xStack DGS-3610 Series

Configuration Guide

Version 10.2

D-Link®

DGS-3610 Series Configuration Guide

Revision No.: Version 10.2

Date:

Copyright Statement

Preface

Version Description

This manual matches the firmware version v10.2.

Target Readers

This manual is intended for the following readers:

- Network engineers
- Technical salespersons
- Network administrators

Conventions in this Document

1. Universal Format Convention

Arial: Arial with the point size 10 is used for the body.

A line is added respectively above and below the prompts such as **caution** and **note** to separate them from the body.

Format of information displayed on the terminal: Courier New, point size 8, indicating the screen output. User's entries among the information shall be indicated with characters in bold.

2. Command Line Format Convention

Arial is used as the font for the command line. The meanings of specific formats are described below:

Bold: Key words in the command line (which shall be entered exactly as they are displayed), shall be indicated with characters in bold.

Italic: Parameters in the command line (which must be replaced with actual values), shall be indicated with italic characters.

[ ]: The part enclosed with [ ] is optional in the command.

{ x | y | ... }: It means one shall be selected among two or more options.

[x | y | ...]: It means one or none shall be selected among two or more options.

//: A Line starting with a double slash "//" is a comment line.

3. Signs

Various striking identifiers are adopted in this manual to indicate the matters that special attention should be paid in the operation, as detailed below:

⚠ **Caution**	Warning, danger or alert in the operation.

✎ **Note**	Description, prompt, tip or any other necessary supplement or explanation for the operation.

✎ **Note**	1. The port types described in the examples in this manual may not be consistent with the actual types. During actual operations, configuration should be made according to the type of ports supported by various products. 2. The display information in some examples in this manual may include the content of other product series (such as the product model and description). For the concrete display information, refer to actual device information used.

Contents

1 Command Line Interface Configuration

This chapter describes how to use the command line interface. You can also manage the equipment using the command line interface.

This chapter covers the following:

- Command Mode
- Obtaining Help
- Abbreviating Commands
- Using **no** and **default** Options
- Understanding CLI Prompt Messages
- Using History Commands
- Using Editing Features
- Filtration and Lookup of CLI Output Information
- Accessing CLI

1.1 Command Mode

The management interface of DGS-3610 series is classfied to several modes. The command mode that users are in determines the commands to be used.

After you input a question mark (?) under the command prompt, the commands will be listed in each command mode.

When a new session connection is set up between user and the switch management interface, you are in user EXEC mode first and can use commands in this mode. In the user EXEC mode, only a few commands are usable with limited functions, for example, the **show** command. The results of using commands in user EXEC mode are not saved.

To use all commands, you firstly need to enter privileged EXEC mode. Usualy, you need input the password of privileged EXEC mode for you to enter the privileged mode. In privileged EXEC mode, you can use all privileged commands and thus enter the global configuration mode.

Using commands in configuration mode (global configuration mode, interface configuration mode, and so on) may affect the current configuration. If you have saved the configuration information, these commands will be saved and re-executed when the system is restarted.

To enter any of the configuration modes, first enter global configuration mode. From global configuration mode, you can access any of the configuration sub-modes like interface configuration mode.

The following table lists the command modes, how to access each mode, prompts of the mode, and how to exit the modes. Suppose the equipment is named "DGS-3610" by default.

Summary of command modes:

Command mode	**Access method**	**Prompt**	**Exit or access next mode**	**About this mode**
User EXEC (User Mode)	To access the network equipment ,first enter this mode.	DGS-3610 >	Input the **exit** command to exit this mode. To enter privileged EXEC mode, input the **enable** command.	This mode is used for basic test and showing system information
Privileged EXEC (Privileged mode)	From user EXEC mode, input the **enable** command to enter this mode.	DGS-3610 #	To return to the user EXEC mode, input **disable** command. To enter global configuration mode, input the **configure** command.	This mode is used to verify the results after setting a command. This mode is protected with password.
Global configuration (Global configuration mode.)	From privileged EXEC mode, input the **configure** command to enter to this mode.	DGS-3610 (config)#	To exit global configuration command mode and to return to privileged EXEC mode, input the **end** or **exit** command, or press Ctrl-C. To access the interface configuration mode, input the **interface** command. You must indicate to enter to the interface configuration sub_mode in the **interface** command. To access the VLAN configuration mode, input the **vlan** vlan_id command.	Commands in this mode are used for configuring the global parameters that can affect the whole network equipment.

Command mode	**Access method**	**Prompt**	**Exit or access next mode**	**About this mode**
Interface configuration (Interface configuration mode)	Input the interface command to enter to this mode in the global configuration mode:	DGS-3610 (config-if)#	To return to Privileged EXEC mode, input **end** command or **Ctrl+C.** To return to Global configuration mode, input **exit** command . You must indicate to enter to the interface configuration sub_mode in the **interface** command.	Configure various interfaces of the network equipment in this mode.
Config-vlan (Vlan configuration Mode)	In the global configuration mode, input the **vlan** *vlan-id* to access this mode:	DGS-3610 (config-vlan)#	To return to Privileged EXEC mode, input **end** or **Ctrl+C.** To return to Global configuration mode, enter **exit**.	This mode is to used for setting VLAN parameters.

1.2 Obtaining Help

You may list the commands supported in each command mode by inputting a question mark (?) at the prompt. You can also list command keywords beginning with the same character or parameters of each command. See following table.

Command	**Description**
Help	Obtain brief description from the help system in any command mode.
abbreviated-command-entry?	Obtains a character string of command keywords beginning with the same. Example: DGS-3610# **di?** dir disable
abbreviated-command-entry<Tab>	Obtains complete keywords of commands. Example: DGS-3610# **show conf<Tab>** DGS-3610# **show configuration**
?	Lists the next keyword associated to the command. Example: DGS-3610# **show ?**

Command	Description
command keyword ?	Lists the next variable associated with the keyword. Example: DGS-3610(config)# **snmp-server** **community ?** WORD SNMP community string

1.3 Abbreviating Commands

To abbreviate a command, simply enter part of the command keyword, but this part should uniquely identify the command keyword.

For example, **show configuration** can be abbreviated to:

```
DGS-3610# show conf
```

1.4 Using no and default Options

Almost all commands have the **no** option. Generally, the **no** option is used to prohibit a feature or function or to perform a reversed action of the command. For example, the interface configuration command **no shutdown** can be executed the reversed operation for disabling the interface command **shutdown**, that is to enable the interface. Use the keyword without **no** option to ebable the features enabled or to enable the features disabled by default.

Most configuration commands have the **default** option, which restores the configuration as default value of the command. Most commands are disabled by default; in this case, the function of **default** and **no** options generally serve the same purpose. However, the default value of part commands are enabled; in this case the **default** and **no** options serve the reversed purposes. The **default** option is used to enable the command and set the variables as enabled status as it is default.

1.5 Understanding CLI Prompt Messages

The following table lists the error prompt messages when user is using the CLIs to manage the network equipments.

Common CLI error messages

Error message	Meaning	How to obtain help
% Ambiguous command: "show c"	If you input insufficient characters, the network equipment can not identify the only command.	Re-input the command and a question mark immediately after the ambiguous word. The possible keywords will be displayed.
% Incomplete command.	User has not input the required keywords or the variable of a command.	Re-input the command and a space followed by a question mark. The possible keywords or variables will be displayed.
% Invalid input detected at '^' marker.	The symbol "^" will indicate the position of the wrong words when user inputs a wrong command,.	Input a question mark at the command prompt to show the allowed command keyword.

1.6 Using History Commands

The system provides a record of the commands you have input. This feature will be very useful when a long and complex commands is re-input.

To re-execute the commands you have input from the history record, perform the following operations.

Operation	Result
Ctrl-P or **Up**	Allows you to browse the previous command in the history record. Repeat this action to find earlier records starting from the latest one.
Ctrl-N or **Down**	After using **Ctrl-P** or **Up**, this operation allows you to return to a more recent command in the history record. To find more recent records, repeat this operation.

1.7 Using Editing Features

This section describes the editing functions that may be used for command line edit, including:

- Edit Shortcut Keys
- Sliding Window of Command Line

1.7.1 Edit Shortcut Keys

The following table lists the edit shortcut keys.

Function	Shortcut Key	Description
Move cursor in editing line	Left direction key or Ctrl-B	Move the cursor left by one character.
	Right direction key or Ctrl-F	Move the cursor right by one character.
	Ctrl-A	Move the cursor to the beginning of the command line.
	Ctrl-E	Move the cursor to the end of the command line.
Delete the entered characters	Backspace	Delete the character to the left of the cursor.
	Delete	Delete the character where the cursor is located.
Scroll up by one line or one page	Return	Scroll up the displayed contents by one line and make the next line appear. Used only before the end of the output.
	Space	Scroll up the displayed contents by one page and make the next page appear. Used only before the end of the output.

1.7.2 Sliding Window of Command Line

You can use the feature of the sliding window to edit the commands that exceed the length of one line so as to extend the length of the command line. When the editing cursor closes to the right border, the whole command line will move to the left by 20 characters. In this case, the cursor can still be moved back to the previous character or the beginning of the command line.

When editing a command line, you can move the cursor using the shortcut keys in the following table:

Function	Shortcut key
Move the cursor to the left by one character	Left direction key or Ctrl-B
Move the cursor to the head of a line	Ctrl-A
Move the cursor to the right by one character	Right direction key or Ctrl-F
Move the cursor to the end of a line	Ctrl-E

For example, the contents of the command **mac-address-table static** may exceed the screen width. When the cursor approaches the line end for the first time, the whole line move left by 20 characters, and the hidden beginning part is replaced by "$" on the screen. The line moves left by 20 characters every time the cursor reaches the right border.

```
mac-address-table  static  00d0.f800.0c0c  vlan  1  interface
$tatic  00d0.f800.0c0c  vlan  1  interface  fastEthernet
$tatic  00d0.f800.0c0c  vlan  1  interface  fastEthernet  0/1
```

Now you can press **Ctrl-A** to return to the beginning of the command line. In this case, the hidden ending part is replaced by "$".

```
-address-table  static  00d0.f800.0c0c  vlan  1 interface  $
```

Note: The default line width on the terminal is 80 characters.

The sliding window combined with history commands enables you to use complicated commands repeatedly. For details about shortcut keys, see Edit Shortcut Keys.

1.8 Filtration and Lookup of CLI Output Information

1.8.1 Lookup and Filtration of Show Command

To look up the specified message in the output information from show command, you can use following commands:

Command	Description
DGS-3610# **show** *any-command* **|** **begin** *regular-expression*	Look up the specified content from the output content of the show command, to output all information of the first line that contains this content and after this line.

Caution

The information content that looks out is case sensitive, and the following is the same.

To filter the specified content in the output information from the show command, you can use following commands:

Command	Description
DGS-3610# **show** *any-command* **|** **exclude** *regular-expression*	Filter the output content from the **show** command, to output other information content, excluding the line that includes the specified content.
DGS-3610# **show** *any-command* **|** **include** *regular-expression*	Filter the output content from the show command, to only output the line that includes specified content, and other information will be filtered.

Caution

To look up and filter the output content from the show command, it is necessary to input the pipeline sign (vertical line, "|"). After the pipeline character, you can select the lookup and filtration rules and content (character or string). The content for the lookup and filtration should be case sensitive.

1.9 Using Command Alias

The system provides the command alias function, and can specify any word as the alias of the command. For example, define the word "mygateway" as the alias of "ip route 0.0.0.0 0.0.0.0 192.1.1.1".

The input of this word is equal to enter the whole following string.

You can use one word to replace one command by configuring the alias of the command. For example, create one alias to represent the front part of one command, and then you can continue to enter the following part.

The command mode that the alias represents is the one which exists in current system. In the global configuration mode, enter **Alias?** to list all command modes that can configure the alias.

```
DGS-3610(config) #alias ?
  aaa-gs              AAA server group mode
  acl                 acl configure mode
  bgp                 Configure bgp Protocol
  config              globle configure mode
......
```

The alias of command supports the help information, and it will show an asterisk (*) before the alias in the following format:

```
*command-alias=original-command
```

For example, in the EXEC mode, the default alias of command "s" indicates the keyword "show". Enter "s?" to obtain the help information on the key word and alias beginning with 's'.

```
DGS-3610#s?
*s=show  show  start-chat  start-terminal-service
```

If the command that the alias represents is more than one word, its command will be included by the quotation marks. For example, in the EXEC mode, configure alais "sv" to replace the command "show version":

```
DGS-3610#s?
*s=show  *sv="show version" show  start-chat
start-terminal-service
```

The alias must begin with the first character from the command line entered, and there should not be blank before it. As above example, it will not indicate the legal alias if the blank is entered before the command.

```
DGS-3610# s?

show    start-chat    start-terminal-service
```

The alias of command can also support the help information to obtain the parameters of the command. For example, the alias of command “ia" represents “ip address” in the configuration interface mode, it is in the interface mode:

```
DGS-3610(config-if)#ia ?

  A.B.C.D    IP address

  dhcp       IP Address via DHCP

DGS-3610(config-if)#ip address
```

Here lists the parameter information after the command “**ip address**”, and replaces the alias with the actual command.

The alias of command must be fully entered when it is used. Otherwise, it can not be identified.

Using **show aliases** command to show the aliases setting in the system.

1.10 Accessing CLI

Before using CLI, you need to first connect a terminal or PC with the equipment.CLI can be used after the equipment is started after the hardware and software are initialized. When you use the equipment for the first time, you can only connect the equipment using the serial port (Console), called Outband management. After configuration, you can connect and manage the equipment on a virtual terminal through a Telnet session. In either case, you can access the command line interface.

2 Configuration of Switch Basic Management

2.1 Overview

This chapter describes how to manage our switches:

- Access Control by Command Authorization
- Logon Authentication Control
- System Time Configuration
- Scheduled Restart
- Configuring a System Name and Command Prompt
- Banner Configuration
- Viewing System Information
- Console Rate Configuration
- Use the telnet
- Set the connection timeout
- Process the command in the execution file in batch
- Set the service switch

Note

For more information about the usage and description of the CLI commands mentioned in this chapter, see the *Configuration of Switch Management Command*.

2.2 Access Control by Command Authorization

2.2.1 Overview

A simple way of controlling terminal access control in your network is to use passwords and assign privilege levels. Password protection restricts access to a network device. Privilege levels control the commands users can use after they have successfully logged in to a network device .

From the view of security, the password is stored in the configuration file. We want to ensure that the password is secure while the file is transmitted on the network (like TFTP). The password is encrypted before stored into the configuration file, and the clear text password is changed to the encrypted text password. The **enable secret** command uses a private encryption algorithm.

2.2.2 Default Password and Privilege Level Configuration

By default, there are not passwords of any levels, and the default level is 15.

2.2.3 Configuring or Changing Passwords of Different Levels

Our prodects provide the following commands for setting or changing the passwords at different levels.

Command	**Purpose**
DGS-3610(config)# **enable password** [**level** *level*] {*password* | *encryption-type encrypted-password*}	Set static password. Currently only 15-level user passwords are allowed, which may become active only when a security password has not been set. If a non-15-level password is set, the system will give a prompt and automatically turn it into the security password. If the 15-level static password set is the same as the 15-level security password, the system will give a warning message.
DGS-3610(config)# **enable secret** [**level** *level*] {*encryption-type encrypted-password*}	Set the security password, which has the same function as the static password but a better password encryption algorithm has been adopted. For the purpose of security, the security password is always recommended.
DGS-3610# **enable** [*level*] and DGS-3610# **disable** [*level*]	Switch the user level. The password for the corresponding level is required when a lower level is switched to a higher level.

When setting a password, the keyword **level** is used to define the password for a specified privilege level. When a password is set for a specified level, the password provided is only applicable for the users who are accessing that level.

2.2.4 Configuring Multiple Privilege Levels

By default, the software has only two password protection modes: normal user (level 1) and privileged user (level 15). You can configure up to 16 authorized levels of commands for each mode. By configuring passwords for different levels, you can allow different authorized levels to use different commands aggregate.

When no password is set for the privileged user level, no password is verified to enter into the privileged level. For security, you are recommended to set the password for the privileged user levels.

2.2.5 Configuration of Command Authorization

You can assign the using right to the users with lower level if you want to have one command used in more authorization levels. To use one command in less range of levels, you can assign the using right to users with higher levels.

You can use following commands to make authorization to a command:

Command	Purpose
DGS-3610# c**onfigure terminal**	Enter the global configuration mode.
DGS-3610(config)**# privilege mode [all] {level** *level* | **reset**} *command-string*	Set the privilege level for a command. Mode – The CLI command mode that the command to be authorized is of. For example, **config** indicates the global configuration mode, **exec** indicates the privilege command mode, and **interface** indicates the interface configuration mode. All – change the privilege of all subcommand for the specified command into the same privilege level. **level** *level* – authorization level, the range is from 0 to 15. **Level** 1 is for the normal user level. **Level** 15 is for the privileged user level. You can switch between various levels by using the **enable/disable** command. *command-string* - Specify the command to be authorized.

To recover a given command privilege, use the **no privilege mode [all] level** *level command* in the global configuration mode.

2.2.6 Example of Command Authorization configuration

The following is the configuration process that authorizes the **reload** command and its subcommand with the level 1, and set the level 1 as the effective level (by setting the command as “**test**”):

```
DGS-3610# configure terminal
DGS-3610(config)# privilege exec all level 1 reload
```

```
DGS-3610(config)# enable secret level 1 0 test
DGS-3610(config)# end
```

Enter the level 1, you can see the command and its subcommand:

```
DGS-3610# disable 1
DGS-3610> reload ?
  at                   reload at a specific time/date
  cancel                cancel pending reload scheme
  in                   reload after a time interval
  <cr>
```

The following is the configuration process that restores the privilege of the reload command and its subcommand as the default value:

```
DGS-3610# configure terminal
DGS-3610(config)# privilege exec all reset reload
DGS-3610(config)# end
```

Enter the level 1, the privilege of command will be taken back.

```
DGS-3610# disable 1
DGS-3610> reload ?
% Unrecognized command.
```

2.2.7 Configuring Line Password Protection

Our products suppors password authentication for remote logons (such as TELNET). A **line** password is required for the protection purpose. Execute the following command in the **line** configuration mode:

Command	Purpose
DGS-3610(config-line)# **password** *password*	Specify the **line** password
DGS-3610(config-line)# **login**	Enable the **line** password protection

Note

If no logon authentication is configuration, the **line** layer password authentication will be ignored even when the **line** password is configured. The logon authentication will be described in the next section.

2.2.8 Supporting Session Locking

Our products allow you to lock the session terminal temporarily using the **lock** command, so as to prevent access. To use the function of locking the session terminal, enable the terminal locking function in the **line** configuration mode, and lock the terminal using the **lock** command in the EXEC mode of the corresponding terminal:

Command	Purpose
DGS-3610(config-line)# **lockable**	Enable the function for locking the **line** terminal
DGS-3610# **lock**	Lock the current **line** terminal

2.3 Logon Authentication Control

2.3.1 Overview

In the previous section, we have described how to control the access to the network devices by configuring the password stored in local files. Besides the line password protection and local authentication, if the AAA mode is enabled, we can also carry out the authentication of the management privilege according to the username and password by some servers when you login the switches for the management. At present, we can also support use the RADIUS servers to control the management privilege of the network devices for users according to the login username and password.

When users login to the switch, we can authenticate users according to the username and password pairs stored centrally on a RADIUS server instead of local files. The divice sends the encrypted user information to the RADIUS server for verification, and the server will uniformly configures the username, user password, shared password and access policy. These make it easy to manage and control user access, and improve the security of the user information.

2.3.2 Configuring Local Users

Our products support the identity authentication system that is based on the local database, which is used for the local authentication through the method list in AAA mode, and the local logon authentication for line logon management in non-AAA mode.

To establish the username identity authentication, run the following specific commands in the global configuration mode:

Command	Function
DGS-3610(config)# **username** *name* [**password** *password* | **password** *encryption-type encrypted password*]	Establish the username identity authentication by using the encryption password.
DGS-3610(config)# **username** *name* [**privilege** *level*]	Set the privilege level for the user (optional).

2.3.3 Configuring Line Logon Authentication

To establish the line logon identity authentication, run the following specific commands in the line configuration mode:

Command	**Function**
DGS-3610(config-line)# **login local**	Set local authentication for line logon not in AAA mode.
DGS-3610(config-line)# **login authentication** {**default** | *list-name*}	Set AAA authentication for line logon in AAA mode. The authentication methods in the AAA method list will be used for the authentication, including the Radius authentication, local authentication and no authentication.

Note

For how to set the AAA mode, configure the Radius service and configure the method list, see the sections in *AAA configuration*.

2.4 System Time Configuration

2.4.1 Overview

Every network device has its system clock, which provides the detaild date (year, month, day) , time (hour, minute, second) and the week. When you use a network device for the first time, you must configure the system clock to current date and time manually. Of course, you can adjust the system clock when necessary. System clock is used for system logging and other functions that need record the time when an event occurs.

2.4.2 Setting the System Time

You can configure the system time on the network device manually. When you have configured the clock on the network device, the network device will work with the time you configured. Even if the network device is powered off, the clock still runs. Once you have configured the system clock, you do not need to configure it again unless you want to adjust the time of the device..

However, for the network devices which don’t provide the hardware clock, the manual setting of the time for the network devices is actually to set the software clock, and it only is valid for the operation of this time. When the network devices are powered down, the manual setting of the time will not be valid.

Command	**Function**
DGS-3610# **clock set** *hh:mm:ss month day year*	Setting the time and date of the system

For example to change the system time to 2003-6-20, 10:10:12-

```
DGS-3610# clock set 10:10:12 6 20 2003    //Set the system time and  date
DGS-3610# show clock                     //Confirm the Modification of the system time is
                                                         valid.
clock: 2003-6-20 10:10:54
```

2.4.3 Setting the System Time and Date

You can show the system time and date by using command **show clock** in the privileged mode. The following is the format:

```
DGS-3610# sh clock                        //Show the current time of the system
clock: 2003-5-20 11:11:34
```

2.5 Scheduled Restart

2.5.1 Overview

This section describes how to use the **relaod [***modifiers***]** command to schedule a restart scheme to restart the system at specified time. This function may facilitate user's operation in some circumstance (for the purpose of test or other reqirements). modifiers is a group of command options provided by the **reload,** making the command more flexible. The optional modifiers can be **in, at** and **cancel**. The following are the details:

1. **reload in** *mmm* | *hhh:mm* [*string*]

This command schedules a reload of the system after specified time. The time can be specified by *mmm* or *hhh:mm* in minutes, users can use any one of the two formats. *string* is a tip for help, and you can give the scheme a memorable name by the string to indicate its purpose. string is a prompt. Users can specify a name that can be memorized easily for this scheme, so as to indicate the purpose of restart. For example, if you need to reload the system in 10 minutes for test, you can input **reload in** *10 test.*

2. **reload at** *hh:mm month day year* [*string*]

This command schedules a reload of the software at the specified time in the future. The value must be a specified time in the future. The parameter *year* is optional. If you do not input it, the default value is the year of the system clock. Because the interval between the reload time and the current time shall not exceed 31 days, generally, you do not need to input the year if the current date is among January 1 to November 30. But if the current system month is December, the system reload date specified may be a day in January in the next year in stead of the day of January in the current year, in which case, you need to input the year to inform the system the reload time is in January of the next year, not in this year. It will fail because the default date will be in the January in this year when the year is not specified. The usage of *string* is just like above. For example, if the current system time is 14:31 on January 10, 2005, and you want the system to reload tomorrow, you can input **reload at** *08:30 11 1 newday*. If the current system time is 14:31 on December 10, 2005, and you want the system to reload at 12:00 a.m. on January 1, 2006, you can input **reload at** *12:00 1 1 2006 newyear.*

3. reload cancel

This command deletes the restart scheme specified by the user. For example, you have specified that the system would reload at 8:30 a.m. tomorrow above, once you input **reload cancel**, the configuration will be deleted.

Note

If you need to use the **at** option, the current system must support the clock function. Before the use, it is recommended to configure the system clock correctly to better meet your needs. If a restart scheme has been set before, the subsequent settings will overwrite the previous settings. If the user has set a reload scheme and then restarts the system before the scheme takes effect, the scheme will be lost.

The span from the time in the reload scheme to the current time shall be within 31 days and must be greater than the current system time. Also, after you set reload sheme, you should not modify the system clock. Otherwise, your setting may fail to take effect, for example, in the case that the system time is set to be later than the reload time.

2.5.2 Specifying the System to Restart at a Specific Time

In the privileged mode, you can configure the system reload at the specified time using the following commands:

Command	Function
DGS-3610# **reload at** *hh:mm day month* [*year*] [*reload-reason*]	The system will reload at hh:mm,month day,year. The reason of reload is *reload-reason* (if any).

The following is an example specifying the system reload at 12:00 a.m. January 11, 2005 (if the current system clock is 8:30 a.m. January 11,2005):

```
DGS-3610# reload at 12:00 1 11 2005 midday   //Set the system reload time and date.
DGS-3610# show reload                        //Confirm the modification of the reload
                                             time is valid.
Reload scheduled in 16581 seconds.
At 2005-01-11 12:00
Reload reason: midday
```

2.5.3 Specifying the System to Restart after a Period of Time

In the privileged mode, you can configure the system reload in the specified time with the following commands:

Command	Function
DGS-3610# **reload in** *mmm* [*reload-reason*]	Configure the system **reload** in *mmm* minutes, where the **reload** reason is described in *reload-reason* (if inputted)
DGS-3610# **reload in** *hhh:mm* [*reload-reason*]	Configure the system **reload** in *hhh* hours and *mm* minutes, where the **reload** reason is described in *reload-reason* (if inputted)

The following example shows how to **reload** the system in 125 minutes (assumes that the current system time is 12:00 a.m. January 10, 2005):

```
DGS-3610# reload in 125 test    //Set the system restart time
```

Or

```
DGS-3610# reload in 2:5 test    //Set the system reload time
DGS-3610# show reload           //Confirm the modification of reload time takes effect
System will reload in 7485 seconds.
```

2.5.4 Immediate Restart

The **reload** command without any **reload** scheme parameter will reload the device immediately. In the privilege mode, the user can resload the system immediately by typing in the **reload** command.

2.5.5 Deleting the Configured Reload Scheme

In the privilege mode, use the following command to delete configured reload scheme:

Command	Function
DGS-3610# **reload cancel**	Delete the configured reload scheme.

If no reload scheme is configured before, you will see the prompt for the wrong operation.

