minutes.

annual - Specifies the Daylight Saving Time to annual mode.
- **s_date, e_date** - (Optional) Specifies to configure the start /end date of Daylight Saving Time.
  - **<start_date 1-31>** - Enter the starting date of Daylight Saving Time here. This range must be between 1 an 31.
  - **<end_date 1-31>** - Enter the ending date of Daylight Saving Time here. This range must be between 1 an 31.
- **s_mth, e_mth** - (Optional) Specifies to configure the start /end month number of Daylight Saving Time.
  - **<start_mth 1-12>** - Enter the starting month number of Daylight Saving Time here. This

value must be between 1 and 12.
<end_mth 1-12> - Enter the ending month number of Daylight Saving Time here. This value must be between 1 and 12.
s_time, e_time - (Optional) Specifies to configure the start /end time of Daylight Saving Time.
<start_time hh:mm> - Enter the starting time of Daylight Saving Time here. This value must be in the hh:mm format.
<end_time hh:mm> - Enter the starting time of Daylight Saving Time here. This value must be in the hh:mm format.
offset - (Optional) Specifies the number of minutes to add or to subtract during summertime. The ranges of offset are 30, 60, 90,120; default value is 60.
30 - Specifies that the offset range will 30 minutes.
60 - Specifies that the offset range will 60 minutes.
90 - Specifies that the offset range will 90 minutes.
120 - Specifies that the offset range will 120 minutes.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure time:

```
DAS-3626:admin# config dst repeating s_week 2 s_day tue s_mth 4 s_time 15:00
e_week
 2 e_day wed e_mth 10 e_time 15:30 offset 30
Command: config dst repeating s_week 2 s_day tue s_mth 4 s_time 15:00 e_week 2
e
_day wed e_mth 10 e_time 15:30 offset 30

Success.

DAS-3626:admin#
```

44-9 show time

Description

This command is used to display time states.

Format

show time

Parameters

None.

Restrictions

None.

Example

To show time:

```
DAS-3626:admin#show time
Command: show time

     Current Time Source  : System Clock
     Boot Time    : 3 Aug 2014  04:50:52
     Current Time : 3 Aug 2014  13:04:13
     Time Zone    : GMT +00:00
     Daylight Saving Time  : Disabled
         Offset In Minutes : 60
         Repeating    From : Apr 1st  Sun 00:00
                      To   : Oct last Sun 00:00
         Annual       From : 29 Apr 00:00
                      To   : 12 Oct 00:00

DAS-3626:admin#
```

Chapter 45 Trace Route Command List

traceroute <ipaddr> {ttl <value 1-60>} {port <value 30000-64900>} {timeout <sec 1-65535>} {probe <value 1-9>}

45-1 traceroute

Description

This command is used to trace the routed path between the switch and a destination end station.

Format

traceroute <ipaddr> {ttl <value 1-60> | port <value 30000-64900> | timeout <sec 1-65535> | probe <value 1-9>}

Parameters

<ipaddr> - Enter the IP address of the destination end station.
ttl - (Optional) Specifies the time to live value of the trace route request. This is the maximum number of routers that a trace route packet can pass. The traceroute command will cross while seeking the network path between two devices. The range for the TTL is 1 to 60 hops. **<value 1-60>** - Enter the time to live value here. This value must be between 1 and 60.
port - (Optional) Specifies the port number. The value range is from 30000 to 64900. **<value 30000-64900>** - Enter the port number here. This value must be between 30000 and 64900.
timeout - (Optional) Specifies the timeout period while waiting for a response from the remote device. A value of 1 to 65535 seconds can be specified. The default is 5 seconds. **<sec 1-65535>** - Enter the timeout period value here. This value must be between 1 and 65535 seconds.
probe - (Optional) Specifies the number of probing. The range is from 1 to 9. If unspecified, the default value is 1. **<value 1-9>** - Enter the probing number value here. This value must be between 1 and 9.

Restrictions

Only Administrators and Operators can issue this command.

Example

Trace the routed path between the switch and 10.48.74.121:

```
DAS-3626:admin# traceroute 10.48.74.121 probe 3
Command: traceroute 10.48.74.121 probe 3

1   <10 ms.     10.12.73.254
2   <10 ms.     10.19.68.1
3   <10 ms.     10.48.74.121

Trace complete.
DAS-3626:admin#
```

Chapter 46 Traffic Control Command List

config traffic control [<portlist> | all | bonding <bgroup_list>] {broadcast [enable | disable] | multicast [enable | disable] | unicast [enable | disable] | action [drop | shutdown] | threshold <value 0-255000> | countdown [<min 0> | <min 3-30> | disable] | time_interval <sec 5-600>}
config traffic trap [none | storm_occurred | storm_cleared | both]
show traffic control {<portlist>| bonding <bgroup_list>}
config traffic control log state [enable | disable]
config traffic control auto_recover_time [<min 0> | <min 1-65535>]

46-1 config traffic control

Description

This command is used to configure broadcast, multicast and unicast packet storm control. Shutdown mode is provided to monitor the traffic rate in addition to the storm control drop mode. If traffic rate is too high, this port will be shut down.

Format

config traffic control [<portlist> | all | bonding <bgroup_list>] {broadcast [enable | disable] | multicast [enable | disable] | unicast [enable | disable] | action [drop | shutdown] | threshold <value 0-255000> | countdown [<min 0> | <min 3-30> | disable] | time_interval <sec 5-600>}

Parameters

<portlist> - Enter a range of ports to be configured.
all - Specifies that all the ports will be used for this configuration.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
broadcast - (Optional) Specifies to enable or disable broadcast storm control. **enable** - Specifies that broadcast storm control will be enabled. **disable** - Specifies that broadcast storm control will be disabled.
multicast - (Optional) Specifies to enable or disable multicast storm control. **enable** - Specifies that multicast storm control will be enabled. **disable** - Specifies that multicast storm control will be disabled.
unicast - (Optional) Specifies to enable or disable unknown packet storm control. (Supported for drop mode only) **enable** - Specifies that unicast storm control will be enabled. **disable** - Specifies that unicast storm control will be disabled.
action - (Optional) Specifies one of the two options for action is specified for storm control, shutdown or drop mode. Shutdown mode is a function of software, drop mode is implemented by the chip. If shutdown mode is specified, it is necessary to configure values for the countdown and time_interval parameters. **drop** - Specifies that the action applied will be drop mode. **shutdown** - Specifies that the action applied will be shutdown mode.
threshold - (Optional) Specifies the upper threshold, at which point the specified storm control is triggered. The <value> is the number of broadcast/multicast packets per second received by the switch that will trigger the storm traffic control measure. The threshold is expressed as PPS (packets per second) and must be an unsigned integer.

<value 0-255000> - Enter the upper threshold value here. This value must be between 0 and 255000.
countdown - (Optional) Specifies timer for shutdown mode. If a port enters the shutdown Rx state and this timer runs out, port will be shutdown forever. The parameter is not applicable if “drop” (mode) is specified for the “action” parameter. **<min 0>** - Enter 0 to disable the forever state, meaning that the port will not enter the shutdown forever state. **<min 3-30>** - Enter the countdown timer value here. This value must be between 3 and 30. **disable** - Specifies that the countdown timer will be disabled.
time_interval - (Optional) Specifies the sampling interval of received packet counts. The possible value will be m-n seconds. The parameter is not applicable if “drop” (mode) is specified for the “action” parameter. **<sec 5-600>** - Enter the time interval value here. This value must be between 5 and 600.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the parameters so that the traffic control status is enabled on ports 1-12:

```
DAS-3626:admin#config traffic control 1-12 broadcast enable action shutdown
threshold 1 countdown 5 time_interval 10
Command: config traffic control 1-12 broadcast enable action shutdown threshold
1 countdown 5 time_interval 10

Success.

DAS-3626:admin#
```

46-2 config traffic trap

Description

This command is used to configure trap modes.

Occurred Mode: This trap is sent when a packet storm is detected by the packet storm mechanism.

Cleared Mode: This trap is sent when the packet storm is cleared by the packet storm mechanism.

Format

config traffic trap [none | storm_occurred | storm_cleared | both]

Parameters

none - Specifies that no trap state is specified for storm control.
storm_occurred - Specifies that the occurred mode is enabled and the cleared mode is disabled.
storm_cleared - Specifies that the occurred mode is disabled and the cleared mode is enabled.
both - Specifies that both the occurred and cleared modes are enabled.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable both the occurred mode and cleared mode traffic control traps:

```
DAS-3626:admin# config traffic trap both
Command: config traffic trap both

Success.

DAS-3626:admin#
```

46-3 show traffic control

Description

This command is used to display the current traffic control settings. If no parameter is specified, the system will display the packet storm control configuration for all ports.

Format

show traffic control {<portlist>| bonding <bgroup_list>}

Parameters

<portlist> - (Optional) Enter a range of ports to be shown.
bonding - (Optional) Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.

Restrictions

None.

Example

To display the traffic control parameters for ports 1 to 10:

```
DAS-3626:admin#show traffic control 1-10
Command: show traffic control 1-10


Traffic Control Trap             : [None]
Traffic Control Log              : Enabled
Traffic Control Auto Recover Time: 0 Minutes

Port Thres  Broadcast Multicast Unicast  Action   Count    Time     Shutdown
     hold   Storm     Storm     Storm              down     Interval Forever
     (fps)                                        (Min)    (Sec)
---- ------ --------- --------- -------- -------- -------- -------- --------
1    1      Enabled   Disabled  Disabled shutdown 5        10
2    1      Enabled   Disabled  Disabled shutdown 5        10
3    1      Enabled   Disabled  Disabled shutdown 5        10
4    1      Enabled   Disabled  Disabled shutdown 5        10
5    1      Enabled   Disabled  Disabled shutdown 5        10
6    1      Enabled   Disabled  Disabled shutdown 5        10
7    1      Enabled   Disabled  Disabled shutdown 5        10
8    1      Enabled   Disabled  Disabled shutdown 5        10
9    1      Enabled   Disabled  Disabled shutdown 5        10
10   1      Enabled   Disabled  Disabled shutdown 5        10

DAS-3626:admin#
```

46-4 config traffic control log state

Description

This command is used to configure the traffic control log state. When the log state is enabled, traffic control states are logged when a storm occurs and when a storm is cleared. If the log state is disabled, traffic control events are not logged.

Note: The log state is only applicable for shutdown mode. Since shutdown mode only support broadcast and multicast storm control, doesn't support unicast storm control. The log only generate for broadcast and multicast storm control.

Format

config traffic control log state [enable | disable]

Parameters

enable - Specifies that both occurred and cleared are logged.
disable - Specifies that neither occurred nor cleared is logged.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the traffic log state on the Switch:

```
DAS-3626:admin# config traffic control log state enable
Command: config traffic control log state enable

Success.

DAS-3626:admin#
```

46-5 config traffic control auto_recover_time

Description

This command is used to configure the traffic auto recover time that allowed for a port to recover from shutdown forever status.

Format

config traffic control auto_recover_time [<min 0> | <min 1-65535>]

Parameters

<min 0> - Enter 0 to disable the auto recovery time. The port remains in shutdown forever mode and requires manual entry of the **config ports [<portlist> | all] state enable** command to return the port to a forwarding state. This is the default.
<min 1-65535> - Enter the auto recovery time value here. This value must be between 1 and 65535.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the auto recover time to 5 minutes:

```
DAS-3626:admin# config traffic control auto_recover_time 5
Command: config traffic control auto_recover_time 5

Success.

DAS-3626:admin#
```

Chapter 47 Traffic Segmentation Command List

config traffic_segmentation [<portlist> | all | bonding <bgroup_list>] forward_list [null | all | <portlist> | bonding <bgroup_list>]
show traffic_segmentation {<portlist> | bonding <bgroup_list>}

47-1 config traffic_segmentation

Description

This command is used to configure the traffic segmentation.

Format

config traffic_segmentation [<portlist> | all | bonding <bgroup_list>] forward_list [null | all | <portlist> | bonding <bgroup_list>]

Parameters

<portlist> - Enter a range of ports to be configured.
all - Specifies that all the ports will be used for this configuration.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
forward_list - Specifies a range of port forwarding domain. **null** - Specifies a range of port forwarding domain is null. **all** – Specifies all ports to be configured. **<portlist>** - Specifies a range of ports to be configured. **bonding** - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure traffic segmentation:

```
DAS-3626:admin#config traffic_segmentation 1-10 forward_list 1-15
Command: config traffic_segmentation 1-10 forward_list 1-15

Success.

DAS-3626:admin#
```

47-2 show traffic_segmentation

Description

This command is used to display current traffic segmentation table. If no parameter is specified, the system will display all current traffic segmentation tables.

Format

show traffic_segmentation {<portlist> | bonding <bgroup_list>}

Parameters

<portlist> - (Optional) Enter a range of ports to be displayed.
bonding - (Optional) Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.

Restrictions

None.

Example

To display traffic segmentation table:

```
DAS-3626:admin#show traffic_segmentation 1-10
Command: show traffic_segmentation 1-10

Traffic Segmentation Table

Port  Forward Portlist
----  ------------------------------------------------------------------------
1      1-15
2      1-15
3      1-15
4      1-15
5      1-15
6      1-15
7      1-15
8      1-15
9      1-15
10     1-15


DAS-3626:admin#
```

Chapter 48 Trusted Host Command List

create trusted_host [<ipaddr> | network <network_address>] {snmp | telnet | ssh | http | https | ping}
delete trusted_host [ipaddr <ipaddr> | network <network_address> | all]
config trusted_host [<ipaddr> | <ipv6addr> | network <network_address> | ipv6_prefix <ipv6networkaddr>] [add | delete] {snmp | telnet | ssh | http | https | ping | all}
show trusted_host

48-1 create trusted_host

Description

This command is used to create the trusted host. The switch allows you to specify up to three IP addresses that are allowed to manage the switch via in-band SNMP or TELNET based management software. These IP addresses must be members of the Management VLAN. If no IP addresses are specified, then there is nothing to prevent any IP address from accessing the switch, provided the user knows the Username and Password.

When the access interface is not specified, the trusted host will be created for all interfaces.

Format

create trusted_host [<ipaddr> | network <network_address>] {snmp | telnet | ssh | http | https | ping}

Parameters

<ipaddr> - Enter the IP address of the trusted host.
network - Specifies the network address of the trusted network. The form of network address is xxx.xxx.xxx.xxx/y. **<network_address>** - Enter the network address used here.
snmp - (Optional) Specifies trusted host for SNMP.
telnet - (Optional) Specifies trusted host for TELENT.
ssh - (Optional) Specifies trusted host for SSH.
http - (Optional) Specifies trusted host for HTTP.
https - (Optional) Specifies trusted host for HTTPs.
ping - (Optional) Specifies trusted host for PING

Restrictions

Only Administrators and Operators can issue this command.

Example

To create the trusted host:

```
DAS-3626:admin# create trusted_host 10.48.74.121
Command: create trusted_host 10.48.74.121

Success.

DAS-3626:admin#
```

48-2 delete trusted_host

Description

This command is used to delete a trusted host entry.

Format

delete trusted_host [ipaddr <ipaddr> | network <network_address> | all]

Parameters

ipaddr - Specifies the IP address of the trusted host. **<ipaddr>** - Enter the IP address used for this configuration here.
network - Specifies the network address of the trusted network. **<network_address>** - Enter the network address used for this configuration here.
all - Specifies that all trusted hosts will be deleted.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete the trusted host:

```
DAS-3626:admin# delete trusted_host 10.48.74.121
Command: delete trusted_host 10.48.74.121

Success.

DAS-3626:admin#
```

48-3 config trusted_host

Description

This command is used to configure the access interfaces for the trusted host.

Format

config trusted_host [<ipaddr> | network <network_address>] [add | delete] {snmp | telnet | ssh | http | https | ping | all}

Parameters

<ipaddr> - Enter the IP address of the trusted host.
network - Specifies the network address of the trusted network. The form of network address is xxx.xxx.xxx.xxx/y. **<network_address>** - Enter the network address used here.
add - Specifies to add interfaces for that trusted host.
delete - Specifies to delete interfaces for that trusted host.
snmp - (Optional) Specifies trusted host for SNMP.
telnet - (Optional) Specifies trusted host for TELENT.
ssh - (Optional) Specifies trusted host for SSH.
http - (Optional) Specifies trusted host for HTTP.
https - (Optional) Specifies trusted host for HTTPs.
ping - (Optional) Specifies trusted host for PING.
all - (Optional) Specifies trusted host for all application.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the trusted host:

```
DAS-3626:admin# config trusted_host 10.48.74.121 add ssh telnet
Command: config trusted_host 10.48.74.121 add ssh telnet

Success.

DAS-3626:admin#
```

48-4 show trusted_host

Description

This command is used to display a list of trusted hosts entered on the switch using the create trusted_host command above.

Format

show trusted_host

Parameters

None.

Restrictions

None.

Example

To display trusted host:

```
DAS-3626:admin#show trusted_host
Command: show trusted_host


Management Stations

IP Address                                  Access Interface
-----------------------------------------------------------------
10.48.74.121/32                             SNMP Telnet SSH HTTP HTTPs Ping

Total Entries: 1


DAS-3626:admin#
```

Chapter 49 Unicast Routing Command List

create iproute [default] <ipaddr> {<metric 1-65535>} {[primary | backup]}
delete iproute [default] <ipaddr>
show iproute

49-1 create iproute

Description

This command is used to create an IP static route.

Selecting “primary” or “backup” means the newly created route is a floating static route.

If none of the following, “primary” or “backup”, is selected, the default route will:

1. be primary if there is no primary route that has the same destination;
2. be backup if there has been a primary route that has the same destination.
3. fail to create if there have been a primary route and a backup route that have the same destination.
4. fail to create if there has been one static multipath route that has the same destination.

It will fail if a user wants to create a floating static route and there has been one static multipath route with the same destination.

It will fail if a user wants to create a static multipath route and there has been a floating static route, whether primary or backup.

Format

create iproute [default] <ipaddr> {<metric 1-65535>} {[primary | backup]}

Parameters

default - Specifies to create an IP default route (0.0.0.0/0).
<ipaddr> - Enter the IP address for the next hop router.
<metric 1-65535> - (Optional) Enter the metric value here. This value must be between 1 and 65535. The default setting is 1.
primary - (Optional) Specifies the route as the primary route to the destination.
backup - (Optional) Specifies the route as the backup route to the destination.

Restrictions

Only Administrators and Operators can issue this command.

Example

To add an IP static route:

```
DAS-3626:admin# create iproute default 10.1.1.254
Command: create iproute default 10.1.1.254

Success.

DAS-3626:admin#
```

49-2 delete iproute

Description

This command is used to delete an IP route entry from the switch's IP routing table.

Format

delete iproute [default] <ipaddr>

Parameters

default - Specifies to delete an IP default route (0.0.0.0/0).
<ipaddr> - Specifies the next hop IP address of the route need to be deleted.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete an IP default route:

```
DAS-3626:admin# delete iproute default 10.1.1.254
Command: delete iproute default 10.1.1.254

Success.

DAS-3626:admin#
```

49-3 show iproute

Description

This command is used to display the switch's current IP routing table.

Format

show iproute

Parameters

None.

Restrictions

None.

Example

To display the contents of the IP routing table:

```
DAS-3626:admin#show iproute
Command: show iproute


Routing Table

IP Address/Netmask  Gateway          Interface     Cost      Protocol
------------------  ---------------  ------------  --------  --------
0.0.0.0/0           10.1.1.254                     1         Default

Total Entries: 0


DAS-3626:admin#
```

Chapter 50 VDSL Command List

create vdsl profile {<profile_id 1-60> | name <profile_name 32>}

delete vdsl profile {<profile_id 1-60> | name <profile_name 32>}

config vdsl profile [<profile_id 1-60> | name <profile_name 32>] [attach [<vdsl_portlist> | all] | profile_name <profile_name 32> | Vdsl2Profile [autoprofile | [{8a | 8b | 8c | 8d | 12a | 12b | 17a | 30a}]] | UPBO [disable | electrical_length [auto | override <int 0-1280>] {us1_a <int 4000-8095> us1_b <int 0-4095> us2_a <int 4000-8095> us2_b <int 0-4095> us3_a <int 4000-8095> us3_b <int 0-4095>}] | DPBO [disable | enable] | DPBOValues {DPBOESEL <int 0-511> | DPBOESCMA <int 0-640> | DPBOESCMB <int 0-640> | DPBOESCMC <int 0-640> | DPBOMUS <int 0-255> | DPBOFMIN <int 0-2048> | DPBOFMAX <int 32-6956> | DPBOEPSD {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>}} | TrellisCoding [disable | enable] | DownRateMode [manual | adaptAtInit | dynamic] | UpRateMode [manual | adaptAtInit | dynamic] | MaxTxRate <vdsl_speed 64-128000> | MaxRxRate <vdsl_speed 64-128000> | MinTxRate <vdsl_speed 0-128000> | MinRxRate <vdsl_speed 0-128000> | [SnrMarginTx | SnrMarginRx] max <vdsl_snr_max 0-124> min <vdsl_snr_min 0-124> target <vdsl_snr_target 0-124> | InterleaveDelayDn <vdsl_inter_delay 0-63> | InterleaveDelayUp <vdsl_inter_delay 0-63> | [MinInpDn | MinInpUp] [0 | 0.5 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16] | [MinInp8Dn | MinInp8Up] [0 | 0.5 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16] | LimitPSDMask [nus0 | eu32 | eu36 | eu40 | eu44 | eu48 | eu52 | eu56 | eu60 | eu64 | eu128 | us2tods2] | BitSwap [disable | enable] | PSDBreakPointTx {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} | PSDBreakPointRx {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} | VirtualNoiseTx [disable | enable {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-

4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>}] | VirtualNoiseRx [disable | enable {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>}] | [GINPDn | GINPUp] [{rtx_mode [FORBIDDEN | PREFERRED | FORCED | TESTMODE] | ETR_min <int 64-128000> | ETR_max <int 64-128000> | net_max <int 64-128000> | delay_max <int 0-63> | delay_min <int 0-63> | INP_min <int 0-63> | SHINEratio <int 0-255> | leftr_thresh <int 0-99> | rein_INP_min <int 0-7> | iat_rein_flag [100hz | 120hz]}] | [SRADn | SRAUp] [{state [disable | enable] | downshiftSnr <int 0-310> | upshiftSnr <int 0-310> | downshiftDuration <int 0-16383> | upshiftDuration <int 0-16383>}] | [SOSDn | SOSUp] [{state [disable | enable] | min_rate <int 32-128000> | crc <int 1-65535> | time_window <int 64-16320> | degraded_tones <int 0-100> | max_number <int 0-15> | roc_snr_margin <int 0-250> | roc_min_inp <int 0-16>}] | [PHYRDn | PHYRUp] [disable | enable | auto] | [DynaDDn | DynaDUp] [disable | enable]]
show vdsl profile [<profile_id 1-60> | name <profile_name 32> | all]
show vdsl profile_list
config vdsl line [<vdsl_portlist> | all] [state [use | no_use] | name <name> | retrain | reset | loop_diagnostic | selt | selt_calibrate | selt_echo [1024tone | 2048tone | 3072tone | 4096tone] agc <int 0-64> duration <int 5-255> | selt_qln [1024tone | 2048tone | 3072tone | 4096tone] duration <int 0-15> | loopback [co_side {[DSP | AFE | HYBRID]} | cpe_side] times <int 1-400> size <int 64-1500>]
show vdsl line [<vdsl_portlist> | all] [status {brief} | bit_map | snr_margin_map | psd_map | hlog_map | qln_map | snr_map | gain_map | loop_diagnostic {hlog | qln | snr | hlin | band_data | chann_data | all} | selt | selt_calibrate | selt_echo {start <int 0-4095> stop <int 0-4095>} | selt_qln {start <int 0-4095> stop <int 0-4095>} | loopback | pm_counters [15mins [interval <int 1-96> | SNR_Margin] | 1day [interval <int 1-30> | SNR_Margin] | current] | inm [near_end | far_end] counter [15mins | 1day | running]]
config vdsl pm_threshold [15min | 1day | both] [near_end [{es <threshold> | fecs <threshold> | ses <threshold> | loss <threshold> | uas <threshold> | crc <threshold> | init <threshold>}] | far_end [{es <threshold> | fecs <threshold> | ses <threshold> | loss <threshold> | uas <threshold> | crc <threshold>}] | both_ends [{es <threshold> | fecs <threshold> | ses <threshold> | loss <threshold> | uas <threshold> | crc <threshold>}]]
show vdsl pm_threshold
show vdsl brief_status [alarms | line_state line [<vdsl_portlist> | all] | profiles | rate | snrmargin | txpower | attenuation]
create vdsl inm_profile name <profile_name 32>
delete vdsl inm_profile name <profile_name 32>
show vdsl inm_profile [name <profile_name 32> | all]
config vdsl inm_profile name <profile_name 32> [attach [<vdsl_portlist> | all] | [near_end | far_end] {state [disable | enable] | inminpeq <int 0-3> | inmcc <int 0-64> | inmiato <int 3-511> | inmiats <int 0-7> | inmss <inmss_value> }]
config vdsl bonding [<bgroup_list> | all] [profile [use [<profile_id 1-60> | name <profile_name 32>] ds_rate_alloc [default | master_weight <int 1-99>] us_rate_alloc [default | master_weight <int 1-99>] | individual] | state [enable | disable] | loopback cpe_side times <int 1-400> size <int 64-1500> | line_state [use | no_use]]
show vdsl bonding [<bgroup_list> | all]

clear vdsl_counter [<vdsl_portlist> | all]
clear vdsl_inm_counter [<vdsl_portlist> | all] [near_end | far_end]

50-1 create vdsl profile

Description

This command is used to create VDSL profiles. The default profile is assigne with profile ID, 1, and profile name, DEFVAL. This default profile cannot be deleted.

Format

create vdsl profile {<profile_id 1-60> | name <profile_name 32>}

Parameters

<profile_id 1-60> - Enter a VDSL profile ID.
name - Specifies the name of VDSL profile. **<profile_name 32>** - Enter the VDSL profile name.

Restrictions

Only Administrators and Operators can issue this command.

Example

To create a VDSL profile:

```
DAS-3626:admin#create vdsl profile 2 name VDSL2
Command: create vdsl profile 2 name VDSL2

Success.

DAS-3626:admin#
```

50-2 delete vdsl profile

Description

This command is used to delete VDSL profiles.

Format

delete vdsl profile {<profile_id 1-60> | name <profile_name 32>}

Parameters

<profile_id 1-60> - Enter a VDSL profile ID.
name - Specifies the name of VDSL profile. **<profile_name 32>** - Enter the VDSL profile name.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete a VDSL profile:

```
DAS-3626:admin#delete vdsl profile 3
Command: delete vdsl profile 3

Success.

DAS-3626:admin#
```

50-3 config vdsl profile

Description

This command is used to configure VDSL profile. Most parameters are based on ITU-T G.993.2 standard.

Format

config vdsl profile [<profile_id 1-60> | name <profile_name 32>] [attach [<vdsl_portlist> | all] | profile_name <profile_name 32> | Vdsl2Profile [autoprofile | [{8a | 8b | 8c | 8d | 12a | 12b | 17a | 30a}]] | UPBO [disable | electrical_length [auto | override <int 0-1280>] {us1_a <int 4000-8095> us1_b <int 0-4095> us2_a <int 4000-8095> us2_b <int 0-4095> us3_a <int 4000-8095> us3_b <int 0-4095>}] | DPBO [disable | enable] | DPBOValues {DPBOESEL <int 0-511> | DPBOESCMA <int 0-640> | DPBOESCMB <int 0-640> | DPBOESCMC <int 0-640> | DPBOMUS <int 0-255> | DPBOFMIN <int 0-2048> | DPBOFMAX <int 32-6956> | DPBOEPSD {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>}} | TrellisCoding [disable | enable] | DownRateMode [manual | adaptAtInit | dynamic] | UpRateMode [manual | adaptAtInit | dynamic] | MaxTxRate <vdsl_speed 64-128000> | MaxRxRate <vdsl_speed 64-128000> | MinTxRate <vdsl_speed 0-128000> | MinRxRate <vdsl_speed 0-128000> | [SnrMarginTx | SnrMarginRx] max <vdsl_snr_max 0-124> min <vdsl_snr_min 0-124> target <vdsl_snr_target 0-124> | InterleaveDelayDn <vdsl_inter_delay 0-63> | InterleaveDelayUp <vdsl_inter_delay 0-63> | [MinInpDn | MinInpUp] [0 | 0.5 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16] | [MinInp8Dn | MinInp8Up] [0 | 0.5 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16] | LimitPSDMask [nus0 | eu32 | eu36 | eu40 | eu44 | eu48 | eu52 | eu56 | eu60 | eu64 | eu128 | us2tods2] | BitSwap [disable | enable] | PSDBreakPointTx {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-

190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>}
{tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int
0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095>
psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level
<int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-
190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>}
{tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int
0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095>
psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level
<int 0-190>} | PSDBreakPointRx {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095>
psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level
<int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-
190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>}
{tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int
0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095>
psd_level <int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} {tone <int 0-4095> psd_level
<int 0-190>} {tone <int 0-4095> psd_level <int 0-190>} | VirtualNoiseTx [disable | enable
{tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone
<int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int
0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-
4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095>
noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095>
noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095>
noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095>
noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095>
noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095>
noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095>
noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095>
noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095>
noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095>
noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095>
noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095>
noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>}] | VirtualNoiseRx
[disable | enable {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level
<int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int
0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-
200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>}
{tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone
<int 0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int
0-4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>} {tone <int 0-
4095> noise_level <int 0-200>} {tone <int 0-4095> noise_level <int 0-200>}] | [GINPDn |
GINPUp] [{rtx_mode [FORBIDDEN | PREFERRED | FORCED | TESTMODE] | ETR_min <int
64-128000> | ETR_max <int 64-128000> | net_max <int 64-128000> | delay_max <int 0-63> |
delay_min <int 0-63> | INP_min <int 0-63> | SHINEratio <int 0-255> | leftr_thresh <int 0-99> |
rein_INP_min <int 0-7> | iat_rein_flag [100hz | 120hz]}] | [SRADn | SRAUp] [{state [disable |
enable] | downshiftSnr <int 0-310> | upshiftSnr <int 0-310> | downshiftDuration <int 0-
16383> | upshiftDuration <int 0-16383>}] | [SOSDn | SOSUp] [{state [disable | enable] |
min_rate <int 32-128000> | crc <int 1-65535> | time_window <int 64-16320> | degraded_tones
<int 0-100> | max_number <int 0-15> | roc_snr_margin <int 0-250> | roc_min_inp <int 0-16>}]
| [PHYRDn | PHYRUp] [disable | enable | auto] | [DynaDDn | DynaDUp] [disable | enable]]

Parameters

<profile_id 1-60> - Enter a VDSL profile ID.

name - Specifies the name of VDSL profile.
- **<profile_name 32>** - Enter the VDSL profile name.

attach - Specifies to profiles to the specific VDSL lines.
- **<vdsl_portlist>** - Enter a list of VDSL lines.
- **all** - Specifies to have all VDSL lines to be configured.

profile_name - Specifies the VDSL profile name.
- **<profile_name 32>** - Enter the VDSL profile name.