2.6 System Name and Command Prompt

2.6.1 Overview

In order to manage the devices easyly, you can configure a system name for the network device to identify it. If you haven't configured a system prompt for CLI, the system name will be the default command prompt (if the system name exceeded to more than 32 characters, the first 32 characters will be intercepted and taked as the system prompt). The prompt will be changed with the system name. By default, the concrete device name will be taken as the system name, for example “DGS-3610-26” and “DGS-3610-26G".

2.6.2 Configuring a System Name

Our products provide the following commands to configure the system name in global configuration mode:

Command	Function
DGS-3610(Config)# **hostname** *name*	Configure a system name. The name must be consisted by the characters to be printed, and the length is not up to 255 byte.

To restore the system name to the default value, use the **no hostname** command in the global configuration mode. The following example shows how to changes the device name to DGS-3610 series:

```
DGS-3610# configure terminal       //Enter to the global configuration mode.
DGS-3610(config)# hostname DGS-3610        //Set the network device name to D-Link
D-Link(config)#                    //The name has been modified successfully.
```

2.6.3 Configuring a Command Prompt

If you have not configured a command prompt, the system prompt will be taken as the default prompt (if the length of the system name exceeded up to 32 characters, the first 32 characters will be intercepted and be taken as the default prompt). The prompt is changed with the change of the system name. You can use the **prompt** command to configure the command prompt in the global configuration mode, and the command prompt is only valid for the EXEC mode.

Command	Function
DGS-3610# **prompt** *string*	Set the command prompt.The name must be consisted by the characters to be printed. If the length of the name exceeds 32 characters, intercept the first 32 characters.

To restore to the default prompt, use the **no prompt** command in the global configuration mode.

2.7 Banner Configuration

2.7.1 Overview

When the user logs in to the switch, you may need to notify the users some required information. You can achieve the purpos by setting a banner. You can create two-type banner: a message-of-the-day (MOTD) and a login banner. The MOTD is used for all users who connect to the network devices. When users log in the network devices, the notification message will be displayed in the terminal firstly. By using the MOTD, you can send some urgent messages (for example, the system is to be disabled) to the network users. The login banner also is displayed after the MOTD, Its main function is to provide some common login messages. By default, the MOTD and login banners are not configured.

2.7.2 Configuring a Message-of-the-Day

You can create a single or multi-line MODT, these information will be displayed on the screen when the users log in to the network devices. You may configure the message of the day in the global configuration mode:

Command	**Function**
DGS-3610(Config)**# banner motd** *c message c*	Configure the text for the message of the day. c denotes the delimiter, it can be any characters of your choice (for example, a pound sign '&' etc.). After inputting the delimiting character, press the **Enter** key. Now, you can start to enter the text, and enter the delimiter again and press Enter to end the inputting of a text. Please note that if you enter more characters after inputting the delimiter for ending the text, such characters will be discarded by the system. To be noted that the text of MOTD should not include the letters regarded as the delimiting character. The length of the text should not exceed to 255 bytes.

Use the **no banner motd** command in the global configuration mode to delete the MOTD configured, The following example shows how to configure an MOTD. The # symbol is used as the delimiter, and the text of the MOTD is "Notice: system will shutdown on July 6th." See the following configuration example:

```
DGS-3610(config)# banner motd #                        //The delimiter for starting
Enter TEXT message.  End with the character '#'.
Notice: system will shutdown on July 6th.
#                                          #       //The delimiter for ending.
DGS-3610(config)#
```

2.7.3 Configuring a Login Banner

You may configure the login banner message in the global configuration mode by executing the following commands:

Command	**Function**
DGS-3610(Config)# **banner login** *c message c*	Set the text of login banner. c denotes for the delimiter, it can be any characters of your choice (for example, a pound sign '&' etc.). After inputting the delimiting character, press the **Enter** key. Now, you can start to enter the text, then enter the delimiter again and press **Enter** to end the inputting of a text. Please note that if you enter more characters after inputting the delimiter for ending the text, such characters will be discarded by the system. To be noted that the text of login banner should not include the letters regarded as the delimiting character. The length of the text should not exceed to 255 bytes.

To delete the login banner, use the **no banner login** command in the global configuration mode.

The following example shows how to configure a login banner for the device by using the pound sign (#) as the beginning and ending delimiters, and the message of the login banner is "Access for authorized users only. Please enter your password.":

```
DGS-3610(config)# banner login #      //Delimiterfor starting
Enter TEXT message. End with the character '#'.
Access for authorized users only. Please enter your password.
#                                     //Delimiter for ending
DGS-3610(config)#
```

2.7.4 Displaying a Banner

The message of a banner is displayed when users login the network devices. The following is an example for displaying the login banner::

```
C:\>telnet 192.168.65.236
 Notice: system will shutdown on July 6th.
 Access for authorized users only. Please enter your password.
 User Access Verification
Password:
```

Where, “Notice: system will shutdown on July 6th." is an MOTD, while "Access for authorized users only. Please enter your password." is a login banner.

2.8 Viewing System Information

2.8.1 Overview

You can view some system information with the **show** command in the command line. The version information of the system and device information in the system are included.

2.8.2 Viewing System Information and Version

System information consists of system description, system power-on time, hardware version of the system , software version of the system , the software version of CTRL layer, and the software version of BOOT layer. You can get the overview of a system through such information. You can show the system information with the following commands in the privileged mode:

Command	Function
DGS-3610# **show version**	Show system information and version

2.8.3 Viewing Hardware Information

Hardware information mainly includes physical device information and the slot and module information on the device. The information of the device itself includes device description, amount of slots in the device; slot information: numbering of the slot in the device, description of the module on the slot (empty description if no module plugged on the slot), amount of physical ports included in the module on the slot, and maximum number of ports possibly included in the slot (number of ports included in the modules plugged). You may use the following commands to show the information of the device and slots in the privilege mode:

Command	Function
DGS-3610# **show version devices**	Show the current information of the network devices
DGS-3610# **show version slots**	Show the current information of the slots and modules on the network devices

2.9 Console Rate Setting

2.9.1 Overview

The network devices comes with a console interface that allows you to manage the network devices. When it is the first time to be used, it is required to configure it through the console interface mode.You can change the rate of the serial interface on the network devices if necessary. To be noted that the rate of the terminal for manageing the network devices should be matched with the rate of the console of the network devices.

2.9.2 Setting Console Rate

In the line configuration mode, you may use the following command to set the console rate:

Command	Function
DGS-3610(config-line)# **speed** *speed*	Set the console transmission rate, in bps. For the serial interface, you can only set the transmission rate as one of 9600, 19200, 38400, 57600 and 115200. 9600 is the default rate.

This example shows how to configure the baud rate of the serial port to 57600 bps:

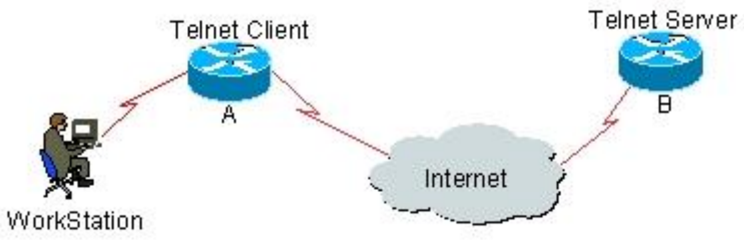
```
DGS-3610# configure terminal              //Enter the global configuration mode.
DGS-3610(config)# line console 0          //Enter the console line configuration mode
DGS-3610(config-line)# speed 57600        //Set the console rate as 57600
DGS-3610(config-line)# end                //Return to the privilege mode
DGS-3610# show line console 0             //View the console configuration
CON    Type    speed   Overruns
* 0    CON     57600   0
Line 0, Location: "", Type: "vt100"
Length: 25 lines, Width: 80 columns
Special Chars: Escape  Disconnect  Activation
            ^^x    none       ^M
Timeouts:    Idle EXEC    Idle Session
            never        never
History is enabled, history size is 10.
Total input: 22 bytes
Total output: 115 bytes
Data overflow: 0 bytes
stop rx interrupt: 0 times
Modem: READY
```

2.10 Using telnet on the Network Devices

2.10.1 Overview

The telnet is an application layer protocol in the TCP/IP protocol family, which provides the specifications of remote logon and virtual terminal communication function. The Telnet Client service is used by the local or remote user who has logged onto the local network device to work with the Telnet Client program to access the other remote system resources on the network. As shown below, the user on the PC establishes the connection with network device A through the terminal emulation program or telnet, and then the user can log onto network device B again by entering the **telnet** command to manage its configuration.

Figure 2-1



2.10.2 Using Telnet Client

You can log in to a remote devices by using the telnet command on the network device:

Command	Function
DGS-3610# **telnet** *host-ip-address*	By using this command **telnet** to log in the remote devices , It may be the host name or IP address.

The following example shows how to establish a **Telnet** session and manage the remote network device with the IP address 192.168.65.119:

```
DGS-3610# telnet 192.168.65.119    //Establish the telnet session to a remote device
Trying 192.168.65.119 ... Open
User Access Verification      //Enter into the logon interface of the remote device
Password:
```

2.11 Connection Timeout Setting

2.11.1 Overview

The established connection (including the accepted connections, and the session from the device to a remote terminal) for a device can be controlled through configuring the connection timeout of the device, When the idle time exceeds the set value and there is no input or output information, this connection will be interrupted.

2.11.2 Connection Timeout

The server will interrupt this connection when there is no any input information for the accepted connection within a specified time, .

Our products provide commands in the LINE configuration mode to configure the connection timeout:

Command	Function
DGS-3610(Config-line)#**exec-timeout** *20*	Configure the timeout for the accepted connection on LINE. When the configured time is due and there is no input information, this connection will be interrupted.

The timeout setting in the LINE can be cancelled by using the **no exec-timeout** command in the LINE configuration mode.

```
DGS-3610# configure terminal           //Enter the global configuration mode.
DGS-3610# line vty 0                   //Enter the LINE configuration mode
DGS-3610(config-line)#exec-timeout 20  //Set the timeout to 20min
```

2.11.3 Session Timeout

When there is no input information for the established session on the current LINE within a specified time, the session connected to the remote terminal currently will be interrupted. The terminal will restored to dle status.

Our products provide commands in the LINE configuration mode to configure the timeout for the session connected to the remote terminal:

Command	Function
DGS-3610(Config-line)#**session-timeout** *20*	Configure the timeout for the session connected to the remote terminal on LINE. If there is no input information within the specified time, this session will be interrupted.

The timeout setting on the LINE for the session connected to the remote terminal can be cancelled by using the **no exec-timeout** command in the LINE configuration mode.

```
DGS-3610# configure terminal             //Enter the global configuration mode.
DGS-3610(config)# line vty 0             //Enter the LINE configuration mode
DGS-3610(config-line)#session-timeout 20 //Set the session timeout to 20min
```

2.12 Process the command in the execution file in batch

In the system management, it is necessary to enter more configuration command to carry out the management of some function sometimes. It will take a long time and cause some error or missing if it is entered through the CLI interface completely. If the configuration commands of these functions are placed in the batch file by the configuration steps, you can execute this batch file if required, to carry out all related configurations.

Command	Function
DGS-3610# **execute** {[**flash**:] *filename*}	Execute a batch file.

For example, the batch file line_rcms_script.text is used to enable the reversed Telnet function of all asynchronous interfaces. The file content is shown as follows:

```
configure terminal
line tty 1 16
transport input all
no exec
end
```

Running Result:

```
DGS-3610# execute flash:line_rcms_script.text
executing script file line_rcms_script.text ......
executing done
DGS-3610# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DGS-3610(config)# line vty 1 16
DGS-3610(config-line)# transport input all
DGS-3610(config-line)# no exec
DGS-3610(config-line)# end
```

Note

The file name of the batch file and the content in the file can be specified. In general, it is transported to the Flash of devices in the TFTP way after it is edited on the user PCs. The batch content will simulate the user input completely. Hence, it is necessary to edit the content of the batch file according to the configuration sequence of the CIL command. Furthermore, for some interactive commands, it is necessary to write corresponding response information in batch file, to ensure the command can be executed normally.

2.13 Setting of Service Switch

During the system running, you can adjust the service provided by the system dynamically, enable and disable the specified service (SSH Server/Telnet Server/Web Server).

Command	Function
DGS-3610(Config)# **enable service ssh-sesrver**	Enabling SSH Server
DGS-3610(Config)# **enable service telnet-server**	Enabling Telnet Server
DGS-3610(Config)# **enable service web-server**	Enabling Http Server

In the configuration mode, you can use the **no enable service** command to disable corresponding service.

```
DGS-3610# configure terminal              //Enter the global configuration mode.
DGS-3610(config)# enable service ssh-server     //Enable SSH Server
```

3 LINE Mode Configuration

3.1 Overview

This chapter describes some operations on LINE:

- Enter the LINE mode
- Increase/decrease LINE VTY quantity
- Configure the allowed communication protocol in LINE

3.2 LINE Mode Configuration

3.2.1 Enter the LINE mode

After entering the specific LINE mode, it is possible to configure the specific LINE in the LINE mode. Run the following commands to enter the specified LINE mode:

Command	Function
DGS-3610(config)# **line [aux | console | tty | vty]** **first-line [last-line]**	Enter the specified LINE mode.

3.2.2 Increase/decrease LINE VTY quantity

By default, the number of line vty is 5. It is possible to run command to increase or decrease the number of line vty, up to 36.

Command	Function
DGS-3610(config)# **line vty** *line-number*	Increase the number of LINE VTY to a value.
DGS-3610(config)# **no line vty** *line-number*	Decrease the number of LINE VTY to a value.

3.2.3 Configure the allowed communication protocol in LINE

To limit the allowed communication protocol type in the LINE, this command can be used for the configuration. By default, the VTY type allows the communication of all protocols, while the other types of TTY do not allow the communication of any protocol.

Command	Description
configure terminal	Enter the configuration mode
Line vty *line number*	Enter the Line configuration mode
transport input {*all* | *ssh* | *telnet* | *none*}	Configure the allowed communication protocol in the corresponding Line
no transport input	Configure forbidding the communication of any protocol in Line
default transport input	Restore the communication protocol to default in Line

3.2.4 Configure the access control list in Line

To configure the access control in line, the command can be used. By default, there is no configuration of access control list in line. That is, all connections are accepted and all egress connection are allowed.

Command	Description
configure terminal	Enter the configuration mode
Line vty *line number*	Enter the Line configuration mode
access-class *access-list-number* **{in | out}**	Configure the access control list in corresponding Line
no access-class *access-list-number* **{in | out}**	Cancel the configuration of the access control list in Line

4 Configuration of System Upgrade and Maintenance

4.1 Overview

The upgrade and maintenance of the system are the process to upgrade or upload/download files via the main program or CTRL program on the command line interface in two ways:the one is upgraded by using the TFTP protocol through the network port, the other is upgraded by using the Xmodem protocol through the serial port.

4.2 Upgrade and Maintenance Method

The following sections describe how to upgrade and maintain the device:

- Transferring Files by Using the TFTP Protocol
- Transferring Files by Using the XMODEM Protocol

4.2.1 Transferring Files by Using the TFTP Protocol

One method is to download files from the host to the equipment, the other is to upload files from the equipment to the host.

In the CLI command mode, download the files by performing the following steps:

Before downloading, firstly start the TFTP server software on the local host. Then, select the directory of the file to be downloaded. Finally, log in to the device. In the privilege mode, download the files by executing the following commands. If no location is specified, you need to separately input the IP address of the TFTP server.

Command	Function
DGS-3610# **copy tftp:** *//location/ filename* **flash:** *filename*	Download the file *filename* specified by URL on the host to the device.

In the CLI command mode, upload the files by performing the following steps:

Before uploading, firstly start the TFTP server software at the local host. Then, select the destination directory for the file to upload at the host. Finally, upload the files by using the following commands in the privilege mode.

Command	Function
DGS-3610# **copy flash:** *filename* **tftp:** *//loca tion/filename*	Upload the file *filename* from the device to the directory specified by the URL on the host. You can also specify another file name.

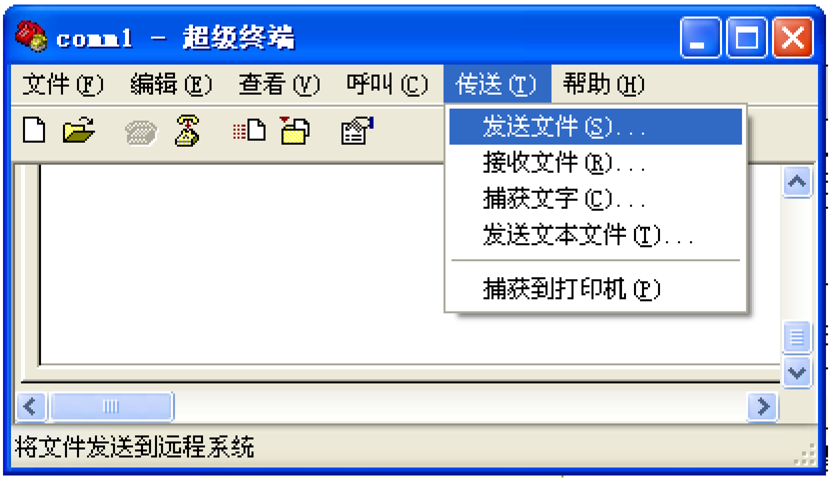
4.2.2 Transferring Files by Using the XMODEM Protocol

The one is to download files from the host to the device, the other is to upload files from the device to the host.

In the CLI command mode, download the files by performing the following steps:

Prior to download, firstly log in to the out-band management interface of the device through the Windows Super Terminal. Then, download the files by using following commands in the privileged mode. Finally, select the “Send File” from the “Transfer” menu on the Windows Super Terminal on the local host, the operation is shown as below:

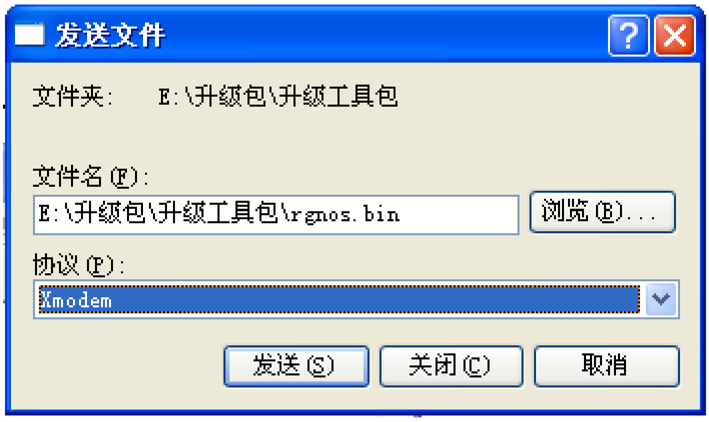
Figure 4-1



将文件发送到远程系统

In the file name option of the pop-up dialog box, select the files to be downloaded and select the “Xmodem” as the protocol. Click “Send”, and the transmistted process and packets will be shown on the Windows Super Terminal.

Figure 4-2



文件夹: E:\升级包\升级工具包

文件名(F): E:\升级包\升级工具包\rgnos.bin

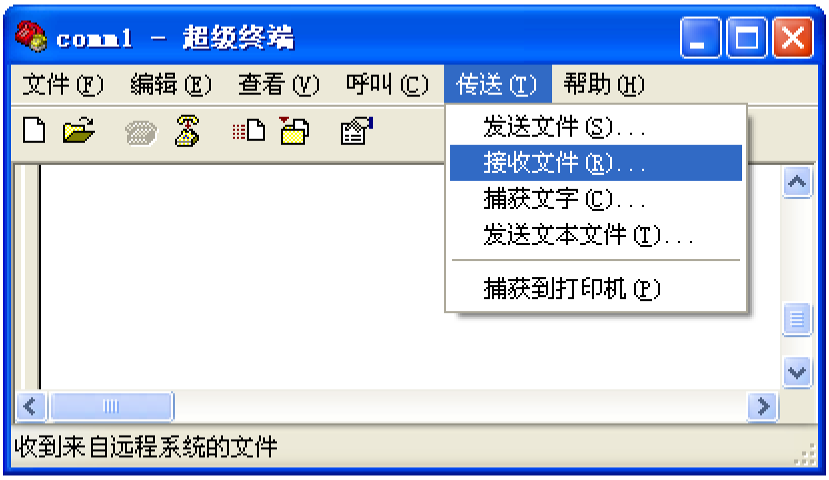
协议(P): Xmodem

Command	Function
DGS-3610# **copy xmodem flash**:*filename*	Download a file from the host to the device and name it *filename*.

In the CLI command mode, upload the files by performing the following steps:

Prior to upload, firstly log in to the out-band management interface of the device through the Windows Super Terminal. Then, upload the files by using following commands in the privileged mode. Finally, select the “Receive File” from the “Transfer” menu on the Windows Super Terminal on the local host. It’s shown in the Figure 4-3:

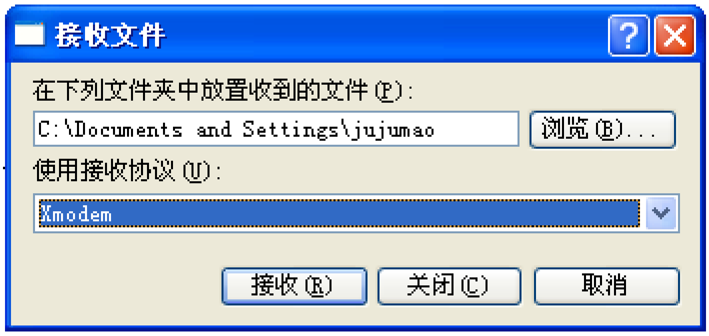
Figure 4-3



收到来自远程系统的文件

In the pop-up dialog box, select the storage location for uploading the files and select the “Xmodem” as the reception protocol. Click “Receive”, the name of the files locally stored will be further displayed on the Windows Super Terminal. Click “OK” to receive the files. The operaton is shown below:

Figure 4-4



接收文件

在下列文件夹中放置收到的文件(P): C:\Documents and Settings\jujumao

使用接收协议(U): Xmodem

Command	Function
DGS-3610# **copy flash**:*filename* **xmodem**	Upload the file *filename* from the device to the host.

4.2.3 Upgrade the System

Whatever the box device or chassis device, you can use above tftp or xmodem to transmit the upgraded files to the device. After being transmited successfully, reboot the device, and the upgraded files will automatically finish the detection and upgrade in the current system. It is not necessary to interrupt and interfere manually.

The upgrade operation of upgrading files in the box devices and chassis devices is slightly different:

1. The upgrade of the box device can complete the upgrade operation of the single board system. After the upgrade is completed, the system will be reset automatically, and the device will be enabled again and run normally.
2. The chassis device includes the management board, the line card and the multi-service card, so it is necessary to carry out the upgrade operation of the whole system by an upgrade file. After the management board is upgraded, the system will be reset. When the equipment is reloaded again, the version automatic synchronization function will be enabled, to carry out the system upgrade of the line card and the multi-service card.

Automatic Upgrade Function: it is a function which runs on the primary management board terminal and carries out the coherence check of the version for the slave management board, line card and multi-service card. If it is detected that the version is not consistent with the corresponding single board in the primary management board, you should transmit the single board upgrade file to complete the upgrade, so as to keep the coherence of the version for the whole system.

Caution

Whenever you upgrade the master management board, the slave one (if any) is upgraded at the same time to keep the version consistent. The upgrade of a line card will upgrade all the line cards inserted into the device.Do not power off the device before the upgrade is completed. Otherwise, the upgrade program may be lost.

Before the chassis device is upgraded, you can check whether the upgrade is finished through checking the **show version** of all line cards and management boards is consistent with the upgraded object version, but can not carry out the primary and slave switching (such as **redundancy force-switchover**). Otherwise, it will cause the upgrade failure and return to the original version.

Note

The upgrade method of the box device is the same as that off the management board.

- Upgrade the chassis devices through the upgrade file:

1) To confirm the upgrade file name *.bin to be loaded

2) To download the file to the device by using above copy command,

3) To wait for the successful updrage of the main program both in the host and slave management boards if there are the host and slave management boards on the devices. The prompt will be shown as below when it’s successful:

```
Upgrade Slave CM MAIN successful!!

Upgrade CM MAIN successful!!
```

4) To execute a resetting operation for the whole device

5) After the system restart again, the upgrade file will begin to run and following prompt will be displayed:

```
Installing is in process ......

Do not restart your machine before finish !!!!!!

......
```

6) After the upgrade operation finished, following prompt will be displayed:

```
Installing process finished ......

Restart machine operation is permited now !!!!!!
```

7) The system will reset automaticly after the upgrade file finished operation, following prompt will be displayed:

```
System restarting, for reason 'Upgrade product !'.
```

8) The whole system of the management boards will finish the upgrade after the system restarted. Then the upgrade file of single board for loading the management board will be operated. The prompt in step 5 and step 6 will be displayed but without the prompt of step 7. However, what the following information will replace it:

```
System load main program from install package ......
```

It will directly run through the main program in the upgrade files loaded the management board

9) The automatic upgrade function will be enabled after the main program runs normally. If the slave management board or other modules in the chassis, following prompt will be displayed:

```
A new card is found in slot [1].
System is doing version synchronization checking ......
Current software version in slot [1] is synchronous.
System needn't to do version synchronization for this card ......
```

Or prompt as below:

```
System is doing version synchronization checking ......
Card in slot [3] need to do version synchronization ......
```

Other print information

```
Version synchronization begain ......
Keep power on, don't draw out the card and don't restart your machine before
finished !!!!!!
```

Other print information

```
Transmission is OK, now, card in slot [3] need restart ...
Software installation of card in slot [3] is in process ......
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Software installation of card in slot [3] has finished successfully ......
The version synchronization of card in slot [3] get finished successfully.
```

In above two cases, the one indicates that the version of the line cards does not need to reupgrade because it has been synchronous while the other indicates that the the version of the line cards needs to be upgraded automaticly, then performs the upgrade operation.

The system will finish above mentiond operation in turn for the slave boards and each module.

The system will wait for finishing the coherence check and upgrading operation according to the prompt. Then the system can work normally.

Caution	During the process of upgrading or automatically upgrading, the prompt will be displayed for not allowing the system to reset. Once the same prompt appears, please do not power off or reset the system or plug/unplug other modules casually.

Note	The same operaton of automatic upgrade and check will be performed for the module system with hot-plugging in.

- . To upgrade the box devices through the upgrade files:

Only need to finish step 1 to 7 above-mentioned for the upgrade of box devices. Then the system will run normally after the automaticaly resetting.

5 Network Communication Detection Tools

5.1 Ping Connectivity Test

For the connectivity test of networks, many network devices support the Echo protocol. The protocol involves sending a special packet to a specified network address and waiting for the packet returned from the address. By the echo protocol, we can evaluate the connectivity, delay and reliability of networks. The ping tool provided by DGS-3610 series can effectively help users diagnose and locate the connectivity problems in networks.