Vdsl2Profile - Specifies to create a VDSL2 profile for the Switch as defined in the standard ITU-T G.993.2 standard.
- **Autoprofile** - Specifies to use all profiles.
- **8a** - Specifies to use the 8a class profile.
- **8b** - Specifies to use the 8b class profile.
- **8c** - Specifies to use the 8c class profile.
- **8d** - Specifies to use the 8d class profile.
- **12a** - Specifies to use the 12a class profile.
- **12b** - Specifies to use the 12b class profile.
- **17a** - Specifies to use the 17a class profile.
- **30a** - Specifies to use the 30a class profile.

UPBO - Specifies to enable or disable Upstream Power Back Off (UPBO) for the profile.
- **disable** - Specifies to disable UPBO.
- **electrical_length** - Specifies electrical length to be used.
  - **auto** - Specifies to automatically determin the electrical length.
  - **override** - Specifies to force the VTU-R using the electrical length, Kl0, to compute the UPBO
    - **<int 0-1280>** - Enter the Kl0 value in dB. The range is from 0 to 1280.
  - **us1_a** - Specifies to use US1a band reference PSD parameter.
    - **<int 4000-8095>** - Enter the value between 4000 (40 dBm/Hz) and 8095 (80.95 dBm/Hz).
  - **us1_b** - Specifies to use US1b band reference PSD parameter.
    - **<int 0-4095>** - Enter the value between 0 (0 dBm/Hz) and 4095 (40.95 dBm/Hz).
  - **us2_a** - Specifies to use US2a band reference PSD parameter.
    - **<int 4000-8095>** - Enter the value between 4000 (40 dBm/Hz) and 8095 (80.95 dBm/Hz).
  - **us2_b** - Specifies to use US2b band reference PSD parameter.
    - **<int 0-4095>** - Enter the value between 0 (0 dBm/Hz) and 4095 (40.95 dBm/Hz).
  - **us3_a** - Specifies to use US3a band reference PSD parameter.
    - **<int 4000-8095>** - Enter the value between 4000 (40 dBm/Hz) and 8095 (80.95 dBm/Hz).
  - **us3_b** - Specifies to use US3b band reference PSD parameter.
    - **<int 0-4095>** - Enter the value between 0 (0 dBm/Hz) and 4095 (40.95 dBm/Hz).

DPBO - Specifies to enable or disable Downstream Power Back Off (DPBO).
- **disable** - Specifies to disable DPBO.
- **enable** - Specifies to enable DPBO.

DPBOValues - Specifies to configure DPBO value.
- **DPBOESEL** - Specifies to use Downstrean Power Back-Off E-side Electrical Legth.
  - **<int 0-511>** - Enter the value between 0 (0 dBm/Hz) and 511 (255.5 dBm/Hz).
- **DPBOESCMA** - Specifies to use Downstrean Power Back-Off E-side Cable Model A.
  - **<int 0-640>** - Enter the value between 0 and 640.
- **DPBOESCMB** - Specifies to use Downstrean Power Back-Off E-side Cable Model B.
  - **<int 0-640>** - Enter the value between 0 and 640.
- **DPBOESCMC** - Specifies to use Downstrean Power Back-Off E-side Cable Model C.
  - **<int 0-640>** - Enter the value between 0 and 640.
- **DPBOMUS** - Specifies to use Downstrean Power Back-Off Minimum Usable Signal.
  - **<int 0-255>** - Enter the value between 0 and 255.
- **DPBOFMIN** - Specifies to use Downstrean Power Back-Off span Minimum Frequency.
  - **<int 0-2048>** - Enter the value between 0 and 2048.
- **DPBOFMAX** - Specifies to use Downstrean Power Back-Off span Maximum Frequency.

<int 32-6956> - Enter the value between 32 and 6956.
DPBOEPSD - Specifies to use Downstrean Power Back-Off assumed Exchange PSD mask.
tone - (Optional) Specifies the tone inex of the breakpoint.
<int 0-4095> - Enter the value between 0 and 4095
psd_level - Specifies the PSD reduction at the breakpoint.
<int 0-190> - Enter the value between 0 (0 dBm/Hz) and 190 (-95 dBm/Hz).

TrellisCoding - Specifies to enable or disable Trellis coding.
disable - Specifies to enable Trellis coding.
enable - Specifies to disable Trellis coding.

DownRateMode - Specifies the rate selection in the downstream direction.
manual - Specifies to change the data rate manually.
adaptAtInit - Specifies to automatically select the data rate when startup and do not change afterwards.
dynamic - Specifies to automatically select the data rate when initialization and continuously adapt during operation through Seamless Rate Adaption (SRA).

UpRateMode - Specifies to the rate selection in the upstream direction.
manual - Specifies to change the data rate manually.
adaptAtInit - Specifies to automatically select the data rate when startup and do not change afterwards.
dynamic - Specifies to automatically select the data rate when initialization and continuously adapt during operation through Seamless Rate Adaption (SRA).

MaxTxRate - Specifies the maximum allowed bit rate for downstream.
<vdsl_speed 64-128000> - Enter the value between 64 and 128000 Kbps.

MaxRxRate - Specifies the maximum allowed bit rate for upstream.
<vdsl_speed 64-128000> - Enter the value between 64 and 128000 Kbps.

MinTxRate - Specifies the minimum allowed bit rate for downstream.
<vdsl_speed 64-128000> - Enter the value between 64 and 128000 Kbps.

MinRxRate - Specifies the minimum allowed bit rate for upstream.
<vdsl_speed 64-128000> - Enter the value between 64 and 128000 Kbps.

SnrMarginTx - Specifies to configure VDSL profile TX SNR margin.
max - Specifies the maximum Noise Margin the xTU-R receiver shall try to sustain. If the Noise Margin is above this level, the xTU-R shall request that the xTU-C reduce the xTU-C transmit power to get a noise margin below this limit.
<vdsl_snr_max 0-124> - Enter the value between 0 and 124.
min - Specifies the minimum Noise Margin the xTU-C receiver shall achieve, relative to the BER requirement for each of the upstream bearer channels, to successfully complete initialization.
<vdsl_snr_min 0-124> - Enter the value between 0 and 124.
target - Specifies the minimum Noise Margin the xTU-R receiver shall achieve, relative to the BER requirement for each of the downstream bearer channels, to successfully complete initialization.
<vdsl_snr_target 0-124> - Enter the value between 0 and 124.

SnrMarginRx - Specifies to configure VDSL profile RX SNR margin.
max - Specifies the maximum Noise Margin the xTU-R receiver shall try to sustain. If the Noise Margin is above this level, the xTU-R shall request that the xTU-C reduce the xTU-C transmit power to get a noise margin below this limit.
<vdsl_snr_max 0-124> - Enter the value between 0 and 124.
min - Specifies the minimum Noise Margin the xTU-C receiver shall achieve, relative to the BER requirement for each of the upstream bearer channels, to successfully complete initialization.
<vdsl_snr_min 0-124> - Enter the value between 0 and 124.
target - Specifies the minimum Noise Margin the xTU-R receiver shall achieve, relative to the BER requirement for each of the downstream bearer channels, to successfully complete initialization.
<vdsl_snr_target 0-124> - Enter the value between 0 and 124.

InterleaveDelayDn - Specifies to configure VDSL profile downstream interleave delay.
<vdsl_inter_delay 0-63> - Enter the value between 0 and 63 in ms.

InterleaveDelayUp - Specifies to configure VDSL profile upstream interleave delay.
<vdsl_inter_delay 0-63> - Enter the value between 0 and 63 in ms.

MinInpDn - Specifies to configiure VDSL profile downstream minimum Impulse Noise Protection (INP).
- **0** - Specifies the value to be 0.
- **0.5** - Specifies the value to be 0.5.
- **1** - Specifies the value to be 1.
- **2** - Specifies the value to be 2.
- **3** - Specifies the value to be 3.
- **4** - Specifies the value to be 4.
- **5** - Specifies the value to be 5.
- **6** - Specifies the value to be 6.
- **7** - Specifies the value to be 7.
- **8** - Specifies the value to be 8.
- **9** - Specifies the value to be 9.
- **10** - Specifies the value to be 10.
- **11** - Specifies the value to be 11.
- **12** - Specifies the value to be 12.
- **13** - Specifies the value to be 13.
- **14** - Specifies the value to be 14.
- **15** - Specifies the value to be 15.
- **16** - Specifies the value to be 16.

MinInpUp - Specifies to configiure VDSL profile upstream minimum INP.
- **0** - Specifies the value to be 0.
- **0.5** - Specifies the value to be 0.5.
- **1** - Specifies the value to be 1.
- **2** - Specifies the value to be 2.
- **3** - Specifies the value to be 3.
- **4** - Specifies the value to be 4.
- **5** - Specifies the value to be 5.
- **6** - Specifies the value to be 6.
- **7** - Specifies the value to be 7.
- **8** - Specifies the value to be 8.
- **9** - Specifies the value to be 9.
- **10** - Specifies the value to be 10.
- **11** - Specifies the value to be 11.
- **12** - Specifies the value to be 12.
- **13** - Specifies the value to be 13.
- **14** - Specifies the value to be 14.
- **15** - Specifies the value to be 15.
- **16** - Specifies the value to be 16.

MinInp8Dn - Specifies to configiure VDSL profile downstream minimum INP 8kHz.
- **0** - Specifies the value to be 0.
- **0.5** - Specifies the value to be 0.5.
- **1** - Specifies the value to be 1.
- **2** - Specifies the value to be 2.
- **3** - Specifies the value to be 3.
- **4** - Specifies the value to be 4.
- **5** - Specifies the value to be 5.
- **6** - Specifies the value to be 6.
- **7** - Specifies the value to be 7.
- **8** - Specifies the value to be 8.
- **9** - Specifies the value to be 9.
- **10** - Specifies the value to be 10.
- **11** - Specifies the value to be 11.
- **12** - Specifies the value to be 12.
- **13** - Specifies the value to be 13.
- **14** - Specifies the value to be 14.
- **15** - Specifies the value to be 15.
- **16** - Specifies the value to be 16.

MinInp8Up - Specifies to configiure VDSL profile upstream minimum INP 8kHz.
- **0** - Specifies the value to be 0.

0.5 - Specifies the value to be 0.5.
1 - Specifies the value to be 1.
2 - Specifies the value to be 2.
3 - Specifies the value to be 3.
4 - Specifies the value to be 4.
5 - Specifies the value to be 5.
6 - Specifies the value to be 6.
7 - Specifies the value to be 7.
8 - Specifies the value to be 8.
9 - Specifies the value to be 9.
10 - Specifies the value to be 10.
11 - Specifies the value to be 11.
12 - Specifies the value to be 12.
13 - Specifies the value to be 13.
14 - Specifies the value to be 14.
15 - Specifies the value to be 15.
16 - Specifies the value to be 16.

LimitPSDMask - Specifies to the US0 PSD masks to be allowed by the near-end xTU on the line. This parameter is only defined for G.993.2 Annex A.
nus0 - Specifies to use nus0.
eu32 - Specifies to use eu32.
eu36 - Specifies to use eu36.
eu40 - Specifies to use eu40.
eu44 - Specifies to use eu44.
eu48 - Specifies to use eu48.
eu52 - Specifies to use eu52.
eu56 - Specifies to use eu56.
eu60 - Specifies to use eu60.
eu64 - Specifies to use eu64.
eu128 - Specifies to use eu128.
us2tods2 - Specifies to use us2 to ds2.

BitSwap - Specifies to enable or disable upstream and downstream bitswap capability.
disable - Specifies to disable upstream and downstream bitswap capability.
enable - Specifies to enable upstream and downstream bitswap capability.

PSDBreakPointTx - Specifies to configure the 32 PSD mask breakpoints in downstream direction.
tone - (Optional) Specifies the tone index of the breakpoint.
<int 0-4095> - Enter the value between 0 and 4095.
psd_level - Specifies the PSD reduction at the breakpoint.
<int 0-190> - Enter the value between 0 (0 dBm/Hz) and 190 (-95 dBm/Hz).

PSDBreakPointRx - Specifies to configure the 32 PSD mask breakpoints in upstream direction.
tone - (Optional) Specifies the tone index of the breakpoint.
<int 0-4095> - Enter the value between 0 and 4095.
psd_level - Specifies the PSD reduction at the breakpoint.
<int 0-190> - Enter the value between 0 (0 dBm/Hz) and 190 (-95 dBm/Hz).

VirtualNoiseTx - Specifies to enable or disable the downstream transmitter-referred virtual noise.
disable - Specifies to disable the downstream transmitter-referred virtual noise.
enable - Specifies to enable the downstream transmitter-referred virtual noise.
tone - (Optional) Specifies the tone index of the breakpoint.
<int 0-4095> - Enter the value between 0 and 4095.
noise_level - Specifies to noise level.
<int 0-200> - Enter the value between 0 and 200.

VirtualNoiseRx - Specifies to enable or disable the upstream transmitter-referred virtual noise.
disable - Specifies to disable the downstream transmitter-referred virtual noise.
enable - Specifies to enable the downstream transmitter-referred virtual noise.
tone - (Optional) Specifies the tone index of the breakpoint.
<int 0-4095> - Enter the value between 0 and 4095.
noise_level - Specifies to noise level.
<int 0-200> - Enter the value between 0 and 200.

GINPDn - Specifies to follow the G.998.4 definition.
- **rtx_mode** - (Optional) Specifies the retransmission mode.
  - **FORBIDDEN** - Specifies that G.998.4 retransmission is not allowed.
  - **PREFERRED** - Specifies that G.998.4 retransmission is preferred.
  - **FORCED** - Specifies to force to use G.998.4 retransmission.
  - **TESTMODE** - Specifies to force to use G.998.4 retransmission in test mode.
- **ETR_min** - (Optional) Specifies the minimum value for the Effective Throughpt Rate (ETR).
  - **<int 64-128000>** - Enter the value between 64 and 128000 Kbps.
- **ETR_max** - (Optional) Specifies the maximum value for the ETR.
  - **<int 64-128000>** - Enter the value between 64 and 128000 Kbps.
- **net_max** - (Optional) Specifies the maximum value for NDR.
  - **<int 64-128000>** - Enter the value between 64 and 128000 Kbps.
- **delay_max** - (Optional) Specifies the maximum delay time.
  - **<int 0-63>** - Enter the value between 0 and 63 milliseconds.
- **delay_min** - (Optional) Specifies the minimum delay time.
  - **<int 0-63>** - Enter the value between 0 and 63 milliseconds.
- **INP_min** - (Optional) Specifies the minimum Impuls Noise Protection (INP) against SHINE in DMT symbols.
  - **<int 0-63>** - Enter the value between 0 and 63 symbols.
- **SHINEratio** - (Optional) Specifies the shineRatio is the assumed fraction (0 to 0.255) of NDR necessary to correct SHINE noise.
  - **<int 0-255>** - Enter the value between 0 and 255.
- **leftr_thresh** - (Optional) Specifies to declare leftr defects expressed in fraction of the NDR.
  - **<int 0-99>** - Enter the value between 0 and 99. Enter 0 means the rate threshold is eaul to 98% of the ETR.
- **rein_INP_min** - (Optional) Specifies the reinCfg that overrules the traffic configuration setting.
  - **<int 0-7>** - Ener the value between 0 and 7.
- **iat_rein_flag** - (Optional) Specifies the REIN frequency.
  - **100hz** - Specifies the frequency to 100 Hz.
  - **120hz** - Specifies the frequency to 120 Hz.

GINPUp - Specifies to follow the G.998.4 definition.
- **rtx_mode** - (Optional) Specifies the retransmission mode.
  - **FORBIDDEN** - Specifies that G.998.4 retransmission is not allowed.
  - **PREFERRED** - Specifies that G.998.4 retransmission is preferred.
  - **FORCED** - Specifies to force to use G.998.4 retransmission.
  - **TESTMODE** - Specifies to force to use G.998.4 retransmission in test mode.
- **ETR_min** - (Optional) Specifies the minimum value for the Effective Throughpt Rate (ETR).
  - **<int 64-128000>** - Enter the value between 64 and 128000 Kbps.
- **ETR_max** - (Optional) Specifies the maximum value for the ETR.
  - **<int 64-128000>** - Enter the value between 64 and 128000 Kbps.
- **net_max** - (Optional) Specifies the maximum value for NDR.
  - **<int 64-128000>** - Enter the value between 64 and 128000 Kbps.
- **delay_max** - (Optional) Specifies the maximum delay time.
  - **<int 0-63>** - Enter the value between 0 and 63 milliseconds.
- **delay_min** - (Optional) Specifies the minimum delay time.
  - **<int 0-63>** - Enter the value between 0 and 63 milliseconds.
- **INP_min** - (Optional) Specifies the minimum Impuls Noise Protection (INP) against SHINE in DMT symbols.
  - **<int 0-63>** - Enter the value between 0 and 63 symbols.
- **SHINEratio** - (Optional) Specifies the shineRatio is the assumed fraction (0 to 0.255) of NDR necessary to correct SHINE noise.
  - **<int 0-255>** - Enter the value between 0 and 255.
- **leftr_thresh** - (Optional) Specifies to declare leftr defects expressed in fraction of the NDR.
  - **<int 0-99>** - Enter the value between 0 and 99. Enter 0 means the rate threshold is eaul to 98% of the ETR.
- **rein_INP_min** - (Optional) Specifies the reinCfg that overrules the traffic configuration setting.
  - **<int 0-7>** - Ener the value between 0 and 7.
- **iat_rein_flag** - (Optional) Specifies the REIN frequency.
  - **100hz** - Specifies the frequency to 100 Hz.
  - **120hz** - Specifies the frequency to 120 Hz.

SRADn - Specifies Seamless Rate Adaptation (SRA) in the downstream direction.
- **state** - (Optional) Specifies the state of SRA in the downstream direction.
  - **disable** - Specifies to enable SRA in the downstream direction.
  - **enable** - Specifies to disable SRA in the downstream direction.
- **downshiftSnr** - (Optional) Specifies the downstream down-shift noise margin value. If the downstream noise margin is lower than the specified value longer than the time specified in the **downshiftDuration** parameter, the xTU-R shall attempt to decrease the downstream net data rate.
  - **<int 0-310>** - Enter the value between 0 (0dB) and 310 (31 dB).
- **upshiftSnr** - (Optional) Specifies the downstream up-shift noise margin value. If the downstream noise margin is higher than the specified value longer than the time specified in the **upshiftDuration** parameter, the xTU-R shall attempt to increase the downstream net data rate.
  - **<int 0-310>** - Enter the value between 0 (0dB) and 310 (31 dB).
- **downshiftDuration** - (Optional) Specifies the downstream down-shift time interval.
  - **<int 0-16383>** - Enter the value between 0 and 16383 in seconds.
- **upshiftDuration** - (Optional) Specifies the downstream up-shift time interval.
  - **<int 0-16383>** - Enter the value between 0 and 16383 in seconds.

SRAUp - Specifies SRA in the upstream direction.
- **state** - (Optional) Specifies the state of SRA in the upstream direction.
  - **disable** - Specifies to enable SRA in the upstream direction.
  - **enable** - Specifies to disable SRA in the upstream direction.
- **downshiftSnr** - (Optional) Specifies the upstream down-shift noise margin value. If the upstream noise margin is lower than the specified value longer than the time specified in the **downshiftDuration** parameter, the xTU-R shall attempt to decrease the upstream net data rate.
  - **<int 0-310>** - Enter the value between 0 (0dB) and 310 (31 dB).
- **upshiftSnr** - (Optional) Specifies the upstream up-shift noise margin value. If the upstream noise margin is higher than the specified value longer than the time specified in the **upshiftDuration** parameter, the xTU-R shall attempt to increase the upstream net data rate.
  - **<int 0-310>** - Enter the value between 0 (0dB) and 310 (31 dB).
- **downshiftDuration** - (Optional) Specifies the upstream down-shift time interval.
  - **<int 0-16383>** - Enter the value between 0 and 16383 in seconds.
- **upshiftDuration** - (Optional) Specifies the upstream up-shift time interval.
  - **<int 0-16383>** - Enter the value between 0 and 16383 in seconds.

SOSDn - Specifies VDSL2 SOS in the downstream direction.
- **state** - (Optional) Specifies the state of VDSL2 SOS in the downstream direction.
  - **disable** - Specifies to disable VDSL2 SOS in the downstream direction.
  - **enable** - Specifies to enable VDSL2 SOS in the downstream direction.
- **min_rate** - (Optional) Specifies the minimum line rate insured after an SOS on each line.
  - **<int 32-128000>** - Enter the value between 32 and 128000.
- **crc** - (Optional) Specifies the SOS CRC.
  - **<int 1-65535>** - Enter the value between 1 and 65535.
- **time_window** - (Optional) Specifies the SOS monitoring time window used to trigger an SOS operation.
  - **<int 64-16320>** - Ener the value between 64 and 16320 in milliseconds.
- **degraded_tones** - (Optional) Specifies the percentage of degraded tones (SOS-NTONES).
  - **<int 0-100>** - Enter value between 0 and 100 percent.
- **max_number** - (Optional) Specifies the maximum number of successful SOS procedures.
  - **<int 0-15>** - Enter the value between 0 and 15. The value 0 indicates that there is no limit on the maximum number of SOS recoveries within this time interval.
- **roc_snr_margin** - (Optional) Specifies the extra margin to be taken for ROC tones.
  - **<int 0-250>** - Enter the value between 0 dB and 250 dB.
- **roc_min_inp** - (Optional) Specifies the minimum INP to be insured on the ROC channel.
  - **<int 0-16>** -Enter the value between 0 and 16.

SOSUp - Specifies VDSL2 SOS in the upstream direction.
- **state** - (Optional) Specifies the state of VDSL2 SOS in the upstream direction.
  - **disable** - Specifies to disable VDSL2 SOS in the upstream direction.
  - **enable** - Specifies to enable VDSL2 SOS in the upstream direction.

min_rate - (Optional) Specifies the minimum line rate insured after an SOS on each line. **<int 32-128000>** - Enter the value between 32 and 128000. **crc** - (Optional) Specifies the SOS CRC. **<int 1-65535>** - Enter the value between 1 and 65535. **time_window** - (Optional) Specifies the SOS monitoring time window used to trigger an SOS operation. **<int 64-16320>** - Ener the value between 64 and 16320 in milliseconds. **degraded_tones** - (Optional) Specifies the percentage of degraded tones (SOS-NTONES). **<int 0-100>** - Enter value between 0 and 100 percent. **max_number** - (Optional) Specifies the maximum number of successful SOS procedures. **<int 0-15>** - Enter the value between 0 and 15. The value 0 indicates that there is no limit on the maximum number of SOS recoveries within this time interval. **roc_snr_margin** - (Optional) Specifies the extra margin to be taken for ROC tones. **<int 0-250>** - Enter the value between 0 dB and 250 dB. **roc_min_inp** - (Optional) Specifies the minimum INP to be insured on the ROC channel. **<int 0-16>** -Enter the value between 0 and 16.
PHYRDn - Specifies to implement retransmission inside the PMS-TC in the downstream direction. **disable** - Specifies to disable the PhyR support. **enable** - Specifies to enable the PhyR support. **auto** - Specifies to automatically switch between PhyR and interleaving to achieve the highest possible rate.
PHYRUp - Specifies to implement retransmission inside the PMS-TC in the upstream direction. **disable** - Specifies to disable the PhyR support. **enable** - Specifies to enable the PhyR support. **auto** - Specifies to automatically switch between PhyR and interleaving to achieve the highest possible rate.
DynaDDn - Specifies to enable or disable SRA dynamic D option in the downstream direction. **disable** - Specifies to enable SRA dynamic D option **enable** - Specifies to disable SRA dynamic D option
DynaDUp - Specifies to enable or disable SRA dynamic D option in the upstream direction. **disable** - Specifies to enable SRA dynamic D option **enable** - Specifies to disable SRA dynamic D option

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure a VDSL profile entry:

```
DAS-3626:admin#config vdsl profile 2 attach all
Command: config vdsl profile 2 attach all

Success.

DAS-3626:admin#
```

50-4 show vdsl profile

Description

This command is used to display the current VDSL configuration profiles.

Format

show vdsl profile [<profile_id 1-60> | name <profile_name 32> | all]

Parameters

<profile_id 1-60> - Enter a VDSL profile ID.
name - Specifies the name of VDSL profile. **<profile_name 32>** - Enter the VDSL profile name.
all - Specifies to display all VDLS profiles.

Restrictions

None.

Example

To display a VDLS profile:

```
DAS-3626:admin#show vdsl profile 2
Command: show vdsl profile 2

Profile ID                                  : 2
Profile Name                                : VDSL2
Binding ports                               : 1-24
DS Maximum Payload Speed (kbps)             : 128000
US Maximum Payload Speed (kbps)             : 128000
DS Minimum Payload Speed (kbps)             : 64
US Minimum Payload Speed (kbps)             : 64
DS Rate Adaptive use                        : Adapt At Init
US Rate Adaptive use                        : Adapt At Init
DS Target  SNR Margin 0-124 (0.25dB Step)   : 24
US Target  SNR Margin 0-124 (0.25dB Step)   : 24
DS Minimum SNR Margin 0-124 (0.25dB Step)   : 4
US Minimum SNR Margin 0-124 (0.25dB Step)   : 4
DS Maximum SNR Margin 0-124 (0.25dB Step)   : 124
US Maximum SNR Margin 0-124 (0.25dB Step)   : 124
DS Maximum Interleave Delay 0-63 (ms)       : 20
US Maximum Interleave Delay 0-63 (ms)       : 20
DS Min. INP. (symbol)                       : 1
US Min. INP. (symbol)                       : 1
DS Min. INP8.(symbol)                       : 1
US Min. INP8.(symbol)                       : 1
Trellis Coding                              : Enable
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

50-5 show vdsl profile_list

Description

This command is used to display the brief information of all VDSL profiles.

Format

show vdsl profile_list

Parameters

None.

Restrictions

None.

Example

To display the brief information of all VDSL profiles:

```
DAS-3626:admin#

DAS-3626:admin# DAS-3626:admin#show vdsl profile_list
Command: show vdsl profile_list

================================================================================
=
                      Ds/Us        Ds/Us   Ds/Us       Ds/Us
ID Profile Name      MaxRate      MinInp  MinInp(30a) MaxDelay Binding ports
================================================================================
=
 1 DEFVAL           128000/128000   1/1     1/1        20/20
--------------------------------------------------------------------------------
-
 2 VDSL2            128000/128000   1/1     1/1        20/20   1-24
--------------------------------------------------------------------------------
-

 Total Entries: 2

DAS-3626:admin#
```

50-6 config vdsl line

Description

This command is used to change the VDSL line state or issue a measurement command to VDSL lines.

Format

config vdsl line [<vdsl_portlist> | all] [state [use | no_use] | name <name> | retrain | reset | loop_diagnostic | selt | selt_calibrate | selt_echo [1024tone | 2048tone | 3072tone | 4096tone] agc <int 0-64> duration <int 5-255> | selt_qln [1024tone | 2048tone | 3072tone | 4096tone] duration <int 0-15> | loopback [co_side {[DSP | AFE | HYBRID]} | cpe_side] times <int 1-400> size <int 64-1500>]

Parameters

<vdsl_portlist> - Enter the VDSL lines between 1 and 24.
all - Specifies to configure all VDSL lines.
state - Specifies the state of the VDSL lines. **use** - Specifies to use (active) the VDSL lines. **no_use** - Specifies to inactive the VDSL lines.
name - Specifies the line name. **<name>** - Enter the line name with the maximum of 32 characters.
retrain - Specifies to restart the handshake procedure between CO and CPE.
reset - Specifies to reset the line state to idle state and stop all issued commands. Then, re-apply the profile parameters to this line and recover the line to handshake state.
loop_diagnostic - Specifies to issue a Dual-Ended Line Test (DELT) command to the specific lines. The traffic between CO and CPE would be broken when measurement is ongoing. The remote CPE should be connected for DELT.
selt - Specifies to issue a Single Ended Loop Test (SELT) command to the specific lines. The remote CPE must be disconnected for SELT.
selt_calibrate - Specifies to issue a SELT calibration command to the specifiec lines. This command uses the default parameters to measure a set of more precised parameters to be used in the SELT command.
selt_echo - Specifies to start VDSL echo measurement. **1024tone** - Specifies the measurement to 1024 tones. **2048tone** - Specifies the measurement to 2048 tones. **3072tone** - Specifies the measurement to 3072 tones. **4096tone** - Specifies the measurement to 4096 tones. **agc** - Specifies the force AGC settings. The unit is 0.5dB. **<int 0-64>** - Enter the value between 0 and 64. **duration** - Specifies the measurement duration in seconds. **<int 5-255>** - Enter the value between 5 and 255.
selt_qln - Specifies to start SELT noise measurement. **1024tone** - Specifies the measurement to 1024 tones. **2048tone** - Specifies the measurement to 2048 tones. **3072tone** - Specifies the measurement to 3072 tones. **4096tone** - Specifies the measurement to 4096 tones. **duration** - Specifies the measurement duration in seconds. **<int 0-15>** - Enter the value between 0 and 15.
loopback - Specifies to start loop-back test in CO side or CPE side. **co_side** - Specifies to start loop-back test in CO side. **DSP** - (Optional) Specifies to use DSP mode. **AFE** - (Optional) Specifies to use AFE mode. **HYBRID** - (Optional) Specifies to to use Hybrid mode. **cpe_side** - Specifies to start loop-back test in CPE side. **times** - Specifies the times for testing. **<int 1-400>** - Enter the value between 1 and 400. **size** - Specifies the packet size for testing. **<int 64-1500>** - Enter the value between 64 and 1500.

Restrictions

Only Administrators and Operators can issue this command.

Example

To start VDSL loop diagnostic testing:

```
DAS-3626:admin#config vdsl line 8 loop_diagnostic
Command: config vdsl line 8 loop_diagnostic

----------------------------------------
*    Line Loop Diagnorstic Result      *
----------------------------------------
  Line        State         Result
--------  ------------  ---------------
     1       HANDSHAKE            NONE
     2       HANDSHAKE            NONE
     3       HANDSHAKE            NONE
     4       HANDSHAKE            NONE
     5       HANDSHAKE            NONE
     6       HANDSHAKE            NONE
     7       HANDSHAKE            NONE
     8       HANDSHAKE            NONE
     9       HANDSHAKE            NONE
    10       HANDSHAKE            NONE
    11       HANDSHAKE            NONE
    12       HANDSHAKE            NONE
    13       HANDSHAKE            NONE
    14       HANDSHAKE            NONE
    15       HANDSHAKE            NONE
    16       HANDSHAKE            NONE
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

50-7 show vdsl line

Description

This command is used to display the detail status of each VDSL lines.