The Ping command runs in the user EXEC mode and privileged EXEC mode. In the user EXEC mode, only basic ping function can be run, which in the privileged EXEC mode, the enlarged function of ping also can be run.

Command	Function
DGS-3610# **ping** [*ip*] [*address* [**length** *length*] [**ntimes** *times*] [**timeout** *seconds*]]	**Ping:** Test tools of network connectivity

The ordinary Ping function can be performed in either normal user mode or privilege user mode. By default, this command sends five 100-byte packets to the specified IP address. Within the specified time (2 seconds by default), if there is a response, the "!" symbol is shown; if there is no response, the "." symbol is shown. Finally, a statistics message is output. This is a normal ping example:

```
DGS-3610# ping 192.168.5.1
Sending 5, 100-byte ICMP Echoes to 192.168.5.1, timeout is 2 seconds:
< press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

The extended Ping function can be performed in the privilege user mode only. With the extended Ping, you can specify the number, length of packets to be sent, and the timeout. Just like the ordinary Ping function, the extended Ping also output a statistics message. The following shows an example of the extended Ping:

```
DGS-3610# ping 192.168.5.197 length 1500 ntimes 100 timeout 3
Sending 100, 1000-byte ICMP Echoes to 192.168.5.197, timeout is 3 seconds:
  < press Ctrl+C to break >
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 2/2/3 ms
DGS-3610#
```

5.2 Traceroute Connectivity Test

The **Traceroute** command can be used to show all the gateways that the packet passes through from the source to the destination. The **Traceroute** command is mainly used to check the network connectivity and exactly locate the fault when the network fails.

One of the network transmission rules is that the number in the TTL field in the packet will decrease by 1 every time when the packet passes through a gateway. When the number in the TTL field is 0, the gateway will discard this packet and send an address unreachable error packet to the source. According to this rule, the execution of the Traceroute command is as follows: At first, it sends one packet with 1 as TTL to the destination address. The first gateway sends one ICMP error message back to indicate that this packet cannot be sent because TTL timeouts. Then, the first gateway re-sends the packet after the TTL domain adds 1. Likewise, the second gateway returns a TTL timeout error and the process lasts until the packet reaches the destination address. Once you record every source address for loopback ICMP TTL timeout information, you have recorded the entire path passed by the IP packet from the source address to the destination address.

The **Traceroute** command can run in user EXEC mode and privileged EXEC mode. The command format is as follows:

Command	Function
DGS-3610# **traceroute** [*protocol*] [*destination*]	Trace the network route for packet sending

The following are two examples that apply traceroute.In one example, network connectivity is good. In another example, some gateways in a network are not connected.

1. Traceroute example where network connectivity is good:

```
DGS-3610# traceroute 61.154.22.36
  < press Ctrl+C to break >
Tracing the route to 61.154.22.36

1      192.168.12.1        0 msec   0 msec   0 msec
2      192.168.9.2         4 msec   4 msec   4 msec
3      192.168.9.1         8 msec   8 msec   4 msec
4      192.168.0.10        4 msec   28 msec  12 msec
5      202.101.143.130     4 msec   16 msec  8 msec
6      202.101.143.154     12 msec  8 msec   24 msec
7      61.154.22.36        12 msec  8 msec   22 msec
```

From the above result, we can know clearly the following information: To access the host with an IP address of 61.154.22.36, the network packet passes gateways 1 to 6 from the source address. At the same time, we know the time it takes the network packet to reach the gateway. This is very useful for network analysis.

2. Traceroute example where some gateways in a network are not connected:

```
DGS-3610# traceroute 202.108.37.42
< press Ctrl+C to break >
Tracing the route to 202.108.37.42
1     192.168.12.1        0 msec   0 msec   0 msec
2     192.168.9.2         0 msec   4 msec   4 msec
3     192.168.110.1       16 msec  12 msec  16 msec
4     *  *  *
5     61.154.8.129        12 msec  28 msec  12 msec
6     61.154.8.17         8 msec   12 msec  16 msec
7     61.154.8.250        12 msec  12 msec  12 msec
8     218.85.157.222      12 msec  12 msec  12 msec
9     218.85.157.130      16 msec  16 msec  16 msec
10    218.85.157.77       16 msec  48 msec  16 msec
11    202.97.40.65        76 msec  24 msec  24 msec
12    202.97.37.65        32 msec  24 msec  24 msec
13    202.97.38.162       52 msec  52 msec  224 msec
14    202.96.12.38        84 msec  52 msec  52 msec
15    202.106.192.226     88 msec  52 msec  52 msec
16    202.106.192.174     52 msec  52 msec  88 msec
17    210.74.176.158      100 msec 52 msec  84 msec
18    202.108.37.42       48 msec  48 msec  52 msec
```

From the above result, we can know clearly the following information: To access the host with an IP address of 202.108.37.42 the network packet passes gateways 1 to 17 from the source address and there is failure in gateway 4.

6 Configuring Interfaces

6.1 Overview of Interface Types

This chapter provides the classification of interfaces used in DGS-3610 series as well as a precise definition of each type. Interfaces on DGS-3610 series are classified into two types:

- L2 Interfaces
- L3 Interfaces (available in layer 3 devices)

6.1.1 L2 Interfaces

This section presents the types of L2 interfaces and their definitions. L2 interfaces fall into the following types

- Switch Port
- L2 Aggregate Ports

6.1.1.1 Switch Port

Switch PortIt consists of a single physical port on the device and has layer 2 switching function only. This port can either be an Access Port or a Trunk Port. You can configure a port to be an Access Port or a Trunk Port by using the Switch Port interface configuration command. Switch Port is used to manage the physical interface and the layer 2 protocol related to it. It does not handle routing or bridging.

6.1.1.1.1 Access Ports

Each access port belongs to only one VLAN, transporting the frames belonging to the same VLAN only. Typically, it is used to connect computers.

Default VLAN

Each Access Port belongs to one VLAN only. Therefore, its default VLAN is the VLAN where it is located, and it is unnecessary for you to set it.

Receiving and sending frames

Access Port sends data frames without tags, and receives frames in the following three formats only:

- Untagged frame
- Tagged frame with VID as the VLAN where the Access Port is located

- Tagged frame with VID 0

Untagged frame

Access Port receives frames without tags, and adds a default VLAN as the tag to the frames without tags. The added tag will be removed before the frames are sent.

Tagged frame

The Access port handles the data frames with tags in the following ways:

- When VID (VLAN ID) in the TAG is the same as the default VLAN ID, the data frame is received, and the TAG is removed before the frame is sent.
- When VID (VLAN ID) in the TAG is 0, this data frame is received. In the TAG, VID=0 is used to identify the frame priority.
- When VID (VLAN ID) in the TAG is different from the default VLAN ID and is not 0, this frame is discarded.

6.1.1.1.2 Trunk Ports

Each Trunk port can belong to multiple VLANs, and can receive and send frames that belong to multiple VLANs. Generally, it is used to connect devices or computers of users.

Default VLAN

Because a Trunk Port can belong to multiple VLANs, you need to set a Native vlan as the default VLAN. By default, the Trunk port transmit frames for all VLANs. In order to reduce device load and minimize bandwidth consumption, you can set the VLAN allowance list to specify frames of which VLANs to be transmitted by the Trunk port.

Caution

It is recommended to set the native vlan of the Trunk port on the local device the same as the native vlan of the Trunk port on the remote device. Otherwise, the port may be unable to forward packets properly.

Receiving and sending frames

The Trunk port can receive Untagged frames and the tagged frames within the allowed VLANs. All the frames sent by Trunk Port outside the Native vlan have tags, and the frames sent by it in the Native vlan have no tags.

Untagged frame

If the Trunk port receives a frame without IEEE802.1Q TAG, this frame will be transmitted in the Native VLAN where this port is located.

Tagged frame

If the Trunk port receives a frame with a tag, the frame will be handled in the following ways:

- When the Trunk Port receives a frame with a tag where the VID is the same as the Native vlan of this Trunk port, this frame is accepted. The tag will be removed before the frame is sent.

- When the Trunk Port receives a frame with a tag where the VID is different from the Native vlan of this Trunk port, but VID is the VLAN ID that the port allows, the frame is accepted. The tag is kept unchanged when the frame is sent.
- When the Trunk Port receives a frame with a tag where the VID is different from the Native vlan of this Trunk port, and the VID is the VLAN ID that the port does not allow, this packet is discarded.

Note

Untagged packets are ordinary Ethernet packets that can be recognized by the network card in the ordinary PC for communication. The structure of TAG packets is changed by appending four bytes of VLAN information, namely the VLAN TAG header, at the end of the source MAC address and the destination MAC address.

6.1.1.1.3 Hybrid port

The Hybrid port can belong to multiple VLANs, receive and send packets for multiple VLANs. It can be used to connect devices or computers of users. The Hybrid port is different from the Trunk port in that the Hybrid port allows untagged packets being sent for multiple VLANs, while the Trunk port only allows untagged packets being sent for the default VLAN. Note that the VLAN that the Hybrid port is added to must already exist.

6.1.1.2 L2 Aggregate Ports

Aggregate port consists of several physical member ports that are aggregated. Multiple physical connections can be bound into a simple logical connection, which is called an aggregate port (referred to as AP below).

For layer 2 switching, AP works like a Switch port with a high bandwidth. It extends the link bandwidth by using the bandwidths of several ports. In addition, the frames that pass through the L2 Aggregate port will undergo traffic balancing on the member ports of the L2 Aggregate port. If one member link of AP fails, the L2 Aggregate port automatically assigns the traffic on this link to other working member links, making the connection more reliable.

Caution

The member port of the L2 Aggregate Port can be either Access port or Trunk Port. However, the member ports in one AP must be of the same type, namely, all the ports are either Access Ports or Trunk ports.

6.1.2 L3 Interfaces

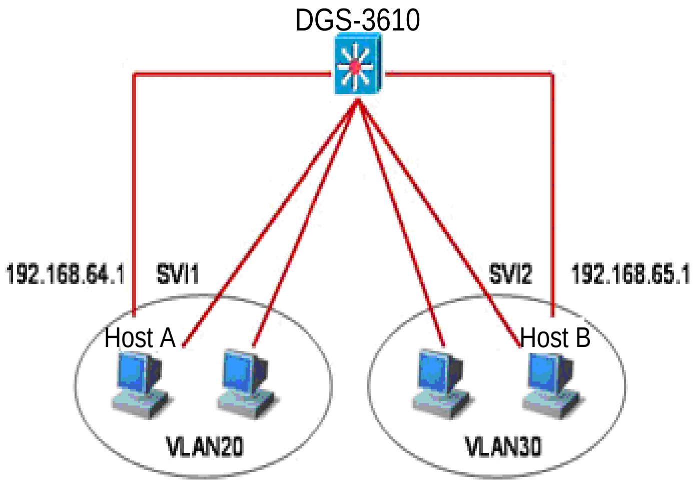
This section discusses the types and definitions of L3 interfaces. L3 interfaces fall into the following categories.

- SVI (Switch virtual interface)
- Routed Port
- L3 Aggregate Ports

6.1.2.1 SVI (Switch virtual interface)

SVI, short for Switch Virtual Interface, is used to implement the logical interface for layer 3 switching. SVI can work as the management interface of the local computer. This interface allows administrator to manage devices. You can also create SVI as a gateway interface, which serves as the virtual sub-interface for each VLAN. It can be used for cross-VLAN routing in the layer 3 device. SVI can be created simply by creating SVI using the **interface vlan** interface configuration command, and assigning an IP address to the SVI to establish a route between VLANs.

As the following figure depicts, the hosts of VLAN20 can communicate directly without routing through an L3 device. If host A in VLAN20 wants to communicate with host B in VLAN30, they have to do this through SVI1 corresponding to VLAN20 and SVI2 corresponding to VLAN30.



6.1.2.2 Routed Port

A Routed Port is a physical port, it’s like a port on the layer 3 device. It can be configured by using a layer 3 routing protocol. On the layer 3 device, a single physical port can be set as Routed port that serves as the gateway interface for layer 3 switching. A Routed Port serves as an access port that is not related to a specific Vlan. Routed port provides no L2 switching functions. You may change an L2 switch port into a Routed port by using the **no switchport** command and then assign an IP address to it for creating a route. Note that using the **no switchport** interface configuration command will disable and restart this port and delete all the features on layer 2 from this port.

Caution

However, when a port is a member port of an L2 Aggregate Port, the **switchport/ no switchport** commands will not be used for swiching between the layers..

6.1.2.3 L3 Aggregate Ports

Just like L2 Aggregate Port, the L3 Aggregate port is a logically aggregated port group that consists of multiple physical member ports. The aggregated ports must be layer 3 ports of the same type. For layer 3 switching, AP that serves as the gateway interface for layer 3 switching, is considered to take multiple physical links in the same aggregate group as one logical link. This is an important method for expanding the link bandwidth. In addition, the frames that pass through the L3 Aggregate port will undergo traffic balancing on the member ports of the L3 Aggregate port. If one member link of AP fails, the L3 Aggregate port automatically assigns the traffic on this link to other working member links, enhancing the connection reliable.

It offers no functions of L2 switching. You may establish routes by first changing an L2 Aggregate port without members into an L3 Aggregate port through using the **no switchport** command and then adding multiple routed ports on this L3 Aggregate port, at last assigning an IP address to it.

6.2 Configuring Interfaces

This section provides the default configuration, guidelines, steps, and examples of configuration.

6.2.1 Numbering Rules for Interfaces

The number of a switch port consists of a slot number and number of the port on the slot. For example, the number of the corresponding interface of the third port in slot 2 is 2/3. The slot number ranges from 0 to the total number of slots. The rule of numbering the slots: For panels facing the device, their slots are numbered from front to back, from left to right, and from top to bottom, starting from 1 and increased in turn. Ports in a slot are numbered from left to right from 1 to the number of ports in the slot. For the devices which can be either optical port or electrical port and in either case, they use the same port number. You may view information on a slot and ports on it by using the **show** command in command lines.

Aggregate Ports are numbered from 1 to the supported number of Aggregate Ports by the device.

The SVI is numbered by the VID of its corresponding VLAN.

Caution

The number of the static slot on a device is always 0. The numbers of dynamic slots (pluggable modules or line cards) start from 1.

6.2.2 Using Interface Configuration Commands

You may use the **interface** command to enter interface configuration mode in global configuration mode.

Command	Function
DGS-3610(config)# **interface** *interface ID*	Input **interface** to enter interface configuration mode. You may also set the certain range of interfaces by using the **interface range** or **interface range macro** command. However, the interfaces in the same range must be of the same types and characteristics.

This example shows the accessing the Gigabitethernet2/1 interface:

```
DGS-3610(config)# interface gigabitethernet 2/1
DGS-3610(config-if)#
```

You may set interface attributes in interface configuration mode.

6.2.3 Using the interface range Command

6.2.3.1 Setting Interface Range

You may set multiple interfaces at once by using the **interface range** command in global configuration mode. When you enter **interface range** configuration mode, all the set attributes are applicable to all interfaces within the range.

Command	Function
DGS-3610(config)# **interface range** {*port-range* | **macro** *macro_name*}	Input the interfaces within some range. You may use the **interface range** command to specify range segments. The **macro** parameter can be defined by the macro of a range. See the section of *Configuring and Using Macro Definition for Interface Range*. Separate each range segments with a comma (,).. Be sure that all interfaces within all the range segments in the same command belong to the same type of interfaces.

When using the **interface range** command, please pay attention to the format of the range parameters:

Effective interface range formats are:

vlan *vlan-ID* - *vlan-ID*, with VLAN ID in the range of 1–4094;

Fastethernet *slot*/{*the first port*} - { the last *port*};

Gigabitethernet *slot*/{*the first port*} - { the last *port*};

TenGigabitethernet *slot*/{*the first port*} - { the last *port*};

Aggregate Port Aggregate *port number*, - *Aggregate port number* in the range of 1~MAX;.

Interfaces contained in an **interface range** must be of the same type, or all of them are fastethernet, gigabitethernet, or are Aggregate port, or SVI.

Following example shows how to use the **interface range** command in global configuration mode:

```
DGS-3610# configure terminal
DGS-3610(config)# interface range fastethernet 1/1 - 10
DGS-3610(config-if-range)# no shutdown
DGS-3610(config-if-range)#
```

This example shows how to separate ranges by a comma “,”:

```
DGS-3610# configure terminal
DGS-3610(config)# interface range fastethernet 1/1-5, 1/7-8
DGS-3610(config-if-range)# no shutdown
DGS-3610(config-if-range)#
```

6.2.3.2 Configuring and Using Macro Definition for Interface Range

You may define some macros instead of inputting port ranges. However, you have to define these macros using the **define interface-range** command before you use the **macro** keywords in the **interface range** command.

Command	Function
DGS-3610(config)# **define interface-range** *macro_name interface-range*	Define the macro for interface range. Name of the interface-range macro, not exceeds to 32 characters. Macro definition may cover multiple range segment. The interfaces within all range segments in the same macro definition must belong to the same type.
DGS-3610(config)# **interface range macro** *macro_name*	The strings of macro definition will be saved in the memory. When you use the **interface range** command, you can use the name of macro definition to replace the string of the interface-range .

To delete a macro definition, use the **no define interface-range macro_name** command in global configuration mode.

When defining an interface range using the **define interface-range** command, please be noted:

Effective formats of interface range are:

– **vlan** *vlan-ID* - *vlan-ID*, with VLAN ID in the range of 1~4094;

– **fastethernet** *slot*/{*the first port*} - { the last *port*};

– **gigabitethernet** *slot*/{*the first port*} - { the last *port*};

– **Aggregate Port Aggregate** *port number*, with *Aggregate port number* in the range of 1~MAX.

Interfaces contained in an i**nterface range** must be of the same type, that is, they should be all switch ports or Aggregate ports, or SVIs.

Following example shows how to define the macro definition of fastethernet1/1-4 by using the **define interface-range** command:

```
DGS-3610# configure terminal
DGS-3610(config)# define interface-range resource
fastethernet 1/1-4
DGS-3610(config)# end
```

Following example shows how to define the macro definition of multiple interface range segments:

```
DGS-3610# configure terminal
DGS-3610(config)# define interface-range ports1to2N5to7
fastethernet 1/1-2, 1/5-7
DGS-3610(config)# end
```

This example uses macro to define the ports1to2N5to7 for setting interfaces within a specified range:

```
DGS-3610# configure terminal
DGS-3610(config)# interface range macro ports1to2N5to7
DGS-3610(config-if-range)#
```

Following example shows how to delete the macro definition ports1to2N5to7:

```
DGS-3610# configure terminal
DGS-3610(config)# no define interface-range ports1to2N5to7
DGS-3610# end
```

6.2.4 Selecting Interface Medium Type

Some interfaces have multiple medium types and allow users to choose. You can choose one of the mediums for use. Once you have selected a ttype of medium, the attributes like connection status of the interface, speed, duplex, and flow control will be determined by the medium. When you change the medium, the attributes of the new type of medium chosen will take their default values. Please reconfigure the attibutes when necessary.

This configuration command is only valid for aphysical port. The Aggregate Port and SVI port do not allow you to set the medium type.

This configuration command is only valid for a port that supports medium selection.

The ports configured as the member of Aggregate Port must have the same media type. Otherwise, they cannot be added to the AP. The port type of Aggregate Port member ports cannot be changed.

Command	Function
DGS-3610(config-if)# **medium-type** { **fiber** | **copper** }	Set the medium type for a port.

This example sets the medium type for the interface gigabitethernet 1/1:

```
DGS-3610# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
DGS-3610(config)# interface gigabitethernet 1/1
DGS-3610(config-if)# medium-type fiber
DGS-3610(config-if)# end
```

6.2.5 Setting Description and Management Status of the Interface

You may give an interface a particular name, namely the description of the interface (description) to identity the interface for you to remember its functions. You may set the concret name of the interface according to the meaning what you want to express, for example, if you want to assign Gigabitethernet 1/1 for the porticular use of user A, you may set its description to “Port for User A”.

Command	Function
DGS-3610(config-if)# **description** *string*	Set the description of the interface in no more than 32 characters

The following example shows how to set the description of Gigabitethernet 1/1:

```
DGS-3610# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
DGS-3610(config)# interface gigabitethernet 1/1
DGS-3610(config-if)# description PortForUser A
DGS-3610(config-if)# end
```

In some circumstances, you may need to disable some interface. You can do this by setting the management status of the interface. Once disabled, no frames will be sent and received on an interface, all the function corresponding to this interface will be lost. You can also restart an interface disabled by setting its management status. The management status of an interface can be two types, namely, **up** or **down**. When a port is disabled, the management status of the port is **down**; otherwise, it is in the status **up**.

Command	Function
DGS-3610(config-if)# **shutdown**	Shut down an interface.

The following example illustrates how to shut down interface Gigabitethernet 1/2.

```
DGS-3610# configure terminal
DGS-3610(config)# interface gigabitethernet 1/2
DGS-3610(config-if)# shutdown
DGS-3610(config-if)# end
```

6.2.6 Setting Speed, Duplexing, and Flow Control for Interfaces

The section describes how to set the speed rate, duplex , and flow control for interfaces.

The following command is only valid for Switch Port and Routed Port.

Command	Function
DGS-3610(config-if)# **speed** {**10** | **100** | **1000** | **auto** }	Select the speed rate parameter of the interface or set it to **auto**. Caution: 1000 applies only to gigabit interfaces. and the rate of the optical interface for the devices is forced to be 1000M.
DGS-3610(config-if)# **duplex** {**auto** | **full** | **half** }	Set duplex mode of the interface
DGS-3610(config-if)# **flowcontrol** {**auto** | **on** | **off** }	Set flow control mode of the interface.. Note: When **speed**, **duplex**, and **flowcontrol** are all set to non-auto, the interface will stop auto-negotiation.

In interface configuration mode, restore the defaulted values (auto-negotiation) of speed rate, duplex, and flow control by using the commands **no speed**, **no duplex**, and **no flowcontrol**. The following example shows how to set the speed rate of Gigabitethernet 1/1 to 1000M, set its duplex mode to **full**, and flow control to **off**.

```
DGS-3610# configure terminal
DGS-3610(config)# interface gigabitethernet 1/1
DGS-3610(config-if)# speed 1000
DGS-3610(config-if)# duplex full
DGS-3610(config-if)# flowcontrol off
DGS-3610(config-if)# end
```

⚠ **Caution**

The cross-chip and cross-stack traffic control does not take effective for the DGS-3610 series switches, so it is necessary to note whether there is cross-chip or cross-stack traffic control when configuring traffic control.

6.2.7 Configuring MTU of the Interface

When a heavy throughout of data switching occurs on a port, there may be a frame beyond the Ethernet standard frame length. This type of frame is called jumbo Frame. A user can control the maximum frame length that the port is allowed to receive and send by setting the MTU of the port.

MTU refers to the length of a valid data segment in a frame, excluding the overhead of Ethernet encapsulation.

The MTU of a port is checked during input but not output. The MTU will not be checked at output. If the frame received by the port is longer than the set MTU, then it will be discarded.

The range of MTU allowed to be set is from 64 to 9216 bytes, the corresponding granularity is 4 bytes and its default is 1500 bytes.

This configuration command is only valid for physical ports. The SVI interface currently does not support the MTU setting.

Command	Function
DGS-3610(config-if)# **Mtu** *num*	Set the MTU for a port *Num*: <64-9216>

This example shows how to set the MTU for the Gigabitethernet 1/1 interface:

```
DGS-3610# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
DGS-3610(config)# interface gigabitethernet 1/1
DGS-3610(config-if)# mtu 64
DGS-3610(config-if)# end
```

6.2.8 Configuring L2 Interfaces

The following table shows the default settings of L2 interfaces. For the configurations of VLAN and ports, please refer to *Configuring VLAN* and *Configuring Flow Control Based on Ports*.

The default configurations of layer 2 interface are shown in the table below.

Attribute	Default Configuration
Working mode	L2 switch mode
Switch port mode	access port
Allowed VLAN range	VLAN 1~4094
Default VLAN (for access port)	VLAN 1
Native VLAN (for trunk port)	VLAN 1
Media Type	copper
Interface management status	Up
Interface Description	Void
Speed	Auto-negotiation
Duplex mode	Auto-negotiation
Flow control	Auto-negotiation

Attribute	Default Configuration
Aggregate port	None
Storm Control	Off
Port protection	Off
Port Security	Off

6.2.8.1 Configuring Switch Port

6.2.8.1.1 Configuring Access/Trunk Port

This section is described to the operation modes(access/trunk port) of setting the Switchport of and the related configuration in each mode.

To set the attributes of a Switch Port, use **switchport** or other commands in interface configuration mode:

Command	Function
DGS-3610(config-if)# **switchport mode** {**access** | **trunk** }	Set the operation mode of the interface.

The following example shows how to set the operation mode of Gigabitethernet 1/2 interface to access port.

```
DGS-3610# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DGS-3610(config)# interface gigabitethernet 1/2
DGS-3610(config-if)# switchport mode access
DGS-3610(config-if)# end
```

Command	Function
DGS-3610(config-if)# **switchport access vlan** *vlan-id*	Set the VLAN to which the access port belongs.

The following example shows how to configure the vlan to which the access port gigabitethernet 2/1 to 100

```
DGS-3610# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DGS-3610(config)# interface gigabitethernet 2/1
DGS-3610(config-if)# switchport access vlan 100
DGS-3610(config-if)# end
```

Set the native VLAN of the trunk port.

Command	Function
DGS-3610(config-if)# **switchport trunk native vlan** *vlan-id*	Set the NATIVE VLAN of the trunk port.

The following example shows how to set the native vlan of the trunk port Gigabitethernet 2/1 to 10.

```
DGS-3610# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DGS-3610(config)# interface gigabitethernet 2/1
DGS-3610(config-if)# switchport trunk native vlan 10
DGS-3610(config-if)# end
```

Set the port-security. For more detailed information about port-security, please refer to *Flow c Control Based on Ports*:

Command	Function
DGS-3610(config-if)# **switchport port-security**	Set the port-security.

The following example shows how to enable port security of Gigabitethernet 2/1.

```
DGS-3610# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DGS-3610(config)# interface gigabitethernet 2/1
DGS-3610(config-if)# switchport port-security
DGS-3610(config-if)# end
```

For configuring the speed rate, duplexe, and flow control of an interface, see the section of *Setting Speed, Duplexe, and Flow Control for Interfaces.*

The following example shows how to set Gigabitethernet 2/1 to access port, its VLAN to 100, its speed, duplexe, and flow control to auto-negotiation and enable port security.