Format

show vdsl line [<vdsl_portlist> | all] [status {brief} | bit_map | snr_margin_map | psd_map | hlog_map | qln_map | snr_map | gain_map | loop_diagnostic {hlog | qln | snr | hlin | band_data | chann_data | all} | selt | selt_calibrate | selt_echo {start <int 0-4095> stop <int 0-4095>} | selt_qln {start <int 0-4095> stop <int 0-4095>} | loopback | pm_counters [15mins [interval <int 1-96> | SNR_Margin] | 1day [interval <int 1-30> | SNR_Margin] | current] | inm [near_end | far_end] counter [15mins | 1day | running]]

Parameters

<vdsl_portlist> - Enter the VDSL lines between 1 and 24.
all - Specifies to configure all VDSL lines.
status - Specifies to display detail status of the specific lines. **brief** - (Optional) Specifies to display brief status of the specific lines.
bit_map - Specifies to display the distribution information of bit allocation in downstream and upstream direction.
snr_margin_map - Specifies to display the distribution information of SNR margin (dB) in downstream and upstream direction.
psd_map - Specifies to display the distribution information of TX PSD (dBm/HZ) in downstream and upstream direction.

hlog_map - Specifies to display the distribution information of real H(f) logarithmic representation values (dB) in downstream and upstream direction.
qln_map - Specifies to display the distribution information of quiet line noise (dB) in downstream and upstream direction.
snr_map - Specifies to display the distribution information of SNR (dB) in downstream and upstream direction.
gain_map - Specifies to display the distribution information of gain (dB) in downstream and upstream direction.
loop_diagnostic - Specifies to display the loop diagnostic testing result. **hlog** - (Optional) Specifies to display the loop diagnostic testing result of real H(f) logarithmic representation values. **qln** - (Optional) Specifies to display the loop diagnostic testing result of quiet line noise. **snr** - (Optional) Specifies to display the loop diagnostic testing result of SNR. **hlin** - (Optional) Specifies to display the loop diagnostic testing result of complex H(f) linear representation values in linear scale. **band_data** - (Optional) Specifies to display the loop diagnostic testing result of each band. **chann_data** - (Optional) Specifies to display the loop diagnostic testing result of each bearer channel. **all** - (Optional) Specifies to display all the loop diagnostic testing result.
selt - Specifies to display the measurement SELT result.
selt_calibrate - Specifies to check the calibrate state of SELT is done or not
selt_echo - Specifies to display the measured SELT echo result for third-party application. **start** - (Optional) Specifies the first tone index. **<int 0-4095>** - Enter the value between 0 and 4095. **stop** - (Optional) Specifies the last tone index. **<int 0-4095>** - Enter the value between 0 and 4095.
selt_qln - Specifies to display the measured SELT noise result for third-party application. **start** - (Optional) Specifies the first tone index. **<int 0-4095>** - Enter the value between 0 and 4095. **stop** - (Optional) Specifies the last tone index. **<int 0-4095>** - Enter the value between 0 and 4095.
loopback - Specifies to display the loopback testing result.
pm_counters - Specifies to display the records of line performance counters in CO and CPE side. **15mins** - Specifies to display the 15-minute history of interval-counters. **interval** - Specifies one of the 15-minute history buckets. **<int 1-96>** - Enter the bucket index between 1 and 96. **SNR_Margin** - Specifies to display the 15-minute history of SNR margin. **1day** - Specifies to display the 1-day history of interval-counters. **interval** - Specifies one of the 1-day history buckets. **<int 1-30>** - Enter the bucket index between 1 and 30. **SNR_Margin** - Specifies to display the 1-day history of SNR margin. **current** - Specifies to display the current performance counters.
inm - Specifies to display the detected impulse noise records in CO and CPE side. **near_end** - Specifies to display the CO side history of impulse noise. **far_end** - Specifies to display the CPE side history of impulse noise. **counter** - Specifies to display the detected impulse noise counters. **15mins** - Specifies to display the 15-minute history of impulse noise counters. **1day** - Specifies to display the 1-day history of impulse noise counters. **running** - Specifies to display the current impulse noise counters.

Restrictions

None.

Example

To display VDSL line status:

```
DAS-3626:admin#show vdsl line 8 status
Command: show vdsl line 8 status

Line 8              : LINE-8
Link State          : HANDSHAKE
Bonding Group       : NONE
Selected protocol   : NONE
Line Config Profile : DEFVAL
Line Type           : InterleavedOnly
Remote CPE Type     : N/A
Line Uptime         : N/A
Band Plan           : N/A
VDSL2 Profile       : none
-----------------------------------------------------------------
                                |    Downstream |      Upstream
-----------------------------------------------------------------
Line Rate                       |    111.484Mbps|     83.970Mbps
Payload Rate                    |    111.313Mbps|     83.813Mbps
Attainable Payload Rate         |    193.696Mbps|    128.165Mbps
SNR Margin              US0     |            N/A|            N/A
                      DS1/US1   |         22.1dB|         26.3dB
                      DS2/US2   |         21.7dB|         22.5dB
                      DS3/US3   |         22.0dB|         19.5dB
Average SNR Margin              |         22.0dB|         21.2dB
Interleave Delay                |            4ms|            4ms
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

50-8 config vdsl pm_threshold

Description

This command is used to configure the detail performance threshold values.

Format

config vdsl pm_threshold [15min | 1day | both] [near_end [{es <threshold> | fecs <threshold> | ses <threshold> | loss <threshold> | uas <threshold> | crc <threshold> | init <threshold>}] | far_end [{es <threshold> | fecs <threshold> | ses <threshold> | loss <threshold> | uas <threshold> | crc <threshold>}] | both_ends [{es <threshold> | fecs <threshold> | ses <threshold> | loss <threshold> | uas <threshold> | crc <threshold>}]]

Parameters

15min - Specifies 15 minute counter threshold.
1day - Specifies 1 day counter threshold.
both - Specifies 15 minute and 1 day counter threshold.
near_end - Specifies to configure the PM threshold value for CO side. **es** - (Optional) Specifies the threshold interval in seconds when errors have occurred. **<threshold>** - Enter the threshold interval in seconds. **fecs** - (Optional) Specifies the threshold interval in seconds when at least one FEC correction event has occurred. **<threshold>** - Enter the threshold interval in seconds. **ses** - (Optional) Specifies the threshold interval in seconds when severe errors have occurred.

	<threshold> - Enter the threshold interval in seconds. **loss** - (Optional) Specifies the threshold interval in seconds when loss of signal has occurred. **<threshold>** - Enter the threshold interval in seconds. **uas** - (Optional) Specifies the threshold interval in seconds when the unavailability state has occurred. **<threshold>** - Enter the threshold interval in seconds. **crc** - (Optional) Specifies the threshold interval in seconds when CRC errors have occurred. **<threshold>** - Enter the threshold interval in seconds. **init** - (Optional) Specifies the threshold interval in seconds when a new training has started. **<threshold>** - Enter the threshold interval in seconds.
far_end	- Specifies to configure the PM threshold value for CPE side. **es** - (Optional) Specifies the threshold interval in seconds when errors have occurred. **<threshold>** - Enter the threshold interval in seconds. **fecs** - (Optional) Specifies the threshold interval in seconds when at least one FEC correction event has occurred. **<threshold>** - Enter the threshold interval in seconds. **ses** - (Optional) Specifies the threshold interval in seconds when severe errors have occurred. **<threshold>** - Enter the threshold interval in seconds. **loss** - (Optional) Specifies the threshold interval in seconds when loss of signal has occurred. **<threshold>** - Enter the threshold interval in seconds. **uas** - (Optional) Specifies the threshold interval in seconds when the unavailability state has occurred. **<threshold>** - Enter the threshold interval in seconds. **crc** - (Optional) Specifies the threshold interval in seconds when CRC errors have occurred. **<threshold>** - Enter the threshold interval in seconds.
both_ends	- Specifies to configure the PM threshold value for both CO and CPE side. **es** - (Optional) Specifies the threshold interval in seconds when errors have occurred. **<threshold>** - Enter the threshold interval in seconds. **fecs** - (Optional) Specifies the threshold interval in seconds when at least one FEC correction event has occurred. **<threshold>** - Enter the threshold interval in seconds. **ses** - (Optional) Specifies the threshold interval in seconds when severe errors have occurred. **<threshold>** - Enter the threshold interval in seconds. **loss** - (Optional) Specifies the threshold interval in seconds when loss of signal has occurred. **<threshold>** - Enter the threshold interval in seconds. **uas** - (Optional) Specifies the threshold interval in seconds when the unavailability state has occurred. **<threshold>** - Enter the threshold interval in seconds. **crc** - (Optional) Specifies the threshold interval in seconds when CRC errors have occurred. **<threshold>** - Enter the threshold interval in seconds.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the PM threshold value for both CO and CPE side in 1-day interval:

```
DAS-3626:admin#config vdsl pm_threshold 1day both_ends es 14400 fecs 14400 ses
14400 loss 14400 uas 0 crc 14400
Command: config vdsl pm_threshold 1day both_ends es 14400 fecs 14400 ses 14400
loss 14400 uas 0 crc 14400


Success.


DAS-3626:admin#
```

50-9 show vdsl pm_threshold

Description

This command is used to display the PM threshold values.

Format

show vdsl pm_threshold

Parameters

None.

Restrictions

None.

Example

To display the PM threshold values:

```
DAS-3626:admin#show vdsl pm_threshold
Command: show vdsl pm_threshold

15 min. PM counters' threshold values
                     |        Near-End |           Far-End
-------------------------------------------------------------
FECS                 |              10|                  10
ES                   |              10|                  10
SES                  |              10|                  10
LOSS                 |              10|                  10
UAS                  |               0|                   0
CRC                  |              10|                  10
INIT                 |              10|

1 day PM counters' threshold values
                     |        Near-End |           Far-End
-------------------------------------------------------------
FECS                 |             14400|                14400
ES                   |             14400|                14400
SES                  |             14400|                14400
LOSS                 |             14400|                14400
UAS                  |               0|                  0
CRC                  |             14400|                14400
INIT                 |              10|

DAS-3626:admin#
```

50-10 show vdsl brief status

Description

This command is used to display the brief status of VDSL lines.

Format

show vdsl brief_status [alarms | line_state line [<vdsl_portlist> | all] | profiles | rate | snrmargin | txpower | attenuation]

Parameters

alarms - Specifies to display the CRC, FEC and ES counters of all VDSL lines.
line_state line - Specifies the line state used for profile and link-up duration of the VDSL lines. **<vdsl_portlist>** - Enter a list of VDSL lines. The value is from 1 to 24. **all** - Specifies to display all VDSL lines.
profiles - Specifies to display all VDSL profiles.
rate - Specifies to display the line rate of all VDSL lines.
snrmargin - Specifies to display the SNR margin of all VDSL lines.
txpower - Specifies to display the transmitting power of all VDSL lines.
attenuation - Specifies to display the attenuation of all VDSL lines.

Restrictions

None.

Example

To display the brief status of VDSL lines:

```
DAS-3626:admin#show vdsl brief_status alarms
Command: show vdsl brief_status alarms


GET VDSL ALARM

VDSL(   1):CRC_I:0/0  RS:0/0  ESs:0/0
VDSL(   2):CRC_I:0/0  RS:0/0  ESs:0/0
VDSL(   3):CRC_I:0/0  RS:0/0  ESs:0/0
VDSL(   4):CRC_I:0/0  RS:0/0  ESs:0/0
VDSL(   5):CRC_I:0/0  RS:0/0  ESs:0/0
VDSL(   6):CRC_I:0/0  RS:0/0  ESs:0/0
VDSL(   7):CRC_I:0/0  RS:0/0  ESs:0/0
VDSL(   8):CRC_I:0/0  RS:0/0  ESs:0/0
VDSL(   9):CRC_I:0/0  RS:0/0  ESs:0/0
VDSL(  10):CRC_I:0/0  RS:0/0  ESs:0/0
VDSL(  11):CRC_I:0/0  RS:0/0  ESs:0/0
VDSL(  12):CRC_I:0/0  RS:0/0  ESs:0/0
VDSL(  13):CRC_I:0/0  RS:0/0  ESs:0/0
VDSL(  14):CRC_I:0/0  RS:0/0  ESs:0/0
VDSL(  15):CRC_I:0/0  RS:0/0  ESs:0/0
VDSL(  16):CRC_I:0/0  RS:0/0  ESs:0/0
VDSL(  17):CRC_I:0/0  RS:0/0  ESs:0/0
VDSL(  18):CRC_I:0/0  RS:0/0  ESs:0/0
VDSL(  19):CRC_I:0/0  RS:0/0  ESs:0/0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

50-11 create vdsl inm_profile name

Description

This command is used to create an impulse noise monitoring profile.

Format

create vdsl inm_profile name <profile_name 32>

Parameters

<profile_name 32> - Enter the impulse noise monitoring profile name with a maximum of 32 characters.

Restrictions

Only Administrators and Operators can issue this command.

Example

To create an impulse noise monitoring profile:

```
DAS-3626:admin#create vdsl inm_profile name inmname
Command: create vdsl inm_profile name inmname

Success.

DAS-3626:admin#
```

50-12 delete vdsl inm_profile name

Description

This command is used to delete an impulse noise monitoring profile.

Format

delete vdsl inm_profile name <profile_name 32>

Parameters

<profile_name 32> - Enter the impulse noise monitoring profile name with a maximum of 32 characters.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete an impulse noise monitoring profile:

```
DAS-3626:admin#delete vdsl inm_profile name inmname
Command: delete vdsl inm_profile name inmname

Success.

DAS-3626:admin#
```

50-13 show vdsl inm_profile

Description

This command is used to display the impulse noise monitoring profiles.

Format

show vdsl inm_profile [name <profile_name 32> | all]

Parameters

name - Specifies the the impulse noise monitoring profile name.
<profile_name 32> - Enter the impulse noise monitoring profile name with a maximum of 32 characters.

all - Specifies to display all impulse noise monitoring profiles.

Restrictions

None.

Example

To display an impulse noise monitoring profile:

```
DAS-3626:admin#

DAS-3626:admin# DAS-3626:admin#show vdsl inm_profile name inmname
Command: show vdsl inm_profile name inmname

Profile Name                                        : inmname
Binding ports                                       :
Near End INM State                                  : Disable
Near End INM_INPEQ mode                             : Mode 0
Near End INM the Cluster Continuation value (symbol) : 0
Near End INM Inter Arrival Time Offset (symbol)     : 3
Near End INM Inter Arrival Time Step                : 0
Near End INM ISDD sensitivity (0.1dB Step)          : 0
Far End INM State                                   : Disable
Far End INM_INPEQ mode                              : Mode 0
Far End INM the Cluster Continuation value (symbol)  : 0
Far End INM Inter Arrival Time Offset (symbol)      : 3
Far End INM Inter Arrival Time Step                 : 0
Far End INM ISDD sensitivity (0.1dB Step)           : 0


DAS-3626:admin#
```

50-14 config vdsl inm_profile name

Description

This command is used to configure an impulse noise monitoring profile.

Format

config vdsl inm_profile name <profile_name 32> [attach [<vdsl_portlist> | all] | [near_end | far_end] {state [disable | enable] | inminpeq <int 0-3> | inmcc <int 0-64> | inmiato <int 3-511> | inmiats <int 0-7> | inmss <inmss_value> }]

Parameters

<profile_name 32> - Enter the impulse noise monitoring profile name with a maximum of 32 characters.
attach - Specifies to apply the profile to specific VDSL lines. **<vdsl_portlist>** - Enter a list of VDSL lines. **all** - Specifies to apply the profile to all VDSL lines.
near_end - Specifies to configure the CO side impulse noise monitoring parameters.

state - (Optional) Specifies to enable or disable the impulse noise monitoring function.
disable - Specifies to disable the impulse noise monitoring function.
enable - Specifies to enable the impulse noise monitoring function.
inminpeq - (Optional) Specifies the equivalent INP.
<int 0-3> - Enter the value between 0 and 3.
0 generates INM histograms without indication of clustered impulses. Each consecutive set of severely degraded symbols is counted as a separate impulse event.
1 generates INM histograms with indication of clustered impulses. The reported histograms give an upperbound on the required INP for correlated impulse noise events.
2 generates INM histograms with indication of clustered impulses. Within each cluster, the gaps are not counted. The reported histograms give a lower bound on the required INP for correlated impulse noise events.
3 generates INM histograms with indication of clustered impulses. The reported histograms give the best estimate of the required INP to correct the impulse noise events.
inmcc - (Optional) Specifies the INM cluster continuation value to be used in the cluster indication process.
<int 0-64> - Enter the value between 0 and 64.
inmiato - (Optional) Specifies the INM inter-arrival time offset for the IAT anomaly generation in order to determine in which bin of the inter-arrival time histogram the IAT is reported.
<int 3-511> - Enter the value between3 and 511.
inmiats - (Optional) Specifies the INM inter-arrival time step for the IAT anomaly generation in order to determine in which bin of the inter-arrival time histogram the IAT is reported.
<int 0-7> - Enter the value between 0 and 7.
inmss - (Optional) Specifies the Indication of Severely Degraded Data sensitivity. The Switch supports an extension to the standard through this proprietary parameter that allows the adjustments to the Impulse Noise Sensor sensitivity.
<inmss_value> - Enter the value between -128 (-12.8 dB) and 127 (12.7dB).

far_end - Specifies to configure the CPE side impulse noise monitoring parameters.
state - (Optional) Specifies to enable or disable the impulse noise monitoring function.
disable - Specifies to disable the impulse noise monitoring function.
enable - Specifies to enable the impulse noise monitoring function.
inminpeq - (Optional) Specifies the equivalent INP.
<int 0-3> - Enter the value between 0 and 3.
0 generates INM histograms without indication of clustered impulses. Each consecutive set of severely degraded symbols is counted as a separate impulse event.
1 generates INM histograms with indication of clustered impulses. The reported histograms give an upperbound on the required INP for correlated impulse noise events.
2 generates INM histograms with indication of clustered impulses. Within each cluster, the gaps are not counted. The reported histograms give a lower bound on the required INP for correlated impulse noise events.
3 generates INM histograms with indication of clustered impulses. The reported histograms give the best estimate of the required INP to correct the impulse noise events.
inmcc - (Optional) Specifies the INM cluster continuation value to be used in the cluster indication process.
<int 0-64> - Enter the value between 0 and 64.
inmiato - (Optional) Specifies the INM inter-arrival time offset for the IAT anomaly generation in order to determine in which bin of the inter-arrival time histogram the IAT is reported.
<int 3-511> - Enter the value between3 and 511.
inmiats - (Optional) Specifies the INM inter-arrival time step for the IAT anomaly generation in order to determine in which bin of the inter-arrival time histogram the IAT is reported.
<int 0-7> - Enter the value between 0 and 7.
inmss - (Optional) Specifies the Indication of Severely Degraded Data sensitivity. The Switch supports an extension to the standard through this proprietary parameter that allows the adjustments to the Impulse Noise Sensor sensitivity.

<inmss_value> - Enter the value between -128 (-12.8 dB) and 127 (12.7dB).

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure an impulse noise monitoring profile:

```
DAS-3626:admin#config vdsl inm_profile name inmname near_end state enable
inminpeq 0 inmcc 0 inmiato 3 inmiats 3 inmss 0
Command: config vdsl inm_profile name inmname near_end state enable inminpeq 0
inmcc 0 inmiato 3 inmiats 3 inmss 0

Success.

DAS-3626:admin#
```

50-15 config vdsl bonding

Description

This command is used to configure the VDSL bonding parameters of each bonding group. When apply the profile to a bonding group, the Maximum line rate would be calculated by following the user configured ratio and apply to the bonding lines. For example, if the MaxTxRate of the profile is 128000kbps and the ratio is 50%:50%, then the maximum line rate of the two bonding lines is 64000kbps.

Format

config vdsl bonding [<bgroup_list> | all] [profile [use [<profile_id 1-60> | name <profile_name 32>] ds_rate_alloc [default | master_weight <int 1-99>] us_rate_alloc [default | master_weight <int 1-99>] | individual] | state [enable | disable] | loopback cpe_side times <int 1-400> size <int 64-1500> | line_state [use | no_use]]

Parameters

<bgroup_list> - Enter a list of VDSL bonding groups. The range is from 1 to 12.
all - Specifies to configure all VDSL bonding groups.
profile - Specifies a VDSL profile.
- **use** - Specifies to use the VDSL profile for selected bonding groups.
  - **<profile_id 1-60>** - Enter a VDSL profile ID. The range is from 1 to 60.
  - **name** - Specifies a VDSL profile name.
    - **<profile_name 32>** - Enter a VDSL profile name with a maximum of 32 characters.
  - **ds_rate_alloc** - Specifies to assign the ratio (%) of total downstream line rate in each bonding lines.
    - **default** - Specifies to use the default ration. The default ration is 50.
    - **master_weight** - Specifies the ratio of the master line.
      - **<int 1-99>** - Enter the value between 1 and 99.
  - **us_rate_alloc** - Specifies to assign the ratio (%) of total upstream line rate in each bonding lines.
    - **default** - Specifies to use the default ration. The default ration is 50.
    - **master_weight** - Specifies the ratio of the master line.

<int 1-99> - Enter the value between 1 and 99. **individual** - Specifies to allow user to use different profiles for each bonding member lines.
state - Specifies to enable (bonding mode) or disable (single line mode) the state of bonding groups. **enable** - Specifies to enable the state of bonding groups. **disable** - Specifies to disable the state of bonding groups.
loopback - Specifies to execute the loopback test for bonding groups. **cpe_side times** - Specifies the times for loopback test. **<int 1-400>** - Enter the value between 1 and 400. **size** - Specifies the packet size for loopback test. **<int 64-1500>** - Enter the value between 64 and 1500.
line_state - Specifies the line state of the bonding lines. **use** - Specifies to configure the bonding lines in active state. **no_use** - Specifies to configure the bonding lines in inactive state.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the VDSL bonding parameters of each bonding group:

```
DAS-3626:admin#config vdsl bonding 1 profile use 2 ds_rate_alloc default
us_rate_alloc default
Command: config vdsl bonding 1 profile use 2 ds_rate_alloc default
us_rate_alloc default

Success.

DAS-3626:admin#
```

50-16 show vdsl bonding

Description

This command is used to display the current VDSL bonding configuration and link status of each bonding group.

Format

show vdsl bonding [<bgroup_list> | all]

Parameters

<bgroup_list> - Enter a list of VDSL bonding groups. The range is from 1 to 12.
all - Specifies to display all VDSL bonding groups.

Restrictions

None.

Example

To display a VDSL bonding:

```
DAS-3626:admin#show vdsl bonding 1
Command: show vdsl bonding 1

================================================================================
  VDSL Bonding Group ID :  1
================================================================================
 Admin Status                 : disabled
 Line Status                  : use
 Master Line                  : 1
 Bonding Lines                : 1-2
 Bonding Config Profile       : vdsl2
--------------------------------------------------------------------------------
 DS Max. Bonding Rate(kbps)   : 128000
 DS Min. Bonding Rate(kbps)   : 128
 Line 1  DS Max. Rate(kbps)   : 64000  (50%)
 Line 1  DS Min. Rate(kbps)   : 64     (50%)
 Line 2  DS Max. Rate(kbps)   : 64000  (50%)
 Line 2  DS Min. Rate(kbps)   : 64     (50%)

 US Max. Bonding Rate(kbps)   : 128000
 US Min. Bonding Rate(kbps)   : 128
 Line 1  US Max. Rate(kbps)   : 64000  (50%)
 Line 1  US Min. Rate(kbps)   : 64     (50%)
 Line 2  US Max. Rate(kbps)   : 64000  (50%)
 Line 2  US Min. Rate(kbps)   : 64     (50%)
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

50-17 clear vdsl_counter

Description

This command is used to clear the VDSL counters.

Format

clear vdsl_counter [<vdsl_portlist> | all]

Parameters

<vdsl_portlist> - Enter a list of VDSL lines. The range is from 1 to 24.
all - Specifies to apply the profile to all VDSL lines.

Restrictions

Only Administrators and Operators can issue this command.

Example

To clear all VDSL counters:

```
DAS-3626:admin#clear vdsl_counter all
Command: clear vdsl_counter all



DAS-3626:admin#
```

50-18 clear vdsl_inm_counter

Description

This command is used to clear the VDSL impulse noise monitoring counters.

Format

clear vdsl_inm_counter [<vdsl_portlist> | all] [near_end | far_end]

Parameters

<vdsl_portlist> - Enter a list of VDSL lines. The range is from 1 to 24.
all - Specifies to apply the profile to all VDSL lines.
near_end - Specifies to clear the CO side counters.
far_end - Specifies to clear the CPE side counters.

Restrictions

Only Administrators and Operators can issue this command.

Example

To clear all VDSL impulse noise monitoring counters at the CO side:

```
DAS-3626:admin#clear vdsl_inm_counter all near_end
Command: clear vdsl_inm_counter all near_end