```
DGS-3610# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DGS-3610(config)# interface gigabitethernet 2/1
DGS-3610(config-if)# switchport access vlan 100
DGS-3610(config-if)# speed auto
DGS-3610(config-if)# duplex auto
DGS-3610(config-if)# flowcontrol auto
DGS-3610(config-if)# switchport port-security
DGS-3610(config-if)# end
```

6.2.8.1.2 Configuring Hybrid Port

You can configure the hybrid port by performing the following steps:

Command	Description
configure terminal	Enter configuration mode
interface <*interface***>**	Enter the interface configuration mode. Megabit, Gigabit, 10 Gigabit
switchport mode hybrid	Configure the port as a hybrid port
no switchport mode	Delete the port mode
switchport hybrid native vlan *id*	Set the default VLAN for the hybrid port

Command	Description
switchport hybrid allowed vlan [[**add**] [**tagged | untaged**]] **|remove**] *vlist*	Set the output rule for the port

```
DGS-3610# configure terminal
DGS-3610(config)# interface g 0/1
DGS-3610(config-if)# switchport mode hybrid
DGS-3610(config-if)# switchport hybrid native vlan 3
DGS-3610(config-if)# switchport hybrid allowed vlan untagged 20-30
DGS-3610(config-if)# end
DGS-3610# show running interface g 0/1
```

6.2.8.2 Configuring L2 Aggregate Ports

This section describes how to create an L2 Aggregate Port and some related settings.

You may create an L2 Aggregate Port by using **aggregateport** in interface configuration mode. For details, see *Configuring Aggregate Port.*

6.2.8.3 Clearing Interface Statistics and Then Resetting this interface

In privileged EXEC mode, you may clear the statistics of an interface and then reset it by using the **clear** command. This command is only applicable to the Switch Port, member of L2 Aggregate port, Routed port, and member of L3 Aggregate port. The **clear** command is as follows.

Command	Function
DGS-3610# **clear counters** [*interface-id*]	Clear interface statistics.
DGS-3610# **clear interrface** *interface-id*	Reset interface hardware.

In privileged EXEC mode, use **show interfaces** to display the counters. In privileged EXEC mode, use **clear counters** to clear the counters. If the interface is not specified, the counters on all interfaces will be cleared.

The following example shows how to clear the counter of gigabitethernet 1/1.

```
DGS-3610# clear counters gigabitethernet 1/1
```

6.2.9 Configuring L3 Interfaces

Configuring L3 Interfaces:

Command	Function
DGS-3610(config-if)# **no switchport**	Shut down the interface and change it to L3 mode. This command applies to Switch Ports and L2 Aggregate ports only.

Command	Function
DGS-3610(config-if)# **ip address** *ip_address subnet_mask* {[**secondary** | **tertiary** | **quartus**][**broadcast**]}	Configure the IP address and subnet mask.

To delete the IP address of an L3 interface, use the **no ip address** command in interface configuration mode.

The **no switchport** operation cannot be performed on one member of L2 Aggregate Ports.

The following example shows how to set an L2 interface to routed port and assign an IP address to it.

```
DGS-3610# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DGS-3610(config)# interface gigabitethernet 2/1
DGS-3610(config-if)# no switchport
DGS-3610(config-if)# ip address 192.20.135.21 255.255.255.0
DGS-3610(config-if)# no shutdown
DGS-3610(config-if)# end
```

6.2.9.1 Configuring SVI

The section describes how to create an SVI and some related configuration of SVI.

You may create an SVI or modify an existing one by using **interface vlan** *vlan-id*.

Configuration of SVI:

Command	Function
DGS-3610(config)# **interface vlan** *vlan-id*	Enter SVI interface configuration mode.

Then, you can configure the attributes related to SVI. For detailed information, please refer to the *Configuring IP Single Address Route*.

The following example shows how to enter interface configuration mode and how to assign an IP address to SVI 100.

```
DGS-3610# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DGS-3610(config)# interface vlan 100
DGS-3610(config-if)# ip address 192.168.1.1 255.255.255.0
DGS-3610(config-if)# end
```

6.2.9.2 Configuring Routed Ports

This section describes how to create Routed port and the related configuration of Routed port.

You may create a Routed port by using **no switchport** after you have entered an interface in interface mode.

Create one Routed port and assign an IP address to the ROuted port:

Command	Function
DGS-3610(config-if)# **no switchport**	Shut down the interface and then change it to L3 mode.
DGS-3610(config-if)# **ip address** *ip_address subnet_mask*	Configure the IP address and subnet mask.

Caution

No layer switching can be performed through using **switchport/ no switchport** when an interface is a member of an L2 Aggregate Port.

The following example shows how to set an L2 interface to Routed port and then assign an IP address to it.

```
DGS-3610# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DGS-3610(config)# interface fastethernet 1/6
DGS-3610(config-if)# no switchport
DGS-3610(config-if)# ip address 192.168.1.1 255.255.255.0
DGS-3610(config-if)# no shutdown
DGS-3610(config-if)# end
```

6.2.9.3 Configuring L3 Aggregate Ports

This section describes how to create an L3 Aggregate Port and some related configuration.

In the interface mode, you can use **no switchport** to change a L2 Aggregate Port to a L3 Aggregate Port:

Command	Function
DGS-3610(config-if)# **no switchport**	Shut down the interface and change it to L3 mode.
DGS-3610(config-if)# **ip address** *ip_address subnet_mask*	Configure the IP address and subnet mask.

The following example shows how to create an L3 Aggregate Port and assign an IP address to it.

```
DGS-3610# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DGS-3610(config)# interface aggregateport 2
DGS-3610(config-if)# no switchport
DGS-3610(config-if)# ip address 192.168.1.1 255.255.255.0
```

```
DGS-3610(config-if)# no shutdown
DGS-3610(config-if)# end
```

6.3 Showing Interface Configuration and Status

This section covers the showing content and the showing instances of the interface. You may view the interface status by using **show** command in privileged EXEC mode. To show interface status, use the following commands.

Command	Function
DGS-3610# **show interfaces** [*interface-id*]	Show all the statuses of a specified interface and its configuration information.
DGS-3610# **show interfaces** *interface-id* **status**	Show the status of an interface.
DGS-3610# **show interfaces** [*interface-id*] **switchport**	Show the status information of administrative and operational on an switchable interface (non-routing interface).
DGS-3610# **show interfaces** [*interface-id*] **description**	Show the description and status of a specified interface.
DGS-3610# **show interfaces** [*interface-id*] **counters**	Show the statistics of a specified port. Where, the rate display may be the error within 0.5%.

The following example shows how to display the interface status of Gigabitethernet 1/1.

```
DGS-3610# show interfaces gigabitethernet 1/1
GigabitEthernet              : Gi 1/1
Description                  : user A
AdminStatus                  : up
OperStatus                   : down
Hardware                     : 1000BASE-TX
Mtu                          : 1500
PhysAddress                  :
LastChange                   : 0:0h:0m:0s
AdminDuplex                  : Auto
OperDuplex                   : Unknown
AdminSpeed                   : 1000M
OperSpeed                    : Unknown
FlowControlAdminStatus       : Enabled
FlowControlOperStatus        : Disabled
Priority   : 1
```

The following is an example of showing the status and configuration information of interface SVI 5.

```
DGS-3610# show interfaces vlan 5
```

```
VLAN   : V5
Description                 : SVI 5
AdminStatus                 : up
OperStatus                  : down
Primary Internet address    : 192.168.65.230/24
Broadcast address           : 192.168.65.255
PhysAddress                 : 00d0.f800.0001
LastChange                  : 0:0h:0m:5s
```

The following is an example of showing the status of aggregate port 3.

```
DGS-3610# show interfaces aggregateport 3:

Interface                   : AggreatePort 3
Description                 :
AdminStatus                 : up
OperStatus                  : down
Hardware                    : -
Mtu                         : 1500
LastChange                  : 0d:0h:0m:0s
AdminDuplex                 : Auto
OperDuplex                  : Unknown
AdminSpeed                  : Auto
OperSpeed                   : Unknown
FlowControlAdminStatus      : Autonego
FlowControlOperStatus       : Disabled
Priority                    : 0
```

This example shows the configuration information of interface GigabitEthernet 1/1:

```
DGS-3610# show interfaces gigabitEthernet 1/1 switchport
Interface  Switchport Mode     Access    Native    Protected VLAN lists
---------- ---------- --------- --------- --------- --------- ------------
gigabitethernet 1/1     Enabled  Access     1        1        Enabled   All
```

This example shows the interface description of interface Gigabitethernet 2/1:

```
DGS-3610# show interfaces gigabitethernet 1/2 description
Interface              Status    Administrative    Description
--------------------  ---------   ---------------    ----------------
gigabitethernet 2/1     down       down            Gi 2/1
```

This example shows statistics of the ports.

```
DGS-3610# show interfaces gigabitethernet 1/2 counters
Interface : gigabitethernet 1/2
5 minute input rate         : 9144 bits/sec, 9 packets/sec
5 minute output rate        : 1280 bits/sec, 1 packets/sec
InOctets                    : 17310045
InUcastPkts                 : 37488
InMulticastPkts             : 28139
InBroadcastPkts             : 32472
OutOctets                   : 1282535
```

```
OutUcastPkts                 : 17284
OutMulticastPkts             : 249
OutBroadcastPkts             : 336
Undersize packets            : 0
Oversize packets             : 0
collisions                   : 0
Fragments                    : 0
Jabbers                      : 0
CRC alignment errors         : 0
AlignmentErrors              : 0
FCSErrors                    : 0
dropped packet events (due to lack of resources): 0
packets received of length (in octets):
  64:46264, 65-127: 47427, 128-255: 3478,
  256-511: 658, 512-1023: 18016, 1024-1518: 125
```

6.4 LinkTrap Policy Configuration

In the devices, you can configure whether the LinkTrap of this interface will be sent on the basis of the interface configuration. When the function is enabled, if the Link status is changed for the interface, SNMP will send the LinkTrap. Otherwise, it will not be sent. By default, this function is enabled.

6.4.1 Configuring Command

Command	Function
DGS-3610(config-if)# **[no] snmp trap link-status**	Enable or disable the function for sending the link trap of this interface.

6.4.2 Configuration Example

The following configuration shows how to configure the interface to unforwarding Link trap:

```
DGS-3610(config)# interface gigabitEthernet 1/1
DGS-3610(config-if)# no snmp trap link-status
```

7 Aggregate Port Configuration

This chapter explains how to configure an aggregate port on DGS-3610 series.

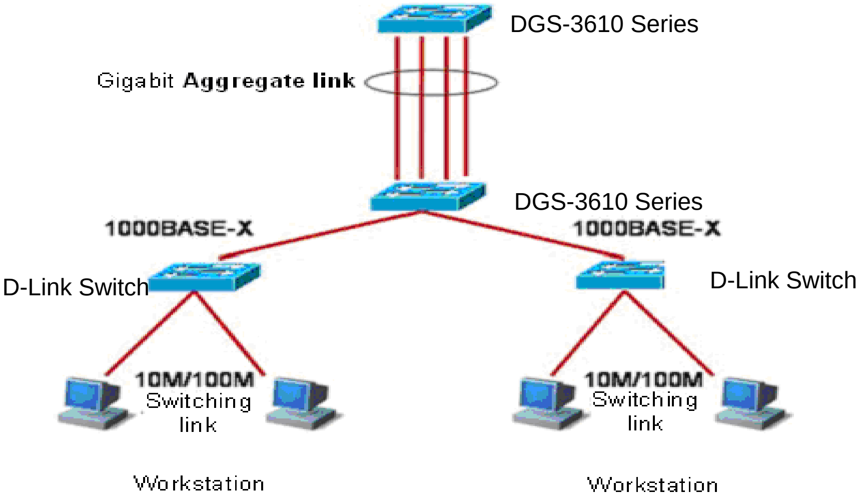
7.1 Overview

7.1.1 Understanding Aggregate Port

Multiple physical connections can be bound together and to form a logical connection, which is called an aggregate port (referred to as AP below). DGS-3610 series provides the devices with AP function that complies with the IEEE802.3ad standard. This function can be used to expand the link bandwidth so as to provide higher reliability for connection .

When a member link in the AP is disconnected, the system will automatically allocate the traffic of the member link to other effective member links in the AP. The broadcast or multicast packets received at one member link in AP will not be forwarded to other member links.

Figure 7-1 Typical AP configurations



7.1.2 Understanding Traffic Balancing

The AP can evenly distribute the traffic to the member links of the AP according to the characteristic values such as of the source MAC address, destination MAC address, source

MAC address + destination MAC address, source IP address, destination IP address and source IP address + destination IP address packets. The **aggregateport load-balance** command can be used to set the traffic distribution style.

The source MAC address traffic balance balancing means that the messages are distributed onto each member link of AP according to the source MAC addresses of the packets. Packets with different source MAC addresses are forwarded to different member links. The packets with the same source MAC are forwarded from the same member link.

The traffic balancing based on destination MAC addresses is to distribute the packets to every member link of the AP according to the destination MAC addresses of the packets. Packets with the same packets from the destination MAC addresses are forwarded from the same member links. The packets with the different destination MAC are forwarded from the different member links.

The traffic balancing based on source + destination MAC addresses is the process to distribute the packets to every member link of the AP according to the source MAC + destination MAC addresses of the packets. The packets with difference source + destination MAC addresses can be distributed to the member link of the same AP.

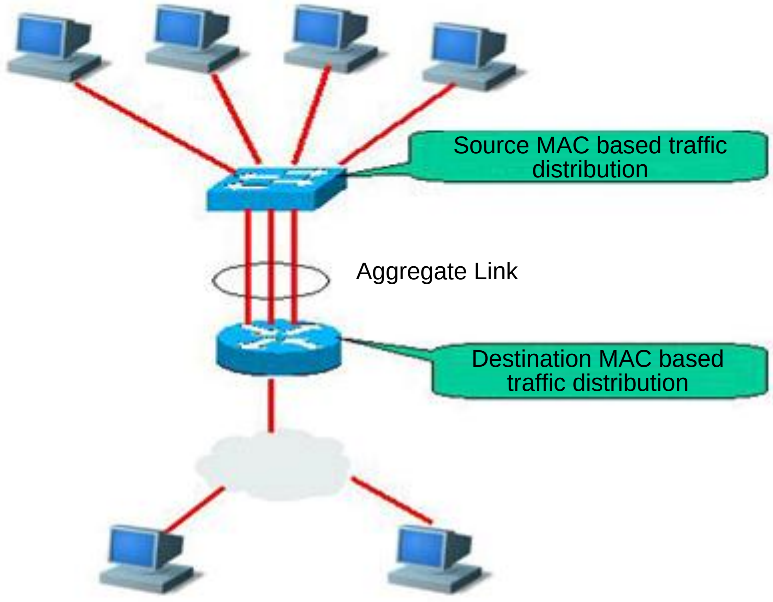
The traffic balancing based on source or destination IP addresses is the process to distribute the packets according to their source or destination IP addresses. Packets with different source or destination IP addresses are forwarded to different member links. The packets with the same source or destination IP addresses are forwarded from the same member link. This traffic balancing mode is used for the L3 packets. If L2 packets are received when this mode is used, the traffic is balanced automatically according to the source or destination MAC address of the L2 packets.

The traffic balancing based on source + destination IP addresses is the process to distribute the packets according to their source + destination IP addresses. This traffic balancing mode is used for the L3 packets. If L2 packets are received when this mode is used, the traffic is balanced according to the MAC addresses of the L2 packets. The packets with difference source + destination IP addresses can be distributed to the member link of the same AP.

An appropriate traffic distribution method should be set according to the different network environments, so that the traffic can be evenly distributed to the links for making full use of the network bandwidth.

In the following diagram, a switch communicates with a router through the AP, and the router serves as the gateway for all the devices within the internal network (such as four PCs on the top of the diagram). The source MAC addresses of all the packets that the devices within the external network (such as two PCs at the bottom of the diagram) sent through the router are the MAC address of the gateway. In order to share the load of the traffic between the router and other hosts to other links, the traffic balancing should be performed according to the destination MAC address. However, the traffic balancing should be performed according to the source MAC address on the switch.

Figure 7-2 AP traffic balancing


Source MAC based traffic distribution
Aggregate Link
Destination MAC based traffic distribution

7.2 Configuring Aggregate Port

7.2.1 Default Configurations of Aggregate Port

The default configurations of AP are shown in the table below.

Attribute	Default value
Layer-2 AP interface	None
Layer-3 AP interface	None
Traffic balancing	Trafficbalancing is distributed according to the source MAC addresses of the input packets. The defaut traffic balancing of DGS-3610 series switches is balanced according to the source MAC address+destination MAC address input.

7.2.2 Configuration Guide for Aggregate Port

The speed rates of the AP member ports must be coherent.

L2 ports can only be added to a L2 AP, and L3 ports can only be added to a L3 AP.

The AP cannot be set with any port security function.

When a port is added to an AP that does not exist, the AP will be created automatically.

Once a port is added to an AP, the attributes of the port will be replaced by those of the AP.

Once a port is removed from an AP, the attributes of the port will be restored as those before it is added to the AP.

Note

When a port is added to the AP, you cannot perform any configuration on the port before the port exits the AP.

7.2.3 Configuring Aggregate Port

In the interface configuration mode, add an interface to the AP by performing the following steps.

Command	Function
DGS-3610(config-if-range)# **port-group** *port-group-number*	Add an AP on the interface (create the AP as well if it does not exist).

In the interface configuration mode, use the **no port-group** command to remove a physical port from the AP.

The example below shows how to configure layer-2 Ethernet interface 1/0 to the members of layer-2 AP 5.

```
DGS-3610# configure terminal
DGS-3610(config)# interface range gigabitEthernet 0/1
DGS-3610(config-if-range)# port-group 5
DGS-3610(config-if-range)# end
```

The command DGS-3610(config)# **interface aggregateport** *n* (n is the AP number) in the global configuration mode can be used to directly create an AP (if AP n does not exist).

7.2.4 Configuring Layer-3 Aggregate Port

By default, an aggregate port is on layer 2. To configure a layer-3 AP, perform the following operations.

The example below shows how to configure a layer-3 AP interface (AP 3) and configure its IP address (192.168.1.1):

```
DGS-3610# configure terminal
DGS-3610(config)# interface aggretegateport 3
DGS-3610(config-if)# no switchport
DGS-3610(config-if)# ip address 192.168.1.1 255.255.255.0
DGS-3610(config-if)# end
```

7.2.5 Configuring Traffic Balancing of Aggregate Port

In the configuration mode, configure the traffic balancing for the AP by performing the following steps:

Command	**Function**
DGS-3610(config)# **aggregateport load-balance** {**dst-mac** | **src-mac | src-dst-mac |** **dst-ip | src-ip | ip** }	Set the AP traffic balancing and select the algorithm to be used: **dst-mac:** Traffic is distributed according to the destination MAC addresses of the input packets. In various AP links, the packets with the same destination MAC address are sent to the same member link, and those with different destination MAC addresses are allocated to different member links. **src-mac:** Traffic is distributed according to the source MAC addresses of the incput packets. In various AP links, the packets from different MAC addresses are allocated to different member links, and those from the same MAC addresses use the same member links. ip: Traffic is distributed according to the source IP and destination IP. Packets with different source- destination IP addresses are forwarded to different member links. The packets with the same source-destination IP addresses are forwarded from the same member link. **dst-ip**: Traffic is distributed according to the destination MAC addresses of the incoming packets. In various AP links, the packets with the same destination IP address are sent to the same member link, and those with different destination IP addresses are allocated to different member links. **src-mac**: The traffic is allocated according to the source MAC addresses of the inputted packets. In various AP links, the packets from different IP addresses are allocated to different member links, and those from the same IP addresses use the same member links. **src-dst-mac:** The traffic is distributed according to the soruce and destination MAC addresses. Packets with different source-destination MAC addresses are forwarded to different member links. The packets with the same source-destination MAC addresses are forwarded from the same member link.

To restore the AP traffic balancing configuration to default, run the following command in the global configuration mode:**no aggregateport loag-balance** command

7.3 Showing Aggregate Port

In the privileged mode, show the AP configuration by performing the following steps.

Command	Function
DGS-3610# **show aggregateport** [*port-number*]{**load-balance | summary**}	Show the AP settings.

```
DGS-3610# show aggregateport load-balance
Load-balance : Source MAC address
DGS-3610# show aggregateport 1 summary
AggregatePort MaxPorts SwitchPort Mode   Ports
------------- -------- ---------- ------
Ag1            8        Enabled         ACCES
```

8 VLAN Configuration

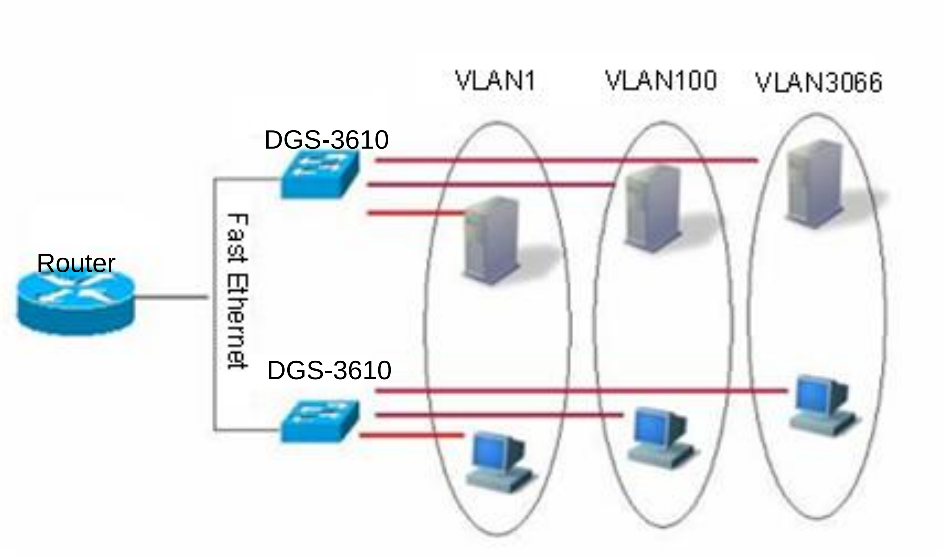
This chapter describes how to configure IEEE802.1q VLAN.

8.1 Overview

Virtual Local Area Network (VLAN) is a logical network divided on a physical network. VLAN corresponds to the L2 network in the ISO model. The division of VLAN is not restricted by the physical locations of network ports. A VLAN has the same attributes as a common physical network. Except no restriction in physical locations, it is the same as a common VLAN. The unicast, broadcast and multicast and frames on L2 are forwarded and distributed within a VLAN, not directly to another VLAN. Therefore, when the host connected to a port wants to communicate with another host in a different VLAN, a layer 3 device must be used. See the following diagram.

You can define one port as the member of one VLAN. All the terminals connected to the particular port are part of the VLAN, and the whole network supports multiple VLANs. When you add, delete, and modify a user, you do not need to modify the network configuration physically.

Figure 8-1



Same as a physical network, the VLAN is usually connected to an IP subnet. A typical example is: all the hosts in the same IP subnet belong to the same VLAN, and a layer 3 device must be used for communication between VLANs. DGS-3610 series can perform IP routing between VLANs through the SVI (Switch Virtual Interfaces). For the configuration about the SVI, please see *Interface Management Configuration and Configuring IP Unicast Routing Configuration*.

8.1.2 Supported VLAN

The VLAN that the product supports complies with the IEEE802.1Q standard, and supports up to 4094 VLANs (VLAN ID 1-4094), where VLAN 1 is the default VLAN that cannot be deleted.

⚠ **Caution**

The DGS-3610 series devices support 4094 VLANs.

8.1.3 VLAN Member Type

You can determine the frames that can pass a port, and the number of VLANs that the port belongs to by configuring the member type of the port in the VLAN. See the following table for the details of the VLAN member type:

VLAN Member Type	VLAN Port Feature
Access	One Access port belongs to only one VLAN, which must be specified manually.
Trunk (802.1Q)	By default, one Trunk port belongs to all the VLANs of the device, and it can forward the frames of all the VLANs. However, you can impose restriction by setting an allowed VLAN list (allowed-VLANs).

8.2 Configuring VLAN

One VLAN is identified by its VLAN ID. In the device, you can add, remove, and modify VLAN 2-4094. VLAN 1 is created by the device automatically and cannot be deleted.

You can configure the VLAN member type of a port, or add, or remove a VLAN in the interface configuration mode.

8.2.1 Saving the VLAN Configuration Information

You can enter the **copy running-config startup-config** command in the privileged mode to save the VLAN configuration information into the configuration file. To view the VLAN configuration information, use the **show vlan** command.

8.2.2 Default VLAN Configuration

Parameter	Default value	Range
VLAN ID	1	1-4094
VLAN Name	VLAN xxxx, where xxxx is the VLAN ID	No range
VLAN State	Active	Active, Inactive

8.2.3 Creating/Modifying a VLAN

In the privileged mode, you can create or modify a VLAN.

Command	Function
DGS-3610(config)# **vlan** *vlan-id*	Enter one VLAN ID. If you enter a new VLAN ID, the device will create a VLAN for you. If you enter an existing VLAN ID, the device modifies the appropriate VLAN.
DGS-3610(config)# **name** *vlan-name*	(Optional) Name the VLAN. If you skip this step, the device automatically assigns a name of VLAN xxxx, where xxxx is the 4-digit VLAN ID starting with 0. For example, VLAN 0004 is the default name of VLAN 4.

To restore the name of the VLAN to its default, simply enter the **no name** command.

The following example creates VLAN 888, names it to test888, and saves them to the configuration file:

```
DGS-3610# configure terminal
DGS-3610(config)# vlan 888
DGS-3610(config-vlan)# name test888
DGS-3610(config-vlan)# end
```

8.2.4 Deleting a VLAN

You cannot delete the default VLAN (VLAN 1).

In the privileged mode, delete a VLAN:

Command	Function
DGS-3610(config)# **no vlan** *vlan-id*	Enter one VLAN ID to delete it.

8.2.5 Assigning Access Ports to the VLAN

If you assign one interface to a non-existent VLAN, the switch will automatically create that VLAN.

In the privileged mode, assign a interface to a VLAN.

Command	Function
DGS-3610(config-if)# **switchport mode access**	Define the VLAN member type of the interface (L2 ACCESS port)
DGS-3610(config-if)# **switchport access vlan** *vlan-id*	Assign the port to one VLAN.

The following example add Ethernet 1/10 to VLAN20 as an access interface:

```
DGS-3610# configure terminal
DGS-3610(config)# interface fastethernet 1/10
DGS-3610(config-if)# switchport mode access
DGS-3610(config-if)# switchport access vlan 20
DGS-3610(config-if)# end
```

The following example shows how to verify the configuration:

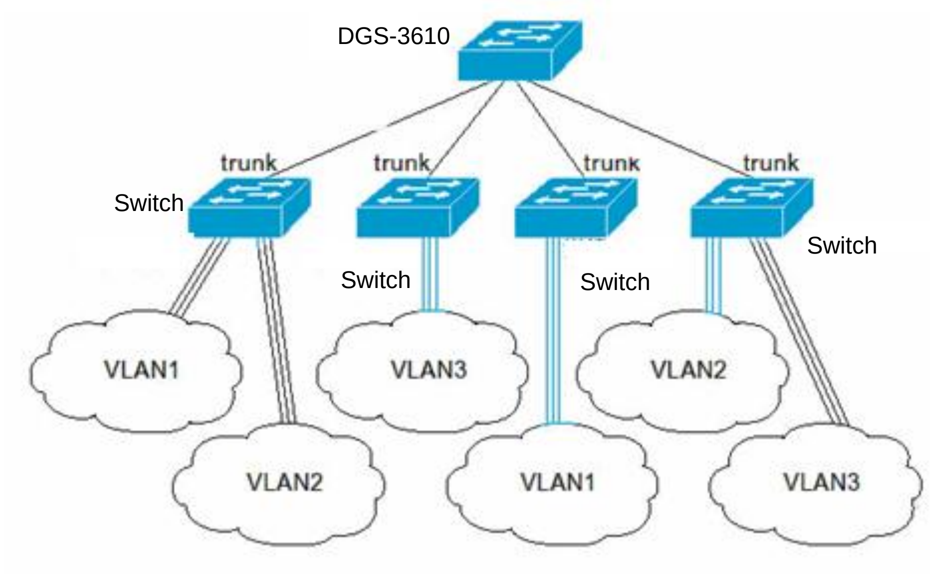
```
DGS-3610(config)#show interfaces gigabitEthernet 3/1 switchport
Switchport is enabled
Mode is access port
Acsess vlan is 1,Native vlan is 1
Protected is disabled
Vlan lists is ALL
```

8.3 Configuring VLAN Trunks

8.3.1 Trunking Overview

A trunk is a point-to-point link that connects one or multiple Ethernet switching interfaces to other network devices (router or switch). One Trunk link can transmit the traffics of multiple VLANs.

The Trunk of DGS-3610 series is encapsulated according to the 802.1Q standard. The following diagram shows one network connected with trunks.



You can set one common Ethernet port or one Aggregate Port to a Trunk port (For the details of Aggregate Port, see *Configuring Aggregate Port*).

To switch an interface between the ACCESS mode and TRUNK mode, use the **switchport mode** command:

Command	Function
DGS-3610(config-if)# **switchport mode access**	Set one interface to the Access mode
DGS-3610(config-if)# **switchport mode trunk**	Set one interface to the Trunk mode

A Native VLAN must be defined for the Trunk interface. A native VLAN means that the UNTAG packets received/sent at the interface are deemed as belonging to the VLAN. Obviously, the default VLAN ID of the interface (that is, the PVID in the IEEE 802.1Q) is the VLAN ID of the native VLAN. In addition, when frames belonging to the native VLAN are sent over the trunk, the UNTAG mode is bound to be used. The default native VLAN of one trunk port is VLAN 1.

When you configure the Trunk link, please make sure that the trunk ports on both ends of the link belong to the same native VLAN.

8.3.2 Configuring a Trunk Port

8.3.2.1 Trunk Port Basic Configuration

In the privileged mode, an interface can be configured to a Trunk port.

Command	Function
DGS-3610(config-if)# **switchport mode trunk**	Define the interface type as a L2 trunk port.
DGS-3610(config-if)# **switchport trunk native vlan** *vlan-id*	Specify one Native VLAN for the interface.

To restore all the trunk attributes of a Trunk port to their defaults, use the **no switchport trunk** interface configuration command.

8.3.3 Defining the Allowed VLAN List of a Trunk Port

By default, a trunk port can transmit all the traffic of VLANs (ID 1-4094) supported by the device. However, you can restrict the traffics of some VLANs from passing the Trunk port by setting its allowed VLAN list.

In the priviledged mode, you can modify the allowed VLAN list of a Trunk port.

Command	Function
DGS-3610(config-if)# **switchport trunk allowed vlan** {**all** | [**add** | **remove** | **except**] } *vlan-list*	(Optional) Configure the allowed VLAN list of the trunk port. The *vlan-list* parameter may be a VLAN or a series of VLANs. It starts with a small VLAN ID and ends with a large VLAN ID, connected with "-",such as 10–20. **all** means that all the supported VLANs are contained in the allowed VLAN list; **add** means to add the allowed VLAN list to the specified VLAN list **remove** means to remove the specified VLAN list from the allowed VLAN list; **except** means to add all the VLANs other than those in the specified VLAN list to the allowed VLAN list;

To restore the allowed VLAN list of the trunk to its default, please use the **no switchport trunk allowed vlan** interface configuration command.

The following example removes VLAN 2 from port 1/15:

```
DGS-3610(config)# interface fastethernet 1/15
DGS-3610(config-if)# switchport trunk allowed vlan remove 2
DGS-3610(config-if)# end
```

```
DGS-3610# show interfaces fastethernet 1/15 switchport
Switchport is enabled
Mode is trunk port
Acsess vlan is 1,Native vlan is 1
Protected is disabled
Vlan lists is
1,3-4094
```

8.3.4 Configure Native VLAN.

One trunk port can receive/send TAG or UNTAG 802.1Q frames. The UNTAG frames are used to transmit the traffic of the Native VLAN. By default, the Native VLAN is VLAN 1.

In the privileged mode, you can configure a native VLAN for a Trunk port.

Command	Function
DGS-3610(config-if)# **switchport trunk native vlan** *vlan-id*	Configure Native VLAN.

To restore the Native VLAN list of the trunk to its default, please use the **no switchport trunk native vlan** interface configuration command.

If a frame carries the VLAN ID of Native VLAN, the TAG will be automatically removed when it is forwarded by the Trunk port.

When you set the Native VLAN of one interface to a non-existent VLAN, the switches will not automatically create the VLAN. In addition, the native VLAN of one interface may not necessarily exist in the VLAN list. In this case, the traffic of the native VLAN does not pass the interface.

8.4 Showing VLAN

Only in the privileged mode can you view the VLAN information, including VLAN VID, VLAN status, VLAN member port, and VLAN configuration information. The related commands are listed as below:

Command	Function
show vlan [**id** *vlan-id*]	Show all or specified VLAN parameters

The following example shows a VLAN:

```
DGS-3610# show vlan
VLAN[1] "VLAN0001"
       GigabitEthernet 3/1
       GigabitEthernet 3/2
       GigabitEthernet 3/3
       GigabitEthernet 3/4
       GigabitEthernet 3/5
       GigabitEthernet 3/6
       GigabitEthernet 3/7
       GigabitEthernet 3/8
       GigabitEthernet 3/9
       GigabitEthernet 3/10
       GigabitEthernet 3/11
       GigabitEthernet 3/12
VLAN[6] "VLAN0006"
       GigabitEthernet 3/1

DGS-3610#show vlan  id 1
VLAN[1] "VLAN0001"
       GigabitEthernet 3/1
       GigabitEthernet 3/2
       GigabitEthernet 3/3
       GigabitEthernet 3/4
       GigabitEthernet 3/5
       GigabitEthernet 3/6
       GigabitEthernet 3/7
       GigabitEthernet 3/8
       GigabitEthernet 3/9
       GigabitEthernet 3/10
       GigabitEthernet 3/11

       GigabitEthernet 3/12
```

9 Super VLAN Configuration

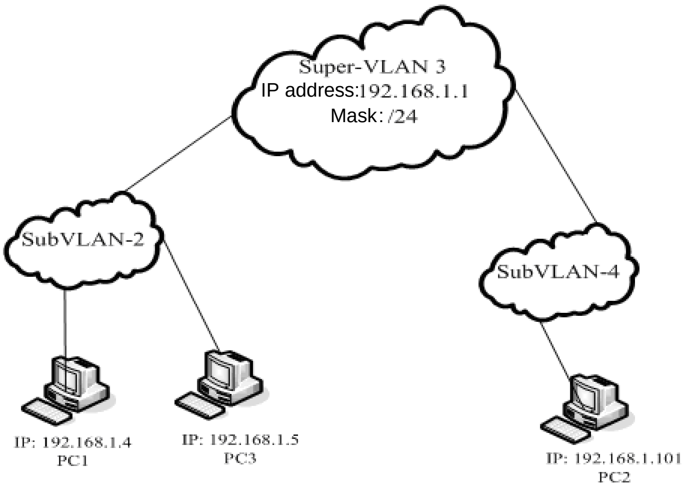
This chapter describes the Super VLAN configuration of DGS-3610 series.

9.1 Overview

Super VLAN is a method for VLAN division. Super VLAN, also called VLAN aggregate, is a management technology for optimizing the IP addresses. Its principle is to assign the IP address of a network segment to different sub VLANs that belong to the same Super VLAN. Each sub VLAN is an independent broadcast domain, and layers 2 of different sub VLANs are isolated from each other. To perform layer 3 communication, the user inside the Sub VLAN uses the IP address of the virtual interface of Super VLAN as the gateway address. This allows multiple VLANs to share one IP address, saving the IP address resources. At the same time the ARP agent function should be used in order to realize interoperation between layers 3 of different sub VLANs, as well as interoperation between the sub VLAN and other networks. The ARP agent can be used to forward and handle the ARP request and response packet, so as to realize layers 3 inteconnection between isolated ports of layer 2. By default, the ARP agent function is enabled for Super VLAN and Sub VLAN.

The Super VLAN technology greatly saves the IP addresses, because it just assigns one IP addresses to the Super VLAN that includes several Sub VLANs. Not only save the addresses but also making network management easy.

Figure 9-1



The process of communication between two aggregated sub VLANs when the VLAN is aggregated is described below. See the above diagram:

Sub VLAN2 and Sub VLAN4 are aggregated to Super VLAN3. An IP sub-net is assigned to Super VLAN3, and both Sub VLAN2 and Sub VLAN4 are located in this subnet. Suppose that the host PC1 in Sub VLAN2 needs to communicate with another host PC2 in the subnet. After knowing that the peer is located in the same network segment, PC1 directly sends an ARP request packet with a destination IP address. Upon receiving this ARP request packet, the layer 3 device directly broadcasts this packet through layer 2 within therange of Sub VLAN2, and sends a copy to the ARP module of the device. This module first checks whether the destination IP address in the ARP request packet is in Sub-VLAN2. If yes, it will discard this packet because it and PC1 are located in the same broadcast domain, and the destination host will directly respond to PC1. If not, it will respond PC1 with the MAC address of SuperVLAN3, acting as an ARP agent. For example, PC1 and PC2 have to communicate through the ARP agent which forwards packets from PC1 to PC2. However, PC1 and PC3 can communicate directly without needing a forwarding device.

Restrictions:

- Super VLAN cannot contain any member port. It only contains Sub VLAN, which contains actual physical ports.
- Super VLAN cannot serve as a sub VLAN of other Super VLANs.
- Super VLAN cannot be used as the normal 1Q VLAN.
- VLan 1 cannot be used as SuperVLAN.
- Sub VLAN cannot be configured as network interface, and cannot be assigned with IP address.
- SVLAN cannot use VRRP and does not support multicast.
- Super VLAN interface-based ACL and QOS configurations are not valid to the Sub VLAN.

9.2 Configuring Super VLAN

Using following command to configure Super VLAN.

Command	Function
DGS-3610# **configure**	Enter the global configuration mode.
DGS-3610(config)# **vlan** *vlan-id*	Enter VLAN configuration mode
DGS-3610(config-vlan)# **supervlan**	Enable the SuperVLAN function
DGS-3610(config-vlan)# **end**	Return to the privilege mode.

The Super VLAN function is disabled by default. The enabled Super VLAN function can be disabled using **no supervlan**.

9.3 Configuring Sub VLAN of Super VLAN

SuperVLAN is meaningful only when SubVLAN is configured for it.

To make VLAN belong to the sub VLAN of Super VLAN, use the following comands.

Note: Sub VLAN configuration may fail due to lack of resources.

Command	**Function**
DGS-3610# **configure**	Enter configuration mode
DGS-3610(config)# **vlan** *vlan-id*	Enter VLAN configuration mode
DGS-3610(config-vlan)# **supervlan**	Set this vlan as a Super VLAN
DGS-3610(config-vlan)# **subvlan** *vlan-id-list*	Specify some sub VLANs and add them to the Super VLAN.
DGS-3610(config-vlan)# **exit**	Exit the global mode.

Delete a sub VLAN from the Super VLAN using the **no subvlan** [*vlan-id-list*] command.

9.4 Setting Address Range of Sub VLAN

The user can configure address range for each sub VLAN, so that the device differenciates which sub VLAN that a given IP address belongs to. The address ranges configured for sub VLANs under the same Super VLAN should not have overlapped contents, and should not include each other.

Perform the following configurations in the global mode.

Command	**Function**
DGS-3610# **configure**	Enter configuration mode
DGS-3610(config)# **vlan** *vlan-id*	Enter VLAN configuration mode
DGS-3610(config-vlan)# **subvlan-address-range** *start-ip end-ip*	Set an address range for the sub VLAN. start-ip is the start IP address of this sub VLAN, and end-ip is the end IP address of this sub VLAN.
DGS-3610(config-vlan)# **end**	Return to the privilege mode.
DGS-3610# **show run**	Verify the configurations made in the previous steps.

Caution

Users can delete the previous configurations by executing **no subvlan-address-range**.

9.5 Setting Virtual Interface for Super VLAN

When a user in Sub VLAN needs to perform layer 3 communication, a virtual layer 3 interface that corresponds to the Super VLAN should be created first.

SVI that corresponds to the Super VLAN itself is used as the virtual interface.

Perform the following configurations in the global mode.

Command	Function
DGS-3610# **configure**	Enter configuration mode
DGS-3610(config)# **interface vlan** *vlan-id*	Enter the SVI mode
DGS-3610(config-vlan)# **ip address** *ip mask*	Set an IP address for the virtual interface
DGS-3610(config-vlan)# **end**	Return to the privilege mode.
DGS-3610# **show run**	Verify the configurations made in the previous steps.

9.6 Setting Agent ARP Function for VLAN

Set the agent ARP function for VLAN using the following commands, so as to allow communication between sub VLANs. This function is enabled by default.

Perform the following configurations in the global mode.

Command	Function
DGS-3610# **configure**	Enter configuration mode
DGS-3610(config)# **vlan** *vlan-id*	Enter the VLAN mode
DGS-3610(config-vlan)# **proxy-arp**	Enable the ARP agent function for VLAN
DGS-3610(config-vlan)# **end**	Return to the privilege mode.
DGS-3610# **show run**	Verify the configurations set in the previous steps.

The ARP agent function of Vlan can be disabled by using **no proxy-arp**.

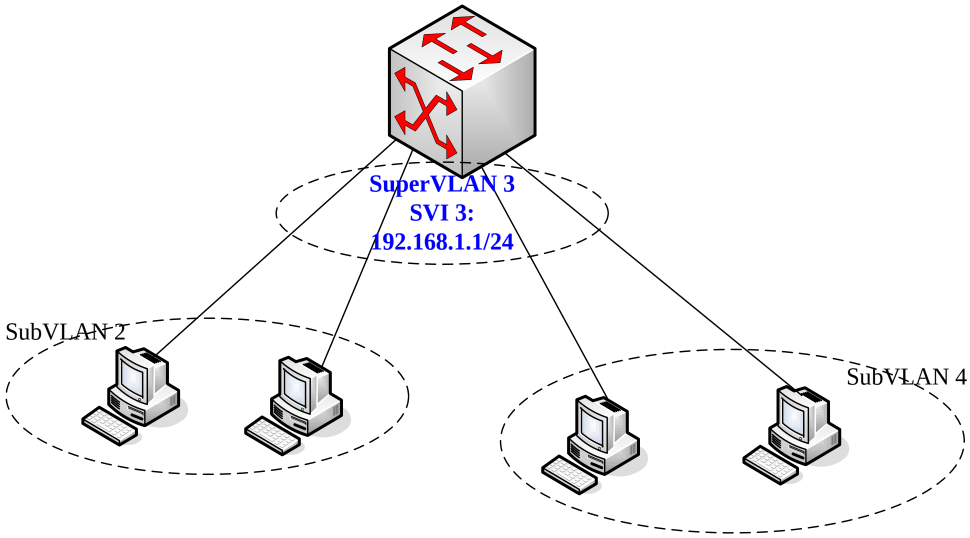
9.7 Showing Super VLAN Setting

Show the Super VLAN setting using the following command.

Command	Function
DGS-3610# **show supervlan**	Show Supervlan setting

9.8 Configuration Example

Figure 9-2



SuperVLAN is used in the above diagram, .To allow the host of Sub VLAN2 and that of SubVLAN4 to communicate with each other, the device can be configured as follows: (only related parts are listed)

```
vlan 1
!
vlan 2
```

# Set an IP address range in the Sub VLAN 2

```
subvlan-address-range 192.168.1.1 192.168.1.100
!
vlan 3
supervlan
subvlan 2,4
!
vlan 4
```

# Set an IP address range in Sub VLAN 4

```
subvlan-address-range 192.168.1.101 192.168.1.254
!
interface FastEthernet 0/23
```

# Add a member port for SubVLAN2

```
switchport access vlan 2
!
interface GigabitEthernet 0/25
```

# Add a member port for SubVLAN4

```
switchport access vlan 4
!
```

# Create a virtual layer 3 interface that corresponds to Super VLAN

```
interface Vlan 3
ip address 192.168.1.1 255.255.255.0
```

10 Protocol VLAN Configuration

10.1 Protocol VLAN Technology

Every packet that the device port receives should be classified based on VLAN, so that the packet belongs to a unique VLAN. There are three possibilities:

1. If the packet is an empty VLAN ID packet (UNTAG or Priority packet), and the device only supports port-based VLAN classification, the VLAN ID in the tag added to the packet is the PVID of the input port.
2. If the packet is an empty VLAN ID packet (UNTAG or Priority packet), and the device supports the packet protocol type-based VLAN classification, the VLAN ID in the VLAN ID set for the protocol group configuration on the input port will be selected as the VLAN ID in the tag added to the packet. However, if the protocol type of the packet doesn’t comply with all the protocol group configurations on the input port, the VLAN ID will be assigned according to the VLAN classfication of the port-based.
3. If the packet is a TAG packet, its VLAN classfication is determined by the VLAN ID in the TAG.

   The Protocol VLAN technology is a VLAN classification technology that is based on the protocol type of the packet. It classifies the empty VLAN ID packet of certain type of protocol into the same VLAN.

   The Protocol VLAN configuration takes effect for the Trunk port only, not for the Access port.

   Our products support two kind of classification technology, such as the global IP address-based VLAN classification technology, and the Ethernet-type VLAN based on the packet type on the port.

   Because IP address-based VLAN classification is a global configuration, it will apply to all the Trunk ports once you have configured it with IP address-based VLAN classification.
4. If the input packet of VLAN ID is empty , and its IP address matches the configured IP address, this packet will be classified into the configured VLAN.
5. If the input packet of VLAN ID is empty, at the same time its packet type and Ethernet type respectively match those you configured on the input port, this packet will be classified into the configured VLAN.

The priority of IP address-based VLAN classification is higher than the priority of the packet type and Ethernet type-based VLAN classification. Hence, if you have configured both the IP address-based and packet type and Ethernet type-based VLAN classifications, and the input packet matches them both, the IP address-based VLAN classification takes effect.

It’s better to configure the Protocol VLAN after finishing the configuration of VLAN, and the Trunk, Access and AP attributes of the port. If you have configured Protocol VLAN for the Trunk port, all the VLANs related to the Protocol VLAN should be included in the allowed VLAN list of the Trunk port .

10.2 Configuring Protocol VLAN

10.2.1 Default Protocol VLAN

No Protocol VLAN is configured by default.

10.2.2 Configuring IP address-based VLAN Classification

Configure using the following commands:

Command	Description
configure terminal	Enter configuration mode
protocol-vlan ipv4 *address* **mask** *address* **vlan <***vid***>**	Configure IP address, subnet mask and VLAN classification
no protocol-vlan ipv4 *address* **mask** *address*	Cancel the configuration of IP address.
no protocol-vlan ipv4	Cancel all the configuration of IP address
end	Exit the VLAN mode
show protocol-vlan ipv4	Show the configuration of IP addresses

Note

Specify the IP address and subnet mask in the x.x.x.x method.

Available VLAN IDs may vary with the product.

The following command configures the IP address as 192.168.100.3, and the VLAN classfication with the mask 255.255.255.0 is VLAN 100.

```
DGS-3610# configure terminal
DGS-3610(config)# protocol-vlan ipv4 192.168.100.3 mask 255. 255.255.0 vlan 100
DGS-3610(config-vlan)# end
DGS-3610# show protocol-vlan ipv4
ip             mask           vlan
-------------  -------------  -----

192.168.100.3  255.255.255.0  100
```

10.2.3 Configuring the Profile of Packet Type and Ethernet Type

Configure the packet type and Ethernet type using the following commands:

Command	Description
configure terminal	Enter configuration mode
protocol-vlan profile id frame-type [*type*] **ether-type** [*type*]	Configuring profile of packet type and Ethernet type
no protocol-vlan profile *id*	Delete certain profile configuration
no protocol-vlan profile	Clear all the profile configurations
end	Exit the VLAN mode
show protocol-vlan profile	Show all profiles configurations
show protocol-vlan profile *id*	Show certain profile configuration

For example:

```
DGS-3610# configure terminal
DGS-3610(config)# protocol-vlan  profile 1 frame-type  ETHERII ether-type EHTER_AARP
DGS-3610(config)# protocol-vlan  profile 2 frame-type  SNAP ether-type 0x809b
DGS-3610(config-vlan)# end
DGS-3610# show protocol-vlan profile
profile    frame-type   ether-type      Interfaces|vid
-------     ---------   ----------       -----------
1           ETHERII     EHTER_AARP       NULL|NULL
2           SNAP        ETHER_APPLETALK  NULL|NULL
```

Note

1. The configuration will not be effective until the profile is applied to the port.
2. Before a profile is updated, this Profile must be deleted first and re-configured.
3. Different products support different numbers of profiles. DGS-3610 sports 16 profiles.

10.2.4 Applying Profile

Through performing the following steps to apply it: :

Command	Description
configure terminal	Enter configuration mode
interface *[interface ID]*	Enter the interface mode
protocol-vlan profile *id* **vlan** ***vid***	Apply certain profile to this interface
no protocol-vlan profile	Clear all profiles on this port

Command	Description
no protocol-vlan profile *id*	Clear certain profile on this port
end	Exit the interface mode

The following example applies profile 1 and profile 2 to the GE port 1 of Slot 3. The VLAN is classfied to VLAN 101 and 102:

```
DGS-3610# configure terminal
DGS-3610(config)# interface gi 3/1
DGS-3610(config-if)# protocol-vlan profile 1 vlan 101
DGS-3610(config-if)# protocol-vlan profile 2 vlan 102
DGS-3610(config-if)# end
DGS-3610# show protocol-vlan profile
profile     frame-type  ether-type      Interfaces|vid
-------     ---------   ----------       --------------
1           ETHERII     EHTER_AARP       gi3/1|101
2           SNAP         ETHER_APPLETALK  gi3/1|102
```

Note

1. Any profiles can be applied to each interface.
2. Different VIDs can be specified for the same profile on different interfaces.
3. According to the various series of products, the quantity of vids specified is different , DGS-3610 series devices can specify 4094 VLANs.

10.3 Showing Protocol VLAN

You can show the contents of Protocol VLAN using the following commands:

Command	Description
show protocol-vlan	Show the contents of Protocol VLAN

```
DGS-3610# show protocol-vlan
ip              mask            vlan
-------------   -------------   ----
192.168.100.3   255.255.255.0   100
profile     frame-type   ether-type      Interfaces|vid
-------     ---------    ----------      --------------
1           ETHERII     EHTER_AARP       gi3/1|101
2           SNAP         ETHER_APPLETALK  gi3/1|1
```

11 Private VLAN Configuration

11.1 Private VLAN Technology

If the service provider offers a VLAN to each subscriber, the service provider supports a limited number of subscribers because one device supports 4096 VLANs at most. On the layer 3 devices, each VLAN is assigned with a subnet address or a series of addresses, which results in IP address waste. The Private VLAN technology is a solution to this problem.

Private VLAN divides layer 2 broadcast domain of a VLAN into several sub-domains. Each sub-domain consists of a private VLAN pair: Primary VLAN and Secondary VLAN.

One private VLAN domain can have multiple private VLAN pair, and each VLAN pair represents a sub-domain. All the private VLAN pairs in one private VLAN domain share a primary VLAN. Each sub-domain has a different secondary VLAN ID.

There is only one primary VLAN in each private VLAN domain. The secondary VLAN is used to separate from layer 2 in the same private VLAN domain. There are two types of secondary VLANs:

- Isolated VLAN: Layer 2 communication is not implemented between the ports in the same isolated VLAN. There is only one isolated VLAN in a private VLAN domain.
- Community VLAN: The ports in the same community VLAN can perform layer 2 communication, but not with the ports in other community VLANs. There can be multiple community VLANs in a private VLAN domains.

Promiscuous Port, a port in the primary VLAN, can communicate with any port, including the isolated ports and community ports of the secondary VLAN in in the same private VLAN domain.

Isolated Port, a port in the isolated VLAN, only communicate with the promiscuous port.

Community port is a port in the community VLAN. Community ports in the same community VLAN can communication with each other, and they can also communicate with promiscuous ports. They cannot communicate with the community ports in other community VLANs and isolated ports in the isolated VLANs.

In a private VLAN, an SVI interface can be created for the primary VLAN only, instead of the secondary VLAN.

A port in the private VLAN can be a SPAN source port instead of a mirrored destination port.

11.2 Private VLAN Configuration

11.2.1 Default Private VLAN Setting

No Private VLAN is configured by default.

11.2.2 Configuring VLAN as a Private VLAN

Configure through using the following commands:

Command	Description
configure terminal	Enter configuration mode
vlan *vid*	Enter VLAN configuration mode
private-vlan{community | isolated| primary}	Configure private VLAN type
no private-vlan{community | isolated | primary}	Cancel the configuration of private VLAN
end	Exit the VLAN mode
show vlan private-vlan [*type*]	Show a private VLAN

Note

The member port in the 802.1Q VLAN cannot be declared as a private VLAN. VLAN 1 cannot be declared as a private VLAN. If there is a Trunk or Uplink port in the 802.1Q VLAN, first delete this VLAN from the allowed VLAN list. The following conditions must be met in order to make Private VLAN become ACTIVE status:

1. Primary VLAN is available
2. Secondary VLAN is available
3. Secondary VLAN is associated with Primary VLAN
4. There are promiscuous ports in the primary VLAN.

The following command configures 802.1Q VLAN as a Private VLAN:

```
DGS-3610# configure terminal
DGS-3610(config)# vlan 303
DGS-3610(config-vlan)# private-vlan community
DGS-3610(config-vlan)# end
DGS-3610# show vlan private-vlan community
VLAN Type  Status    Routed   Interface   Associated VLANs
--- ----   --------  ------   ---------   ------------------
303 comm   inactive  Disabled              no association
DGS-3610# configure terminal
DGS-3610(config)# vlan 404
DGS-3610(config-vlan)# private-vlan isolated
DGS-3610(config-vlan)# end
DGS-3610# show vlan private-vlan
```

```
VLAN Type  Status    Routed   Interface   Associated VLANs
--- ----  --------  ------   ---------   ------------------
303 comm  inactive  Disabled             no association
404 isol  inactive  Disabled             no association
```

11.2.3 Associating Secondary VLAN with Primary VLAN

The secondary VLAN can be associated with the primary VLAN using the following commands:

Command	Description
configure terminal	Enter configuration mode
vlan *p_vid*	Enter the Primary VLAN configuration mode
private-vlan association **{svlist | add** *svlist* **| remove** *svlist***}**	Associate the secondary VLAN
no private-vlan association	Clear association with all the secondary VLANs
end	Exit from VLAN mode
show vlan private-vlan [*type***]**	Show the private VLAN

For example:

```
DGS-3610# configure terminal
DGS-3610(config)# vlan 202
DGS-3610(config-vlan)# private-vlan association 303-307,309,440
DGS-3610(config-vlan)# end
DGS-3610# show vlan private-vlan
VLAN Type  Status    Routed   Interface   Associated VLANs
--- ----  --------  ------   ---------   ------------------
202 prim  inactive  Disabled               303-307,309,440
303 comm  inactive  Disabled               202
304 comm  inactive  Disabled               202
305 comm  inactive  Disabled               202
306 comm  inactive  Disabled               202
307 comm  inactive  Disabled               202
309 comm  inactive  Disabled               202
440 comm  inactive  Disabled               202
```

Note

This operation is performed in the configuration mode for the VLAN declared as the primary VLAN.

11.2.4 Mapping Layer 3 Interfaces of Secondary VLAN and Primary VLAN

You can perform the following configuration to complete the command:

Command	Description
configure terminal	Enter configuration mode
interface vlan *p_vid*	Enter interface mode of Primary VLAN
private-vlan mapping **{**svlist **| add** *svlist* **| remove** *svlist***}**	Map Secondary VLAN to the SVI layer 3 switching of Primary VLAN.
end	Exit the interface mode

The following example configures the Secondary VLAN routes:

```
DGS-3610# configure terminal
DGS-3610(config)# interface vlan 202
DGS-3610(config-if)# private-vlan mapping add 303-307,309,440
DGS-3610(config-if)# end
DGS-3610#
```

Note

Primary VLAN and Secondary VLAN in this process are associated.

11.2.5 Configuring Layer 2 Interface as Host Port of Private VLAN

To configure the layer 2 interface as the host port of the private VLAN, perform the following steps:

Command	Description
configure terminal	Enter configuration mode
interface <*interface***>**	Enter the interface configuration mode. *fastethernet, gigabitethernet, tengigabitethernet*
switchport mode private-vlan host	Configure as the layer 2 switching mode
no switchport mode	Clear private VLAN configuration
End	Exit the SVI interface mode
switchport private-vlan host-association *p_vid s_vid*	Associate the layer 2 interface with the private VLAN
no switchport private-vlan host-association	Clear the association

For example:

```
DGS-3610# configure terminal
DGS-3610(config)# interface gigabitEthernet 0/2
DGS-3610(config-if)# switchport mode private-vlan host
DGS-3610(config-if)# switchport private-vlan host-association
202 203
DGS-3610(config-if)# end
DGS-3610#
```

Note

Primary VLAN and Secondary VLAN in this process are associated.

11.2.6 Configuring Layer 2 Interface as Promiscuous Port of Private VLAN

To configure the layer 2 interface as the port of private VLAN, use the following commands:

Command	Description
configure terminal	Enter configuration mode
interface <*interface***>**	Enter the interface configuration mode. Megabit, Gigabit, 10 Gigabit
switchport mode private-vlan promiscuous	Configure as the layer 2 switching mode of private VLAN
no switchport mode	Delete the private VLAN configuration for the port
switchport private-vlan mapping *p_vid*{*svlist* **| add** *svlist* **| remove** *svlist*}	Select the VLAN where the promiscuous port of the private VLAN is located and mixed secondary VLAN list
no switchport private-vlan mapping	Cancel all promiscuous secondary VLANs.

Following example to describe how to configure:

```
DGS-3610# configure terminal
DGS-3610(config)# interface gigabitEthernet 0/2
DGS-3610(config-if)# switchport mode private-vlan promiscuous
DGS-3610(config-if)# switchport private-vlan mapping 202 add 203
DGS-3610(config-if)# end
```

Note

Primary VLAN and Secondary VLAN in this process are associated.

11.3 Private VLAN Showing

11.3.1 Showing private VLAN

You can show the contents of Private VLAN using the following commands:

Command	Description
show vlan private-vlan [*type*]	Show the contents of private VLAN

```
DGS-3610# show vlan private-vlan
VLAN Type  Status    Routed   Interface   Associated VLANs
--- ----   --------  ------   ---------   ------------------
202 prim   active   Enabled    Gi0/1      303-307,309,440
303 comm   active   Disabled   Gi0/2      202
304 comm   active   Disabled   Gi0/3      202
305 comm   active   Disabled   Gi0/4      202
306 comm   active   Disabled              202
307 comm   active   Disabled              202
309 comm   active   Disabled              202
440 comm   active   Enabled    Gi0/5      20
```

12 802.1Q Tunneling

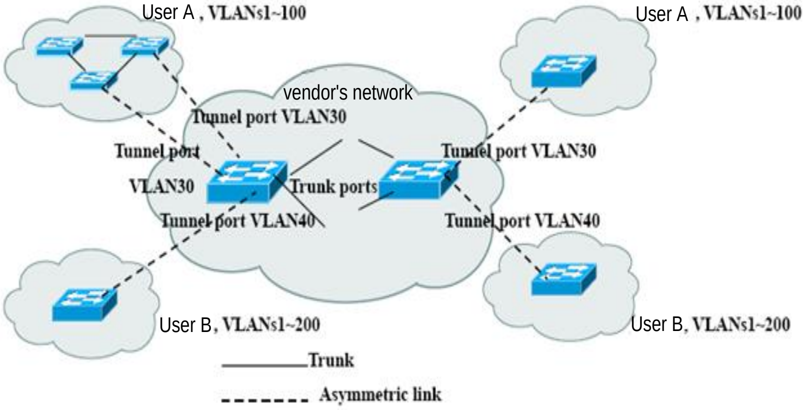
12.1 Understanding 802.1Q Tunneling

The commercial users of the network service providers usually have special requirements for the supported VLAN and VLAN IDs. There may be superposition in the range of the VLANs needed by the users of the same vendor, and the switching channels of different users through the core network of the vendors may be mixed together. To define a VLAN range for every individual user may cause restrictions on the user configurations, and the VLAN number of 4096, as defined by the 802.1Q, may be easily exceeded.

The features of the IEEE 802.1Q Tunneling enable the vendor to use one VLAN (vendor VLAN) to support the users with multiple VLANs. The VLAN of the user is reserved. In this way, the traffic of different users to the vendor can be transmitted separately in the vendor's internal network even if its VLANs are the same. Through dual Tags, the tunneling extends the range of the VLAN. A port that supports the IEEE 802.1Q Tunneling is called a tunnel port. In the configuration of tunneling, a VLAN can be assigned to the tunnel port as the dedicated VLAN. Thus, every user just needs to use the VLAN of one vendor. The user's traffic is packaged into dual-tagged frames while being transmitted in the vendor's network, and is transmitted in the network through the VLAN of the vendor.

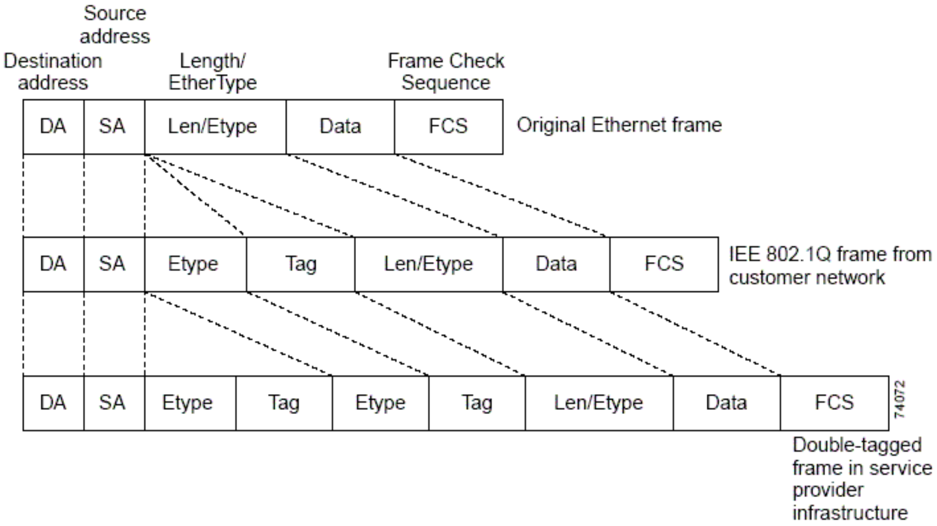
The switching traffic of the user goes from one of its TRUNK port, carrying normal 802.1Q TAGs, to a tunnel port of the edge device of the vendor. Such an asymmetrical connection between the user and vendor is called the asymmetrical link, because one end is to a Trunk port while the other end to a tunnel port. The tunnel ports of different users are assigned with different VLANs. See the following application scheme diagram:

Figure 12-1



The frames from the user end Trunk port to the tunnel port of the network edge device of the vendor are usually carrying IEEE 802.1Q Tag with one VLAN ID. After the frames enter the tunnel port, they will be added with another 802.1Q Tag (called the vendor Tag) to include another VLAN ID that varies with every individual user. The user's tags will be reserved inside the frames. In this way, the frames to the vendor's network are dual-tagged, of which the vendor Tag contains the user's VID and the internal Tag maintains the VID of the incoming frame. The following diagram shows the process for adding the dual Tag

Figure 12-2



When the dual-tagged frames output from the tunnel port of the edge device, the vendor Tag will be removed and the frames resume their original 802.1Q frame format before they enter the edge device, and the user VLAN is restored.

All frames to the edge device are regarded as Untagged frames, no matter whether they are Untagged or are attached with 802.1Q tag header. When the frames go through the vendor network, they are encapsulationed with the vendor Tag and VLAN number (that is, the access VLAN of the tunnel port). The priority field of the vendor Tag is the priority configured on the tunnel port (0 by default in case of no configuration).

In the application scheme diagram, user A is assigned with VLAN 30, and user B with VLAN 40. When the frames with 802.1Q Tag at the edge device are enveloped with a vendor tag and become dual-Tagged, the vendor Tag contains VLAN 30 or 40 while the internal Tag contains the original VLAN information (such as VLAN 40) of the frames. Even if the frames of both users A and B to the vendor network have VID 100, their traffic is transmitted separately in the vendor network because their vendor Tags contain different VIDs. Every user can assign its VLAN range, which is independent of other users and of the vendor network.

12.2 Configuring 802.1Q tunneling

This chapter includes:

- Default Configurations of the 802.1Q Tunneling
- 802.1Q Tunneling Configuration Guide
- Restriction of 802.1Q Tunneling Configuration
- Configuring an 802.1Q Tunneling Port
- Configuring an Uplink Port
- Configuring TPID Value in Vendor Tag
- Configuring Priority Duplication of User Tag

12.2.1 Default Configurations of the 802.1Q Tunneling

By default, the 802.1Q tunneling function is disabled.

12.2.2 802.1Q Tunneling Configuration Guide

In configuring the 802.1Q, it is required to confirm that the connection with the 802.1Q tunnel is an asymmetric link, with a VLAN dedicated for each tunnel. Also it is required to confirm the correct configuration for the Native VLAN and the longest frame.

Configuration of Native VLAN: In configuring the 802.1Q tunneling at an edge device, it is required to connect a tunnel port through the 802.1Q trunk interface. The switching path of frames inside the network of the vendor may vary, possibly 802.1Q trunk or non-trunk interface. When the connection between core devices is a trunk, the Native VLAN of the trunk interface on the device should be different from the ACCESS VLAN of the tunnel port, because the tag will be removed when the frame with VID as Native VLAN goes out of the trunk port.

The longest frame of the system: Because the 802.1Q tunneling port adds additional 4-byte vendor VLAN Tag, the maximum length of the frame increases from 1518 to 1522.

Uplink port: The Up-link port is used to link the vendor device of other user networks or uplink the ports of the devices. For example, the Trunk Ports of the vendor network in Figure 12-1. The Uplink port is actually a special Trunk port except that the packets that output from the Uplink port are tagged. The packets that output from the Trunk Port, however, are not tagged if they are forwarded from the Native VLAN.

TPID value in the vendor Tag: TPID (Tag Protocol Identifier) is a field in the VLAN Tag. The IEEE 802.1Q protocol specifies that the value of this field is 0x8100.

Tag priority duplication: It is a process where the priority of the inner tag (user tag) is duplicated to the outer tag (vendor tag) when two tags are available.

12.2.3 Restriction of 802.1Q Tunneling Configuration

The following restrictions apply to configuration of 802.1Q tunneling:

- The routing ports cannot be configured as tunnel ports.
- The AP port can be configured as a tunnel port.
- The 802.1x function cannot be enabled for the port configured as a tunnel port.
- Cluster cannot be enabled for the port configured as a tunnel port.
- The STP algorithm cannot be added to the port configured as a tunnel port.
- GVRP cannot be enabled for the port configured as a tunnel port.
- System-guard cannot be enabled for the port configured as a tunnel port.
- For DGS-3610 series, it's recommended to configure the egress of the user's network to Uplink port, which is connected to the vendor network shown in the Figure 12-1. If you configured the TPID of the vendor Tag on the 802.1Q tunneling in the user's network, it's required to configure the same TPID of the vendor Tag on the Uplink port.

12.2.4 Configuring an 802.1Q Tunneling Port

In the global configuration mode, type in **interface** command to enter the interface configuration mode. Follow these steps to configure the tunnel port:

Command	Description
configure terminal	Enter the global configuration mode.
interface <*interface***>**	Enter the interface configuration mode.
switchport access vlan <*vid***>**	Configure the Access VLAN. The Access VLAN should vary with each user.
switchport mode dot1q-tunnel	Set the interface as 802.1Q tunnel.
end	Exit the interface mode
show running-config	View the global configuration

Note

The routing port cannot be set as a tunnel port because System-guard, GVRP, cluster, and 802.1x cannot be enabled and the STP algorithm cannot be added to the port configured as Tunnel.

The following example demonstrates how to configure a 802.1q Tunneling port:

```
DGS-3610(config)# interface fastEthernet 0/1
DGS-3610(config-if)# switchport access vlan 22
DGS-3610(config-if)# switchport mode dot1q-tunnel
DGS-3610(config)# end
```

12.2.5 Configuring an Uplink Port

In the global configuration mode, using the **interface** command to enter the interface configuration mode. Follow these steps to configure the tunnel port:

Command	Description
configure terminal	Enter the global configuration mode.
interface <*interface*>	Enter the interface configuration mode.
switchport mode uplink	Configure the port as an uplink port
end	Exit from interface mode

The following example demonstrates how to configure a tunnel port:

```
DGS-3610(config)# interface gigabitEthernet 0/1
DGS-3610(config-if)# switchport mode up-link
DGS-3610(config)# end
```

12.2.6 Configuring TPID Value in Vendor Tag

In the global configuration mode, using **interface** command to enter the interface configuration mode. Follow these steps to perform configuration:

Command	Description
configure terminal	Enter configuration mode
interface <*interface***>**	Enter the interface configuration mode.
frame-tag tpid <*tpid***>**	Set TPID in the frame tag. If you want to set it to 0x9100, Directly input frame-tag tpid 9100. Note that the hexadecimal system is used by default.
end	Exit the interface mode
show frame-tag *tpid*	View the TPID value list for the port.

The following example demonstrates how to configure TPID:

```
DGS-3610(config)# interface gigabitethernet 0/1
DGS-3610(config-if)# frame-tag tpid 9100
DGS-3610(config)# end
DGS-3610# show frame-tag tpid interface gigabitethernet 0/1
Port     tpid
------- -------------
Gi0/1    0x9100
```

12.2.7 Configuring Priority Duplication of User Tag

In the global configuration mode, using **interface** command to enter the interface configuration mode. Follow these steps to perform configuration:

Command	**Description**
configure terminal	Enter configuration mode
interface <*interface***>**	Enter the interface configuration mode.
inner-priority-trust enable	Copy the priority field value of the inner tag (user tag) to the priority field value of the outer tag (vendor tag).
end	Exit from interface mode.
show inner-priority-trust	View the duplication configuration for the user tag priority.

The following example shows how to configure the priority duplication for the user tag:

```
DGS-3610(config)# interface gigabitethernet 0/1
DGS-3610(config-if)# inner-priority-trust enable
DGS-3610(config)# end
DGS-3610# show inner-priority-trust interface gigabitethernet 0/1
Port     inner-priority-trust
------   -------------------
Gi0/1    enable
```

13 MAC Address Configuration

13.1 Managing the MAC Address Table

13.1.1 Overview

The MAC address table contains address information used for forwarding packets between ports. The MAC address table includes three types of addresses: Dynamic address, Static address, Filtering address. We will describe the MAC address table in the following sections:

13.1.1.1 Dynamic Address

A dynamic address is an MAC address learnt by the device from the packets it receives. When the device receives a packet on each port, the device will add the source address of the packet and its associated port number to the address table. The device learns new addresses in this way.

When the device receives a packet, if the destination MAC address of the packet is the dynamic address learnt by the device, the packet will be directly forwarded to the port associated with the MAC address. Otherwise, the packet will be forwarded to all other ports.

The device updates the dynamic address table through learning the new addresses and the address aged out that are not in use. For an address in the address table, if the device does not receive any packets with the same source MAC address for a long time (According to the aging time), the address will be aged. You can adjust the aging time of dynamic address according to the actual situation. If the aging time is too short, the address in the address table will be aged too early and the address will be taken as an unknown address again for the devices. When the device receives the packets with the destination MAC address, the packets will be broadcast to other ports in the VLAN, leading to the needless broadcast flow . If the aging time is too long, the address will be aged slowly and the address table will full be ocupied. When the table is full, no new address can be leant, and all other addresses will become unknown addresses before there is room for the address table to learn this address. When the device receives the packets with the destination address, the packet will be broadcasted to other ports in the VLAN to lead to the needless broadcast being generated..

When the device is reset, all the dynamic addresses that the device have learnt will be lost, therefore, the device need to learn these addresses again.

13.1.1.2 Static Address

A static address is a MAC address manually configured. Static address is the same as the dynamic address in function, but oppositely, static address canl only be added and deleted manually (instead of learning and aging). Static address can be stored in the configuration file, and will not be lost even if the device reloads.

13.1.1.3 Filtering Address

A filtering address is a MAC address manually added. The packets whose source addresses are the filtering addresses and received by the device will be directly discarded Filtering addresses are not be aged forever. They can only be added and deleted manually. The filtering addresses are stored in the configuration file, and will not be lost even if the device is reset.

If you want the device to shield some illegal users, you can specify their MAC address as filtering addresses, so that these illegal users can not communicate with the outside world through the device.

13.1.1.4 Association between MAC Address and VLAN

All MAC addresses are associated with VLANs. The same MAC address can exist in multiple VLANs. This addresses in different VLAN can be associated with different ports. Each VLAN maintains its own logical address table. An MAC address learnt by the VLAN may be unknown in another VLAN. Thus it needs to learn.

13.1.2 Configuring MAC Address

13.1.2.1 Default Configuration of MAC Address Table

The following table shows the default MAC address table configuration:

Item	Default Configuration
Aging time of the address table	300 seconds
Dynamic addresses table	Automatically learned
Static addresses table	No static addresses are configured.
Filtering addresses table	No filtering addresses are configured.

⚠ **Caution**

There may be some deviation between the actual aging time and the setting value of the address table. However, it will not exceed 2 times of the setting value.

13.1.2.2 Setting the Address Aging Time

The following table shows how to set the aging time of address:

Command	Function
DGS-3610(config)# **mac-address-table aging-time** [*0* |*10-1000000*]	Set the interval for keeping an addresse learnt in the dynamic address table , in seconds, the range is within 10-1000000 seconds. The default is 300s. When this value is set to 0, the address aging function is disabled, and the learnt addresses will not be aged.

To return to the default values, use the **no mac-address-table aging-time** command in the global configuration mode.

13.1.2.3 Removing Dynamic Address Entries

To remove all dynamic entries, use the **clear mac-address-table dynamic** command in privileged EXEC mode. You can also delete a specified MAC address using the **clear mac-address-table dynamic address** *mac-address* command. Execute the **clear mac-address-table dynamic interface** *interface-id* command to delete all the addresses on the specified physical port or all the dynamic addresses on the Aggregate Port; You can also execute the **clear mac-address-table dynamic vlan** *vlan-id* command to delete all the dynamic addresses on a specified VLAN.

To verify whether the corresponding dynamic addresses have been deleted, use the **show mac-address-table dynamic** privileged EXEC command.

13.1.2.4 Adding and Deleting Static Address Entries

If a static address will be added, it’s requied to specify the MAC address (the destination address of the packets)., the VLAN (the static address will be added to the address table of this VLAN), and the interface (packets with the destination address as the specified MAC address are forwarded to this interface).

Add a static address:

Command	Function
DGS-3610(config)# **mac-address-table static** *mac-add* **vlan** *vlan-id* **interface** *interface-id*	mac-addr: Specify the destination MAC address that the entry corresponds to. vlan-id: Specify the VLAN to which this address belongs. interface-id, specify the interface (it can be physical port or aggregate port) to which the received packet is forwarded. When the packets of destination address received with the specification of mac-addr in the specified VLAN, they are forwarded to the specified interface specified by interface-id.

To delete a static address entry, use the **no mac-address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id* command in the global configuration mode.

The following example shows how to configure the static address 00d0.f800.073c. When a packet is received in VLAN 4 with this MAC address as its destination address, this packet is forwarded to the specified port gigabitethernet 1/3.

```
DGS-3610(config)# mac-address-table static 00d0.f800.073c vlan 4 interface
gigabitethernet 1/3
```

13.1.2.5 Adding and Deleting Filtering Address Entries

If you want to add a filtering address, it’s needed to specify the MAC address to be filtered which belongs to the VLAN address. The packet will be directly discarded when the packet received with this MAC address regarded as the destination address within this VLAN by the device.

Add a filtered address:

Command	Function
DGS-3610(config)# **mac-address-table filtering** *mac-addr* **vlan** *vlan-id*	mac-addr: Specify the MAC address to be filtered by the device. vlan-id: Specify the VLAN to which this address belongs.

To remove filtering address entries, use the **no mac-address-table filtering** *mac-addr* **vlan** *vlan-id* command in the global configuration mode.

This example shows how to configure the device to filter packets in VLAN1 with the source MAC address 00d0.f800.073c:

```
DGS-3610(config)# mac-address-table filtering 00d0.f800.073c vlan 1
```

13.1.3 Viewing MAC Addresses Information

View information of the MAC address table in the device:

Command	Function
DGS-3610# **show mac-address-table**	Show all types of MAC addresses information (including dynamic address, static address and filtering address)
DGS-3610# **show mac-address-table aging-time**	Show the current aging time of the address
DGS-3610# **show mac-address-table Dynamic**	Show the all dynamic MAC addresses
DGS-3610# **show mac-address-table static**	Show the all static MAC addresses
DGS-3610# **show mac-address-table filtering**	Show the all filtering MAC addresses
DGS-3610# **show mac-address-table Interface** *interface ID*	Show all types of MAC addresses information in the specified interface
DGS-3610# **show mac-address-table vlan** *ID*	Show all types of MAC addresses information for the specified VLAN
DGS-3610# **show mac-address-table count**	Show the statistic information of the MAC addresses in MAC address table:

The following examples show MAC addresses:

Show the MAC address table:

```
DGS-3610# show mac-address-table dynamic
Vlan       MAC Address        Type     Interface
---------  ------------------ -------- -------------------
1         0001.960c.a740      DYNAMIC  gigabitethernet 1/1
1         0009.b715.d40c      DYNAMIC  gigabitethernet 1/1
1         0080.ad00.0000      DYNAMIC  gigabitethernet 1/1
```

Show the statistic information of MAC addresses in MAC address table:

```
DGS-3610# show mac-address-table count
Dynamic Address Count  : 30
Static  Address Count  : 0
Filtering Address Count: 0
Total Mac Addresses    : 30
Total Mac Address Space Available: 8159
```

Caution

The total address space of the MAC address table available on the DGS-3610 series devices is 16384.

Show the setting of address aging time:

```
DGS-3610# show mac-address-table aging-time
Aging time   : 300
```

13.2 The Changing Notification of the MAC Address

13.2.1 Overview

If you want to know the situation of user changes in the network for the device, the MAC address notification is an effective function. After the function of MAC address notification is enabled, whenever the device learns or removes a MAC address, a notification reflecting the MAC address change can be generated and sent to the NMS (Network Management Workstation) with the form of SNMP Trap. If a notification about adding MAC address has been generated, you know a new user (marked by the MAC address) is using the device. If a notification about deleting MAC address (if there is no communication in the specified time according to the aging time between the switch with the user, the address of the user will be deleted from the address table on the device) has been generated, you know that a user does not use the device any more.

When many users use the device, it's possible to generate lots of MAC address changes within a short time (for example when the device is powered on), resulting in increase of the network traffic. In order to decrease the network load, you can set the time interval of sending MAC address notifications. The specified information of the address notification within the interval will be bound by the system. Thus, some information of MAC address changes are contained in each messages of address notification so as to decrease the network traffic.

At the same time when the MAC address notifications are generated, the notification information will be recorded in the MAC address notification history list. If you do not configure the NMS for receiving the traps or you do not receive the Traps in time, you can know the latest MAC address changing information by viewing the MAC address notification history list.

MAC address notification function is based on the interface. But the MAC address notification has a global switch. When the global switch is disabled, the MAC address notification will not be generated on all interfaces. This interface will generate a MAC address change notification only when the global switch is turned on and the MAC address change function on the interface is enabled. No notification will be generated when there is MAC address change on the interface with the disabled notification function. You can set the interface to send either of address increase or decrease notification, or send both.

Caution MAC address notifications are generated only for dynamic addresses, and notifications are not generated for static addresses.

13.2.2 Configuring MAC Address Changing Notification Function

By default, the global switch of MAC address is disabled, so all the functions of MAC address notification are disabled on all interfaces.

Configure the MAC address notification function for the device:

Command	Function
DGS-3610(config)# **snmp-server host** host-addr **traps** { [**version** {**1|2c}} |3 [auth | noauth | priv**]}] *community-string*	Configure the NMS for receiving the MAC address notification. host-addr: Specifies the IP of the recipient. version **-** Specify the version of the Trap to be sent. community-string: Specify the authentication name attached on the Trap sent.
DGS-3610(config)#**snmp-server enable traps**	Allows the switch to send Trap.
DGS-3610(config)# **mac-address-table notification**	Turn on the global switch of MAC address notification .
DGS-3610(config)# **mac-address-table notification** {interval *value* | history-size *value*}	interval value :Specify the interval of generating MAC address notification (optional). The interval is measured in seconds, within the range of 0~3600, defaulted to 1 second. history-size value: It is the maximum number of the records in the MAC notification history record table, within the range of 1-200, defaulted to 50.
DGS-3610(config-if)# **snmp trap mac-notification {added | removed**}	Enable the MAC address notification on the specified interface. added: Enable the MAC notification when a MAC address is **added** on this interface. Removed: Give a notice when the address is deleted

To disable the device from sending MAC address notification Traps, use the **no snmp-server enable traps mac-notification** command in the global configuration mode. To turn off the global switch for the MAC address notification, use the **no mac-address-table notification** command. To disable the MAC address notification on a specified interface, use the **no snmp trap mac-notification** {**added** | **removed**} command in the interface configuration mode.

This example shows how to enable the MAC address notification function and send the Trap of MAC address change notification to the NMS with the IP address 192.168.12.54 with the authentication name public. The interval of generating the MAC address change notification is 40 seconds. The size of history list of the MAC address notification is 100. and enable notification function whenever a MAC address is added or removed on the specified interface gigabitethernet 1/3.