DAS-3626:admin#
```

Chapter 51 VDSL CPE Remote Control Command List

config rmt LAN_IP [ports <vdsl_portlist> | bonding <bgroup_list> | all] lan_id <int 1-4> [enable | disable] IP <string 32> mask <string 32>
show rmt LAN_IP [ports <vdsl_portlist> | bonding <bgroup_list> | all]
config rmt TR069 [ports <vdsl_portlist> | bonding <bgroup_list> | all] {cpe_id <string 32> | interface <int 1-8> | TR069_enable [disable | enable] | username <string 32> | password <string 32> | acs_url <string 128> | connection_acs_port <int 0-65535> | connection_request_username <string 32> | connection_request_password <string 32> | connection_request_relam <string 128> | inform [disable | Periodic] | periodic_interval <uint 0-4294967295>}
show rmt TR069 [ports <vdsl_portlist> | bonding <bgroup_list> | all]
config rmt bridge [ports <vdsl_portlist> | bonding <bgroup_list> | all] connection <int 1-8> filter_DHCP_request [enable | disable]
show rmt bridge [ports <vdsl_portlist> | bonding <bgroup_list> | all]
config rmt cfm-config [ports <vdsl_portlist> | bonding <bgroup_list> | all] [cfm_status [enable | disable] | md_name [<string 16> | clear] | md_level <int 0-7> | ma_name [<string 16> | clear] | mep_index <int 1-8191> | vlan_id <int 1-4094> | vlan_priority <int 0-7> | ccm_status [enable | disable] | ccm_interval [1s | 10s | 1min | 10min]]
config rmt cfm-lbm [ports <vdsl_portlist> | bonding <bgroup_list> | all] [[des_mac <macaddr> | multicast_mac 01-80-c2-00-00-31] lbm_num <int 1-255> | clear-lbr]
config rmt cfm-ltm [ports <vdsl_portlist> | bonding <bgroup_list> | all] [target_mac <macaddr> | mep_id <int 1-8191> | clear-ltr]
show rmt cfm-lbm [ports <vdsl_portlist> | bonding <bgroup_list> | all]
show rmt cfm-ltm [ports <vdsl_portlist> | bonding <bgroup_list> | all]
show rmt cfm-config [ports <vdsl_portlist> | bonding <bgroup_list> | all]
show rmt cfm-database [ports <vdsl_portlist> | bonding <bgroup_list> | all]
show rmt antenna_count [ports <vdsl_portlist> | bonding <bgroup_list> | all]
config rmt dhcp-pool [ports <vdsl_portlist> | bonding <bgroup_list> | all] pool_id <int 1-4> {dhcp_mode [sever | relay] | dhcp_server [enable | disable] | dhcp_pool_start <ipaddr> | dhcp_pool_end <ipaddr> | dhcp_pool_lease_time [1_hour | 2_hours | 3_hours | 1_day | 2_days | 3_days | 1_week]}
config rmt dhcp-pool-option [ports <vdsl_portlist> | bonding <bgroup_list> | all] [add | rule_id <int 1-8>] [60 option_value <string 20> | 61 iaid <string 11> [mac <macaddr> | enterprise_num <string 32>] | 125 enterprise_num <hex 0x0-0xffff> manufacture_oui <string 32> serial_number <string 32> product_class <string 32> gateway_oui <string 32> | SSID [index <int 1-4> | VLAN vid <int 1-4094>] start_ip <ipaddr> end_ip <ipaddr> lease_time <sec 0-9999999> gateway_ip <ipaddr> subnet <ipaddr> [enable | disable]
config rmt dhcp-pool-option-status [<vdsl_portlist> | all] [near_end | far_end] [enable | disable]
show rmt dhcp-pool [ports <vdsl_portlist> | bonding <bgroup_list> | all]
show rmt dhcp-pool-option [ports <vdsl_portlist> | bonding <bgroup_list> | all]
config rmt connection [ports <vdsl_portlist> | bonding <bgroup_list> | all] id <int 1-8> mode [[bridge | pppoe | static | dynamic] {vlan [enable | disable] | vid <int 1-4094> | pid <int 0-7>} | disable]
show rmt connection_id <int 1-8> [ports <vdsl_portlist> | bonding <bgroup_list> | all]
config rmt dynamic-mode [ports <vdsl_portlist> | bonding <bgroup_list> | all] {host_name <string 32> | mtu <int 1000-1500> | default-route [enable | disable] | nat [enable | disable] | pppoe-passthrough [enable | disable] | dhcp_option60 [enable vendor-id <string 32> | disable] | dhcp_option61 [enable duid [address_plus_time | vendor_id {ent_num} <uint 0-4294967295> | identifier} <string 64>} | address] {iaid <string 32>} | disable] | dhcp_option125 [enable {man_oui <string 64> | pro_class <string 64> | mod_name <string 64> | ser_num <string 64>} | disable]}
show rmt dynamic-mode [ports <vdsl_portlist> | bonding <bgroup_list> | all]

config rmt eth-mode [ports <vdsl_portlist> | bonding <bgroup_list> | all] [port [LAN_1 | LAN_2 | LAN_3 | LAN_4] speed-duplex [auto | 10H | 10F | 100H | 100F] | admin [enable | disable]]
show rmt eth-mode [ports <vdsl_portlist> | bonding <bgroup_list> | all]
config rmt filter [ports <vdsl_portlist> | bonding <bgroup_list> | all] [[delete rule_id <int 1-10>] | [[add | rule_id <int 1-10>] {rule_state [inactive | active] | rule_action [allow | deny] | outgoing_if [1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | lan | all] | protocol [any | tcp | udp | icmp] | src_ip [any_ip | single_ip <ipaddr> | ip_range <ipaddr> <ipaddr> | netmask <network_address>] | src_mac <macaddr> | des_ip [any_ip | single_ip <ipaddr> | ip_range <ipaddr> <ipaddr> | netmask <network_address>] | src_port [any_port | single_port <value 0-65535> | port_range <value 0-65535> <value 0-65535>] | des_port [any_port | single_port <value 0-65535> | port_range <value 0-65535> <value 0-65535>]}]]
show rmt filter [ports <vdsl_portlist> | bonding <bgroup_list> | all]
config rmt igmp-proxy [ports <vdsl_portlist> | bonding <bgroup_list> | all] [enable | disable] interface <int 1-8>
config rmt igmp-status [ports <vdsl_portlist> | bonding <bgroup_list> | all] [enable | disable]
config rmt igmpsnooping [ports <vdsl_portlist> | bonding <bgroup_list> | all] [enable | disable] [group1 | group2 | group3 | group4] [Standard | Blocking]
show rmt igmp-status [ports <vdsl_portlist> | bonding <bgroup_list> | all]
show rmt igmpsnooping [ports <vdsl_portlist> | bonding <bgroup_list> | all]
show rmt igmp-proxy [ports <vdsl_portlist> | bonding <bgroup_list> | all]
config rmt loopback [ports <vdsl_portlist> | bonding <bgroup_list> | all] packet_count <int 1-90> packet_length <int 12-255>
show rmt loopback [ports <vdsl_portlist> | bonding <bgroup_list> | all]
config rmt port_group_lan [ports <vdsl_portlist> | bonding <bgroup_list> | all] | {LAN1 [group1 | group2 | group3 | group4]} | {LAN2 [group1 | group2 | group3 | group4]} | {LAN3 [group1 | group2 | group3 | group4]} | {LAN4 [group1 | group2 | group3 | group4]} | {SSID1 [group1 | group2 | group3 | group4]} | {SSID2 [group1 | group2 | group3 | group4]} | {SSID3 [group1 | group2 | group3 | group4]} | {SSID4 [group1 | group2 | group3 | group4]}
config rmt port_group_wan [ports <vdsl_portlist> | bonding <bgroup_list> | all] | {group1 [NONE | WAN1 | WAN2 | WAN3 | WAN4 | WAN5 | WAN6 | WAN7 | WAN8]} | {group2 [NONE | WAN1 | WAN2 | WAN3 | WAN4 | WAN5 | WAN6 | WAN7 | WAN8]} | {group3 [NONE | WAN1 | WAN2 | WAN3 | WAN4 | WAN5 | WAN6 | WAN7 | WAN8]} | {group4 [NONE | WAN1 | WAN2 | WAN3 | WAN4 | WAN5 | WAN6 | WAN7 | WAN8]}
show rmt port_group [ports <vdsl_portlist> | bonding <bgroup_list> | all]
config rmt pppoe [ports <vdsl_portlist> | bonding <bgroup_list> | all] connection_id <int 1-8> {serivce_name [<string 256> | clear] | ac_name [<string 256> | clear] | nat [disable | enable] | default_route [disable | enable] | pppoe_passthrouth [disable | enable] | mtu <int 46-1500> | connection_mode_select [always_on | manual | connect_on_demand max_idle_time <min 1-65536>]}
show rmt pppoe connection_id <int 1-8> [ports <vdsl_portlist> | bonding <bgroup_list> | all]
config rmt protovlan [ports <vdsl_portlist> | bonding <bgroup_list> | all] [add | rule_id <int 1-8>] type [Ether_Type <protocol_value> | [Source_IP <string 32> | Destination_IP <string 32>] Protocol [None | TCP | UDP | ICMP | IGMP] | SSID <string 31> | Source_MAC <string 32> | Destination_MAC <string 32> | Port [1 | 2 | 3 | 4] | [Source_IPv6 <string 64> | Destination_IPv6 <string 64>] Protocol [None |TCP | UDP | ICMP | IGMP] | DHCP option [60 option_value <string 20>|61 [type1 {iaid <string 11>} {mac <macaddr>} | type2 {iaid <string 11>} {enterprise_num <string 32>} {identifier <string 32>}] | 125 enterprise_num <string 32> manufacture_oui <string 32> serial_number <string 32> product_class <string 32> gateway_oui <string 32>]] <priority 0-7> <vlanid 1-4094> [enable | disable]
show rmt protovlan [ports <vdsl_portlist> | bonding <bgroup_list> | all]
config rmt qos [ports <vdsl_portlist> | bonding <bgroup_list> | all] [disable_all | 802_1p | dscp | remark_1p_by_dscp | Port LAN_1 priority <int 0-7> LAN_2 priority <int 0-7> LAN_3 priority <int 0-7> LAN_4 priority <int 0-7> | VLAN [Priority_0 | Priority_1 | Priority_2 | Priority_3 | Priority_4 | Priority_5 | Priority_6 | Priority_7] total vid [1 <int 1-4094> | 2 <int 1-4094> <int 1-4094> | 3 <int 1-4094> <int 1-4094> <int 1-4094> | 4 <int 1-4094> <int 1-4094> <int 1-4094> <int 1-4094> | 5 <int 1-4094> <int 1-4094> <int 1-4094> <int 1-4094> <int 1-4094>]]
show rmt qos [ports <vdsl_portlist> | bonding <bgroup_list> | all]
config rmt qos-shaping [ports <vdsl_portlist> | bonding <bgroup_list> | all] {Priority_1 <int 0-

200000> | Priority_2 <int 0-200000> | Priority_3 <int 0-200000> | Priority_4 <int 0-200000> | Priority_5 <int 0-200000> | Priority_6 <int 0-200000> | Priority_7 <int 0-200000>}
show rmt Qos_shaping [ports <vdsl_portlist> | bonding <bgroup_list> | all]
config rmt reboot [ports <vdsl_portlist> | bonding <bgroup_list> | all]
config rmt reset [ports <vdsl_portlist> | bonding <bgroup_list> | all]
config rmt reset-config [ports <vdsl_portlist> | bonding <bgroup_list> | all]
config rmt save [ports <vdsl_portlist> | bonding <bgroup_list> | all]
config rmt server [ports <vdsl_portlist> | bonding <bgroup_list> | all] [telnet_lan | telnet_wan | web_lan | web_wan | ssh_lan | ssh_wan | tftp_lan | tftp_wan | snmp_lan | snmp_wan | icmp_wan | all] state [enable | disable]
show rmt server [ports <vdsl_portlist> | bonding <bgroup_list> | all]
config rmt static-mode [ports <vdsl_portlist> | bonding <bgroup_list> | all] {network_addr <network_address> | gateway_addr <ipaddr> | mtu <int 1000-1500> | default_route [enable | disable] | nat [enable | disable] | pppoe-passthrough [enable | disable]}
show rmt static-mode [ports <vdsl_portlist> | bonding <bgroup_list> | all]
config rmt snmp-agent-state [ports <vdsl_portlist> | bonding <bgroup_list> | all] [enable | disable]
config rmt snmp-community [ports <vdsl_portlist> | bonding <bgroup_list> | all] [[delete rule_id <int 1-9>] | [add | rule_id <int 1-9>] name <string 31> access [read-only | read-write]]
config rmt snmp-trap [ports <vdsl_portlist> | bonding <bgroup_list> | all] [[delete host_id <int 1-9>] | [add | host_id <int 1-9>] ip_addr <ipaddr> community_name <string 32> snmp_version [snmp_v1 | snmp_v2c] | [status [enable | disable]]]
show rmt snmp-agent-state [ports <vdsl_portlist> | bonding <bgroup_list> | all]
show rmt snmp-community [ports <vdsl_portlist> | bonding <bgroup_list> | all]
show rmt snmp-info [ports <vdsl_portlist> | bonding <bgroup_list> | all]
show rmt snmp-trap [ports <vdsl_portlist> | bonding <bgroup_list> | all]
config rmt ssid [ports <vdsl_portlist> | bonding <bgroup_list> | all] [[add SSID <int 1-4> state [enable | disable] message <string 32>] | [delete SSID <int 1-4>]]
show rmt ssid [ports <vdsl_portlist> | bonding <bgroup_list> | all]
config rmt static-route [ports <vdsl_portlist> | bonding <bgroup_list> | all] [add | rule_id <int 1-20>] Destination_IP <network_address> gateway_addr <ipaddr> status [enable | disable]
show rmt static-route [ports <vdsl_portlist> | bonding <bgroup_list> | all]
config rmt system-pwd [ports <vdsl_portlist> | bonding <bgroup_list> | all] <string 32>
show rmt system-pwd [ports <vdsl_portlist> | bonding <bgroup_list> | all]
config rmt vlan-type [ports <vdsl_portlist> | bonding <bgroup_list> | all] [none | lan-group | protovlan]
show rmt vlan-type [ports <vdsl_portlist> | bonding <bgroup_list> | all]
config rmt wireless [ports <vdsl_portlist> | bonding <bgroup_list> | all] state [enable | disable]
show rmt wireless [ports <vdsl_portlist> | bonding <bgroup_list> | all]
show rmt counters [ports <vdsl_portlist> | bonding <bgroup_list> | all] [LAN | WAN | WIRELESS]
show rmt rate [ports <vdsl_portlist> | bonding <bgroup_list> | all] [LAN | WAN | WIRELESS]
show rmt version [ports <vdsl_portlist> | bonding <bgroup_list> | all]
show rmt model-id [ports <vdsl_portlist> | bonding <bgroup_list> | all]
show rmt cpe-mac [ports <vdsl_portlist> | bonding <bgroup_list> | all]
show rmt cpe-fdb [ports <vdsl_portlist> | bonding <bgroup_list> | all]

51-1 config rmt LAN_IP

Description

This command is used to configure the IP settings of the LAN interface for the remote CPE device. These settings may be referred to as private settings.

Format

config rmt LAN_IP [ports <vdsl_portlist> | bonding <bgroup_list> | all] lan_id <int 1-4> [enable | disable] IP <string 32> mask <string 32>

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL portlist here. The range of VDSL lines is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to use all VDSL lines or bonding groups.
lan_id - Specifies the LAN interface of the CPE. **<int 1-4>** - Enter the LAN interface's ID here. This value is from 1 to 4. **enable** - Specifies to enable the LAN interface of the CPE here. **disable** - Specifies to disable the LAN interface of the CPE here.
IP - Specifies the LAN interface's IP address. **<string 32>** - Enter the LAN interface's IP address here.
mask - Specifies the LAN interface's subnet mask. **<string 32>** - Enter the LAN interface's subnet mask here.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the IP settings of the LAN interface for the remote CPE device:

```
DAS-3626:admin#config rmt LAN_IP ports 2 lan_id 2 enable IP 192.168.1.15 mask
255.0.0.0
Command: config rmt LAN_IP ports 2 lan_id 2 enable IP 192.168.1.15 mask
255.0.0.0


Update configuration to CPE 2  ..... Success.
Success.


DAS-3626:admin#
```

51-2 show rmt LAN_IP

Description

This command is used to display the IP settings of the LAN interface on the remote CPE device.

Format

show rmt LAN_IP [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL lines' portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to display information related to all VDSL lines or bonding groups.

Restrictions

None.

Example

To display the IP settings of the LAN interface on the remote CPE device:

```
DAS-3626:admin# show rmt LAN_IP ports 2
Command: show rmt LAN_IP ports 2

Line2: LINE-2
Link State : SHOWTIME
   LAN 1 : Disable
   LAN 1 IP   : 192.168.1.1
   LAN 1 MASK : 255.255.255.0
   LAN 2 : Enable
   LAN 2 IP   : 192.168.1.15
   LAN 2 MASK : 255.0.0.0
   LAN 3 : Disable
   LAN 3 IP   : 192.168.3.1
   LAN 3 MASK : 255.255.255.0
   LAN 4 : Disable
   LAN 4 IP   : 192.168.4.1
   LAN 4 MASK : 255.255.255.0

DAS-3626:admin#
```

51-3 config rmt TR069

Description

This command is used to configure the TR-069 function on the remote CPE device.

Format

config rmt TR069 [ports <vdsl_portlist> | bonding <bgroup_list> | all] {cpe_id <string 32> | interface <int 1-8> | TR069_enable [disable | enable] | username <string 32> | password <string 32> | acs_url <string 128> | connection_acs_port <int 0-65535> | connection_request_username <string 32> | connection_request_password <string 32> | connection_request_relam <string 128> | inform [disable | Periodic] | periodic_interval <uint 0-4294967295>}

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to configure all VDSL lines or bonding groups.
cpe_id - (Optional) Specifies the CPE's name. **<string 32>** - Enter the CPE's name here. This name can be up to 32 characters long.
interface - (Optional) Specifies the transport interface used for all TR69 communications.

<int 1-8> - Enter the transport interface's ID here. This value is from 1 to 8.
TR069_enable - (Optional) Specifies the TR-069 remote management function's state. **disable** - Specifies to disable the TR-069 remote management function. **enable** - Specifies to enable the TR-069 remote management function.
username - (Optional) Specifies the username used by the TR-069 client for HTTP-based authentication with the ACS. **<string 32>** - Enter the username here. This name can be up to 32 characters long.
password - (Optional) Specifies the password used by the TR-069 client for HTTP-based authentication with the ACS. **<string 32>** - Enter the password here. This name can be up to 32 characters long.
acs_url - (Optional) Specifies the URL used by the TR-069 client to connect to the ACS. This URL must be in a valid HTTP or HTTPS format. **<string 128>** - Enter the ACS URL string here. This string can be up to 128 characters long.
connection_acs_port - (Optional) Specifies the port assigned for ACS initiated messaging. **<int 0-65535>** - Enter the connection ACS port number here. This value is from 0 to 65535.
connection_request_username - (Optional) Specifies the username used by the ACS for HTTP-based authentication with the TR-069 client. **<string 32>** - Enter the username here. This name can be up to 32 characters long.
connection_request_password - (Optional) Specifies the password used by the ACS for HTTP-based authentication with the TR-069 client. **<string 32>** - Enter the password here. This name can be up to 32 characters long.
connection_request_relam - (Optional) Specifies to override the TR69 ACS connect request in the authentication realm. **<string 128>** - Enter the connection request realm string here. This string can be up to 128 characters long.
inform - (Optional) Specifies to determine whether or not the TR-069 client will periodically send information. **disable** - Specifies to disable the sending of information. **Periodic** - Specifies to send information periodically.
periodic_interval - (Optional) Specifies the interval used to periodically send information to the ACS in an inform method call. **<uint 0-4294967295>** - Enter the periodic interval value here. This value is from 0 and 4294967295.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable the TR-069 function and set the ACS URL:

```
DAS-3626:admin# config rmt TR069 ports 2 TR069_enable enable
Command: config rmt TR069 ports 2 TR069_enable enable

Update configuration to CPE 2  ..... Success.
Success.

DAS-3626:admin# config rmt TR069 ports 2 acs_url http://alpha.ims1.com.tw/
core/Cosmos/ACSServer
Command: config rmt TR069 ports 2 acs_url http://
alpha.ims1.com.tw/core/Cosmos/ACSServer

Update configuration to CPE 2  ..... Success.
Success.

DAS-3626:admin#
```

51-4 show rmt TR069

Description

This command is used to display the current configuration of the TR-069 remote function.

Format

show rmt TR069 [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL lines' portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to display information related to all VDSL lines or bonding groups.

Restrictions

None.

Example

To display the current configuration of the TR-069 remote function:

```
DAS-3626:admin# show rmt TR069 ports 2
Command: show rmt TR069 ports 2

Line2: LINE-2
Link State : SHOWTIME
 CPE ID : WlaBm1OI8-HGWW-X0
 Interface  : 3
 TR069 : Enable
 Username  : acsadmin
 Password  : acsadmin
 ACS URL   : http://domain.com/core/Cosmos/ACSServer
 Connection Request Url : http://192.168.1.119:8888/random_path
 Connection ACS Port : 8888
 Connection Request Username : user1
 Connection Request Password  : pass1
 Connection Request Relam : domain.com
 Inform : Periodic
 Perioid Interval : 3600

DAS-3626:admin#
```

51-5 config rmt bridge

Description

This command is used to configure the remote CPE WAN bridge's filter DHCP request status.

Format

config rmt bridge [ports <vdsl_portlist> | bonding <bgroup_list> | all] connection <int 1-8> filter_DHCP_request [enable | disable]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to configure all VDSL lines or bonding groups.
connection - Specifies the connection ID. **<int 1-8>** - Enter the connection ID here. This value is from 1 to 8.
filter_DHCP_request - Specifies the WAN bridge's filter DHCP request status. **enable** - Specifies to enable the WAN bridge's filter DHCP request status. **disable** - Specifies to disable the WAN bridge's filter DHCP request status.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the remote CPE WAN bridge's filter DHCP request status:

```
DAS-3626:admin# config rmt bridge bonding 1 connection 1 filter_DHCP_request
enable
Command: config rmt bridge bonding 1 connection 1 filter_DHCP_request enable

Update configuration to CPE 1  ..... Success.
Success.

DAS-3626:admin#
```

51-6 show rmt bridge

Description

This command is used to display the WAN bridge's filter DHCP request status.

Format

show rmt bridge [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL lines' portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to display information related to all VDSL lines or bonding groups.

Restrictions

None.

Example

To display the WAN bridge's filter DHCP request status:

```
DAS-3626:admin#show rmt bridge ports 2
Command: show rmt bridge ports 2

Line2: LINE-2
Link State : SHOWTIME
  Bridge Connection 1 Filter DHCP Request : enabled

DAS-3626:admin#
```

51-7 config rmt cfm-config

Description

This command is used to configure the remote CPE's CFM.

Format

config rmt cfm-config [ports <vdsl_portlist> | bonding <bgroup_list> | all] [cfm_status [enable | disable] | md_name [<string 16> | clear] | md_level <int 0-7> | ma_name [<string 16> | clear] | mep_index <int 1-8191> | vlan_id <int 1-4094> | vlan_priority <int 0-7> | ccm_status [enable | disable] | ccm_interval [1s | 10s | 1min | 10min]]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to configure all VDSL lines or bonding groups.
cfm_status - Specifies the CFM feature's status on the remote CPE. **enable** - Specifies to enable the CFM feature's status on the remote CPE. **disable** - Specifies to disable the CFM feature's status on the remote CPE.
md_name - Specifies the maintenance domain name. **<string 16>** - Enter the maintenance domain name here. This string can be up to 16 characters long. **clear** - Specifies to clear the maintenance domain name.
md_level - Specifies the maintenance domain level. **<int 0-7>** - Enter the maintenance domain level here. This value is from 0 to 7.
ma_name - Specifies the maintenance association name. **<string 16>** - Enter the maintenance association name here. This string can be up to 16 characters long. **clear** - Specifies to clear the maintenance association name.
mep_index - Specifies to MEP's index value. **<int 1-8191>** - Enter to MEP's index value here. This value is from 1 to 8191.
vlan_id - Specifies the VLAN ID. **<int 1-4094>** - Enter the VLAN ID here. This value is from 1 to 4094.
vlan_priority - Specifies the VLAN priority value. **<int 0-7>** - Enter the VLAN priority value here. This value is from 0 to 7.
ccm_status - Specifies the CCM transmission's state. **enable** - Specifies to enable the CCM transmission's state. **disable** - Specifies to disable the CCM transmission's state.
ccm_interval - Specifies the CCM interval value. **1s** - Specifies that the CCM interval value is 1 second. **10s** - Specifies that the CCM interval value is 10 seconds. **1min** - Specifies that the CCM interval value is 1 minute. **10min** - Specifies that the CCM interval value is 10 minutes.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the remote CPE’s CFM MD name:

```
DAS-3626:admin#config rmt cfm-config bonding 1 md_name md5
Command: config rmt cfm-config bonding 1 md_name md5

Update configuration to CPE 1  ..... Success.
Success.

DAS-3626:admin#
```

To configure the remote CPE's CFM MD level:

```
DAS-3626:admin# config rmt cfm-config bonding 1 md_level 5
Command: config rmt cfm-config bonding 1 md_level 5

Update configuration to CPE 1  ..... Success.
Success.

DAS-3626:admin#
```

To configure the remote CPE's CFM MA name:

```
DAS-3626:admin# config rmt cfm-config bonding 1 ma_name ma5
Command: config rmt cfm-config bonding 1 ma_name ma5

Update configuration to CPE 1  ..... Success.
Success.

DAS-3626:admin#
```

To configure the remote CPE's CFM MEP index value:

```
DAS-3626:admin# config rmt cfm-config bonding 1 mep_index 1
Command: config rmt cfm-config bonding 1 mep_index 1

Update configuration to CPE 1  ..... Success.
Success.

DAS-3626:admin#
```

To configure the remote CPE's CFM VLAN ID:

```
DAS-3626:admin# config rmt cfm-config bonding 1 vlan_id 103
Command: config rmt cfm-config bonding 1 vlan_id 103

Update configuration to CPE 1  ..... Success.
Success.

DAS-3626:admin#
```

To configure the remote CPE's CFM VLAN priority value:

```
DAS-3626:admin# config rmt cfm-config bonding 1 vlan_priority 7
Command: config rmt cfm-config bonding 1 vlan_priority 7

Update configuration to CPE 1  ..... Success.
Success.

DAS-3626:admin#
```

To configure the remote CPE's CFM CCM status:

```
DAS-3626:admin# config rmt cfm-config bonding 1 ccm_status enable
Command: config rmt cfm-config bonding 1 ccm_status enable

Update configuration to CPE 1  ..... Success.
Success.

DAS-3626:admin#
```

To configure the remote CPE's CFM CCM interval value:

```
DAS-3626:admin# config rmt cfm-config bonding 1 ccm_interval 1s
Command: config rmt cfm-config bonding 1 ccm_interval 1s

Update configuration to CPE 1  ..... Success.
Success.

DAS-3626:admin#
```

To configure the remote CPE's CFM status:

```
DAS-3626:admin# config rmt cfm-config bonding 1 cfm_status enable
Command: config rmt cfm-config bonding 1 cfm_status enable

Update configuration to CPE 1  ..... Success.
Success.

DAS-3626:admin#
```

51-8 config rmt cfm-lbm

Description

This command is used to send loopback messages in the remote CPE to verify connectivity with another MEP or MIP for a specific MA/MEG.

Format

config rmt cfm-lbm [ports <vdsl_portlist> | bonding <bgroup_list> | all] [[des_mac <macaddr> | multicast_mac 01-80-c2-00-00-31] lbm_num <int 1-255> | clear-lbr]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to configure all VDSL lines or bonding groups.
des_mac - Specifies the destination MAC address of the loopback message. **<macaddr>** - Enter the destination MAC address of the loopback message here.
multicast_mac - Specifies the MD level 1 multicast address of the loopback message. **01-80-c2-00-00-31** - Specifies the MD level 1 multicast address of the loopback message.
lbm_num - Specifies the message number this needs to be send. **<int 1-255>** - Enter the message number this needs to be send here. This value is from 1 to 255.
clear-lbr - Specifies to clear the received loopback reply messages.

Restrictions

Only Administrators and Operators can issue this command.

Example

To send CFM MD level 1 loopback messages:

```
DAS-3626:admin#config rmt cfm-lbm ports 2 multicast_mac 01-80-c2-00-00-31
lbm_num 10
Command: config rmt cfm-lbm ports 2 multicast_mac 01-80-c2-00-00-31 lbm_num 10

Update configuration to CPE 2  ..... Success.
Success.

DAS-3626:admin#
```

51-9 config rmt cfm-ltm

Description

This command is used to send multicast link-trace messages in the remote CPE to identify adjacency relationships with remote MEPs and MIPs at the same administrative level.

Format

config rmt cfm-ltm [ports <vdsl_portlist> | bonding <bgroup_list> | all] [target_mac <macaddr> | mep_id <int 1-8191> | clear-ltr]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to configure all VDSL lines or bonding groups.
target_mac - Specifies the unicast MAC address of the target MEP. **<macaddr>** - Enter the unicast MAC address of the target MEP here.
mep_id - Specifies the MEP ID of the target MEP.

<int 1-8191> - Enter the MEP ID of the target MEP here. This value is from 1 to 8191.
clear-ltr - Specifies to clear received link-trace reply messages.

Restrictions

Only Administrators and Operators can issue this command.

Example

To send CFM link-trace messages:

```
DAS-3626:admin#config rmt cfm-ltm ports 2 target_mac 00-0E-04-B7-2D-79
Command: config rmt cfm-ltm ports 2 target_mac 00-0E-04-B7-2D-79

Update configuration to CPE 2  ..... Success.
Success.

DAS-3626:admin#
```

51-10 show rmt cfm-lbm

Description

This command is used to display the testing result of the CFM loopback test in the remote CPE device.

Format

show rmt cfm-lbm [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL lines' portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to display information related to all VDSL lines or bonding groups.

Restrictions

None.

Example

To display the testing result of the CFM loopback test in the remote CPE device:

```
DAS-3626:admin#show rmt cfm-lbm ports 2
Command: show rmt cfm-lbm ports 2

Line2: LINE-2
Link State : SHOWTIME

Send LBM
=====================================
Destination MAC Address :       01-80-c2-00-00-31
Number of LBM :                 10

LBM Status
=====================================
LBM Transmit Finished :         LBM is still Transmiting
LBM Transmit Result :           Success
LBM Transmit TransId :          0
LBM Transmit Next Lbm TransId : 1
Total number of valid LBR In :  0

DAS-3626:admin#
```

51-11 show rmt cfm-ltm

Description

This command is used to display the result of the CFM link-trace test.

Format

show rmt cfm-ltm [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL lines' portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to display information related to all VDSL lines or bonding groups.

Restrictions

None.

Example

To display the result of the CFM link-trace test:

```
DAS-3626:admin#show rmt cfm-ltm ports 2
Command: show rmt cfm-ltm ports 2

Line2: LINE-2
Link State : SHOWTIME

Send LTM
=====================================
Target MAC Address :       00-0e-04-b7-2d-79
Target MEP ID :

LTM Status
=====================================
LTM sequence number :      1
LTM next sequence number : 2
Unexpect LTR :             0
Flag :                     None
Target :                   00:0e:04:b7:2d:79
TTL :                      64
Result :                   Success

DAS-3626:admin#
```

51-12 show rmt cfm-config

Description

This command is used to display the remote CPE's CFM configuration.

Format

show rmt cfm-config [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL lines' portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to display information related to all VDSL lines or bonding groups.

Restrictions

None.

Example

To display the remote CPE's CFM configuration:

```
DAS-3626:admin#show rmt cfm-config bonding 2
Command: show rmt cfm-config bonding 2

bonding2
Link State : Up
CFM :
==============================
CFM Status    : disable
CCM Status    : disable

CCM Status :
==============================
CCM Transmit        :
CCM Sequence Errors : 0
CCM Defect Prioity  :
CCM Defect          :
CCM sequence number : 0

DAS-3626:admin#
```

51-13 show rmt cfm-database

Description

This command is used to display the remote CPE's CFM database.

Format

show rmt cfm-database [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL lines' portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to display information related to all VDSL lines or bonding groups.

Restrictions

None.

Example

To display the remote CPE's CFM database:

```
DAS-3626:admin#show rmt cfm-database bonding 1
Command: show rmt cfm-database bonding 1

bonding1
Link State : Up

Remote MEP
====================================
MD Name :
MA Name :
Remote Mep ID :
VID :
Source MAC Address :
====================================

LBR Record Table
====================================
 Tran.ID | Source MAC Address
====================================

LTR Record Table
================================================================================
 Seq.ID | Hop | TTL |     Terminal      | Forward | Relay  | TLVs content
        |     |     |                   |         | Action |
================================================================================

DAS-3626:admin#
```

51-14 show rmt antenna_count

Description

This command is used to display the antenna count of the remote CPE device.

Format

show rmt antenna_count [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL lines' portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to display information related to all VDSL lines or bonding groups.

Restrictions

None.

Example

To display the antenna count of the remote CPE device:

```
DAS-3626:admin#show rmt antenna_count bonding 2
Command: show rmt antenna_count bonding 2

bonding2
Link State : Up
 Antenna Count :      2

DAS-3626:admin#
```

51-15 config rmt dhcp-pool

Description

This command is used to configure the DHCP pool on the remote CPE device.

Format

config rmt dhcp-pool [ports <vdsl_portlist> | bonding <bgroup_list> | all] pool_id <int 1-4> {dhcp_mode [sever | relay] | dhcp_server [enable | disable] | dhcp_pool_start <ipaddr> | dhcp_pool_end <ipaddr> | dhcp_pool_lease_time [1_hour | 2_hours | 3_hours | 1_day | 2_days | 3_days | 1_week]}

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to configure all VDSL lines or bonding groups.
pool_id - Specifies the DHCP pool ID. **<int 1-4>** - Enter the DHCP pool ID here. The value is from 1 to 4.
dhcp_mode - (Optional) Specifies the DHCP pool mode. **server** - Specifies that the DHCP pool mode is server. **relay** - Specifies that the DHCP pool mode is relay.
dhcp_server - (Optional) Specifies the DHCP pool server's status. **enable** - Specifies to enable the DHCP pool server's status. **disable** - Specifies to disable the DHCP pool server's status.
dhcp_pool_start - (Optional) Specifies the starting IP address in the pool hosted by the DHCP server. **<ipaddr>** - Enter the starting IP address in the pool hosted by the DHCP server
dhcp_pool_end - (Optional) Specifies the ending IP address in the pool hosted by the DHCP server. **<ipaddr>** - Enter the ending IP address in the pool hosted by the DHCP server.
dhcp_pool_lease_time - (Optional) Specifies the DHCP server's lease time. **1_hour** - Specifies that the DHCP server's lease time will be 1 hour. **2_hours** - Specifies that the DHCP server's lease time will be 2 hours. **3_hours** - Specifies that the DHCP server's lease time will be 3 hours. **1_day** - Specifies that the DHCP server's lease time will be 1 day. **2_days** - Specifies that the DHCP server's lease time will be 2 days. **3_days** - Specifies that the DHCP server's lease time will be 3 days. **1_week** - Specifies that the DHCP server's lease time will be 1 week.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the DHCP pool on the remote CPE device.

```
DAS-3626:admin# config rmt dhcp-pool ports 24 pool_id 1 dhcp_mode sever
dhcp_pool_start 192.168.1.1 dhcp_pool_end 192.168.1.100 dhcp_pool_lease_time
2_hours dhcp_server enable
Command: config rmt dhcp-pool ports 24 pool_id 1 dhcp_mode sever
dhcp_pool_start 192.168.1.1 dhcp_pool_end 192.168.1.100 dhcp_pool_lease_time
2_hours dhcp_server enable

Update configuration to CPE 24 ..... Success.
Success.

DAS-3626:admin#
```

51-16 config rmt dhcp-pool-option

Description

This command is used to configure DHCP pool on the remote CPE device.

Format

config rmt dhcp-pool-option [ports <vdsl_portlist> | bonding <bgroup_list> | all] [add | rule_id <int 1-8>] [60 option_value <string 20> | 61 iaid <string 11> [mac <macaddr> | enterprise_num <string 32>] | 125 enterprise_num <hex 0x0-0xffff> manufacture_oui <string 32> serial_number <string 32> product_class <string 32> gateway_oui <string 32> | SSID [index <int 1-4> | VLAN vid <int 1-4094>] start_ip <ipaddr> end_ip <ipaddr> lease_time <sec 0-9999999> gateway_ip <ipaddr> subnet <ipaddr> [enable | disable]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to configure all VDSL lines or bonding groups.
add - Specifies to add a new DCHP option.
rule_id - Specifies the DHCP option's rule ID. **<int 1-8**> - Enter the DHCP option's rule ID here. This value is from 1 to 8.
60 - Specifies to use DHCP Option 60. **option_value** - Specifies the DHCP Option 60's option value. **<string 20>** - Enter the DHCP Option 60's option value here. This string can be up to 20 characters long.
61 - Specifies to use DHCP Option 61. **iaid** - Specifies the Identity Association Identifier used in Option 61. **<string 11>** - Enter the IAID string here. This string can be up to 11 characters long. **mac** - Specifies the MAC address used in Option 61. **<macaddr>** - Enter the MAC address used in Option 61 here. **enterprise_num** - Specifies the enterprise number used in Option 61. **<string 32>** - Enter the enterprise number used in Option 61 here. This string can be up to

32 characters long.
125 - Specifies to use DHCP Option 125. **enterprise_num** - Specifies the enterprise number used in Option 125. **<hex 0x0-0xffff>** - Enter the enterprise number used in Option 125. **manufacture_oui** - Specifies the Organizationally Unique Identifier (OUI) of the device manufacturer as provided to the gateway by the device. **<string 32>** - Enter the OUI string here. This string can be up to 32 characters long. **serial_number** - Specifies the serial number of the device as provided to the gateway by the device. **<string 32>** - Enter the serial number here. This string can be up to 32 characters long. **product_class** - Specifies the identifier of the class of the product for which the device's serial number applies to as provided to the gateway by the device. **<string 32>** - Enter the product class string here. This string can be up to 32 characters long. **gateway_oui** - Specifies the gateway OUI used in Option 125. **<string 32>** - Enter the gateway OUI used in Option 125 here.
SSID - Specifies the option type's SSID. **index** - Specifies the option type's SSID index. **<int 1-4>** - Enter the option type's SSID index value here. This value is from 1 to 4.
VLAN - Specifies the option type's VLAN. **vid** - Specifies the option type's VLAN ID. **<int 1-4094>** - Enter the option type's VLAN ID here. This value is from 1 to 4094.
start_ip - Specifies the starting IP address in the DHCP pool range. **<ipaddr>** - Enter the starting IP address in the DHCP pool range here.
end_ip - Specifies the ending IP address in the DHCP pool range. **<ipaddr>** - Enter the ending IP address in the DHCP pool range here.
lease_time - Specifies the DHCP lease time. **<sec 0-9999999>** - Enter the DHCp lease time value here. This value is from 0 to 9999999 seconds.
gateway_ip - Specifies the gateway's IP address. **<ipaddr>** - Enter the gateway's IP address here.
subnet - Specifies the subnet mask. **<ipaddr>** - Enter the subnet mask here.
enable - Specifies to enable this rule after configuration. **disable** - Specifies to disable this rule after configuration.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure DHCP pool on the remote CPE device:

```
DAS-3626:admin#config rmt dhcp-pool-option ports 24 rule_id 1 60 option_value
CHT start_ip 192.168.1.0 end_ip 192.168.1.99 lease_time 10000 gateway_ip
192.168.1.101 subnet 255.255.255.0 enable
Command: config rmt dhcp-pool-option ports 24 rule_id 1 60 option_value CHT
start_ip 192.168.1.0 end_ip 192.168.1.99 lease_time 10000 gateway_ip
192.168.1.101 subnet 255.255.255.0 enable

Update configuration to CPE 24 ..... Success.
Success.

DAS-3626:admin#
```

51-17 config rmt dhcp-pool-option-status

Description

This command is used to configure the DHCP pool's option status on remote CPE devices.

Format

config rmt dhcp-pool-option-status [<vdsl_portlist> | all] [near_end | far_end] [enable | disable]

Parameters

<vdsl_portlist> - Enter the VDSL portlist here. This value is from 1 to 24.
all - Specifies to configure all VDSL lines.
near_end - Specifies to configure the near end. **far_end** - Specifies to configure the far end.
enable - Specifies to enable this feature. **disable** - Specifies to disable this feature.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the DHCP pool's option status on remote CPE devices:

```
DAS-3626:admin#config rmt dhcp-pool-option-status ports 24 enable
Command: config rmt dhcp-pool-option-status ports 24 enable

Update configuration to CPE 24 ..... Success.
Success.

DAS-3626:admin#
```

51-18 show rmt dhcp-pool

Description

This command is used to display all information of DHCP server pools.

Format

show rmt dhcp-pool [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL lines' portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to display information related to all VDSL lines or bonding groups.

Restrictions

None.

Example

To display all information of DHCP server pools:

```
DAS-3626:admin#show rmt dhcp-pool ports 24
Command: show rmt dhcp-pool ports 24

Line24: LINE-24
Link State : SHOWTIME

 Pool ID |  Mode  | DHCP Server |   Pool Start   |    Pool end    | Lease Time
---------------------------------------------------------------------------------
       1 | Server |      Enable |  192.168.1.101 |  192.168.1.199 | 1 Day
---------------------------------------------------------------------------------

DAS-3626:admin#
```

51-19 show rmt dhcp-pool-option

Description

This command is used to display option field information of the DHCP packet.

Format

show rmt dhcp-pool-option [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL lines' portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to display information related to all VDSL lines or bonding groups.

Restrictions

None.

Example

To display option field information of the DHCP packet:

```
DAS-3626:admin#show rmt dhcp-pool-option ports 24
Command: show rmt dhcp-pool-option ports 24

Line24: LINE-24
Link State : SHOWTIME
 DHCP Pool by Option Status : Enable

 Entry ID           : 1
 Option Type        : 60
 Option Value       : CHT
 Start IP           : 192.168.1.0
 End IP             : 192.168.1.99
 Lease Time         : 10000
 Gateway IP         : 192.168.1.101
 Subnet             : 255.255.255.0
 Enable             : Yes

DAS-3626:admin#
```

51-20 config rmt connection

Description

This command is used to configure the CPE's WAN connection mode either in the bridge or router mode.

Format

config rmt connection [ports <vdsl_portlist> | bonding <bgroup_list> | all] id <int 1-8> mode [[bridge | pppoe | static | dynamic] {vlan [enable | disable] | vid <int 1-4094> | pid <int 0-7>} | disable]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to configure all VDSL lines or bonding groups.
id - Specifies the connection ID of the WAN port. **<int 1-8>** - Enter the connection ID of the WAN port here. This value is from 1 to 8.
mode - Specifies the WAN connection mode of the CPE device. **bridge** - Specifies that the WAN connection mode of the CPE device is bridge. **pppoe** - Specifies that the WAN connection mode of the CPE device is PPPoE. **static** - Specifies that the WAN connection mode of the CPE device is Static. **dynamic** - Specifies that the WAN connection mode of the CPE device is Dynamic.
vlan - (Optional) Specifies the VLAN feature's state on the WAN port. **enable** - Specifies to enable the VLAN feature's state on the WAN port. **disable** - Specifies to disable the VLAN feature's state on the WAN port.
vid - (Optional) Specifies the VLAN's ID on the WAN port. **<int 1-4094>** - Enter the VLAN's ID here. This value is from 1 to 4094.
pid - (Optional) Specifies the 802.1p priority of the WAN port. **<int 0-7>** - Enter the 802.1p priority value of the WAN port here. This value is from 0 to 7.
disable - Specifies to disable this feature.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the CPE's WAN connection mode:

```
DAS-3626:admin#config rmt connection ports 2 id 1 mode bridge vlan disable vid
1 pid 0
Command: config rmt connection ports 2 id 1 mode bridge vlan disable vid 1 pid
0

Update configuration to CPE 2  ..... Success.
Success.

DAS-3626:admin#
```

51-21 show rmt connection_id

Description

This command is used to display the connection mode of the remote CPE device.

Format

show rmt connection_id <int 1-8> [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

<int 1-8> - Enter the connection ID here. This value is from 1 to 8.
ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL lines' portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to display information related to all VDSL lines or bonding groups.

Restrictions

None.

Example

To display the connection mode of the remote CPE device.

```
DAS-3626:admin#show rmt connection_id 1 ports 2
Command: show rmt connection_id 1 ports 2

Line2: LINE-2
Link State : SHOWTIME
Connection : 1
Mode       : Bridge
VLAN       : Disable
VID        : 11
Priority   : 0

DAS-3626:admin#
```

51-22 config rmt dynamic-mode

Description

This command is used to configure the remote CPE dynamic mode settings.

Format

config rmt dynamic-mode [ports <vdsl_portlist> | bonding <bgroup_list> | all] {host_name <string 32> | mtu <int 1000-1500> | default-route [enable | disable] | nat [enable | disable] | pppoe-passthrough [enable | disable] | dhcp_option60 [enable vendor-id <string 32> | disable] | dhcp_option61 [enable duid [address_plus_time | vendor_id {ent_num} <uint 0-4294967295> | identifier} <string 64>} | address] {iaid <string 32>} | disable] | dhcp_option125 [enable {man_oui <string 64> | pro_class <string 64> | mod_name <string 64> | ser_num <string 64>} | disable]}

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to configure all VDSL lines or bonding groups.
host_name - (Optional) Specifies the hostname. **<string 32>** - Enter the hostname here. This string can be up to 32 characters long.
mtu - (Optional) Specifies the MTU size. **<int 1000-1500>** - Enter the MTU size here. This value is from 1000 to 1500.
default-route - (Optional) Specifies the default route's state. **enable** - Specifies to enable the default route. **disable** - Specifies to disable the default route.
nat - (Optional) Specifies the NAT's state. **enable** - Specifies to enable NAT. **disable** - Specifies to disable NAT.
pppoe-passthrough - (Optional) Specifies the PPPoE pass-through feature's state. **enable** - Specifies to enable PPPoE pass-through. **disable** - Specifies to disable PPPoE pass-through.
dhcp_option60 - (Optional) Specifies to configure DHCP Option 60. **enable** - Specifies to enable DHCP Option 60. **vendor-id** - Specifies the vendor ID. **<string 32>** - Enter the vendor ID here. This string can be up to 32 characters long. **disable** - Specifies to disable DHCP Option 60.

dhcp_option61 - (Optional) Specifies to configure DHCP Option 61. **enable** - Specifies to enable DHCP Option 61. **duid** - Specifies the DUID. **address_plus_time** - Specifies the address plus time. **vendor_id** - Specifies the vendor ID. **ent_num** - Specifies the enterprise number. **<uint 0-4294967295>** - Enter the enterprise number here. This value is from 0 to 4294967295. **identifier** - Specifies the identifier. **<string 64>** - Enter the identifier here. This string can be up to 64 characters long. **address** - Specifies the address. **iaid** - Specifies the IAID. **<string 32>** - Enter the IAID here. This string can be up to 32 characters long. **disable** - Specifies to disable DHCP Option 61.
dhcp_option125 - (Optional) Specifies to configure DHCP Option 125. **enable** - Specifies to enable DHCP Option 125. **man_oui** - Specifies to configure the MAN OUI. **<string 64>** - Enter the MAN OUI here. This string can be up to 64 characters long. **pro_class** - Specifies the pro class. **<string 64>** - Enter the pro class here. This string can be up to 64 characters long. **mod_name** - Specifies the MOD name. **<string 64>** - Enter the MOD name here. This string can be up to 64 characters long. **ser_num** - Specifies the serial number. **<string 64>** - Enter the serial number here. This string can be up to 64 characters long. **disable** - Specifies to disable DHCP Option 125.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the remote CPE dynamic mode settings:

```
DAS-3626:admin#config rmt dynamic-mode bonding 1 pppoe-passthrough enable
Command: config rmt dynamic-mode bonding 1 pppoe-passthrough enable

Update configuration to CPE 1  ..... Success.
Success.

DAS-3626:admin#
```

51-23 show rmt dynamic-mode

Description

This command is used to display the remote CPE's dynamic mode settings.

Format

show rmt dynamic-mode [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

ports - Specifies the VDSL lines.

<vdsl_portlist> - Enter the VDSL lines' portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups.
<bgroup_list> - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to display information related to all VDSL lines or bonding groups.

Restrictions

None.

Example

To display the remote CPE's dynamic mode settings:

```
DAS-3626:admin#show rmt dynamic-mode bonding 1
Command: show rmt dynamic-mode bonding 1

bonding1
Link State : Up
Dynamic IP Address
====================================
Host name           :
MTU                 : 0
Default route       : Disable
NAT                 : Enable
PPPoE passthrough   : Disable

DHCP Option
====================================
DHCP Option 60      : Disable
  -Vendor ID        :
DHCP Option 61      : Disable
  -DUID             :
   Enterprise Number:
   Identifier       :
  -IAID             :
DHCP Option 125     : Disable
   Manufacturer OUI :
   Product Class    :
   Model Name       :
   serial Number    :
====================================
 IP Address         :
 Subnet Mask        :
 Gateway            :

DAS-3626:admin#
```

51-24 config rmt eth-mode

Description

This command is used to configure the current CPE's LAN port configuration. The remote device's ports should be in the showtime state for successful configuration.

Format

config rmt eth-mode [ports <vdsl_portlist> | bonding <bgroup_list> | all] [port [LAN_1 | LAN_2 | LAN_3 | LAN_4] speed-duplex [auto | 10H | 10F | 100H | 100F] | admin [enable | disable]]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to configure all VDSL lines or bonding groups.
port - Specifies the LAN port on the remote CPE device. **LAN_1** - Specifies to use LAN port 1. **LAN_2** - Specifies to use LAN port 2. **LAN_3** - Specifies to use LAN port 3. **LAN_4** - Specifies to use LAN port 4.
speed-duplex - Specifies to configure the speed and mode. **auto** - Specifies that the remote CPE's LAN port speed must be auto-negotiation. **10H** - Specifies that the remote CPE's LAN port speed is 10 Mbps in the half-duplex mode. **10F** - Specifies that the remote CPE's LAN port speed is 10 Mbps in the full-duplex mode. **100H** - Specifies that the remote CPE's LAN port speed is 100 Mbps in the half-duplex mode. **100F** - Specifies that the remote CPE's LAN port speed is 100 Mbps in the full-duplex mode.
admin - Specifies to configure LAN port's administrative state. **enable** - Specifies to enable LAN port. **disable** - Specifies to disable LAN port.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the current CPE’s LAN port configuration:

```
DAS-3626:admin#config rmt eth-mode bonding 1 port LAN_1 speed-duplex auto
Command: config rmt eth-mode bonding 1 port LAN_1 speed-duplex auto

Update configuration to CPE 1  ..... Success.
Success.

DAS-3626:admin#
```

51-25 show rmt eth-mode

Description

This command is used to display the remote CPE’s LAN port settings.

Format

show rmt eth-mode [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL lines' portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to display information related to all VDSL lines or bonding groups.

Restrictions

None.

Example

To display the remote CPE's LAN port settings:

```
DAS-3626:admin#show rmt eth-mode bonding 1
Command: show rmt eth-mode bonding 1

bonding1
Link State : Up
LAN Port 1 Status :
    -LAN Port 1 Link Speed  : none
    -LAN Port 1 Link State  : link down
    -LAN Port 1 admin State  : enabled
    -LAN Port 1 Link Duplex : none
    -LAN Port 1 Auto Negotiation : enabled
    -LAN Port 1 Uptime : 0 days 0 hours 0 minutes 0 seconds
LAN Port 2 Status :
    -LAN Port 2 Link Speed  : none
    -LAN Port 2 Link State  : link down
    -LAN Port 2 admin State  : enabled
    -LAN Port 2 Link Duplex : none
    -LAN Port 2 Auto Negotiation : enabled
    -LAN Port 2 Uptime : 0 days 0 hours 0 minutes 0 seconds
LAN Port 3 Status :
    -LAN Port 3 Link Speed  : none
    -LAN Port 3 Link State  : link down
    -LAN Port 3 admin State  : enabled
    -LAN Port 3 Link Duplex : none
    -LAN Port 3 Auto Negotiation : enabled
    -LAN Port 3 Uptime : 0 days 0 hours 0 minutes 0 seconds
LAN Port 4 Status :
    -LAN Port 4 Link Speed  : none
    -LAN Port 4 Link State  : link down
    -LAN Port 4 admin State  : enabled
    -LAN Port 4 Link Duplex : none
    -LAN Port 4 Auto Negotiation : enabled
    -LAN Port 4 Uptime : 0 days 0 hours 0 minutes 0 seconds

DAS-3626:admin#
```

51-26 config rmt filter

Description

This command is used to configure the remote CPE's filter settings. Filters manage the LAN users' access to the Internet. It is possible to permit or restrict access to the Internet for specific IP addresses within the LAN. Filters can also be defined to control access to ports.

Format

config rmt filter [ports <vdsl_portlist> | bonding <bgroup_list> | all] [[delete rule_id <int 1-10>] | [[add | rule_id <int 1-10>] {rule_state [inactive | active] | rule_action [allow | deny] | outgoing_if [1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | lan | all] | protocol [any | tcp | udp | icmp] | src_ip [any_ip | single_ip <ipaddr> | ip_range <ipaddr> <ipaddr> | netmask <network_address>] | src_mac <macaddr> | des_ip [any_ip | single_ip <ipaddr> | ip_range <ipaddr> <ipaddr> | netmask <network_address>] | src_port [any_port | single_port <value 0-65535> | port_range <value 0-65535> <value 0-65535>] | des_port [any_port | single_port <value 0-65535> | port_range <value 0-65535> <value 0-65535>]}]]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to configure all VDSL lines or bonding groups.
delete - Specifies that a rule will be deleted. **rule_id** - Specifies the rule ID that will be deleted. **<int 1-10>** - Enter the rule ID that will be deleted here. This value is from 1 to 10.
add - Specifies that a rule will be added. **rule_id** - Specifies the rule ID that will be added. **<int 1-10>** - Enter the rule ID that will be added here. This value is from 1 to 10.
rule_state - (Optional) Specifies the rule's state. **inactive** - Specifies that the rule will be inactive after being created. **active** - Specifies that the rule will be active after being created.
rule_action - (Optional) Specifies the rule's action. **allow** - Specifies to apply the allow action to this rule. **deny** - Specifies to apply the deny action to this rule.
outgoing_if - (Optional) Specifies the outgoing interface that will be used in this rule. **1** - Specifies that the outgoing interface will be WAN interface 1. **2** - Specifies that the outgoing interface will be WAN interface 2. **3** - Specifies that the outgoing interface will be WAN interface 3. **4** - Specifies that the outgoing interface will be WAN interface 4. **5** - Specifies that the outgoing interface will be WAN interface 5. **6** - Specifies that the outgoing interface will be WAN interface 6. **7** - Specifies that the outgoing interface will be WAN interface 7. **8** - Specifies that the outgoing interface will be WAN interface 8. **lan** - Specifies that the outgoing interface will be the LAN interface. **all** - Specifies that all interfaces will be used in this rule.
protocol - (Optional) Specifies the protocol used in this rule. **any** - Specifies to use all available protocols in this rule. **tcp** - Specifies to use the TCP protocol in this rule. **udp** - Specifies to use the UDP protocol in this rule. **icmp** - Specifies to use the ICMP protocol in this rule.
src_ip - (Optional) Specifies the source IP address or address range that will be used in this rule. **any_ip** - Specifies to use any source IP address in this rule. **single_ip** - Specifies to use a single IP address in this rule.

<ipaddr> - Enter the single source IP address that will be used in this rule here. **ip_range** - Specifies to use a range of source IP addresses in this rule. **<ipaddr>** - Enter the starting source IP address in the range here. **<ipaddr>** - Enter the ending source IP address in the range here. **netmask** - Specifies the source netmask of the IP addresses used in this rule. **<network_address>** - Enter the source netmask here.
src_mac - (Optional) Specifies the source MAC address used in this rule. **<macaddr>** - Enter the source MAC address used in this rule here.
des_ip - (Optional) Specifies the destination IP address or address range that will be used in this rule. **any_ip** - Specifies to use any destination IP address in this rule. **single_ip** - Specifies to use a destination IP address in this rule. **<ipaddr>** - Enter the single destination IP address that will be used in this rule here. **ip_range** - Specifies to use a range of destination IP addresses in this rule. **<ipaddr>** - Enter the starting destination IP address in the range here. **<ipaddr>** - Enter the ending destination IP address in the range here. **netmask** - Specifies the destination netmask of the IP addresses used in this rule. **<network_address>** - Enter the destination netmask here.
src_port - (Optional) Specifies the source port number used in this rule. **any_port** - Specifies that any source port number is used in this rule. **single_port** - Specifies that a single source port number will be used in this rule. **<value 0-65535>** - Enter the single source port number here. **port_range** - Specifies that a range of source port numbers will be used in this rule. **<value 0-65535>** - Enter the starting source port number for this rule here. **<value 0-65535>** - Enter the ending source port number for this rule here.
des_port - (Optional) Specifies the destination port number used in this rule. **any_port** - Specifies that any destination port number is used in this rule. **single_port** - Specifies that a single destination port number will be used in this rule. **<value 0-65535>** - Enter the single destination port number here. **port_range** - Specifies that a range of destination port numbers will be used in this rule. **<value 0-65535>** - Enter the starting destination port number for this rule here. **<value 0-65535>** - Enter the ending destination port number for this rule here.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the remote CPE's filter settings:

```
DAS-3626:admin#config rmt filter ports 1 add rule_state active rule_action
allow outgoing_if 1
Command: config rmt filter ports 1 add rule_state active rule_action allow
outgoing_if 1


Update configuration to CPE 1  ..... Success.
Success.


DAS-3626:admin#
```

51-27 show rmt filter

Description

This command is used to display the filter configuration.

Format

show rmt filter [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL lines' portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to display information related to all VDSL lines or bonding groups.

Restrictions

None.

Example

To display the filter configuration:

```
DAS-3626:admin#
DAS-3626:admin#show rmt filter ports 1
Command: show rmt filter ports 1

Line1: LINE-1
Link State : SHOWTIME
FILTER :
=====================================
Rule ID :               1
Rule State :            Inactive
Rule Action :           Deny

Outgoing Interface :    2
Source IP Type :        Any
Source MAC :            00-00-00-00-00-00

Destination IP Type :   Any

Protocol :              TCP
Source Port Type :      Any

Destination Port Type : Range
Destination Port :      20 ~ 21

FILTER :
=====================================
Rule ID :               2
Rule State :            Inactive
Rule Action :           Deny

Outgoing Interface :    2
Source IP Type :        Any
Source MAC :            00-00-00-00-00-00

Destination IP Type :   Any

Protocol :              TCP
Source Port Type :      Any

Destination Port Type : Single
Destination Port :      80

FILTER :
=====================================
Rule ID :               3
                              <Output Truncated>
```

51-28 config rmt igmp-proxy

Description

This command is used to configure the IGMP proxy settings on the remote CPE device.

Format

config rmt igmp-proxy [ports <vdsl_portlist> | bonding <bgroup_list> | all] [enable | disable] interface <int 1-8>

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to configure all VDSL lines or bonding groups.
enable - Specifies to enable the IGMP proxy feature on the remote CPE device's WAN interface. **disable** - Specifies to disable the IGMP proxy feature on the remote CPE device's WAN interface.
interface - Specifies the WAN interface. **<int 1-8>** - Enter the WAN interface's ID here. This value is from 1 to 8.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the IGMP proxy settings on the remote CPE device:

```
DAS-3626:admin#config rmt igmp-proxy ports 1 disable interface 1
Command: config rmt igmp-proxy ports 1 disable interface 1

Update configuration to CPE 1  ..... Success.
Success.

DAS-3626:admin#
```

51-29 config rmt igmp-status

Description

This command is used to configure the IGMP status on the remote CPE device.

Format

config rmt igmp-status [ports <vdsl_portlist> | bonding <bgroup_list> | all] [enable | disable]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to configure all VDSL lines or bonding groups.
enable - Specifies to enable the IGMP feature on the remote CPE device. **disable** - Specifies to disable the IGMP feature on the remote CPE device.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the IGMP status on the remote CPE device:

```
DAS-3626:admin#config rmt igmp-status ports 1 enable
Command: config rmt igmp-status ports 1 enable

Update configuration to CPE 1  ..... Success.

DAS-3626:admin#
```

51-30 config rmt igmpsnooping

Description

This command is used to configure the IGMP snooping feature on the remote CPE device.

Format

config rmt igmpsnooping [ports <vdsl_portlist> | bonding <bgroup_list> | all] [enable | disable] [group1 | group2 | group3 | group4] [Standard | Blocking]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to configure all VDSL lines or bonding groups.
enable - Specifies to enable the IGMP snooping feature. **disable** - Specifies to disable the IGMP snooping feature.
group1 - Specifies LAN group 1. **group2** - Specifies LAN group 2. **group3** - Specifies LAN group 3. **group4** - Specifies LAN group 4.
Standard - Specifies to forward unknown multicast packets to the group. **Blocking** - Specifies to filter unknown multicast packets without sending to the group.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the IGMP snooping feature on the remote CPE device:

```
DAS-3626:admin#config rmt igmpsnooping ports 1 enable group1 Blocking
Command: config rmt igmpsnooping ports 1 enable group1 Blocking

Update configuration to CPE 1  ..... Success.
Success.

DAS-3626:admin#
```

51-31 show rmt igmp-status

Description

This command is used to display the IGMP feature's status on remote CPE devices.

Format

show rmt igmp-status [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL lines' portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to display information related to all VDSL lines or bonding groups.

Restrictions

None.

Example

To display the IGMP feature's status on remote CPE devices:

```
DAS-3626:admin#show rmt igmp-status ports 1
Command: show rmt igmp-status ports 1

Line1: LINE-1
Link State : SHOWTIME
IGMP Status : Enable

DAS-3626:admin#
```

51-32 show rmt igmpsnooping

Description

This command is used to display the IGMP snooping configuration on remote CPE devices.

Format

show rmt igmpsnooping [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL lines' portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to display information related to all VDSL lines or bonding groups.

Restrictions

None.

Example

To display the IGMP snooping configuration on remote CPE devices:

```
DAS-3626:admin# show rmt igmpsnooping bonding 2
Command: show rmt igmpsnooping bonding 2

bonding2
Link State : Up

IGMP SNOOPING
Group1: Blocking
Status: Enable
Group2: Blocking
Status: Enable
Group3: Blocking
Status: Enable
Group4: Blocking
Status: Enable

DAS-3626:admin#
```

51-33 show rmt igmp-proxy

Description

This command is used to display the IGMP proxy configuration on remote CPE devices.

Format

show rmt igmp-proxy [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL lines' portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to display information related to all VDSL lines or bonding groups.

Restrictions

None.

Example

To display the IGMP proxy configuration on remote CPE devices:

```
DAS-3626:admin# show rmt igmp-proxy bonding 2
Command: show rmt igmp-proxy bonding 2

bonding2
Link State : Up
IGMP Proxy interface: WAN1
IGMP Proxy state:     disabled
IGMP Proxy interface: WAN2
IGMP Proxy state:     disabled
IGMP Proxy interface: WAN3
IGMP Proxy state:     disabled
IGMP Proxy interface: WAN4
IGMP Proxy state:     disabled
IGMP Proxy interface: WAN5
IGMP Proxy state:     disabled
IGMP Proxy interface: WAN6
IGMP Proxy state:     disabled
IGMP Proxy interface: WAN7
IGMP Proxy state:     disabled
IGMP Proxy interface: WAN8
IGMP Proxy state:     disabled

DAS-3626:admin#
```

51-34 config rmt loopback

Description

This command is used to configure the loopback test for remote CPE devices. This command is used to test the loopback between the CO side and the CPE side.

Format

config rmt loopback [ports <vdsl_portlist> | bonding <bgroup_list> | all] packet_count <int 1-90> packet_length <int 12-255>

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to configure all VDSL lines or bonding groups.
packet_count - Specifies the amount of loopback packets to count. **<int 1-90>** - Enter the packet count value here. This value is from 1 to 90.

packet_length - Specifies the length of the loopback packet. **<int 12-255>** - Enter the packet length value here. This value is from 12 to 255.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the loopback test for remote CPE devices:

```
DAS-3626:admin# config rmt loopback ports 24 packet_count 2 packet_length 100
Command: config rmt loopback ports 24 packet_count 2 packet_length 100

Update configuration to CPE 24 ..... Success.
Success.

DAS-3626:admin#
```

51-35 show rmt loopback

Description

This command is used to display the result of the loopback test.

Format

show rmt loopback [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL lines' portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to display information related to all VDSL lines or bonding groups.

Restrictions

None.

Example

To display the result of the loopback test:

```
DAS-3626:admin# show rmt loopback ports 24
Command: show rmt loopback ports 24

Line24: LINE-24
Link State : SHOWTIME
CPE LOOPBACK :
==============================
Packet count   : 2
Packet length  : 100
Min. Time(ms)  : 16
Max. Time(ms)  : 90
Avg. Time(ms)  : 53.0000
Avg. Packet Loss : 0.00000

DAS-3626:admin#
```

51-36 config rmt port_group_lan

Description

This command is used to configure the LAN port group and SSID group on remote CPE devices.

Format

config rmt port_group_lan [ports <vdsl_portlist> | bonding <bgroup_list> | all] | {LAN1 [group1 | group2 | group3 | group4]} | {LAN2 [group1 | group2 | group3 | group4]} | {LAN3 [group1 | group2 | group3 | group4]} | {LAN4 [group1 | group2 | group3 | group4]} | {SSID1 [group1 | group2 | group3 | group4]} | {SSID2 [group1 | group2 | group3 | group4]} | {SSID3 [group1 | group2 | group3 | group4]} | {SSID4 [group1 | group2 | group3 | group4]}

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to configure all VDSL lines or bonding groups.
LAN1 - Specifies to configure LAN port 1. **group1** - Specifies the group 1. **group2** - Specifies the group 2. **group3** - Specifies the group 3. **group4** - Specifies the group 4.
LAN2 - Specifies to configure LAN port 2. **group1** - Specifies the group 1. **group2** - Specifies the group 2. **group3** - Specifies the group 3. **group4** - Specifies the group 4.
LAN3 - Specifies to configure LAN port 3. **group1** - Specifies the group 1. **group2** - Specifies the group 2. **group3** - Specifies the group 3. **group4** - Specifies the group 4.
LAN4 - Specifies to configure LAN port 4. **group1** - Specifies the group 1.

	group2 - Specifies the group 2. **group3** - Specifies the group 3. **group4** - Specifies the group 4.
SSID1 - Specifies to configure SSID 1.	**group1** - Specifies the group 1. **group2** - Specifies the group 2. **group3** - Specifies the group 3. **group4** - Specifies the group 4.
SSID2 - Specifies to configure SSID 2.	**group1** - Specifies the group 1. **group2** - Specifies the group 2. **group3** - Specifies the group 3. **group4** - Specifies the group 4.
SSID3 - Specifies to configure SSID 3.	**group1** - Specifies the group 1. **group2** - Specifies the group 2. **group3** - Specifies the group 3. **group4** - Specifies the group 4.
SSID4 - Specifies to configure SSID 4.	**group1** - Specifies the group 1. **group2** - Specifies the group 2. **group3** - Specifies the group 3. **group4** - Specifies the group 4.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the LAN port group and SSID group on remote CPE devices:

```
DAS-3626:admin#config rmt port_group_lan ports 24 LAN2 group1 SSID3 group1
Command: config rmt port_group_lan ports 24 LAN2 group1 SSID3 group1

Update configuration to CPE 24 ..... Success.

DAS-3626:admin#
```

51-37 config rmt port_group_wan

Description

This command is used to configure the WAN group on remote CPE devices.

Format

config rmt port_group_wan [ports <vdsl_portlist> | bonding <bgroup_list> | all] | {group1 [NONE | WAN1 | WAN2 | WAN3 | WAN4 | WAN5 | WAN6 | WAN7 | WAN8]} | {group2 [NONE | WAN1 | WAN2 | WAN3 | WAN4 | WAN5 | WAN6 | WAN7 | WAN8]} | {group3 [NONE | WAN1 | WAN2 | WAN3 | WAN4 | WAN5 | WAN6 | WAN7 | WAN8]} | {group4 [NONE | WAN1 | WAN2 | WAN3 | WAN4 | WAN5 | WAN6 | WAN7 | WAN8]}

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to configure all VDSL lines or bonding groups.
group1 - Specifies the group 1. **NONE** - Specifies the group without any WAN. **WAN1** - Specifies WAN 1. **WAN2** - Specifies WAN 2. **WAN3** - Specifies WAN 3. **WAN4** - Specifies WAN 4. **WAN5** - Specifies WAN 5. **WAN6** - Specifies WAN 6. **WAN7** - Specifies WAN 7. **WAN8** - Specifies WAN 8.
group2 - Specifies the group 2. **NONE** - Specifies the group without any WAN. **WAN1** - Specifies WAN 1. **WAN2** - Specifies WAN 2. **WAN3** - Specifies WAN 3. **WAN4** - Specifies WAN 4. **WAN5** - Specifies WAN 5. **WAN6** - Specifies WAN 6. **WAN7** - Specifies WAN 7. **WAN8** - Specifies WAN 8.
group3 - Specifies the group 3. **NONE** - Specifies the group without any WAN. **WAN1** - Specifies WAN 1. **WAN2** - Specifies WAN 2. **WAN3** - Specifies WAN 3. **WAN4** - Specifies WAN 4. **WAN5** - Specifies WAN 5. **WAN6** - Specifies WAN 6. **WAN7** - Specifies WAN 7. **WAN8** - Specifies WAN 8.
group4 - Specifies the group 4. **NONE** - Specifies the group without any WAN. **WAN1** - Specifies WAN 1. **WAN2** - Specifies WAN 2. **WAN3** - Specifies WAN 3. **WAN4** - Specifies WAN 4. **WAN5** - Specifies WAN 5. **WAN6** - Specifies WAN 6. **WAN7** - Specifies WAN 7. **WAN8** - Specifies WAN 8.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the WAN group on remote CPE devices:

```
DAS-3626:admin#config rmt port_group_wan ports 24 group1 WAN4 group2 WAN1
Command: config rmt port_group_wan ports 24 group1 WAN4 group2 WAN1

Update configuration to CPE 24 ..... Success.

DAS-3626:admin#
```

51-38 show rmt port_group

Description

This command is used to display group information on remote CPE devices.

Format

show rmt port_group [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL lines' portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to display information related to all VDSL lines or bonding groups.

Restrictions

None.

Example

To display group information on remote CPE devices:

```
DAS-3626:admin#show rmt port_group ports 24
Command: show rmt port_group ports 24

Line24: LINE-24
Link State : SHOWTIME
 Group1 : WAN4 LAN1 LAN2 LAN3 LAN4 SSID1 SSID3
 Group2 : WAN1
 Group3 :
 Group4 :

DAS-3626:admin#
```

51-39 config rmt pppoe

Description

This command is used to configure the remote CPE PPPoE settings.

Format

config rmt pppoe [ports <vdsl_portlist> | bonding <bgroup_list> | all] connection_id <int 1-8> {serivce_name [<string 256> | clear] | ac_name [<string 256> | clear] | nat [disable | enable] | default_route [disable | enable] | pppoe_passthrouth [disable | enable] | mtu <int 46-1500> | connection_mode_select [always_on | manual | connect_on_demand max_idle_time <min 1-65536>]}

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to configure all VDSL lines or bonding groups.
connection_id - Specifies the connection ID. **<int 1-8>** - Enter the connection ID here. This value is from 1 to 8.
service_name - Specifies the service name. **<string 256>** - Enter the service name here. This string can be up to 256 characters long. **clear** - Specifies to clear the service name.
ac_name - Specifies the access concentrator's name. **<string 256>** - Enter the access concentrator's name here. This string can be up to 256 characters long. **clear** - Specifies to clear the access concentrator's name.
nat - Specifies the NAT feature's state. **disable** - Specifies that the NAT feature will be disabled. **enable** - Specifies that the NAT feature will be enabled.
default_route - Specifies the default route's state. **disable** - Specifies that the default route will be disabled. **enable** - Specifies that the default route will be enabled.
pppoe_passthrouth - Specifies the PPPoE pass-through feature's state. **disable** - Specifies that the PPPoE pass-through feature will be disabled. **enable** - Specifies that the PPPoE pass-through feature will be enabled.
mtu - Specifies the MTU size. **<int 46-1500>** - Enter the MTU size value here. This value is from 46 to 1500.
connection_mode_select - Specifies the connection mode. **always_on** - Specifies that the connection mode will be always on. **manual** - Specifies that the connection mode will be manual. **connect_on_demand** - Specifies that the connection mode will be connect on demand.
max_idle_time - Specifies to configure the maximum idle time value. **<min 1-65536>** - Enter to configure the maximum idle time value here. This value is from 1 to 65535 minutes.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the remote CPE PPPoE settings:

```
DAS-3626:admin#config rmt pppoe bonding 1 connection_id 1
connection_mode_select always_on
Command: config rmt pppoe bonding 1 connection_id 1 connection_mode_select
always_on

Update configuration to CPE 1  ..... Success.
Success.

DAS-3626:admin#
```

51-40 show rmt pppoe connection_id

Description

This command is used to display the remote CPE's PPPoE settings.

Format

show rmt pppoe connection_id <int 1-8> [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

<int 1-8> - Enter the connection ID here. This value is from 1 to 8.
ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL lines' portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to display information related to all VDSL lines or bonding groups.

Restrictions

None.

Example

To display the remote CPE's PPPoE settings:

```
DAS-3626:admin# show rmt pppoe connection_id 1 bonding 2
Command: show rmt pppoe connection_id 1 bonding 2

bonding2
Link State : Up
Connection : 1
The current WAN Mode is not PPPoE Mode !!

DAS-3626:admin#
```

51-41 config rmt protovlan

Description

This command is used to configure the protocol VLAN settings. There are six kinds of VLAN assignment rule classifications: Ethernet type, IP address and protocol, DHCP option, MAC, LAN

port, and SSID. Each kind of rule can specify a VLAN ID and the related priority. Each rule has a state option to activate the rule.

Format

config rmt protovlan [ports <vdsl_portlist> | bonding <bgroup_list> | all] [add | rule_id <int 1-8>] type [Ether_Type <protocol_value> | [Source_IP <string 32> | Destination_IP <string 32>] Protocol [None | TCP | UDP | ICMP | IGMP] | SSID <string 31> | Source_MAC <string 32> | Destination_MAC <string 32> | Port [1 | 2 | 3 | 4] | [Source_IPv6 <string 64> | Destination_IPv6 <string 64>] Protocol [None |TCP | UDP | ICMP | IGMP] | DHCP option [60 option_value <string 20>|61 [type1 {iaid <string 11>} {mac <macaddr>} | type2 {iaid <string 11>} {enterprise_num <string 32>} {identifier <string 32>}] | 125 enterprise_num <string 32> manufacture_oui <string 32> serial_number <string 32> product_class <string 32> gateway_oui <string 32>]] <priority 0-7> <vlanid 1-4094> [enable | disable]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to configure all VDSL lines or bonding groups.
add - Specifies that a new VLAN assignment rule will be added. **rule_id** - Specifies the rule ID. **<int 1-8>** - Enter the new rule's ID here. This value is from 1 to 8.
type - Specifies the type.
Ether_Type - Specifies the Ethernet type information as the main classification condition of the protocol VLAN rule. **<protocol_value>** - Enter the protocol value here.
Source_IP - Specifies the source IP address. **<string 32>** - Enter the source IP address here.
Destination_IP - Specifies the destination IP address. **<string 32>** - Enter the destination IP address here.
Protocol - Specifie the protocol used. **None** - Specifies that no protocol will be used. **TCP** - Specifies that the TCP protocol will be used. **UDP** - Specifies that the UDP protocol will be used. **ICMP** - Specifies that the ICMP protocol will be used. **IGMP** - Specifies that the IGMP protocol will be used.
SSID - Specifies the SSID. **<string 31>** - Enter the SSID here. This string can be up to 31 characters long.
Source_MAC - Specifies the source MAC address. **<string 32>** - Enter the source MAC address here.
Destination_MAC - Specifies the destination MAC address. **<string 32>** - Enter the destination MAC address here.
Port - Specifies the port number. **1** - Specifies port number 1. **2** - Specifies port number 2. **3** - Specifies port number 3. **4** - Specifies port number 4.
Source_IPv6 - Specifies the source IPv6 address. **<string 64>** - Enter the source IPv6 address here. This string can be up to 64 characters long.
Destination_IPv6 - Specifies the destination IPv6 address. **<string 64>** - Enter the destination IPv6 address here. This string can be up to 64 characters long.
Protocol - Specifies the protocol.

None - Specifies that the no protocol is used. **TCP** - Specifies that the protocol used is TCP. **UDP** - Specifies that the protocol used is UDP. **ICMP** - Specifies that the protocol used is ICMP. **IGMP** - Specifies that the protocol used is IGMP. **DHCP** - Specifies that the protocol used is DHCP.
option - Specifies to use a DHCP option.
60 - Specifies to use DHCP Option 60. **option_value** - Specifies the DHCP Option 60's option value. **<string 20>** - Enter the Option 60's option value here.
61 - Specifies to use DHCP Option 61. **type1** - Specifies to use the type 1 DHCP Option 61. **iaid** - Specifies the DHCP Option 61's type 1 IAID. **<string 11>** - Enter the DHCP Option 61's type 1 IAID here. This string can be up to 11 characters long. **mac** - Specifies the MAC address. **<macaddr>** - Enter the MAC address here. **type2** - Specifies to use the type 2 DHCP Option 61. **iaid** - Specifies the DHCP Option 61's type 2 IAID. **<string 11>** - Enter the DHCP Option 61's type 2 IAID here. This string can be up to 11 characters long. **enterprise_num** - Specifies the DHCP Option 61 enterprise number. **<string 32>** - Enter the DHCP Option 61 enterprise number here. This string can be up to 32 characters long. **identifier** - Specifies the DHCP Option 61 identifier. **<string 32>** - Enter the DHCP Option 61 identifier here. This string can be up to 32 characters long.
125 - Specifies to use DHCP Option 125. **enterprise_num** - Specifies the DHCP Option 125 enterprise number. **<string 32>** - Enter the DHCP Option 125 enterprise number here. This string can be up to 32 characters long. **manufacture_oui** - Specifies the manufacture OUI. **<string 32>** - Enter the manufacture OUI here. This string can be up to 32 characters long. **serial_number** - Specifies the serial number. **<string 32>** - Enter the serial number here. This string can be up to 32 characters long. **product_class** - Specifies the product class. **<string 32>** - Enter the product class here. This string can be up to 32 characters long. **gateway_oui** - Specifies the gateway OUI. **<string 32>** - Enter the gateway OUI here. This string can be up to 32 characters long.
<priority 0-7> - Enter the VLAN tag priority value for assignment here. This value is from 0 to 7.
<vlanid 1-4094> - Enter the VLAN ID for the assignment here. This value is from 1 to 4094.
enable - Specifies to enable this rule after being created. **disable** - Specifies to disable this rule after being created.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the protocol VLAN settings:

```
DAS-3626:admin#config rmt protovlan ports 1 add type Ether_Type 88A8 1 32
enable
Command: config rmt protovlan ports 1 add type Ether_Type 88A8 1 32 enable

Success.

DAS-3626:admin#
```

51-42 show rmt protovlan

Description

This command is used to display the protocol-based VLAN configuration and current status.

Format

show rmt protovlan [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL lines' portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to display information related to all VDSL lines or bonding groups.

Restrictions

None.

Example

To display the protocol-based VLAN configuration and current status:

```
DAS-3626:admin# show rmt protovlan ports 1
Command: show rmt protovlan ports 1

Line1: LINE-1
Link State : SHOWTIME
 Rule ID | Mapping Rule |          Mapping Value           | VID | Priority
 --------|--------------|----------------------------------|-----|---------
    1    |   Ether Type |                             88a8 |   32|        1
         |              | status:                  enabled |     |
 --------|--------------|----------------------------------|-----|---------

DAS-3626:admin#
```

51-43 config rmt qos

Description

This command is used to configure the QoS function on remote CPE devices.

Format

config rmt qos [ports <vdsl_portlist> | bonding <bgroup_list> | all] [disable_all | 802_1p | dscp | remark_1p_by_dscp | Port LAN_1 priority <int 0-7> LAN_2 priority <int 0-7> LAN_3 priority <int 0-7> LAN_4 priority <int 0-7> | VLAN [Priority_0 | Priority_1 | Priority_2 | Priority_3 | Priority_4 | Priority_5 | Priority_6 | Priority_7] total vid [1 <int 1-4094> | 2 <int 1-4094> <int 1-4094> | 3 <int 1-4094> <int 1-4094> <int 1-4094> | 4 <int 1-4094> <int 1-4094> <int 1-4094> <int 1-4094> | 5 <int 1-4094> <int 1-4094> <int 1-4094> <int 1-4094> <int 1-4094>]]

Parameters

ports - Specifies the VDSL lines.
- **<vdsl_portlist>** - Enter the VDSL portlist here. This value is from 1 to 24.

bonding - Specifies the VDSL bonding groups.
- **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.

all - Specifies to configure all VDSL lines or bonding groups.

disable_all - Specifies to clear the QoS settings on the remote CPE.

802_1p - Specifies the packet classified by 802.1Q.

dscp - Specifies the packet classified by DSCP.

remark_1p_by_dscp - Specifies the packet remarked by DSCP.

Port - Specifies the packet classified by port.
- **LAN_1** - Specifies LAN port 1.
  - **priority** - Specifies the priority of LAN port 1.
    - **<int 0-7>** - Enter the priority of LAN port 1 here. This value is from 0 to 7.
- **LAN_2** - Specifies LAN port 2.
  - **priority** - Specifies the priority of LAN port 2.
    - **<int 0-7>** - Enter the priority of LAN port 2 here. This value is from 0 to 7.
- **LAN_3** - Specifies LAN port 3.
  - **priority** - Specifies the priority of LAN port 3.
    - **<int 0-7>** - Enter the priority of LAN port 3 here. This value is from 0 to 7.
- **LAN_4** - Specifies LAN port 4.
  - **priority** - Specifies the priority of LAN port 4.
    - **<int 0-7>** - Enter the priority of LAN port 4 here. This value is from 0 to 7.

VLAN - Specifies the priority of the VLAN.
- **Priority_0** - Specifies that the priority of the VLAN will be 0.
- **Priority_1** - Specifies that the priority of the VLAN will be 1.
- **Priority_2** - Specifies that the priority of the VLAN will be 2.
- **Priority_3** - Specifies that the priority of the VLAN will be 3.
- **Priority_4** - Specifies that the priority of the VLAN will be 4.
- **Priority_5** - Specifies that the priority of the VLAN will be 5.
- **Priority_6** - Specifies that the priority of the VLAN will be 6.
- **Priority_7** - Specifies that the priority of the VLAN will be 7.
- **total** - Specifies the VLAN total.
- **vid** - Specifies the VLAN ID.
  - **1** - Specifies to associate 1 VLAN.
    - **<int 1-4094>** - Enter the VLAN ID here. This value is from 1 to 4094.
  - **2** - Specifies to associate 2 VLANs.
    - **<int 1-4094>** - Enter the 1st VLAN ID here. This value is from 1 to 4094.
    - **<int 1-4094>** - Enter the 2nd VLAN ID here. This value is from 1 to 4094.
  - **3** - Specifies to associate 3 VLANs.
    - **<int 1-4094>** - Enter the 1st VLAN ID here. This value is from 1 to 4094.
    - **<int 1-4094>** - Enter the 2nd VLAN ID here. This value is from 1 to 4094.
    - **<int 1-4094>** - Enter the 3rd VLAN ID here. This value is from 1 to 4094.
  - **4** - Specifies to associate 4 VLANs.
    - **<int 1-4094>** - Enter the 1st VLAN ID here. This value is from 1 to 4094.
    - **<int 1-4094>** - Enter the 2nd VLAN ID here. This value is from 1 to 4094.
    - **<int 1-4094>** - Enter the 3rd VLAN ID here. This value is from 1 to 4094.

<int 1-4094> - Enter the 4th VLAN ID here. This value is from 1 to 4094.
5 - Specifies to associate 5 VLANs.
<int 1-4094> - Enter the 1st VLAN ID here. This value is from 1 to 4094.
<int 1-4094> - Enter the 2nd VLAN ID here. This value is from 1 to 4094.
<int 1-4094> - Enter the 3rd VLAN ID here. This value is from 1 to 4094.
<int 1-4094> - Enter the 4th VLAN ID here. This value is from 1 to 4094.
<int 1-4094> - Enter the 5th VLAN ID here. This value is from 1 to 4094.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the QoS function on remote CPE devices:

```
DAS-3626:admin#config rmt qos ports 24 Port LAN_1 priority 2 LAN_2 priority 3
LAN_3 priority 3 LAN_4 priority 4
Command: config rmt qos ports 24 Port LAN_1 priority 2 LAN_2 priority 3 LAN_3
priority 3 LAN_4 priority 4

Update configuration to CPE 24 ..... Success.
Success.

DAS-3626:admin#config rmt qos ports 24 802_1p
Command: config rmt qos ports 24 802_1p

Update configuration to CPE 24 ..... Success.
Success.

DAS-3626:admin#
```

51-44 show rmt qos

Description

This command is used to display the QoS settings on the remote CPE device.

Format

show rmt qos [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL lines' portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to display information related to all VDSL lines or bonding groups.

Restrictions

None.

Example

To display the QoS settings on the remote CPE device:

```
DAS-3626:admin#show rmt qos ports 24
Command: show rmt qos ports 24

Line24: LINE-24
Link State : SHOWTIME
 Classified by :       Port
 LAN1 Priority:        2
 LAN2 Priority:        3
 LAN3 Priority:        3
 LAN4 Priority:        4

DAS-3626:admin#
```

51-45 config rmt qos-shaping

Description

This command is used to configure the QoS shaping function on remote CPE devices.

Format

config rmt qos-shaping [ports <vdsl_portlist> | bonding <bgroup_list> | all] {Priority_1 <int 0-200000> | Priority_2 <int 0-200000> | Priority_3 <int 0-200000> | Priority_4 <int 0-200000> | Priority_5 <int 0-200000> | Priority_6 <int 0-200000> | Priority_7 <int 0-200000>}

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to configure all VDSL lines or bonding groups.
Priority_1 - Specifies the priority 1 of the VDSL line. **<int 0-200000>** - Enter the priority 1 value of the VDSL line here. This value is from 0 to 200000.
Priority_2 - Specifies the priority 2 of the VDSL line. **<int 0-200000>** - Enter the priority 2 value of the VDSL line here. This value is from 0 to 200000.
Priority_3 - Specifies the priority 3 of the VDSL line. **<int 0-200000>** - Enter the priority 3 value of the VDSL line here. This value is from 0 to 200000.
Priority_4 - Specifies the priority 4 of the VDSL line. **<int 0-200000>** - Enter the priority 4 value of the VDSL line here. This value is from 0 to 200000.
Priority_5 - Specifies the priority 5 of the VDSL line. **<int 0-200000>** - Enter the priority 5 value of the VDSL line here. This value is from 0 to 200000.
Priority_6 - Specifies the priority 6 of the VDSL line. **<int 0-200000>** - Enter the priority 6 value of the VDSL line here. This value is from 0 to 200000.

Priority_7 - Specifies the priority 7 of the VDSL line. **<int 0-200000>** - Enter the priority 7 value of the VDSL line here. This value is from 0 to 200000.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the QoS shaping function on remote CPE devices:

```
DAS-3626:admin#config rmt qos-shaping ports 1 Priority_1 20000
Command: config rmt qos-shaping ports 1 Priority_1 20000

DAS-3626:admin#config rmt qos-shaping bonding 2 Priority_3 1 Priority_7 45000
Command: config rmt qos-shaping bonding 2 Priority_3 1 Priority_7 45000

DAS-3626:admin#
```

51-46 show rmt Qos_shaping

Description

This command is used to display the QoS shaping function on remote CPE devices.

Format

show rmt Qos_shaping [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL lines' portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to display information related to all VDSL lines or bonding groups.

Restrictions

None.

Example

To display the QoS shaping function on remote CPE devices:

```
DAS-3626:admin#show rmt Qos_shaping ports 24
Command: show rmt Qos_shaping ports 24

Line24: LINE-24
Link State : SHOWTIME
 Priority 1 : 100000
 Priority 2 : 100000
 Priority 3 : 100000
 Priority 4 : 100000
 Priority 5 : 100000
 Priority 6 : 100000
 Priority 7 : 100000

DAS-3626:admin#
```

51-47 config rmt reboot

Description

This command is used to configure the reboot function for remote CPE devices.

Format

config rmt reboot [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to configure all VDSL lines or bonding groups.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the reboot function for remote CPE devices:

```
DAS-3626:admin#config rmt reboot ports 1
Command: config rmt reboot ports 1

Update configuration to CPE 1  ..... Success.
Success.

DAS-3626:admin#
```

51-48 config rmt reset

Description

This command is used to configure the reset function for remote CPE devices.

Format

config rmt reset [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to configure all VDSL lines or bonding groups.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the reset function for remote CPE devices:

```
DAS-3626:admin#config rmt reset ports 1
Command: config rmt reset ports 1

Send Reset Config command to CPE 1  ..... Success.
Success.

DAS-3626:admin#
```

51-49 config rmt reset-config

Description

This command is used to configure the reset configuration function for remote CPE devices.

Format

config rmt reset-config [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to configure all VDSL lines or bonding groups.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the reset configuration function for remote CPE devices:

```
DAS-3626:admin#config rmt reset-config ports 1
Command: config rmt reset-config ports 1

Send Reset Config command to CPE 1  ..... Success.
Success.

DAS-3626:admin#
```

51-50 config rmt save

Description

This command is used to configure the save function for remote CPE devices.

Format

config rmt save [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to configure all VDSL lines or bonding groups.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the save function for remote CPE devices:

```
DAS-3626:admin#config rmt save ports 1
Command: config rmt save ports 1

Bonding group 1 is link down, ignore it.
Success.

DAS-3626:admin#
```

51-51 config rmt server

Description

This command is used to configure the current server service status of remote CPE devices. Remote devices contains some services like Telnet, Web, SSH, SNMP, TFTP and ICMP. These features can remotely be enabled using this command. This command should be incorporated with the ACL rule configurations. Remote access control lists needs to be configured correctly for user access to IPs and masks. The ICMP service is enabled by default on the LAN interface.

Format

config rmt server [ports <vdsl_portlist> | bonding <bgroup_list> | all] [telnet_lan | telnet_wan | web_lan | web_wan | ssh_lan | ssh_wan | tftp_lan | tftp_wan | snmp_lan | snmp_wan | icmp_wan | all] state [enable | disable]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to configure all VDSL lines or bonding groups.
telnet_lan - Specifies to configure the Telnet access service's state to the LAN interface of the remote device.
telnet_wan - Specifies to configure the Telnet access service's state to the WAN interface of the remote device.
web_lan - Specifies to configure the Web access service's state to the LAN interface of the remote device.
web_wan - Specifies to configure the Web access service's state to the WAN interface of the remote device.
ssh_lan - Specifies to configure the SSH access service's state to the LAN interface of the remote device.
ssh_wan - Specifies to configure the SSH access service's state to the WAN interface of the remote device.
tftp_lan - Specifies to configure the TFTP access service's state to the LAN interface of the remote device.
tftp_wan - Specifies to configure the TFTP access service's state to the WAN interface of the remote device.
snmp_lan - Specifies to configure the SNMP access service's state to the LAN interface of the remote device.
snmp_wan - Specifies to configure the SNMP access service's state to the WAN interface of the remote device.
icmp_wan - Specifies to configure the ICMP access service's state to the WAN interface of the remote device.
all - Specifies to configure all access services' state to the LAN and WAN interfaces of the remote device.
state - Specifies to configure the service's state to the LAN and WAN interfaces of the remote device. **enable** - Specifies to enable the service's state to the LAN and WAN interfaces of the remote device. **disable** - Specifies to disable the service's state to the LAN and WAN interfaces of the remote device.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the current server service status of remote CPE devices:

```
DAS-3626:admin#config rmt server ports 1 telnet_lan state enable
Command: config rmt server ports 1 telnet_lan state enable

Update configuration to CPE 1  ..... Success.
Success.

DAS-3626:admin#
```

51-52 show rmt server

Description

This command is used to display the remote CPE server's service state.

Format

show rmt server [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL lines' portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to display information related to all VDSL lines or bonding groups.

Restrictions

None.

Example

To display the remote CPE server's service state:

```
DAS-3626:admin# show rmt server ports 1
Command: show rmt server ports 1

Line1: LINE-1
Link State : SHOWTIME

Server Status :
    -TELNET Status
        -TELNET LAN Status       : On
        -TELNET WAN Status       : On
    -WEB Status
        -WEB LAN Status          : On
        -WEB WAN Status          : On
    -SSH Status
        -SSH LAN Status          : On
        -SSH WAN Status          : On
    -SNMP Status
        -SNMP LAN Status         : On
        -SNMP WAN Status         : Off
    -ICMP Status
        -ICMP LAN Status         : On
        -ICMP WAN Status         : On
    -Tftp Status
        -Tftp LAN Status         : On
        -Tftp WAN Status         : Off

DAS-3626:admin#
```

51-53 config rmt static-mode

Description

This command is used to configure remote CPE device's static mode settings.

Format

config rmt static-mode [ports <vdsl_portlist> | bonding <bgroup_list> | all] {network_addr <network_address> | gateway_addr <ipaddr> | mtu <int 1000-1500> | default_route [enable | disable] | nat [enable | disable] | pppoe-passthrough [enable | disable]}

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to configure all VDSL lines or bonding groups.
network_addr - Specifies the network address. **<network_address>** - Enter the network address here.
gateway_addr - Specifies the gateway's IP address. **<ipaddr>** - Enter the gateway's IP address here.
mtu - Specifies the MTU value. **<int 1000-1500>** - Enter the MTU value here. This value is from 1000 to 1500.

default_route - Specifies the default route's state. **enable** - Specifies to enable the default route. **disable** - Specifies to disable the default route.
nat - Specifies the NAT feature's state. **enable** - Specifies to enable the NAT feature. **disable** - Specifies to disable the NAT feature.
pppoe-passthrough - Specifies the PPPoE pass-through feature's state. **enable** - Specifies to enable the PPPoE pass-through feature. **disable** - Specifies to disable the PPPoE pass-through feature.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure remote CPE device's static mode settings:

```
DAS-3626:admin# config rmt static-mode bonding 1 network_addr 192.168.1.31/8
Command: config rmt static-mode bonding 1 network_addr 192.168.1.31/8

Update configuration to CPE 1  ..... Success.
Success.

DAS-3626:admin#
```

51-54 show rmt static-mode

Description

This command is used to display the remote CPE's static mode settings.

Format

show rmt static-mode [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL lines' portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to display information related to all VDSL lines or bonding groups.

Restrictions

None.

Example

To display the remote CPE's static mode settings:

```
DAS-3626:admin# show rmt static-mode bonding 1
Command: show rmt static-mode bonding 1

bonding1
Link State : Up
Static IP Address
====================================
IP address        : 192.168.1.31
Subnet mask       : 255.0.0.0
Geteway address   : 10.1.0.254
MTU               : 1500
Default route     : Disable
NAT               : Enable
PPPoE passthrough : Disable

DAS-3626:admin#
```

51-55 config rmt snmp-agent-state

Description

This command is used to configure the remote CPE device's SNMP agent state.

Format

config rmt snmp-agent-state [ports <vdsl_portlist> | bonding <bgroup_list> | all] [enable | disable]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to configure all VDSL lines or bonding groups.
enable - Specifies that the SNMP agent's state will be enabled. **disable** - Specifies that the SNMP agent's state will be disabled.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the remote CPE device's SNMP agent state:

```
DAS-3626:admin#config rmt snmp-agent-state bonding 2 enable
Command: config rmt snmp-agent-state bonding 2 enable

Update configuration to CPE 3  ..... Success.
Success.

DAS-3626:admin#
```

51-56 config rmt snmp-community

Description

This command is used to configure the remote CPE device's SNMP community.

Format

config rmt snmp-community [ports <vdsl_portlist> | bonding <bgroup_list> | all] [[delete rule_id <int 1-9>] | [add | rule_id <int 1-9>] name <string 31> access [read-only | read-write]]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to configure all VDSL lines or bonding groups.
delete - Specifies to delete the rule. **rule_id** - Specifies the rule's ID that will be deleted. **<int 1-9>** - Enter the rule's ID that will be deleted here. This value is from 1 to 9.
add - Specifies to add the rule. **rule_id** - Specifies the rule's ID that will be added. **<int 1-9>** - Enter the rule's ID that will be added here. This value is from 1 to 9.
name - Specifies the SNMP community name. **<string 31>** - Enter the SNMP community name here. This string can be up to 31 characters long.
access - Specifies to configure the access level for the SNMP community. **read-only** - Specifies that the access level for the SNMP community will be read-only. **read-write** - Specifies that the access level for the SNMP community will be read/write.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the remote CPE device's SNMP community:

```
DAS-3626:admin#config rmt snmp-community bonding 2 add name test access read-
only
Command: config rmt snmp-community bonding 2 add name test access read-only

Update configuration to CPE 3  ..... Success.
Success.

DAS-3626:admin#
```

51-57 config rmt snmp-trap

Description

This command is used to configure the remote CPE's SNMP trap settings.

This command is used to configure the remote CPE's SNMP trap host information. Users need to specify a host with an IP address, community and SNMP protocol version. The rule can be enabled or disabled manually. This command also has the ability to configure each SNMP trap entry with the specified host ID.

Format

config rmt snmp-trap [ports <vdsl_portlist> | bonding <bgroup_list> | all] [[delete host_id <int 1-9>] | [add | host_id <int 1-9>] ip_addr <ipaddr> community_name <string 32> snmp_version [snmp_v1 | snmp_v2c] | [status [enable | disable]]]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to configure all VDSL lines or bonding groups.
delete - Specifies to delete an existing trap host entry. **host_id** – Specifies the host ID of the trap entry that will be deleted. **<int 1-9**> - Enter the host ID of the trap entry that will be deleted here. This value is from 1 to 9.
add - Specifies to add a new trap host entry. **host_id** - Specifies the host ID of the trap entry that will be added. **<int 1-9>** - Enter the host ID of the trap entry that will be added here. This value is from 1 to 9.
ip_addr - Specifies the host's IP address. **<ipaddr>** - Enter the host's IP address here.
community_name - Specifies the host's community name. **<string 32>** - Enter the host's community name here. This string can be up to 32 characters long.
snmp_version - Specifies the working SNMP version. **snmp_v1** - Specifies that the working SNMP version is SNMPv1. **snmp_v2c** - Specifies that the working SNMP version is SNMPv2c.
status - Specifies the SNMP trap's state. **enable** - Specifies that the SNMP trap's state will be enabled. **disable** - Specifies that the SNMP trap's state will be disabled.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the remote CPE's SNMP trap settings:

```
DAS-3626:admin#config rmt snmp-trap ports 1 add ip_addr 1.1.1.1 community_name
public snmp_version snmp_v1
Command: config rmt snmp-trap ports 1 add ip_addr 1.1.1.1 community_name public
snmp_version snmp_v1

Update configuration to CPE 1  ..... Success.
Success.

DAS-3626:admin#
```

51-58 show rmt snmp-agent-state

Description

This command is used to display the remote CPE device's SNMP agent state.

Format

show rmt snmp-agent-state [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL lines' portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to display information related to all VDSL lines or bonding groups.

Restrictions

None.

Example

To display the remote CPE device's SNMP agent state:

```
DAS-3626:admin#show rmt snmp-agent-state bonding 2
Command: show rmt snmp-agent-state bonding 2

bonding2
Link State : Up
SNMP agent state: disabled

DAS-3626:admin#
```

51-59 show rmt snmp-community

Description

This command is used to display the remote CPE device's SNMP community information.

Format

show rmt snmp-community [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL lines' portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to display information related to all VDSL lines or bonding groups.

Restrictions

None.

Example

To display the remote CPE device's SNMP community information.

```
DAS-3626:admin#show rmt snmp-community bonding 2
Command: show rmt snmp-community bonding 2

bonding2
Link State : Up
 Community ID : 1
 Community name : public
 Community access : rocommunity

 Community ID : 2
 Community name : private
 Community access : rwcommunity

 Community ID : 3
 Community name : test
 Community access : rocommunity

DAS-3626:admin#
```

51-60 show rmt snmp-info

Description

This command is used to display the SNMP information and current status.

Format

show rmt snmp-info [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL lines' portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to display information related to all VDSL lines or bonding groups.

Restrictions

None.

Example

To display the SNMP information and current status:

```
DAS-3626:admin#show rmt snmp-info ports 1
Command: show rmt snmp-info ports 1

Line1: LINE-1
Link State : SHOWTIME
SNMP Information
====================================
SNMP Vendor ID : 1.3.6.1.4.1.171
SNMP Name      : DSL-7740C
SNMP Location  : D-Link
SNMP Contact   : admin@dlink.com

DAS-3626:
```

51-61 show rmt snmp-trap

Description

This command is used to display the SNMP trap configuration and current status.

Format

show rmt snmp-trap [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL lines' portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to display information related to all VDSL lines or bonding groups.

Restrictions

None.

Example

To display the SNMP trap configuration and current status:

```
DAS-3626:admin#show rmt snmp-trap ports 1
Command: show rmt snmp-trap ports 1

Line1: LINE-1
Link State : SHOWTIME
 SNMP traps state: enabled
 Host ID |   IP Address    |          Community name          | SNMP Version
 --------|-----------------|----------------------------------|--------------
       1 |         1.1.1.1 |                           public |      SNMP V1
 --------|-----------------|----------------------------------|--------------

DAS-3626:admin#
```

51-62 config rmt ssid

Description

This command is used to configure the Service Set Identifier (SSID) of the LAN interface on the remote CPE device.

Format

config rmt ssid [ports <vdsl_portlist> | bonding <bgroup_list> | all] [[add SSID <int 1-4> state [enable | disable] message <string 32>] | [delete SSID <int 1-4>]]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to configure all VDSL lines or bonding groups.
add - Specifies to add an SSID for the LAN interface. **SSID** - Specifies the SSID that will be added. **<int 1-4>** - Enter the the SSID that will be added here. This value is from 1 to 4. **state** - Specifies the SSID's state for the LAN interface. **enable** - Specifies that the SSID's state will be enabled. **disable** - Specifies that the SSID's state will be disabled. **message** - Specifies the SSID's name for the LAN interface. **<string 32>** - Enter the SSID's name for the LAN interface here. This string can be up to 32 characters long.
delete - Specifies to delete an SSID from the LAN interface. **SSID** - Specifies the SSID that will be deleted. **<int 1-4>** - Enter the SSID that will be deleted here. This value is from 1 to 4.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the SSID of the LAN interface on the remote CPE device:

```
DAS-3626:admin# config rmt ssid ports 1 add SSID 1 state enable message DSL-
7740C
Command: config rmt ssid ports 1 add SSID 1 state enable message DSL-7740C

Update configuration to CPE 1  ..... Success.
Success.

DAS-3626:admin#
```

51-63 show rmt ssid

Description

This command is used to display the SSID of the LAN interface on remote CPE devices.

Format

show rmt ssid [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL lines' portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to display information related to all VDSL lines or bonding groups.

Restrictions

None.

Example

To display the SSID of the LAN interface on remote CPE devices:

```
DAS-3626:admin# show rmt ssid bonding 2
Command: show rmt ssid bonding 2

Line3: LINE-3
Link State : SHOWTIME
SSID_id     : 1
SSID_status : enabled
SSID        : DSL-7740C

SSID_id     : 2
SSID_status : disabled
SSID        : DSL-7740C_2

SSID_id     : 3
SSID_status : disabled
SSID        : DSL-7740C_3

SSID_id     : 4
SSID_status : disabled
SSID        : DSL-7740C_4

DAS-3626:admin#
```

51-64 config rmt static-route

Description

This command is used to configure and enable the static route for the remote CPE device.

Format

config rmt static-route [ports <vdsl_portlist> | bonding <bgroup_list> | all] [add | rule_id <int 1-20>] Destination_IP <network_address> gateway_addr <ipaddr> status [enable | disable]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to configure all VDSL lines or bonding groups.
add - Specifies to add a rule. **rule_id** - Specifies the rule's ID that will be added. **<int 1-20>** - Enter the rule's ID that will be added here. This value is from 1 to 20.
Destination_IP - Specifies the destination host's IPv4 address and network mask. **<network_address>** - Enter the destination host's IPv4 address and network mask here. For example, 192.168.0.50/24.
gateway_addr - Specifies the gateway's IP address. **<ipaddr>** - Enter the gateway's IP address here.
status - Specifies the static route's state. **enable** - Specifies that this static route entry will be enabled after configuration. **disable** - Specifies that this static route entry will be disabled after configuration.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure and enable the static route for the remote CPE device:

```
DAS-3626:admin#



DAS-3626:admin#
```

51-65 show rmt static-route

Description

This command is used to display the static routes of the remote CPE device.

Format

show rmt static-route [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

ports - Specifies the VDSL lines. **<vdsl_portlist>** - Enter the VDSL lines' portlist here. This value is from 1 to 24.
bonding - Specifies the VDSL bonding groups. **<bgroup_list>** - Enter the VDSL bonding group list here. This value is from 1 to 12.
all - Specifies to display information related to all VDSL lines or bonding groups.

Restrictions

None.

Example

To display the static routes of the remote CPE device:

```
DAS-3626:admin#show rmt static-route ports 1
Command: show rmt static-route ports 1

Line1: LINE-1
Link State : SHOWTIME

 Rule ID | Destination IP  | Destination Mask |   Gateway IP    | Status
---------------------------------------------------------------------------
        1 |      172.16.0.0 |      255.240.0.0 |                 | enable
        2 |        10.0.0.0 |        255.0.0.0 |                 | enable
        3 |    192.168.11.0 |    255.255.255.0 |                 | disable
        4 |    192.168.12.0 |    255.255.255.0 |                 | disable
        5 |    192.168.13.0 |    255.255.255.0 |                 | disable
        6 |    192.168.14.0 |    255.255.255.0 |                 | disable
        7 |    192.168.15.0 |    255.255.255.0 |                 | disable
        8 |    192.168.16.0 |    255.255.255.0 |                 | disable
        9 |    192.168.17.0 |    255.255.255.0 |                 | disable
       10 |    192.168.18.0 |    255.255.255.0 |                 | disable
       11 |      172.16.0.1 |        255.0.0.0 |  172.16.1.254   | enable

DAS-3626:admin#
```

51-66 config rmt system-pwd

Description

This command is used to configure the password of the remote CPE devices.

Format

config rmt system-pwd [ports <vdsl_portlist> | bonding <bgroup_list> | all] <string 32>

Parameters

ports - Specifies a list of VDSL lines. **<vdsl_portlist>** - Enter a list of VDSL lines. The range is from 1 to 24.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
all - Specifies to configure all VDSL lines.
<string 32> - Enter the password here. The string can be up to 32 characters long.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the password of the remote CPE device:

```
DAS-3626:admin# config rmt system-pwd ports 1 1234
Command: config rmt system-pwd ports 1 1234

Update configuration to CPE 1  ..... Success.
Success.

DAS-3626:admin#
```

51-67 show rmt system-pwd

Description

This command is used to display the password of the CPE devices.

Format

show rmt system-pwd [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

ports - Specifies a list of VDSL lines. **<vdsl_portlist>** - Enter a list of VDSL lines. The range is from 1 to 24.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
all - Specifies to configure all VDSL lines.

Restrictions

None.

Example

To dipaly the password of the CPE device:

```
DAS-3626:admin# show rmt system-pwd ports 1

Line1: LINE-1
Link State : SHOWTIME

SYSTEM Password : 1234

DAS-3626:admin#
```

51-68 config rmt vlan-type

Description

This command is used to configure VLAN type of the remote devices.

Format

config rmt vlan-type [ports <vdsl_portlist> | bonding <bgroup_list> | all] [none | lan-group | protovlan]

Parameters

ports - Specifies a list of VDSL lines. **<vdsl_portlist>** - Enter a list of VDSL lines. The range is from 1 to 24.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
all - Specifies to configure all VDSL lines.
none - Specifies that there is no VLAN in the CPE devices.
lan-group - Specifies to group LAN ports with specified WAN group.
protovlan - Specifies that the CPE device assigns VLAN tag to each incoming packet by the user-defined rule. All packets are forwarded to different VLAN local network port according to the rules.

Restrictions

Only Administrators and Operators can issue this command.

Example

To assign VALN type as lan-group:

```
DAS-3626:admin# config rmt vlan-type ports 1 lan-group
Command: config rmt vlan-type ports 1 lan-group

Update configuration to CPE 1  ..... Success.
Success.


DAS-3626:admin#
```

51-69 show rmt vlan-type

Description

This command is used to display the current VLAN type configuration and link status of the specified lines.

Format

show rmt vlan-type [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

ports - Specifies a list of VDSL lines. **<vdsl_portlist>** - Enter a list of VDSL lines. The range is from 1 to 24.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
all - Specifies to display all VDSL lines.

Restrictions

None.

Example

To display the VLAN type and link status of port 1:

```
DAS-3626:admin# show rmt vlan-type ports 1
Command: show rmt vlan-type ports 1

Line1: LINE-1
Link State : SHOWTIME
VLAN Type : Lan-Group


DAS-3626:admin#
```

51-70 config rmt wireless

Description

This command is used to configure the remote cpe wireless function state. The Switch can enable or disable the wireless ability of the specified remote CPE devices.

Format

config rmt wireless [ports <vdsl_portlist> | bonding <bgroup_list> | all] state [enable | disable]

Parameters

ports - Specifies a list of VDSL lines. **<vdsl_portlist>** - Enter a list of VDSL lines. The range is from 1 to 24.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
all - Specifies to configure all VDSL lines.
state - Specifies the wireless state of the CPE devices. **enable** - Specifies to active the wireless function of the CPE devices. **disable** - Specifies to inactive the wireless function of the CPE devices.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable the wireless state of the bonding group 1:

```
DAS-3626:admin# config rmt wireless bonding 1 state enable
Command: config rmt wireless bonding 1 state enable

Update configuration to CPE 1  ..... Success.
Success.

DAS-3626:admin#
```

51-71 show rmt wireless

Description

This command is used to display the current remote CPE wireless configuration and wireless function status of the specified remote CPE wireless function state.

Format

show rmt wireless [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

ports - Specifies a list of VDSL lines. **<vdsl_portlist>** - Enter a list of VDSL lines. The range is from 1 to 24.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
all - Specifies to display all VDSL lines.

Restrictions

None.

Example

To display the wireless status of bonding group 1:

```
DAS-3626:admin# show rmt wireless bonding 1
Command: show rmt wireless bonding 1

bonding1
Link State : Up
Wireless Port Status : On
CPE Model ID : DSL-7740C


DAS-3626:admin#
```

51-72 show rmt counters

Description

This command is used to display the statistics counters of the remote CPE devices.

Format

show rmt counters [ports <vdsl_portlist> | bonding <bgroup_list> | all] [LAN | WAN | WIRELESS]

Parameters

ports - Specifies a list of VDSL lines. **<vdsl_portlist>** - Enter a list of VDSL lines. The range is from 1 to 24.

bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
all - Specifies to display all VDSL lines.
LAN - Specifies to display the counters of LAN port.
WAN - Specifies to display the counters of WAN port.
WIRELESS - Specifies to display the counters of wireless port.

Restrictions

None.

Example

To dislay the WAN counters of bonding group 2:

```
DAS-3626:admin# show rmt counters bonding 2 WAN
Command: show rmt counters bonding 2 WAN

bonding2
Link State : Up
WAN Port 1 Status :
    WAN Port Transmit Counter(Pkts) : 7
    WAN Port Receive Counter(Pkts)  : 333
    WAN Port Transmit Counter(Bytes): 672
    WAN Port Receive Counter(Bytes) : 15318
WAN Port 2 Status :
    WAN Port Transmit Counter(Pkts) : 0
    WAN Port Receive Counter(Pkts)  : 333
    WAN Port Transmit Counter(Bytes): 0
    WAN Port Receive Counter(Bytes) : 15318
WAN Port 3 Status :
    WAN Port Transmit Counter(Pkts) : 118
    WAN Port Receive Counter(Pkts)  : 333
    WAN Port Transmit Counter(Bytes): 70092
    WAN Port Receive Counter(Bytes) : 21312
WAN Port 4 Status :
    WAN Port Transmit Counter(Pkts) : 0
    WAN Port Receive Counter(Pkts)  : 0
    WAN Port Transmit Counter(Bytes): 0
    WAN Port Receive Counter(Bytes) : 0
WAN Port 5 Status :
    WAN Port Transmit Counter(Pkts) : 0
    WAN Port Receive Counter(Pkts)  : 0
    WAN Port Transmit Counter(Bytes): 0
    WAN Port Receive Counter(Bytes) : 0
WAN Port 6 Status :
    WAN Port Transmit Counter(Pkts) : 0
    WAN Port Receive Counter(Pkts)  : 0
    WAN Port Transmit Counter(Bytes): 0
    WAN Port Receive Counter(Bytes) : 0
WAN Port 7 Status :
    WAN Port Transmit Counter(Pkts) : 0
    WAN Port Receive Counter(Pkts)  : 0
    WAN Port Transmit Counter(Bytes): 0
    WAN Port Receive Counter(Bytes) : 0
WAN Port 8 Status :
    WAN Port Transmit Counter(Pkts) : 0
    WAN Port Receive Counter(Pkts)  : 0
    WAN Port Transmit Counter(Bytes): 0
    WAN Port Receive Counter(Bytes) : 0
Total WAN Transmit Counter(Pkts) : 125
Total WAN Receive Counter(Pkts) : 999
Total WAN Transmit Counter(Bytes) : 70764
Total WAN Receive Counter(Bytes) : 51948

DAS-3626:admin#
```

51-73 show rmt rate

Description

This command is used to display the detail transmit rate and receive rate of LAN, WAN and WIRELESS port on the remote CPE devices.

Format

show rmt rate [ports <vdsl_portlist> | bonding <bgroup_list> | all] [LAN | WAN | WIRELESS]

Parameters

ports - Specifies a list of VDSL lines. **<vdsl_portlist>** - Enter a list of VDSL lines. The range is from 1 to 24.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
all - Specifies to display all VDSL lines.
LAN - Specifies to display the rate of LAN port.
WAN - Specifies to display the rate of WAN port.
WIRELESS - Specifies to display the rate of wireless port.

Restrictions

None.

Example

To display the LAN rate of VDSL line 24:

```
DAS-3626:admin# show rmt rate ports 24 LAN
Command: show rmt rate ports 24 LAN

Line24: LINE-24
Link State : SHOWTIME
LAN Port 1 Status :
    LAN Port Transmit Rate(Pkts) : 3030
    LAN Port Receive Rate(Pkts)  : 0
    LAN Port Transmit Rate(Bytes): 209648
    LAN Port Receive Rate(Bytes) : 0
LAN Port 2 Status :
    LAN Port Transmit Rate(Pkts) : 3030
    LAN Port Receive Rate(Pkts)  : 0
    LAN Port Transmit Rate(Bytes): 209648
    LAN Port Receive Rate(Bytes) : 0
LAN Port 3 Status :
    LAN Port Transmit Rate(Pkts) : 3030
    LAN Port Receive Rate(Pkts)  : 0
    LAN Port Transmit Rate(Bytes): 209648
    LAN Port Receive Rate(Bytes) : 0
LAN Port 4 Status :
    LAN Port Transmit Rate(Pkts) : 792
    LAN Port Receive Rate(Pkts)  : 1119
    LAN Port Transmit Rate(Bytes): 55066
    LAN Port Receive Rate(Bytes) : 77537
Total LAN Transmit Rate(Pkts) : 9882
Total LAN Receive Rate(Pkts) : 1119
Total LAN Transmit Rate(Bytes) : 684010
Total LAN Receive Rate(Bytes) : 77537

DAS-3626:admin#
```

51-74 show rmt version

Description

This command is used to display the firmware version of the remote CPE devices.

Format

show rmt version [ports <vdsl_portlist>| bonding <bgroup_list> | all]

Parameters

ports - Specifies a list of VDSL lines. **<vdsl_portlist>** - Enter a list of VDSL lines. The range is from 1 to 24.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
all - Specifies to display all VDSL lines.

Restrictions

None.

Example

To display the firmware version of bonding group 2:

```
DAS-3626:admin#show rmt version bonding 2
Command: show rmt version bonding 2

bonding2
Link State : Up
CPE Firmware Image_1 Version : DSL7740C.N6.TR069.20140915
CPE Firmware Image_2 Version : DSL7740C-N1.20120927
CPE VDSL Firmware Version    : A2pvbF038m.d24k

DAS-3626:admin#
```

51-75 show rmt model-id

Description

This command is used to display the model IDs of the remote CPE devices.

Format

show rmt model-id [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

ports - Specifies a list of VDSL lines. **<vdsl_portlist>** - Enter a list of VDSL lines. The range is from 1 to 24.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
all - Specifies to display all VDSL lines.

Restrictions

None.

Example

To display the model ID of bonding group 2:

```
DAS-3626:admin# show rmt model-id bonding 2
Command: show rmt model-id bonding 2

bonding2
Link State : Up
CPE Model ID : DSL-7740C

DAS-3626:admin#
```

51-76 show rmt cpe-mac

Description

This command is used to display the MAC address of the remote CPE device.

Format

show rmt cpe-mac [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

ports - Specifies a list of VDSL lines. **<vdsl_portlist>** - Enter a list of VDSL lines. The range is from 1 to 24.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
all - Specifies to display all VDSL lines.

Restrictions

None.

Example

To display the MAC address of bonding group 2:

```
DAS-3626:admin# show rmt cpe-mac bonding 2
Command: show rmt cpe-mac bonding 2

bonding2
Link State : Up
CPE MAC address : 90-94-E4-0A-5A-95


DAS-3626:admin#
```

51-77 show rmt cpe-fdb

Description

This command is used to display the forwarding entries in each interface of the remote CPE devices.

Format

show rmt cpe-fdb [ports <vdsl_portlist> | bonding <bgroup_list> | all]

Parameters

ports - Specifies a list of VDSL lines. **<vdsl_portlist>** - Enter a list of VDSL lines. The range is from 1 to 24.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
all - Specifies to display all VDSL lines.

Restrictions

None.

Example

To display the forwarding table of bonding group 2:

```
DAS-3626:admin# show rmt cpe-fdb bonding 2
Command: show rmt cpe-fdb bonding 2

bonding2
Link State : Up
CPE FDB TABLE :
================================
Interface  MAC Address
---------  -----------------
lan3       00-0E-04-B7-2D-79
vdsl       00-79-96-20-00-03

Total Entries : 2

DAS-3626:admin#
```

Chapter 52 VLAN Count Command List

show vlan_counter <vlanid 1-4094> [<port> | bonding_group <bgroup>]

52-1 show vlan_counter

Description

This command is used to display the total count of port with VLAN ID.

Format

show vlan_counter <vlanid 1-4094> [<port> | bonding_group <bgroup>]

Parameters

<vlanid 1-4094> - Enter the VLAN ID used here. This value must be between 1 and 4094. **<port>** - Enter a port number. The range is from 1 to 26. **bonding_group** - Specifies a bonding number. **<bgroup>** - Enter a bonding number. The range is from 1 to 12.

Restrictions

Only Administrators and Operators can issue this command.

Example

To show VLAN counter:

```
DAS-3626:admin#show vlan_counter 1 1
Command: show vlan_counter 1 1


 VLAN Counter
 VLAN Counter Port : 1
 VLAN Counter VLAN ID : 1
 ================================================
 Frame Type             Total                    Total/sec
 ---------------------- ------------------------ ----------
 Unicast RX Bytes       0                        0
 Unicast RX Packets     0                        0
 Unicast TX Bytes       0                        0
 Unicast TX Packets     0                        0
 Multicast RX Bytes     0                        0
 Multicast RX Packets   0                        0
 Multicast TX Bytes     0                        0
 Multicast TX Packets   0                        0
 Broadcast RX Bytes     0                        0
 Broadcast RX Packets   0                        0
 Broadcast TX Bytes     0                        0
 Broadcast TX Packets   0                        0

CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

Chapter 53 VLAN Trunking Command List

enable vlan_trunk
disable vlan_trunk
config vlan_trunk [ports [<portlist> | all] | bonding <bgroup_list>] | state [enable | disable]
show vlan_trunk

53-1 enable vlan_trunk

Description

This command is used to enable the VLAN trunk function. When the VLAN trunk function is enabled, the VLAN trunk ports shall be able to forward all tagged frames with any VID.

Format

enable vlan_trunk

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable the VLAN Trunk:

```
DAS-3626:admin# enable vlan_trunk
Command: enable vlan_trunk

Success.

DAS-3626:admin#
```

53-2 disable vlan_trunk

Description

This command is used to disable the VLAN trunk function.

Format

disable vlan_trunk

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable the VLAN Trunk:

```
DAS-3626:admin# disable vlan_trunk
Command: disable vlan_trunk

Success.

DAS-3626:admin#
```

53-3 config vlan_trunk

Description

This command is used to configure a port as a VLAN trunk port. By default, none of the port is a VLAN trunk port.

If the user enables the global VLAN trunk function and configurethe VLAN trunk ports, then the trunk port will be member port of all VLANs. That is, if a VLAN is already configured by the user, but the trunk port is not member port of that VLAN, this trunk port will atutomatically become tagged member port of that VLAN. If a VLAN is not created yet, the VLAN will be automatically created, and the trunk port will become tagged member of this VLAN.

When the user disables the VLAN trunk globally, all VLANs automatically created by VLAN Trunk enabled shall be destroyed, and all the automatically added port membership will be removed.

A VLAN trunk port and a non-VLAN trunk port cannot be grouped as an aggregated link. To change the VLAN trunk setting for an aggregated link, the user must apply the command to the master port. However, this setting will disappear as the aggregated link is destroyed, and the VLAN trunk setting of the individual port will follow the original setting of the port.

If the command is applied to link aggregation member port excluding the master, the command will be rejected.

The ports with different VLAN configurations are not allowed to form an aggregated link. However, if they are specified as VLAN trunk port, they are allowed to form an aggregated link.

For a VLAN trunk port, the VLANs on which the packets can be by passed will not be advertised by GVRP on this port. However, since the traffic on these VLANs are forwarded, this vlan trunk port should participate the MSTP instances corresponding to these VLAN.

Format

config vlan_trunk [ports [<portlist> | all] | bonding <bgroup_list>] | state [enable | disable]

Parameters

ports - Specifies a list of ports to be configured. **<portlist>** - Enter a list of ports used for the configuration here. **all** - Specifies that all the ports will be used for this configuration.
bonding - Specifies a list of VDSL bonding groups. **<bgroup_list>** - Enter a list of VDSL bonding groups. The range is from 1 to 12.
state - Specifies that the port is a VLAN trunk port or not. **enable** - Specifies that the port is a VLAN trunk port. **disable** - Specifies that the port is not a VLAN trunk port.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure a VLAN trunk port:

```
DAS-3626:admin#config vlan_trunk ports 1-5 state enable
Command: config vlan_trunk ports 1-5 state enable

Success.

DAS-3626:admin#
```

53-4 show vlan_trunk

Description

This command is used to show the VLAN trunk configuration.

Format

show vlan_trunk

Parameters

None.

Restrictions

None.

Example

To show the VLAN Trunk information:

```
DAS-3626:admin#show vlan_trunk
Command: show vlan_trunk


VLAN Trunk Global Setting
----------------------------
VLAN Trunk Status  : Enabled
VLAN Trunk Member Ports : 1-5


DAS-3626:admin#
```

The following example displays the VLAN information which will also display VLAN trunk setting:

```
DAS-3626:admin#show vlan
Command: show vlan


VLAN Trunk State        : Enabled
VLAN Trunk Member Ports : 1-5


VID             : 1               VLAN Name     : default
VLAN Type       : Static          Advertisement : Enabled
Member Ports    : 1-26
Static Ports    : 1-26
Current Tagged Ports  :
Current Untagged Ports: 1-26
Static Tagged Ports   :
Static Untagged Ports : 1-26
Forbidden Ports       :

Total Static VLAN Entries: 1
Total GVRP VLAN Entries: 0


DAS-3626:admin#
```

Chapter 54 Web-Based Access Control (WAC) Command List

enable wac
disable wac
config wac ports [<portlist> | all] {state [enable | disable] | aging_time [infinite | <min 1-1440>] | idle_time [infinite | <min 1-1440>] | block_time [<sec 0-300>]} (1)
config wac method [local | radius]
config wac default_redirpath <string 128>
config wac virtual_ip <ipaddr>
config wac switch_http_port <tcp_port_number 1-65535> {[http | https]}
create wac user <username 15> {[vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}
delete wac [**user** <username 15> | all_users]
config wac user <username 15> [vlan <vlan_name 32> | vlanid <vlanid 1-4094> | clear_vlan]
show wac
show wac ports {<portlist>}
show wac user
show wac auth_state ports {<portlist>}
clear wac auth_state [ports [<portlist> | all] {authenticated | authenticating | blocked} | macaddr <macaddr>]

54-1 enable wac

Description

This command is used to enable WAC function.

Format

enable wac

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable WAC:

```
DAS-3626:admin# enable wac
Command: enable wac

Success.

DAS-3626:admin#
```

54-2 disable wac

Description

This command is used to disable WAC function. All authentication entries related to WAC will be deleted.

Format

disable wac

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable WAC:

```
DAS-3626:admin# disable wac
Command: disable wac

Success.

DAS-3626:admin#
```

54-3 config wac ports

Description

This command is used to configure the state and other parameters of the ports.

Format

config wac ports [<portlist> | all] {state [enable | disable] | aging_time [infinite | <min 1-1440>] | idle_time [infinite | <min 1-1440>] | block_time [<sec 0-300>]} (1)

Parameters

<portlist> - Enter a port range to set their WAC state.

all - Specifies to configure all the Switch ports' WAC state.
state - Specifies the port state of WAC. **enable** - Specifies that the port state of WAC will be enabled. **disable** - Specifies that the port state of WAC will be disabled.
aging_time - Specifies a time period during which an authenticated host will keep in authenticated state. **infinite** - Specifies to indicate never to age out the authenticated host on the port. **<min 1-1440>** - Enter the aging time period here. This value must be between 1 and 1440 minutes.
idle_time - Specifies the idle time. If there is no traffic during idle time, the host will be moved back to unauthenticated state **infinite** - Specifies never to check the idle state of the authenticated host on the port. **<min 1-1440>** - Enter the idle time period here. This value must be between 1 and 1440 minutes.
block_time - Specifies the block time. If a host fails to pass the authentication, it will be blocked for a period specified by "block_time". **<sec 0-300>** - Enter the blocking time here. This value must be between 0 and 300 seconds.

Restrictions

Only Administrators and Operators can issue this command.

Example

To config state and other parameters of the ports:

```
DAS-3626:admin# config wac ports 1-9 state enable
Command: config wac ports 1-9 state enable

Success.

DAS-3626:admin#
```

54-4 config wac method

Description

This command is used to configure the WAC authentication method. The command allows you to specify the RADIUS protocol used by WAC to complet RADIUS authentication.

WAC shares other RADIUS configuration with 802.1X, when using this command to set the RADIUS protocol. The RADIUS server must be configured.

Format

config wac method [local | radius]

Parameters

local - Specifies that the authentication will be done via the local database.
radius - Specifies that the authentication will be done via the RADIUS server.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure WAC auth method:

```
DAS-3626:admin# config wac method radius
Command: config wac method radius

Success.

DAS-3626:admin#
```

54-5 config wac default_redirpath

Description

This command is used to configure the WAC default redirect path. If default redirect path is configured, the user will be redirected to the default redirect path after successful authentication.

When the string is cleared, the client will not be redirected to another URL after successful authentication.

Format

config wac default_redirpath <string 128>

Parameters

<string 128> - Enter the URL that the client will be redirected to after successful authentication. By default, the redirected path is cleared. This value can be up to 128 characters long.

Restrictions

Only Administrators and Operators can issue this command.

Example

To config WAC default redirect URL:

```
DAS-3626:admin#config wac default_redirpath http://www.dlink.com
Command: config wac default_redirpath http://www.dlink.com

Success.

DAS-3626:admin#
```

54-6 config wac virtual_ip

Description

This command is used to configure the virtual IP of WAC. The virtual IP of WAC is used to accept authentication request from unauthenticated host. Only requests sent to this IP will get response correctly.

This IP does not respond to ARP request or ICMP packet!

Format

config wac virtual_ip <ipaddr>

Parameters

<ipaddr> - Enter the IP address of the virtual IP.

Restrictions

Only Administrators and Operators can issue this command.

Example

Set virtual IP address:

```
DAS-3626:admin# config wac virtual_ip 1.1.1.1
Command: config wac virtual_ip 1.1.1.1

Success.

DAS-3626:admin#
```

54-7 config wac switch_http_port

Description

This command is used to configure the TCP port for HTTP or HTTPs. The TCP port for HTTP or HTTPs is used to identify the HTTP or HTTPs packets.

That will be trapped to CPU for authentication processing, or to access the login page.

If not specified, the default port number for HTTP is 80, and the default port number for HTTPS is 443.

If no protocol specified, the protocol is HTTP.

The HTTP cannot run at TCP port 443, and the HTTPS cannot run at TCP port 80.

Format

config wac switch_http_port <tcp_port_number 1-65535> {[http | https]}

Parameters

<tcp_port_number 1-65535> - Enter a TCP port which the WAC Switch listens to and uses to finish the authenticating process. The range of port number is 1-65535.
http - (Optional) Specifiesthe WAC runs HTTP protocol on this TCP port.
https - (Optional) Specifiesthe WAC runs HTTPS protocol on this TCP port.

Restrictions

Only Administrators and Operators can issue this command.

Example

To config HTTP(s) port of the switch used by WAC:

```
DAS-3626:admin# config wac switch_http_port 8888 http
Command: config wac switch_http_port 8888 http

Success.

DAS-3626:admin#
```

54-8 create wac user

Description

This command is used to create accounts for web-base access control.

This user account is independent with login user account.

If VLAN is not specified, the user will not get a VLAN assigned after the authentication.

Format

create wac user <username 15> {[vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}

Parameters

<username 15> - Enter the user name for web-base access control. This name can be up to 15 characters long.
vlan - (Optional) Specifies the target VLAN name for authenticated hosts which will uses this user account to pass authentication. **<vlan_name 32>** - Enter the name of the VLAN here. This name can be up to 32 characters long.
vlanid - (Optional) Specifies the target VLAN ID for authenticated hosts which will uses this user account to pass authentication. **<vlanid 1-4094>** - Enter the VLAN ID used here. This value must be between 1 and 4094.

Restrictions

Only Administrators and Operators can issue this command.

Example

To create a WAC local user:

```
DAS-3626:admin#create wac user Jim
Command: create wac user Jim

Enter a case-sensitive new password:***
Enter the new password again for confirmation:***
Success.

DAS-3626:admin#
```

54-9 delete wac user

Description

This command is used to delete WAC users from the local DB.

Format

delete wac [user <username 15> | all_users]

Parameters

user - Specifies the user name to be deleted. **<username 15>** - Enter the username used here. This name can be up to 15 characters long.
all_users - All user accounts in local DB will be deleted.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete a WAC local user:

```
DAS-3626:admin#delete wac user user123
Command: delete wac user user123

Success.

DAS-3626:admin#
```

54-10 config wac user

Description

This command is used to update the local user DB. Only created user can be configured

Format

config wac user <username 15> [vlan <vlan_name 32> | vlanid <vlanid 1-4094> | clear_vlan]

Parameters

<username 15> - Enter the username used here. This name can be up to 32 characters long.
vlan - Specifies the VLAN name for authenticated host which uses this user account to pass authentication. **<vlan_name 32>** - Enter the name of the VLAN here. This name can be up to 32 characters long.
vlanid - Specifies target VLAN ID for authenticated host which uses this user account to pass authentication. **<vlanid 1-4094>** - Enter the VLAN ID used here. This value must be between 1 and 4094.
clear_vlan - Specifies that the VLAN details for the specified user will be cleared.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure WAC local user:

```
DAS-3626:admin#config wac user Jim vlanid 3
Command: config wac user Jim vlanid 3

Enter a old password:***
Enter a case-sensitive new password:****
Enter the new password again for confirmation:****
Success.

DAS-3626:admin#
```

54-11 show wac

Description

This command is used to display the WAC global setting.

Format

show wac

Parameters

None.

Restrictions

None.

Example

Show global configuration about WAC:

```
DAS-3626:admin#show wac
Command: show wac

 Web-based Access Control
 --------------------------------
 State                   : Enabled
 Method                  : RADIUS
 Redirect Path           : http://www.dlink.com
 Virtual IP              : 1.1.1.1
 Switch HTTP Port        : 80 (HTTP)
 RADIUS Authorization    : Enabled
 Local Authorization     : Enabled

DAS-3626:admin#
```

54-12 show wac ports

Description

This command is used to display the port level setting.

Format

show wac ports {<portlist>}

Parameters

<portlist> - (Optional) Enter a list of ports to display here.

Restrictions

None.

Example

To show WAC port state and other parameters:

```
DAS-3626:admin#show wac ports 1-3
Command: show wac ports 1-3

 Port    State        Aging Time    Idle Time      Block Time
                        (min)         (min)          (sec)
 -----  --------    -------------  -------------  -------------
 1      Enabled     1440           Infinite       60
 2      Enabled     1440           Infinite       60
 3      Enabled     1440           Infinite       60

DAS-3626:admin#
```

54-13 show wac user

Description

This command is used to show web authentication account.

Format

show wac user

Parameters

None.

Restrictions

None.

Example

To show WAC local user:

```
DAS-3626:admin#show wac user
Command: show wac user

 User Name          Password           VID
 -----------------  -----------------  ---------
   Jim                jim3               3

 Total Entries:1


DAS-3626:admin#
```

54-14 show wac auth_state

Description

This command is used to display the authentication state of a port.

Format

show wac auth_state ports {<portlist>}

Parameters

<portlist> - (Optional) Enter a list of ports to display here.

Restrictions

None.

Example

Supposed that port 1 is in host-based mode:

1. MAC 00-00-00-00-00-01 is authenticated without VLAN assigned (may be the specified target VLAN does not exist or target VLAN has not been specified at all), the ID of RX VLAN will be displayed (RX VLAN ID is 20 and the assigned VLAN ID is 4004 in this example).
2. MAC 00-00-00-00-00-02 is authenticated with target VLAN assigned, the ID of target VLAN will be displayed (RX VLAN ID is 20 and the assigned VLAN ID is 1234 in this example).
3. MAC 00-00-00-00-00-03 failed to pass authentication, the VID field will be shown as "-" indicating that packets with SA 00-00-00-00-00-03 will be dropped no matter which VLAN these packets are from.
4. MAC 00-00-00-00-00-04 attempts to start authentication, the VID field will be shown as "-" until authentication completed.

Supposed that ports 2 and 3 are in port-based mode:

1. MAC 00-00-00-00-00-10 is the MAC which made port 2 pass authentication; MAC address is followed by "(P)" to indicate the port-based mode authentication. Supposed that port 3 is in port-based mode:
2. MAC 00-00-00-00-00-20 attempts to start authentication, MAC address is followed by "(P)" to indicate the port-based mode authentication.
3. MAC 00-00-00-00-00-21 failed to pass authentication, MAC address is followed by "(P)" to indicate the port-based mode authentication.

```
DAS-3626:admin# show wac auth_state ports 1-3
Command: show wac auth_state ports 1-3

P:Port-based Pri: Priority

Port    MAC Address          Original  State        VID Pri Aging Time/ Idle
                                 RX VID                          Block Time
Time
------ ------------------- ---- ------------- ---- -- ----------- ----
1      00-00-00-00-00-01      20   Authenticated   -   3  Infinite    40
1      00-00-00-00-00-02      20   Authenticated  1234 -  Infinite    50
1      00-00-00-00-00-03    4004   Blocked          -    -  60           -
1      00-00-00-00-00-04    4004   Authenticating  -    -  10           -
2      00-00-00-00-00-10(P) 2040   Authenticated  1234 2  1440         20
3      00-00-00-00-00-20(P) 2045   Authenticating  -    -  5            -
3      00-00-00-00-00-21(P) 2045   Blocked          -    -  100          -

Total Authenticating Hosts :2
Total Authenticated Hosts  :3
Total Blocked Hosts        :2

DAS-3626:admin#
```

54-15 clear wac auth_state

Description

This command is used to clear the authentication state of a port. If the port is port-based mode, the port will return to un-authenticated state. The entire timer associated with the port will be reset.

If the port is host based mode, users on this port will be cleared. The user needs to be re-authenticated to access the network.

Format

clear wac auth_state [ports [<portlist> | all] {authenticated | authenticating | blocked} | macaddr <macaddr>]

Parameters

ports - Specifies the list of ports whose WAC state will be cleared.	
	<portlist> - Enter a list of ports used for the configuration here.
	all - Specifies that all the ports will be used for this configuration.
	authenticated - (Optional) Specified to clear all authenticated users for a port.
	authenticating - (Optional) Specified to clear all authenticating users for a port.
	blocked - (Optional) Specified to clear all blocked users for a port.
macaddr - Specifies the MAC address of the users to be cleared.	
	<macaddr> - Enter the MAC address of the users to be cleared here.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete WAC hosts on ports 1 to 5:

```
DAS-3626:admin# clear wac auth_state ports 1-5
Command: clear wac auth_state ports 1-5

Success.

DAS-3626:admin#
```

Appendix A System Log Entries

The following table lists all possible entries and their corresponding meanings that will appear in the System Log of this Switch.

Category	Event Description	Log Information	Severity	Remark
System	System started up	**System started up**	Critical	
	Configuration saved to flash	**Configuration saved to flash by console (Username: <username>,)**	Informational	
	Configuration saved to flash	**Configuration saved to flash (Username: <username>, IP: <ipaddr>)**	Informational	For Telnet and SSH
	Configuration and log saved to flash	**Configuration and log saved to flash by console (Username: <username>)**	Informational	
	Configuration and log saved to flash	**Configuration and log saved to flash (Username: <username>, IP: <ipaddr>)**	Informational	For Telnet and SSH
	Internal AC Power failed	**Internal AC Power Failed**	Critical	
	Internal AC Power is recovered	**Internal AC Power is recovered**	Critical	
	Internal DC Power failed	**Internal DC Power Failed**	Critical	
	Internal DC Power is recovered	**Internal DC Power is recovered**	Critical	
Up/Down-load	Firmware upgraded successfully	**Firmware upgraded by console successfully (Username: <username>)**	Informational	
	Firmware upgraded successfully	**Firmware upgraded by telnet/SSH was successfully (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational	For Telnet/SSH
	Firmware upgrade was unsuccessful	**Firmware upgrade by console was unsuccessful! (Username: <username>)**	Warning	
	Firmware upgrade was unsuccessful	**Firmware upgrade by telnet/SSH was successful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Warning	For Telnet/SSH

	Configuration successfully downloaded	**Configuration successfully downloaded by console (Username: <username>)**	Informational	
	Configuration successfully downloaded	**Configuration successfully downloaded by telnet/SSH name: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational	For Telnet/SSH
	Configuration download was unsuccessful	**Configuration download by console was unsuccessful! (Username: <username>)**	Warning	
	Configuration download was unsuccessful	**Configuration download by telnet/ SSH was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Warning	For Telnet/SSH
	Configuration successfully uploaded	**Configuration successfully uploaded by console (Username: <username>)**	Informational	
	Configuration successfully uploaded	**Configuration successfully uploaded by telnet/ SSH (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational	For Telnet/SSH
	Configuration upload was unsuccessful	**Configuration upload by console was unsuccessful! (Username: <username>)**	Warning	
	Configuration upload was unsuccessful	**Configuration upload by telnet/SSH was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Warning	For Telnet/SSH
	Log message successfully uploaded	**Log message successfully uploaded by console (Username: <username>)**	Informational	
	Log message successfully uploaded	**Log message successfully uploaded by telnet/ssh(Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational	For Telnet/SSH
	Log message upload was unsuccessful	**Log message upload by console was unsuccessful! (Username: <username>)**	Warning	
	Log message upload was unsuccessful	**Log message upload by telnet/SSH was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Warning	For Telnet/SSH
Interface	Port link up	**Port <portNum> link up, <link state>**	Informational	link state, for ex: , 100Mbps FULL duplex
	Port link down	**Port <portNum> link down**	Informational	
Console	Successful login through Console	**Successful login through Console (Username: <username>)**	Informational	
	Login failed	**Login failed through Console**	Warning	

	through Console	**(Username: <username>)**		
	Logout through Console	**Logout through Console (Username: <username>)**	Informational	
	Console session timed out	**Console session timed out (Username: <username>)**	Informational	
Web	Successful login through Web	**Successful login through Web (Username: <username>, IP: <ipaddr>)**	Informational	
	Login failed through Web	**Login failed through Web (Username: <username>, IP: <ipaddr>)**	Warning	
	Logout through Web	**Logout through Web (Username: <username>, IP: <ipaddr>)**	Informational	
	Web session timed out	**Web session timed out (Username:<username>, IP: <ipaddr>)**	Informational	
	Successful login through Web (SSL)	**Successful login through Web (SSL) (Username: <username>, IP: <ipaddr>)**	Informational	
	Login failed through Web (SSL)	**Login failed through Web (SSL) (Username: <username>, IP: <ipaddr>)**	Warning	
	Logout through Web (SSL)	**Logout through Web (SSL) (Username: <username>, IP: <ipaddr>)**	Informational	
	Web (SSL) session timed out	**Web (SSL) session timed out (Username: <username>, IP: <ipaddr>)**	Informational	
Telnet	Successful login through Telnet	**Successful login through Telnet (Username: <username>, IP: <ipaddr>)**	Informational	
	Login failed through Telnet	**Login failed through Telnet (Username: <username>, IP: <ipaddr>)**	Warning	
	Logout through Telnet	**Logout through Telnet (Username: <username>, IP: <ipaddr>)**	Informational	
	Telnet session timed out	**Telnet session timed out (Username: <username>, IP: <ipaddr>)**	Informational	
STP	Topology changed	**Topology changed**	Informational	Detected Topology changed port
	New Root selected	**New Root bridge selected (MAC: <macaddr>, Priority: <int>)**	Informational	root bridge MAC address and priority at the instance
SSH	Successful login through SSH	**Successful login through SSH (Username: <username>, IP: <ipaddr>)**	Informational	
	Login failed	**Login failed through SSH (Username: <username>, IP:**	Warning	

	through SSH	**<ipaddr>)**		
	Logout through SSH	**Logout through SSH (Username: <username>, IP: <ipaddr>)**	Informational	
	SSH session timed out	**SSH session timed out (Username: <username>, IP: <ipaddr>)**	Informational	
AAA	Successful login through Web authenticated by AAA local method	**Successful login through Web from <userIP> authenticated by AAA local method (Username: <username>)**	Informational	
	Login failed through Web authenticated by AAA local method	**Login failed through Web from <userIP> authenticated by AAA local method (Username: <username>)**	Warning	
	Successful login through Web (SSL) authenticated by AAA local method	**Successful login through Web (SSL) from <userIP> authenticated by AAA local method (Username: <username>)**	Informational	
	Login failed through Web (SSL) authenticated by AAA local method	**Login failed through Web (SSL) from <userIP> authenticated by AAA local method (Username: <username>)**	Warning	
	Successful login through Telnet authenticated by AAA local method	**Successful login through Telnet from <userIP> authenticated by AAA local method (Username: <username>)**	Informational	
	Login failed through Telnet authenticated by AAA local method	**Login failed through Telnet from <userIP> authenticated by AAA local method (Username: <username>)**	Warning	
	Successful login through SSH authenticated by AAA local method	**Successful login through SSH from <userIP> authenticated by AAA local method (Username: <username>)**	Informational	
	Login failed through SSH authenticated by AAA local method	**Login failed through SSH from <userIP> authenticated by AAA local method (Username: <username>)**	Warning	
	Successful login through Web authenticated by AAA none method	**Successful login through Web from <userIP> authenticated by AAA none method (Username: <username>)**	Informational	

	Successful login through Web (SSL) authenticated by AAA none method	**Successful login through Web (SSL) from <userIP> authenticated by AAA none method (Username: <username>)**	Informational	
	Successful login through Telnet authenticated by AAA none method	**Successful login through Telnet from <userIP> authenticated by AAA none method (Username: <username>)**	Informational	
	Successful login through SSH authenticated by AAA none method	**Successful login through SSH from <userIP> authenticated by AAA none method (Username: <username>)**	Informational	
	Successful login through Web authenticated by AAA server	**Successful login through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Informational	
	Login failed through Web authenticated by AAA server	**Login failed through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Warning	
	Login failed through Web due to AAA server timeout or improper configuration	**Login failed through Web from <userIP> due to AAA server timeout or improper configuration (Username: <username>)**	Warning	
	Successful login through Web (SSL) authenticated by AAA server	**Successful login through Web(SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Informational	
	Login failed through Web (SSL) authenticated by AAA server	**Login failed through Web (SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Warning	
	Login failed through Web (SSL) due to AAA server timeout or improper configuration	**Login failed through Web (SSL) from <userIP> due to AAA server timeout or improper configuration (Username: <username>)**	Warning	
	Successful login through Telnet authenticated by AAA server	**Successful login through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Informational	
	Login failed through Telnet authenticated by	**Login failed through Telnet from <userIP> authenticated by AAA server <serverIP> (Username:**	Warning	

	AAA server	**<username>)**		
	Successful login through SSH authenticated by AAA server	**Successful login through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Informational	
	Successful Enable Admin through Web authenticated by AAA local_enable method	**Successful Enable Admin through Web from <userIP> authenticated by AAA local_enable method (Username: <username>)**	Informational	
	Enable Admin failed through Web authenticated by AAA local_enable method	**Enable Admin failed through Web from <userIP> authenticated by AAA local_enable method (Username: <username>)**	Warning	
	Successful Enable Admin through Telnet authenticated by AAA local_enable method	**Successful Enable Admin through Telnet from <userIP> authenticated by AAA local_enable method (Username: <username>)**	Informational	
	Successful Enable Admin through SSH authenticated by AAA local_enable method	**Successful Enable Admin through SSH from <userIP> authenticated by AAA local_enable method (Username: <username>)**	Informational	
	Enable Admin failed through SSH authenticated by AAA local_enable method	**Enable Admin failed through SSH from <userIP> authenticated by AAA local_enable method (Username: <username>)**	Warning	
	Successful Enable Admin through Web authenticated by AAA none method	**Successful Enable Admin through Web from <userIP> authenticated by AAA none method (Username: <username>)**	Informational	
	Successful Enable Admin through Web (SSL) authenticated by AAA none method	**Successful Enable Admin through Web (SSL) from <userIP> authenticated by AAA none method (Username: <username>)**	Informational	
	Successful Enable Admin	**Successful Enable Admin through Telnet from <userIP>**	Informational	

	through Telnet authenticated by AAA none method	**authenticated by AAA none method (Username: <username>)**		
	Successful Enable Admin through SSH authenticated by AAA none method	**Successful Enable Admin through SSH from <userIP> authenticated by AAA none method (Username: <username>)**	Informational	
	Successful Enable Admin through Web authenticated by AAA server	**Successful Enable Admin through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Informational	
	Enable Admin failed through Web authenticated by AAA server	**Enable Admin failed through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Warning	
	Enable Admin failed through Web due to AAA server timeout or improper configuration	**Enable Admin failed through Web from <userIP> due to AAA server timeout or improper configuration (Username: <username>)**	Warning	
	Successful Enable Admin through Web (SSL) authenticated by AAA server	**Successful Enable Admin through Web (SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Informational	
	Enable Admin failed through Web (SSL) authenticated by AAA server	**Enable Admin failed through Web (SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Warning	
	Enable Admin failed through Web (SSL) due to AAA server timeout or improper configuration	**Enable Admin failed through Web (SSL) from <userIP> due to AAA server timeout or improper configuration (Username: <username>)**	Warning	
	Successful Enable Admin through Telnet authenticated by AAA server	**Successful Enable Admin through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Informational	
	Enable Admin failed through Telnet authenticated by AAA server	**Enable Admin failed through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Warning	

	Enable Admin failed through Telnet due to AAA server timeout or improper configuration	**Enable Admin failed through Telnet from <userIP> due to AAA server timeout or improper configuration (Username: <username>)**	Warning	
	Successful Enable Admin through SSH authenticated by AAA server	**Successful Enable Admin through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Informational	
	Enable Admin failed through SSH authenticated by AAA server	**Enable Admin failed through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>)**	Warning	
	Enable Admin failed through SSH due to AAA server timeout or improper configuration	**Enable Admin failed through SSH from <userIP> due to AAA server timeout or improper configuration (Username: <username>)**	Warning	
IP-MAC-PORT Binding	Unauthenticated IP address and discard by IP MAC port binding	**Unauthenticated IP-MAC address and discarded by IMPB (IP: <ipaddr>, MAC: <macaddr>, Port < portNum>)**	Warning	
	Dynamic IMPB entry is conflict with static FDB	**Dynamic IMPB entry is conflict with static FDB (IP:<ipaddr>, MAC:<macaddr>, Port<portNum>)**	Warning	
	Dynamic IMPB entry is conflict with static ARP	**Dynamic IMPB entry is conflict with static ARP (IP:<ipaddr>, MAC:<macaddr>, Port<portNum>)**	Warning	
	Dynamic IMPB entry is conflict with static IMPB	**Dynamic IMPB entry is conflict with static IMPB (IP:<ipaddr>, MAC:<macaddr>, Port<portNum>)**	Warning	
	Creating IMPB entry Failed due to no ACL rule available	**Creating IMPB entry Failed due to no ACL rule available(IP:<ipaddr>, MAC:<macaddr>, Port<portNum>)**	Warning	
	Port enter IMPB block state	**Port <portNum> enter IMPB block state**	Warning	
	Port recover from IMPB block state	**Port <portNum> recover from IMPB block state**	Warning	
Packet Storm	Broadcast storm occurrence	**Port <portNum> Broadcast storm is occurring**	Warning	
	Broadcast storm cleared	**Port <portNum> Broadcast storm has cleared**	Informational	

	Multicast storm occurrence	**Port <portNum> Multicast storm is occurring**	Warning	
	Multicast storm cleared	**Port <portNum> Multicast storm has cleared**	Informational	
	Port shut down due to a packet storm	**Port <portNum> is currently shut down due to a packet storm**	Warning	
Loopback Detection	Port loop occurred	**Port <portNum> LBD loop occurred. Port blocked.**	Critical	
	Port loop detection restarted after interval time	**Port <portNum> LBD port recovered. Loop detection restarted.**	Informational	
	Port with VID loop occurred	**Port <portNum> VID vlanID> LBD loop occurred. Packet discard begun.**	Critical	
	Port with VID Loop detection restarted after interval time	**Port <portNum> VID <vlanID> LBD recovered. Loop detection restarted.**	Informational	
DHCP	Detect untrusted DHCP server IP address	**Detected untrusted DHCP server(IP: <ipaddr>, Port: <portNum>)**	Informational	
MBAC	Login OK	**MAC-based Access Control host login successful (MAC: <macaddr>, port: <portNum>, VID: <vlanID>)**	Informational	
	Login Fail	**MAC-based Access Control unauthenticated host (MAC: <macaddr>, port: <portNum>, VID: <vlanID>)**	Warning	
	Aged out	**MAC-based Access Control host aged out (MAC: <macaddr>, port: <portNum>, VID: <vlanID>)**	Informational	

Appendix B Trap Log Entries

This table lists the trap logs found on the Switch.

Log Entry	Description	ID
coldStart	A coldStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself and that its configuration may have been altered.	1.3.6.1.6.3.1.1.5.1
warmStart	A warmStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself such that its configuration is unaltered.	1.3.6.1.6.3.1.1.5.2
linkDown	A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.	1.3.6.1.6.3.1.1.5.3
linkUp	A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus.	1.3.6.1.6.3.1.1.5.4
authenticationFailure	An authenticationFailure trap signifies that the SNMP entity has received a protocol message that is not properly authenticated. While all implementations of SNMP entities MAY be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.	1.3.6.1.6.3.1.1.5.5
risingAlarm	This trap is an SNMP notification that is generated when a high capacity alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps.	1.3.6.1.2.1.16.29.2.0.1
fallingAlarm	This trap is an SNMP notification	1.3.6.1.2.1.16.29.2.0.2

	that is generated when a high capacity alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps.	
newRoot	The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon action of the Topology Change Timer immediately subsequent to its election. Implementation of this trap is optional.	1.3.6.1.2.1.17.0.1
topologyChange	A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a newRoot trap is sent for the same transition. Implementation of this trap is optional.	1.3.6.1.2.1.17.0.2
xdsl2LinePerfFECSThreshXtuc	This notification indicates that the FEC seconds threshold has been reached/exceeded for the referred XTU-C.	1.3.6.1.4.1.171.12.54.10.1.0.1
xdsl2LinePerfFECSThreshXtur	This notification indicates that the FEC seconds threshold has been reached/exceeded for the referred XTU-R	1.3.6.1.4.1.171.12.54.10.1.0.2
xdsl2LinePerfESThreshXtuc	This notification indicates that the errored seconds threshold has been reached/exceeded for the referred XTU-C.	1.3.6.1.4.1.171.12.54.10.1.0.3
xdsl2LinePerfESThreshXtur	This notification indicates that the errored seconds threshold has been reached/exceeded for the referred XTU-R.	1.3.6.1.4.1.171.12.54.10.1.0.4
xdsl2LinePerfSESThreshXtuc	This notification indicates that the severely-errored seconds threshold has been reached/exceeded for the referred XTU-C.	1.3.6.1.4.1.171.12.54.10.1.0.5
xdsl2LinePerfSESThreshXtur	This notification indicates that the severely-errored seconds threshold has been reached/exceeded for the referred XTU-R.	1.3.6.1.4.1.171.12.54.10.1.0.6
xdsl2LinePerfLOSSThreshXtuc	This notification indicates that the LOS seconds threshold has been reached/exceeded for the referred XTU-C.	1.3.6.1.4.1.171.12.54.10.1.0.7

xdsl2LinePerfLOSSThreshXtur	This notification indicates that the LOS seconds threshold has been reached/exceeded for the referred XTU-R.	1.3.6.1.4.1.171.12.54.10.1.0.8
xdsl2LinePerfUASThreshXtuc	This notification indicates that the unavailable seconds threshold has been reached/exceeded for the referred XTU-C.	1.3.6.1.4.1.171.12.54.10.1.0.9
xdsl2LinePerfUASThreshXtur	This notification indicates that the unavailable seconds threshold has been reached/exceeded for the referred XTU-R.	1.3.6.1.4.1.171.12.54.10.1.0.10
xdsl2LinePerfCodingViolationsThreshXtuc	This notification indicates that the coding violations threshold has been reached/exceeded for the referred XTU-C.	1.3.6.1.4.1.171.12.54.10.1.0.11
xdsl2LinePerfCodingViolationsThreshXtur	This notification indicates that the coding violations threshold has been reached/exceeded for the referred XTU-R.	1.3.6.1.4.1.171.12.54.10.1.0.12
xdsl2LinePerfCorrectedThreshXtuc	This notification indicates that the corrected blocks(FEC events) threshold has been reached/exceeded for the referred XTU-C.	1.3.6.1.4.1.171.12.54.10.1.0.13
xdsl2LinePerfCorrectedThreshXtur	This notification indicates that the corrected blocks(FEC events) threshold has been reached/exceeded for the referred XTU-R.	1.3.6.1.4.1.171.12.54.10.1.0.14
xdsl2LinePerfFailedFullInitThresh	This notification indicates that the failed full initializations threshold has been reached/exceeded for the referred ADSL/ADSL2 or ADSL2 line.	1.3.6.1.4.1.171.12.54.10.1.0.15
xdsl2LinePerfFailedShortInitThresh	This notification indicates that the failed short initializations threshold has been reached/exceeded for the referred VDSL2/ADSL/ADSL2 or ADSL2+ line.	1.3.6.1.4.1.171.12.54.10.1.0.16
xdsl2LineStatusChangeXtuc	This notification indicates that a status change is detected for the referred XTU-C.	1.3.6.1.4.1.171.12.54.10.1.0.17
xdsl2LineStatusChangeXtur	This notification indicates that a status change is detected for the referred XTU-R.	1.3.6.1.4.1.171.12.54.10.1.0.18
agentCpuThreshold	CPU threshold notification.	1.3.6.1.4.1.171.12.1.4.2.0.5
agentMemoryThreshold	Memory threshold notification.	1.3.6.1.4.1.171.12.1.4.2.0.6

agentPktBufferThreshold	Packet buffer threshold notification.	1.3.6.1.4.1.171.12.1.4.2.0.7
swPowerStatusChg	Power Status change notification.	1.3.6.1.4.1.171.12.11.2.2.2.0.1
swPowerFailure	Power Failure notification.	1.3.6.1.4.1.171.12.11.2.2.2.0.2
swPowerRecover	Power Recover notification.	1.3.6.1.4.1.171.12.11.2.2.2.0.3
swFanFailure	Fan Failure notification	1.3.6.1.4.1.171.12.11.2.2.3.0.1
swFanRecover	Fan Recover notification	1.3.6.1.4.1.171.12.11.2.2.3.0.2
swFanSlotUp	The trap is sent whenever the fan slot is connected and working.	1.3.6.1.4.1.171.12.11.2.2.3.0.3
swFanSlotDown	The trap is sent whenever the fan slot is disconnected or malfunctions.	1.3.6.1.4.1.171.12.11.2.2.3.0.4
swHighTemperature	High Temperature notification	1.3.6.1.4.1.171.12.11.2.2.4.0.1
swHighTemperatureRecover	High Temperature notification.	1.3.6.1.4.1.171.12.11.2.2.4.0.2
swLowTemperature	Low Temperature notification.	1.3.6.1.4.1.171.12.11.2.2.4.0.3
swLowTemperatureRecover	Low Temperature notification.	1.3.6.1.4.1.171.12.11.2.2.4.0.4
swDdmAlarmTrap	The trap is sent when any parameter value exceeds the alarm threshold value or recover to normal status depending on the configuration of the trap action.	1.3.6.1.4.1.171.12.72.4.0.1
swDdmWarningTrap	The trap is sent when any parameter value exceeds the warning threshold value or recover to normal status depending on the configuration of the trap action.	1.3.6.1.4.1.171.12.72.4.0.2
vdslPerfLofsThreshNotification	Loss of Framing 15-minute interval threshold (vdslLineAlarmConfThresh15MinLofs) reached.	1.3.6.1.2.1.10.97.1.0.1
vdslPerfLossThreshNotification	Loss of Signal 15-minute interval threshold (vdslLineAlarmConfThresh15MinLoss) reached.	1.3.6.1.2.1.10.97.1.0.2
vdslPerfLprsThreshNotification	Loss of Power 15-minute interval threshold (vdslLineAlarmConfThresh15MinLprs) reached.	1.3.6.1.2.1.10.97.1.0.3
vdslPerfLolsThreshNotification	Loss of Link 15-minute interval threshold (vdslLineAlarmConfThresh15MinLols) reached.	1.3.6.1.2.1.10.97.1.0.4
vdslPerfESsThreshNotifica	Errored Seconds 15-minute interval threshold	1.3.6.1.2.1.10.97.1.0.5

tion	(vdslLineAlarmConfThresh15MinESs) reached.	
vdslPerfSESsThreshNotification	Severely Errored Seconds 15-minute interval threshold (vdslLineAlarmConfThresh15MinSESs) reached.	1.3.6.1.2.1.10.97.1.0.6
vdslPerfUASsThreshNotification	Unavailable Seconds 15-minute interval threshold (vdslLineAlarmConfThresh15MinUASs) reached.	1.3.6.1.2.1.10.97.1.0.7
vdslDownMaxSnrMgnNotification	The downstream Signal to Noise Margin exceeded vdslLineConfDownMaxSnrMgn. The object vdslPhysCurrSnrMgn will contain the Signal to Noise margin as measured by the VTU-R.	1.3.6.1.2.1.10.97.1.0.8
vdslDownMinSnrMgnNotification	The downstream Signal to Noise Margin fell below vdslLineConfDownMinSnrMgn. The object vdslPhysCurrSnrMgn will contain the Signal to Noise margin as measured by the VTU-R.	1.3.6.1.2.1.10.97.1.0.9
vdslUpMaxSnrMgnNotification	The upstream Signal to Noise Margin exceeded vdslLineConfUpMaxSnrMgn. The object vdslPhysCurrSnrMgn will contain the Signal to Noise margin as measured by the VTU-C.	1.3.6.1.2.1.10.97.1.0.10
vdslUpMinSnrMgnNotification	The upstream Signal to Noise Margin fell below vdslLineConfUpMinSnrMgn. The object vdslPhysCurrSnrMgn will contain the Signal to Noise margin as measured by the VTU-C.	1.3.6.1.2.1.10.97.1.0.11
vdslInitFailureNotification	Vtu initialization failed. See vdslPhysCurrStatus for potential reasons.	1.3.6.1.2.1.10.97.1.0.12