```
DGS-3610(config)# snmp-server host 192.168.12.54 traps public
DGS-3610(config)# snmp-server enable traps
DGS-3610(config)# mac-address-table notification
DGS-3610(config)# mac-address-table notification interval 40
DGS-3610(config)# mac-address-table notification  history-size 100
DGS-3610(config)# interface gigabitethernet 1/3
DGS-3610(config-if)# snmp trap mac-notification added
DGS-3610(config-if)# snmp trap mac-notification removed
```

13.2.3 Viewing the InformationMAC Address change Notification

In the privileged mode, you can view the information in the MAC address table of the device by using the commands listed in the following table:

Command	Function
DGS-3610# **show mac-address-table notification**	Show the global configuration of MAC address change notification function
DGS-3610# **show mac-address-table notification interface**	Show the enabled status of MAC address change notification on the interface
DGS-3610# **show mac-address-table notification history**	Show History List of the MAC address change notification

The following examples show how to view the information of MAC address change notifications.

View the global configuration for MAC address notification:

```
DGS-3610# show mac-address-table notification
MAC Notification Feature : Enabled
Interval(Sec): 2
Maximum History Size : 154
Current History Size : 2
DGS-3610# show mac-address-table notification interface
Interface          MAC Added Trap MAC Removed Trap
---------------- -------------- ----------------
Gi1/1             Disabled      Enabled
Gi1/2             Disabled      Disabled
Gi1/3             Enabled       Enabled
Gi1/4             Disabled      Disabled
Gi1/5             Disabled      Disabled
Gi1/6             Disabled      Disabled
```

```
DGS-3610# show mac-address-table notification history
History Index:1
Entry Timestamp: 15091
MAC Changed Message :
Operation  VLAN MAC Address   Interface
---------- ---- -------------- --------------------
Added      1    00d0.f808.3cc9 Gi1/1
Removed     1    00d0.f808.0c0c Gi1/1
History Index:2
Entry Timestamp: 21891
MAC Changed Message :
Operation  VLAN  MAC Address   Interface
----------- ---- ------------- --------------------
Added      1     00d0.f80d.1083 Gi1/1
```

13.3 IP and MAC Address Binding

13.3.1 Overview

Through configuring the binding function of IP and MAC address, you can control the filtering to the input packets. If you bind a specified IP address with a MAC address, the swith only receives the packets binding address matched both with the source IP address and MAC address; otherwise this packet will be discarded.

You can strictly control the legality check of the input source for the device by adopting the characteristic of binding with the address. To be noted that the control of switch input through address binding has priority over 802.1X, port-based security and ACL.

13.3.2 Configuring Address Binding

In the global mode, you can set address binding by performing the steps below:

Command	Function
DGS-3610(config)# **address-bind** *ip-address mac-address*	Configure the binding of IP address and MAC address
DGS-3610(config)# **address-bind install**	Eable the binding function to take effect

To cancel the binding for IP and MAC address, use the **no address-bind** *ip-address mac-address* command in the global configuration mode.

Disable the binding function by executing the commanc **no address-bind install**.

13.3.3 Viewing the Address Binding Table

To show the address binding table for IP and MAC address, use the **show address-bind** command in the privilege mode:

```
DGS-3610# show address-bind
IP Address     Binding MAC Addr
----------    -----------------------
3.3.3.3       00d0.f811.1112
3.3.3.4       00d0.f811.1117
```

13.3.4 Configuring the Exceptional Ports for Address Binding

If you wish the address binding policy not to take effect on special ports, you can set these ports as the exceptional ports. To do this, enter the privideged mode and perform the steps below:

Command	Function
DGS-3610# **configure terminal**	Enter the global configuration mode.
DGS-3610(config)# **address-bind uplink** *intf-id*	Configure the exceptional ports for address binding
DGS-3610(config)# **address-bind install**	Install the exceptional ports for address binding

You can run **no address-bind uplink** *interface-id* or **no address-bind install** in the global configuration mode to cancel the setting of exceptional ports or cancel the installation of exceptional ports respectively.

13.3.5 Viewing Exceptional Ports for Address Binding

You can use **show address-bind uplink** in the privileged mode to show the exceptional ports set to the switch:

```
DGS-3610# show address-bind uplink
Ports       State
------------ ------
Fa0/1       Enabled
Fa0/2       Disabled
Fa0/3       Disabled
Fa0/4       Disabled
Fa0/5       Disabled
Fa0/6       Disabled
Fa0/7       Disabled
Fa0/8       Disabled
Fa0/9       Disabled
Fa0/10      Disabled
```

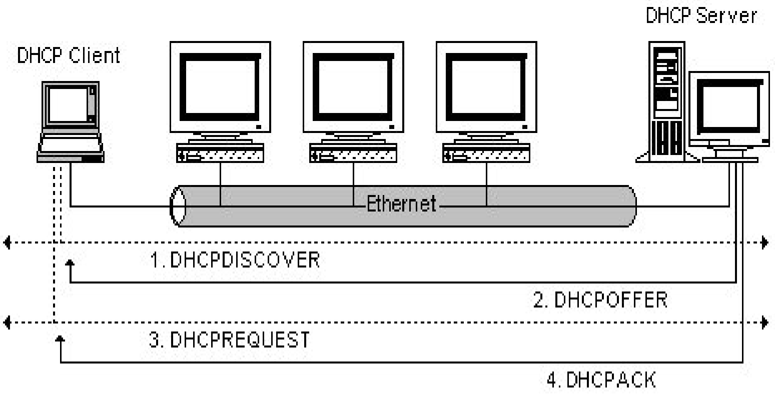
14 DHCP Snooping Configuration

14.1 DHCP Snooping Overview

14.1.1 Understanding DHCP

The DHCP is widely used to dynamically allocate the reusable network resources, for example, IP address. A typical IP acquisition process using DHCP is shown below:

Figure 14-1



The DHCP Client sends a DHCP DISCOVER broadcast packet to the DHCP Server. The Client will send the DHCP DISCOVER again if it does not receive a response from the server with a specified time.

After the DHCP Server receives DHCP DISCOVER packets, it allocates resources to the Client (for example, IP address) according to the appropriate policy, and sends the DHCP OFFER packets.

After receiving the DHCP OFFER packet, the DHCP Client sends a DHCP REQUEST for obtaining the server lease, and notifies other servers that it has accepted this server for address assignment.

After receiving the DHCP REQUEST packet, the server verifies whether the resource can be distributed. If yes, it sends the DHCP ACK packet. If not, it sends the DHCP NAK packet. Upon receiving the DHCP ACK packet, DHCP Client starts to use the resources assigned by the server. If it receives DHCP NAK, then it will send the DHCP DISCOVER packet again.

14.1.2 Understanding DHCP Snooping

DHCP Snooping monitors users by snooping the packets between the client and the server. DHCP Snooping can also be used to filter DHCP packets. It can be configured properly to filter illegal servers. Some terms and functions used in DHCP Snooping are explained below:

DHCP Snooping TRUST port: Because the packets for obtaining IP using DHCP are broadcast, some illegal servers may prevent users from obtaining the IP, or even illegal servers are used to cheat and steal user information. In order to avoid the problem of illegal server, DHCP Snooping classified the ports into two types: TRUST port and UNTRUST port. The device only forwards the DHCP Reply packets received through the TRUST port, while discarding all the DHCP Reply packets from the UNTRUST port. This way, the illegal DHCP Server can be shielded by setting the port connected to the legal DHCP Server as a TURST port and other ports as UNTRUST ports.

DHCP Snooping binding database: It’s usually that the users in the network set the IP addresses by themselves in the DHCP networks.. This makes it difficult to maintain the network and makes users who obtains IP addresses using DHCP unable to normally use the network due to conflict. DHCP Snooping snoops the packets between the Client and the Server, and combines the IP information that the user obtains, user MAC, VID, PORT and lease into a record entry. This creates a user database of DHCP Snooping, which is used with the ARP inspection function to control users' access to the network.

DHCP Snooping checks the validity of DHCP packets that pass the device, discard illegal DHCP packets, and records user information to create a DHCP Snooping binding database for ARP to inspecte and query. The following DHCP packets are considered illegal:

1. The DHCP reply packets received through UNTRUST ports, including DHCPACK, DHCPNACK, DHCPOFFER, etc.
2. Packets with different DHCP Client field values in the source MAC and DHCP packets when MAC check is enabled.
3. DHCPRELEASE packets with user information in the DHCP Snooping binding database but the port information inconsistent with the port information in the device information stored in the DHCP binding database.

14.1.3 Understanding DHCP Snooping information option

Part of network administrators hope to assign the IP to users according to their position when they carry out the IP management for current users. Namely, they hope to carry out the IP assignment according to the information of the network device that connects with users, so that the switch can add the device information related to some users into the DHCP request message in the DHCP option way, according to RFC3046 when they carry out the DHCP snooping. The used option number is 82, and the content server that is uploaded by option82 can obtain more user information, so as to assign the IP to users more accurately. The format of option82 that uploaded by DHCP snooping is shown as follows:

Figure 14-2 Agent Circuit ID

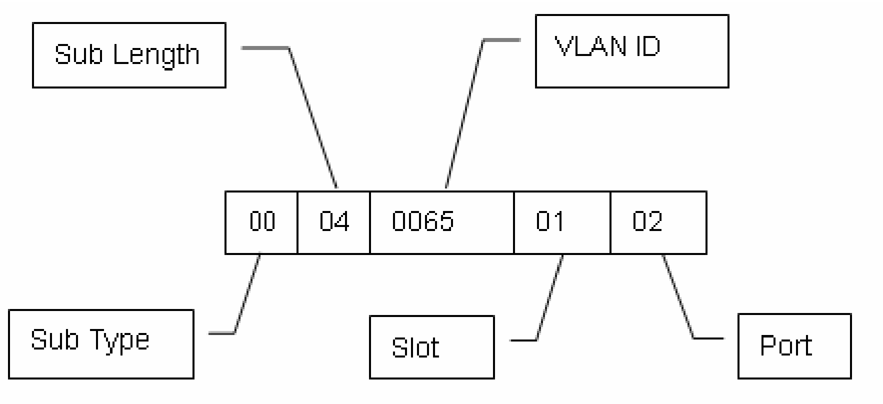
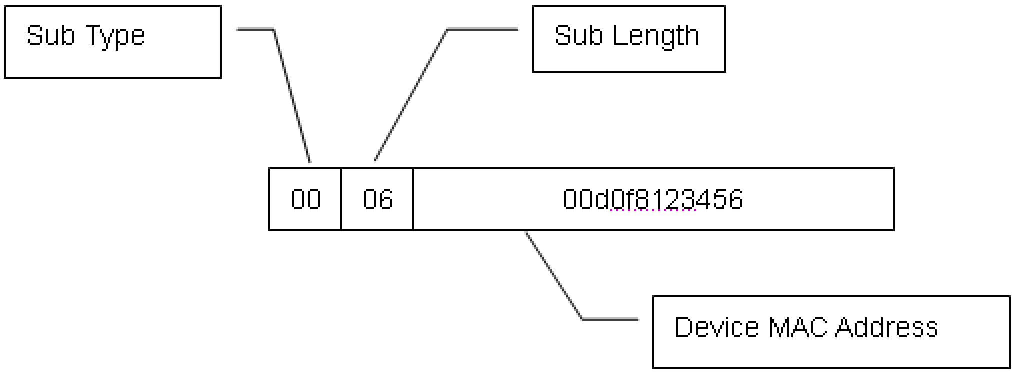


Figure 14-3 Agent Remote ID



14.1.4 Related Security Functions of DHCP snooping

Under the DHCP network environment, the administrators usually suffer from such problem that some users modify the used the static IP address other than the dynamic IP address, and the use of the static IP address will cause some users who have the priority to use the dynamic IP address can not use the network normally, which increases the complication of the network application environment and make it harder for administrators to manage the network. The DHCP dynamic binding means that the device will obtain the information by recording the IP address of the legal users during the DHCP snooping, and carry out related record and associated security processing. Current security control provides two ways, the one is the address binding function that used the hardware filtration, and the other is the DAI (dynamic arp inspection) that used the software, to carry out the legality check of users by the control of ARP.

Caution

When the address binding is used, the switch can only support the limited DHCP users for the limit of the hardware list item, if the users are too much on the switch, it may cause that the legal user can not add the hardware list item and use the network normally. When the DAI function is used, it will serious effect on the performance of the switch for all ARP messages should be forwarded and processed by CPU.

14.1.5 Understanding Address Binding Function of DHCP Snooping

The address binding function of the DHCP snooping is that the switch binds the IP obtained by users and the MAC of users by the snooping of the DHCP process, so as to limit that only the users who obtain the IP by DHCP can use the network, to prevent users to set the IP by themselves.

Furthermore, for the DHCP binding only filters to the IP message other than the ARP message, to improve the security and prevent the ARP cheating, it carries out the legality check of ARP for the users with DHCP binding. Refer to *DAI configuration* for the details.

14.1.6 Relationship between DHCP Snooping and ARP Detectation

ARP detection refers to check all the ARP packets that pass the device. DHCP Snooping needs to provide database information for ARP detectation. When the device that has the DAI function enabled receives ARP packets, the DAI module queries the binding database of DHCP snooping according to the packets. The ARP packet is considered legal and is thus learnt and forwarded only when its MAC, IP and port information match. Otherwise, the packet will be discarded.

14.1.7 Other Precautions on DHCP Snooping Configuration

The DHCP Snooping function and the DHCP Option 82 function of 1x are mutually exclusive, namely they cannot be used at the same time.

DHCP Snooping only snoops the DHCP process of user. If you want to restrict users to use IP addresses assigned using DHCP for network access, you must use the ARP detectation function. Note that the ARP detectation function affects the overall performance of the device because the ARP detectation module detects all the ARP packets.

14.2 DHCP Snooping Configuration

14.2.1 Configuration of Enabling and Disabling DHCP Snooping

The DHCP Snooping function of the device is disabled by default. It can be enabled by using the **ip dhcp snooping** command to start monitoring DHCP packets.

Command	**Description**
DGS-3610# **configure terminal**	Enter configuration mode
DGS-3610(config)# [**no**] **ip dhcp snooping**	Enable and disable DHCP snooping

The following example demonstrates how to enable the DHCP snooping function of the device:

```
DGS-3610# configure terminal
DGS-3610(config)# ip dhcp snooping
DGS-3610(config)# end
DGS-3610#
```

14.2.2 Configuring DHCP Source MAC Check Function

After this command is configured, the device will check the MAC addresses in the source MAC and Client fields in the DHCP Request packet from the UNTRUST port. It discards illegal packets with different MAC values. The packets are not checked by default.

Command	**Description**
DGS-3610# **configure terminal**	Enter configuration mode
DGS-3610(config)# [**no**]**ip dhcp snooping verify mac-address**	Enable and disable the source MAC check function

The following example shows how to enable the DHCP source MAC check function:

```
DGS-3610# configure terminal
DGS-3610(config)# ip dhcp snooping verify mac-address
DGS-3610(config)# end
DGS-3610#
```

14.2.3 Configuring Static DHCP Snooping User

This piece of user information can be configured statically when users under some ports want to use some static IP addresses in some applications.

Command	Description
DGS-3610# **configure terminal**	Enter configuration mode
DGS-3610(config)# **[no] ip dhcp snooping bindingbinding** *mac-addrees* **vlan** *vlan_id* **ip** *ip-addressaddress* **interface** *interface-id*	Set a DHCP static user to the DHCP snooping binding database

The following example shows how to add a static user to Port 9 of the device:

```
DGS-3610# configure terminal
DGS-3610(config)# ip dhcp snooping binding 00d0.f801.0101 vlan 1 ip 192.168.4.243
interface gigabitEthernet 0/9
DGS-3610(config)# end
DGS-3610#
```

Caution

The static configuration will not cover the dynamic users, and the users with the static binding can still obtain the IP address in the dynamic way.

14.2.4 Configuring Static DHCP Snooping Information Option

It will add the option82 option into each DHCP request by configuring the following commands when the DHCP snooping is forwarded.

Command	Function
DGS-3610# **configure terminal**	Enter the configuration mode
DGS-3610(config)# [**no**] **ip dhcp snooping Information option**	Set the DHCP snooping Information option

The following configuration is to enable the function of DHCP information option:

```
DGS-3610# configure terminal
DGS-3610(config)# ip dhcp snooping information option
DGS-3610(config)# end
DGS-3610#
```

Caution

After this function is configured, the information option82 function of DHCP relay will not be valid.

14.2.5 Configuring Static Address Binding of DHCP snooping

It will configure this command to enable the address binding function on the port in the interface mode. By default, the address binding function of all ports is not enabled.

Command	Function
DGS-3610# **configure terminal**	Enter the configuration mode.
DGS-3610(config)# **interface** *interface*	Enter the interface configuration mode.
DGS-3610(config-if)# [**no**] **ip dhcp snooping address-bind**	Enable/disable the address binding function of DHCP snooping on the port

The following configuration is to enable the address binding functions of snooping:

```
DGS-3610# configure terminal
DGS-3610(config)# interface gigabitEthernet 0/1
DGS-3610(config-if)# ip dhcp snooping address-bind
DGS-3610(config)# end
DGS-3610#
```

14.2.6 Schedule Writing of DHCP Snooping Database Information to flash

DHCP Snooping provides a command that can be configured to schedule writing of DHCP Snooping database information to the flash in order to prevent loss of DHCP user information on the device due to restart of device following electricity failure. By default, the time interval is 0, namely the information is not written to the flash regularly.

Command	Description
DGS-3610# **configure terminal**	Enter configuration mode
DGS-3610(config)# [**no**] **ip dhcp snooping database write-delay** [*time*]	Set delay time of DHCP information written to flash *time*: 600s--86400s. Default value: 0

The following example demonstrates how to set the delay time of DHCP Snooping writing to the flash to 3600s:

```
DGS-3610# configure terminal
DGS-3610(config)# ip dhcp snooping database write-delay 3600
DGS-3610(config)# end
DGS-3610#
```

Caution

You need to set a proper value for the time of delaying writing to the flash since erasing and writing to the flash frequently shortens the life of the flash. A shorter time helps to save the device information more effectively. A longer time reduces the number of writing to the flash and thus the flash has a longer life.

14.2.7 Writing DHCP Snooping Database Information to Flash Manually

In order to prevent loss of DHCP user information in the device due to restart of device following electricity failure, you can write information in the current DHCP Snooping binding database to the flash manually if required in addition to schedule writing to the flash.

Command	Description
DGS-3610# **configure terminal**	Enter configuration mode
DGS-3610(config)# **ip dhcp snooping database write-to-flash**	Write information in the DHCP Snooping database to the flash

The following example demonstrates how to write information in the DHCP Snooping database to the flash:

```
DGS-3610# configure terminal
DGS-3610(config)# ip dhcp snooping database write-to-flash
DGS-3610(config)# end
```

14.2.8 Configuring Port as TRUST Port

You can set a port as a TRUST port by using this command. By default, all the ports are UNTRUST ports:

Command	Description
DGS-3610# **configure terminal**	Enter configuration mode
DGS-3610(config)# **interface** *interface*	Enter the interface configuration mode.
DGS-3610(config-if)# [**no**] **ip dhcp snooping trust**	Set the port as a trust port

The following example shows how to set Port 1 of the device as a TRUST port:

```
DGS-3610# configure terminal
DGS-3610(config)# interface gigabitEthernet 0/1
DGS-3610(config-if)# ip dhcp snooping trust
DGS-3610(config-if)# end
DGS-3610#
```

Caution

When DHCP Snooping is enabled, only the DHCP response packets sent by the servers connected with the TRUST port will be forwarded.

14.2.9 Clearing Dynamic User Information from DHCP Snooping Database

This command is used to clear information from the current DHCP Snooping database.

Command	Description
DGS-3610# **clear ip dhcp snooping binding**	Clear information from the current database

The following example shows how to clear information from the current database manually:

```
DGS-3610# clear ip dhcp snooping binding
```

14.3 Showing DHCP Snooping Configuration

14.3.1 Showing DHCP snooping

To show the contents of ip dhcp snooping, perform the following steps:

Command	Description
DGS-3610# **show ip dhcp snooping**	Show configuration information of DHCP snooping.

For example:

```
DGS-3610# show ip dhcp snooping
Switch DHCP snooping  status                   :   ENABLE
DHCP snooping  Verification of hwaddr status   :   ENABLE
DHCP snooping database wirte-delay time        :   3600
Interface                  Trusted
------------------------   -------
GigabitEthernet 0/1          YES
```

14.3.2 Showing DHCP Snooping Database Information

To show information in the **ip dhcp snooping** database, perform the following steps:

Command	Description
DGS-3610# **show ip dhcp snooping binding**	View the static user information in the DHCP Snooping binding database

For example:

```
DGS-3610# show ip dhcp snooping binding
MacAddress  IpAddress   Lease(sec) Type  VLAN  Interface
------------------ --------------- ---------- -------------
00d0.f801.0101 192.168.4.243 -  static 1 GigabitEthernet 0/9
```

15 IGMP Snooping Configuration

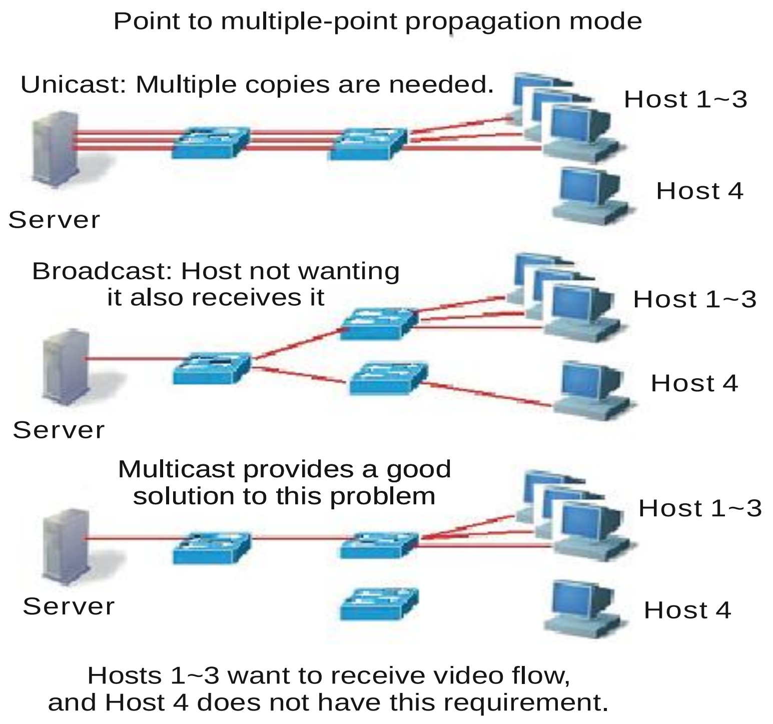
15.1 Overview

15.1.1 Understanding IGMP

Before understanding the IGMP, let us first describe the concept and function of IP multicast.

On the Internet, the multimedia services such as video conference and video on demand (VOD) with the sending mode of single point to multiple-point are becoming an important part of information transmission. The point-to-point unicast transmission mode cannot accommodate such service transmission feature, since the server must provide every receiver with a same copy of the IP packet. In addition, the same packets are transmitted repeatedly on the network, occupying enormous resources. Similarly, IP broadcast cannot meet such requirements. Despite the IP broadcast allows the host to send one IP packet to all the hosts of one network, the network resources are still wasted since not all hosts need such packets. In this situation, the multicast emerges, providing a solution to the method for one host to send messages to multiple designated receivers. See the figure below.

Figure 15-1


Point to multiple-point propagation mode
Unicast: Multiple copies are needed.
Host 1~3
Host 4
Server
Broadcast: Host not wanting it also receives it
Host 1~3
Host 4
Server
Multicast provides a good solution to this problem
Host 1~3
Server
Host 4
Hosts 1~3 want to receive video flow, and Host 4 does not have this requirement.

The IP multicast refers to the transmission of an IP message to a “Host Group”, and this host group which includes zero to multiple hosts is identified by a separate IP address.

The host group address is also called “Multicast Address”, or Class D address, namely, 224.0.0.0 ~ 239.255.255.255. 224.0.0.0~224.0.0.255 are reserved, wherein:

- 224.0.0.1 – all hosts in the network segment that support multicast.
- 224.0.0.2 – all routers in the network segment that support multicast.

The multicast address (multicast MAC address) on the second layer is mapped from the IP multicast address. Calculate the last 23 bits of the multicast IP and 01-00-5e-00-00-00, and the result obtained is multicast MAC address. For example, the multicast IP address is 224.255.1.1, its hex notation denotes as e0-ff-01-01, the last 23 bits is 7f-01-01. Calculate it with 01-00-5e-00-00-00, the result is: 01-00-5e-7f-01-01. 01-00-5e-7f-01-01 is the MAC multicast address of group 224.255.1.1.

The IGMP (Internet Group Management Protocol) runs between the host and the unicast routers connected to the host. Through this protocol, the host informs the local router its intention to join and receive the information of a particular multicast group. At the same time, the router checks whether the member of a known group in the LAN is in the active status (that is, whether the network segment belongs to the member of a multicast group) through this protocol at periodical intervals, to collect and maintain the membership of the network group connected. Currently, there are three versions of IGMP: IGMPv1 is described in rfc 1112, IGMPv2 is described in rfc 2236, and IGMPv3 is described in RFC 3376.

We describe respectively, as below, how the host joins or leaves a multicast in IGMPv1, IGMPv2 (suppose joining in 224.1.1.1).

In IGMPv1, the host sends the IGMP report packet of 224.1.1.1 to a certain interface on the router to ask for joining this group. After receiving this request, the interface on the router forwards the message of the corresponding multicast group for the reason of trusting the multicast members being existed on the interface. The router interface periodically sends the IGMP Query message of 224.0.0.1 (all hosts). If the host continues to receive the message of this group, it shall respond the corresponding IGMP Report packet. If a certain interface cannot receive the IGMP Report packet of any host, it is believed that there are no multicast members on this interface, so the message of the corresponding group is not forwarded to the interface.

IGMPv2 is downward compatible with v1. It extends the message —— adding the IGMP Leave message, so that the host can initiatively request for leaving the multicast group. In IGMPv2, the process for the host to join the group is consistent with its process in IGMPv1. The host sends an IGMP Report packet to request for joining a certain group. The router periodically sends the IGMP Query message of 224.0.0.1. If the host wants to continue to receive the message of this group, it should return the response IGMP Report packet. If the router cannot receive the IGMP Report packet of any host, it will remove this group. In IGMPv2, the host can also actively leave a certain group. When the host no longer needs a certain multicast flow, it actively sends the IGMP Leave message to the router and actively logs out from this group. After receiving the IGMP Leave message, the router sends the IGMP Query message of the group to determine whether any other hosts in the group need to receive the multicast information. At this time, if other hosts need to receive the multicast group, it responds with the IGMP Report packet. If the router fails to receive the response from any host, it cancels the group.

On the basis of the IGMPV1/V2, the IGMPV3 provides an additional source filtering multicast function. IGMPv3 to interact with the router is the same as that of IGMPv2. In the IGMP V1/V2, the host determines to join a group and receive the multicast traffic to the group address from any source only based on the group address. On the other hand, the host running the IGMP V3 notifies this host the desired multicast group to join, and also the addresses of the multicast sources to receive. The host can indicate that it wants to receive multicast traffic from which sources through a list or an exclusion list. At the same time, another benefit of the IGMP v3 is that it saves bandwidth to avoid unnecessary, invalid multicast data traffics from occupying network bandwidth. It is particularly useful in the case where multiple multicast sources share one multicast address.

Compared with IGMPv2, IGMPv3 specifies two types of packets: Membership Query and Version 3 Membership Report. There are three types of Membership Query:

- General Query: Used to query all the multicast members under the interface:

- Group-Specific Query: Used to query the members of the specified group under the interface:
- Group-and-Source-Specific Query: This type is the new one in the IGMPv3, used to query whether any member under the interface needs to receive the multicast traffic of the particular group from the sources in the specified source list.

IGMP Version3 is backward compatible with IGMP Version1 and IGMP Version2.

For more information about IP multicast, refer to RFC 1112, RFC 2236 and RFC 3376.

15.1.2 Understanding IGMP Snooping

Under Layer 2 equipment, the multicast frame is forwarded as broadcast, which may easily lead to multicast flow storm, wasting the network bandwidth. The typical multicast frame on the network is video flow. In a VLAN, if a user registers the video flow of a certain group, then all members in this VLAN can receive this video flow, whether they want or not.

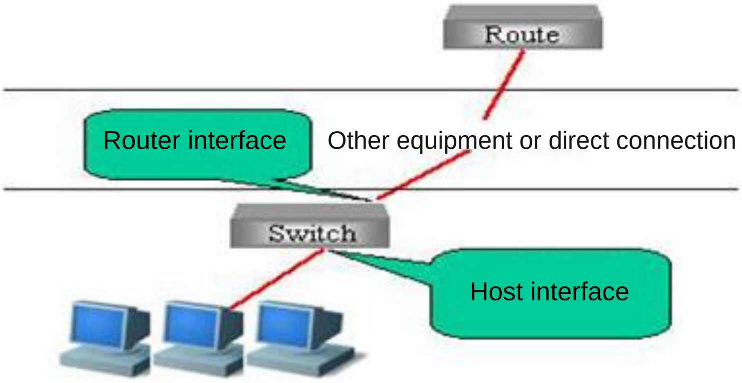
The function of IGMP Snooping is to solve this problem. It can enable the video flow to be forwarded only to the port where the register user is located, without influencing other users.

IGMP Snooping is the multicast restriction mechanism running on the Ethernet switch to monitor the IGMP packets between the router and user to manage and control the multicast group. The meaning of IGMP Snooping is “snoop”. From the meaning, we can easily understand its operation process: the switch “snoops” the interactive message between the user host and the router, and tracks the group information and the port applied for. When the switch snoops the IGMP report (request) message that the host sends to the router, the switch adds this port into the multicast forwarding table. The switch deletes this port from the table when it “snoops” the IGMP Leave message. The router will periodically send the IGMP Query message. If the switch receives no IGMP Report packet from the host within a certain period of time, the switch deletes this port from the table.

15.1.3 Understanding Router Interface

The router interface is the port connecting the multicast router, as shown below.

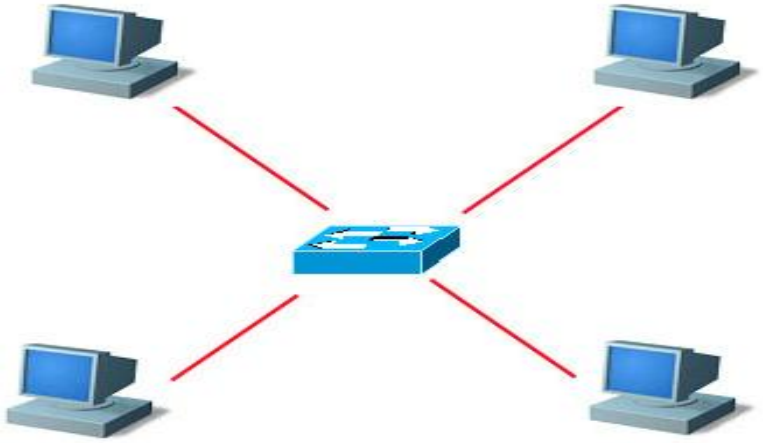
Figure 15-2



The messages sent from the host, such as IGMP Report, and IGMP Leave will be forwarded from this port to the router. Only the IGMP Query messages received from this port will be deemed as legal messages, and forwarded to the host port. The IGMP Query messages received from non-router interface will be discarded. How to configure route connection, see the Configuring Router Interface section.

Notethat in some network environments, if no multicast router exists in the network, it is unnecessary to configure the router interface, and the IGMP snooping can still operate normally, as shown below. as shown in the following diagram:

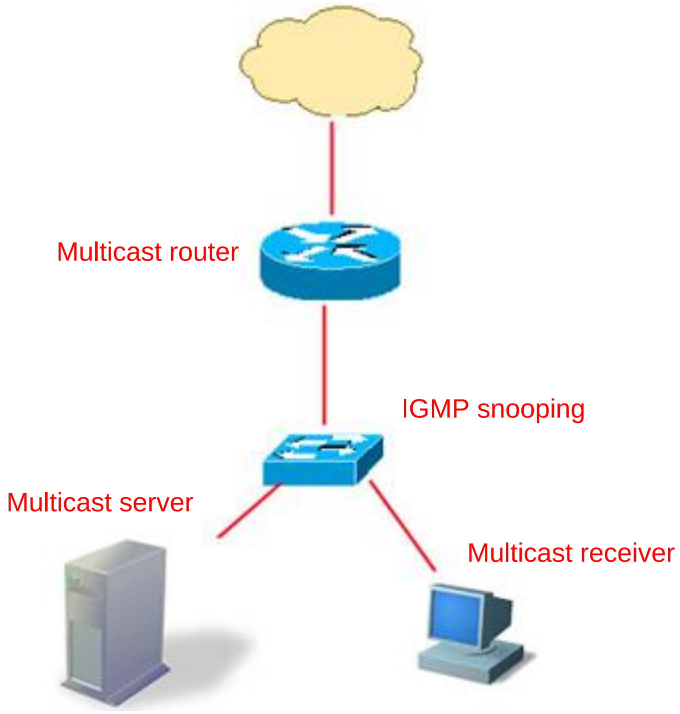
Figure 15-3



In this network environment, there is no multicast router, and these four PC can be both senders and receivers of the multicast flow. At this moment, the switch among them actually satisfies the requirement only by enabling the IGMP snooping, without having to set any port as the router interface.

In addition, the router interface defaults to become the receiver of the multicast data within this VLAN, as shown below.

Figure 15-4



The switch that supports IGMP snooping not only has to forward the multicast data the multicast flow receiver, but also has to forward the multicast data to the router interface, so that the multicast router can forward the multicast data flow to other networks. But probably the administrator does not want the upper-level multicast router to know a certain batch of multicast data. You can configure the router interface to make sure which multicast data needs forwarding, and which multicast data needs filtering, to satisfy requirements of network administrator .

Caution

In the above network topology, if there is no “multicast traffic receiver”, the switch will also create a multicast entry in the multicast router. However, such multicast forwarding entry generated by the “multicast data traffic” may be unstable. The change of the route connection port will delete the multicast forwarding entries generated by the multicast traffic. It’s recommended for the administrators to directly configure one static multicast forwarding entry for the route connection interface (Please see *Configuring IGMP snooping Static Member*) to ensure stable forwarding of the multicast traffic.

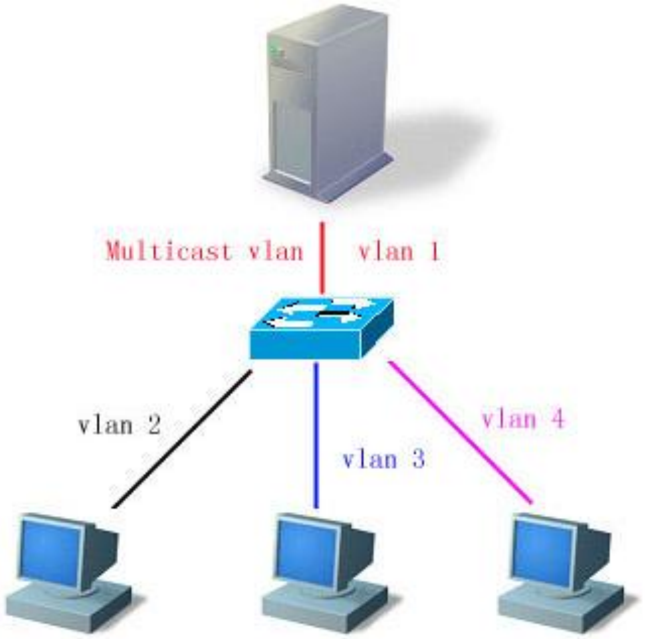
15.1.4 Understanding Operation Modes of IGMP Snooping

DISABLE mode: In this mode, IGMP Snooping is not effective, that is, the switch does not "snoop" the IGMP message between the host and the router or multicast frame when the broadcast is forwarded within the VLAN.

IVGL operation mode: In this mode, the multicast flows among various VLANs are independent. The host can only request multicast with the router interface which is located in the same VLAN with it.

SVGL operation mode: In this mode, the hosts of various VLANs share the same multicast flow. The host can apply for multicast flow across VLANs. Designate one Multicast VLAN, and the multicast data flows received in this VLAN can be forwarded to other cross-VLAN hosts, as shown below. See the figure below.

Figure 15-5



So long as the VID of the multicast data flow is Multicast VLAN (or UNTAG data flow, the native VLAN of the receiving port is Multicast VLAN), all will be forwarded to the member port of this multicast address, whether this member port is within this VLAN or not. The VID of the generated multicast forwarding table will be Multicast VLAN. In the SVGL mode, except the router interface, for other ports, only when they are in the Multicast VLAN, can the multicast sent by them be forwarded within the VLAN.

IVGL and SVGL modes can coexist. You can allocate a batch of multicast addresses to SVGL. Within this batch of multicast addresses, the multicast forwarding tables (GDA table) are all forwarded across VLANs, while other multicast addresses are forwarded in IVGL mode.

The IVGL mode and SVGL mode of IGMP Snooping provided by DGS-3610 strengthens the network application flexibility, enabling it to adapt to different network environment.

15.1.5 Understanding Source Port Check

DGS-3610 series support IGMP SNOOPING source port check function and improve the security of the network.

IGMP source port check refers to the entry port of strictly restricting the IGMP multicast flow. When IGMP source port check is disabled, the video flow entering through any port is legal. The switch will forward them to the registered port. When the IGMP source port check is enabled, only the video flows entering through the router interface are legal, the switch forwards them to the registered port; while the video flows entering through non- router interface are deemed as illegal and will be discarded.

15.1.6 Understanding fast-leave

According to the IGMP protocol, the Leave packets must meet the following requirement: “Ports should not be allowed to leave a group immediately. Instead, the multicast router should first send IGMP Query packets, and ports are allowed to leave the group only when the host does not respond”. However, in specific environments (for example, one port is connected to only one multicast group user), the IGMP snooping can immediately leave after receiving LEAVE packets, a mechanism known as Fast Leave.

15.1.7 Understanding IGMP Snooping Suppression

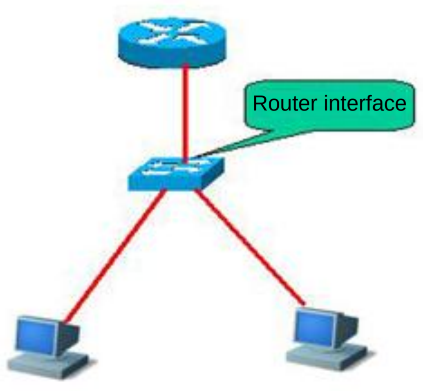
For the devices enabled with IGMP Snooping, every group address may have multiple IGMP users. When every user joins the group and receives the Query message, it will send a Report packet. For every Report packet, DGS-3610 series will forward it to the multicast router. In this way, when the multicast router sends a Query to the port enabled with the Snooping device, it will receive multiple Report packets. To lighten the pressure of the server in processing Report packets, the switch only forwards the first report packet received to the routing port when multiple hosts request to join a multicast group, suppressing other report packets. This function is called IGMP Snooping Suppression.

Due to the special form of the IGMP v3 Report packets, IGMP Snooping Suppression only supports suppression of v1 and v2 Report packets.

15.1.8 Typical Application

The multicast is applied more and more widely. It is primarily applied in campus network and residential community network. The multicast technology can be applied in services such as weather forecast, news broadcasting, and VoD, and currently the most common is the VOD. The following figure shows the common network topology.

Figure 15-6



Equipment requirement: The switch supports IGMP Snooping.

Required setup:

1. Enable IGMP Snooping function.

2. Set upper link as router interface.

Characteristics:

1. Simple configuration;

2. Effectively reducing broadcast storm, improving network bandwidth utilization rate.

15.2 Configuring IGMP Snooping

We will describe how to configure IGMP snooping in the following chapters

- IGMP Snooping Default
- Configuring IGMP Profiles
- Configuring Router Interface
- Configuring Range of Multicast Frame Forwarding by Router Interface
- Configuring IVGL Mode
- Configuring SVGL Mode
- Configuring Coexistence Mode of IVGL and SVGL
- Configuring DISABLE Mode
- Configuring Maximum Response Time of Query Message
- Configuring Source Port Check
- Configuring Source IP Check
- Configuring IGMP Static members
- Configuration IGMP Filtering

15.2.1 IGMP Snooping Default

IGMP snooping status	**DISABLE status**
Router interface	All interfaces are not router interface, and do not conduct dynamic learning.
Source port check	Off
IGMP Profile	Entry is null, and the default action is deny.
Multicast Vlan of SVGL	VLAN 1
IGMP filtering	None
Static members of GMP snooping	None

Caution

You are recommended to configure VLAN, port access, trunk, and AP attribute before configuring IGMP snooping, otherwise it is impossible to meet your expected requirement. As the above attributes are all the basic configuration attributes of the switch, if these attributes are modified after the multicast forwarding table is generated, abnormal result will occur afterwards.

In addition, if the switch is enabled with private vlan, it does not support igmp snooping.

The Igmp snooping multicast address may cause the Hash conflict. If the quantity of multicasts in the system doesn't exceed the limit of the index at some moment, while the new multicast address fails to be added, it may be cause the Hash conflict.

15.2.2 Configuring IGMP Profiles

Let us first describe an IGMP Profile entry, which can define a set of multicast address ranges and permit/deny actions for the functions to be adopted, such as "multicast address range for applying SVGL mode", "filtering multicast data range of route connection interface " and "IGMP Filtering range". Note that: After an IGMP Profile is already associated with a function application, the multicast forwarding table generated by the function will be affected if you modify the IGMP Profile.

In the configuration mode, set a profile by performing the following steps:

Command	**Function**
DGS-3610(config)# **ip igmp profile** *profile-number*	Enter IGMP Profile mode, and allocate a figure for identification. The range is 1–65535.

Command	**Function**
DGS-3610(config-profile)# **permit** | **deny**	(Optional) Permit or deny this batch of multicast addresses ranges, and the default is deny. This action indicates: permit/deny these multicast addresses within the following ranges, and deny/permit other multicast addresses.
DGS-3610(config-profile)# **range** *ip multicast-address*	Add one or more multicast address ranges.
DGS-3610# **end**	Return to the privileged mode.

To delete one of the IGMP profiles, use **no ip igmp profile profile number.**

To delete one range in the profiles, use **no range ip multicast address.**

This example shows the profile configuration process:

```
DGS-3610(config)# ip igmp profile 1
DGS-3610(config-profile)# permit
DGS-3610(config-profile)# range 224.1.1.1 225.1.1.1
DGS-3610(config-profile)# range 226.1.1.1
DGS-3610(config-profile)# end
DGS-3610# show ip igmp profile 1
IGMP Profile 1
permit
range 224.1.1.1 225.1.1.1
range 226.1.1.1
```

According to the above-mentioned configuration, the rule of the IGMP Profile is the multicast addresses from 224.1.1.1 to 225.1.1.1, and 226.1.1.1, while all other multicast addresses are denied.

15.2.3 Configuring Router Interface

The router interface is the port for the multicast router to connect to the switch (it does not refer to the port connecting to the video server). When the source port check is enabed, only the video flows entering through the router interface are forwarded, and other flows will be discarded. You can statically configure the router interface, and you can also configure the IGMP query/dvmrp dynamically snooped by the switch or PIM message, so as to automatically identify the router interface.

In the privileged mode, you can set a router interface by performing the following steps:

Command	**Function**
DGS-3610(config)# **ip igmp Snooping vlan** *vlan-id* **mrouter** {**interface** *interface-id* | **learnpim-dvmrp**}	Set the interface as router interface. Use the **no** form of this command to delete a router interface. You can also configure the router interface for the switch to dynamically learn it.. Use the corresponding **no** command to disable the dynamic learning and clear all router interfaces dynamically learnt. By default, dynamic learning is disabled.
DGS-3610(config)# **end**	Return to the privileged mode.

This example shows how to set the Ethernet interface 1/1 as the router interface, and configures the automatic learning router interface:

```
DGS-3610# configure terminal
DGS-3610(config)# ip igmp snooping vlan 1 mrouter interface gigabitEthernet 0/7
DGS-3610(config)# ip igmp snooping vlan 1 mrouter learn pim-dvmrp
DGS-3610(config)# end
DGS-3610# show ip igmp snooping mrouter
Vlan    Interface            State        IGMP profile
----    ---------            ------       -------------
1   GigabitEthernet 0/7   static           0
1   GigabitEthernet 0/12  dynamic          0
DGS-3610# show ip igmp snooping mrouter learn
Vlan   learn method
----   ------------------
1      pim-dvmrp
```

15.2.4 Configuring the Range of Multicast Frame Forwarded by Router Interface

As the default router interface is regarded as the member of all multicast addressed within this VLAN to forward the multicast data flow . But it is possible that some multicast data is not expected to be forwarded to the multicast router. The administrator can use the IGMP Profile to filter the range of multicast data to be forwarded by the router interface.

In the configuration mode, configure the range of the multicast frame forwarded by the route interface by performing the following steps:

Command	**Function**
DGS-3610(config)# **ip igmp snooping vlan** *vlan-id* **mrouter interface** *interface-id* **profile** profile name	Set this port as this router interface, and set the associated profile. Only the multicast flows complying with this profile can be forwarded to this router interface.
DGS-3610(config)# **end**	Return to the privileged mode.

You can delete the association with the profile by using no **ip igmp snooping vlan** *vlan-id* **mrouter interface** *interface-id* **profile**.

This example configures the range of multicast frame forwarded by the router interface:

```
DGS-3610# configure terminal
DGS-3610(config)# ip igmp Snooping vlan 1 mrouter interface gigabitEthernet 0/7 profile
1
DGS-3610(config)# end
DGS-3610# show ip igmp Snooping mrouter
Vlan    Interface         State    IGMP profile
----    ---------         ------   -------------
1   GigabitEthernet 0/7    static        1
1   GigabitEthernet 0/12   dynamic       0
```

15.2.5 Configuring the Aging Time of the Route Interface in Dynamic Learning

When dynamic route interface learning is enabled, the route interface of dynamic learning will use the default 300s as the aging time. If no packets are received from the new learning Mrtoue port within the aging time, the route interface learnt will be deleted. The following commands can set the aging time within the range of 1-3600s .

In the configuration mode, configure the range of the multicast frame forwarded by the route interface by performing the following steps:

Command	Function
DGS-3610(config)# **ip igmp snooping dyn-mr-aging-time** *time*	Configure the aging time for the dynamic router interface , *Time:* <1-3600> The default is 300s.
DGS-3610(config)# **end**	Return to the privileged mode.

You can use the **no ip igmp snooping dyn-mr-aging-time** command to restore the aging time to the default value.

The following example configures the aging time of the dynamic route interface to 100:

```
DGS-3610# configure terminal
DGS-3610(config)# ip igmp snooping dyn-mr-aging-time 100
DGS-3610(config)# end
```

15.2.6 Configuring IVGL Mode

In the configuration mode, enable IGMP Snooping and set its mode as IVGL mode by performing the following steps:

Command	**Function**
DGS-3610(config)# **ip igmp Snooping ivgl**	Enable IGMP Snooping and set it to the IVGL mode.
DGS-3610(config)# **end**	Return to the privileged mode.

Following example shows to enables IGMP Snooping and sets it to the IVGL mode:

```
DGS-3610# configure Terminal
DGS-3610(config)# IP igmp Snooping ivgl
DGS-3610(config)# end
```

15.2.7 Configuring SVGL Mode

In the configuration mode, enable IGMP Snooping and set it as SVGL mode by performing the following steps:

Command	**Function**
DGS-3610(config)# **ip igmp snooping svgl**	Enable IGMP Snooping and configure it as the SVGL mode.
DGS-3610(config)# **end**	Return to the privileged mode.

This example enables IGMP Snooping, and sets it to the SVGL mode,

```
DGS-3610# configure Terminal
DGS-3610(config)# iP igmp snooping svgl
DGS-3610(config)# end
```

15.2.8 Configuring Coexistence Mode of IVGL and SVGL

In the configuration mode, enable IGMP Snooping and set its mode as IVGL, SVGL coexistence mode by performing the following steps:

Command	**Function**
DGS-3610(config)# **ip igmp snooping ivgl-svgl**	Enable IGMP Snooping and configure it as the IVGL, SVGL coexistence mode
DGS-3610(config)# **end**	Return to the privileged mode.

This examples enables IGMP Snooping and sets it to the IVGL mode:

```
DGS-3610# configure Terminal
DGS-3610(config)# iP igmp snooping ivgl-svgl
DGS-3610(config)# end
```

15.2.9 Configuring DISABLE Mode

In the configuration mode, set IGMP Snooping to the DISABLE mode by performing the following steps:

Command	Function
DGS-3610(config)# **no ip igmp snooping**	Disable IGMP Snooping
DGS-3610(config)# **end**	Return to the privileged EXEC mode.

15.2.10 Configuring Maximum Response Time of Query Message

The multicast router periodically sends the IGMP Query message to query whether multicast member exists or not. Within a certain period of time after the Query message is sent, if the multicast router has not received the IGMP Report message of the host, the switch will think this port no longer receives multicast flows, and delete this port from the multicast forwarding table. The default time is 10 seconds.

In the configuration mode, you can set the maximum response time of Query packets by performing the following steps:

Command	Function
DGS-3610(config)# **ip igmp Snooping query-max-respone-time** *seconds*	Set the maximum response time of Query message. The range is 1-65535, and the default time is 10 seconds.
DGS-3610(config)# **end**	Return to the privileged mode.

Use **no ip igmp snooping query-max-response-time** to restore its default value.

15.2.11 Configuring Source Port Check

In the configuration mode, set source port check by performing the following steps:

Command	Function
DGS-3610(config)# **ip igmp Snooping source-check port.**	Enable the source port check.
DGS-3610(config)# **end**	Return to the privileged mode.

You can disable source port check by using the **no ip igmp snooping source-check port** command.

15.2.12 Configuring Source IP Check

In the configuration mode, you can set **igmp snooping** source IP check by performing the following steps:

Command	Function
DGS-3610(config)# **ip igmp snooping source-check default-server** *address*	Enable source IP check and add the multicast-source IP entry.
DGS-3610(config)# **ip igmp snooping limit-ipmc vlan** *vid* **address** *address* **server** *address*	Add multicast addresses—source IP address (multicast server address) corresponding entry
DGS-3610(config)# **end**	Return to the privileged mode.

You can disable the source IP check by using the **no ip igmp snooping source-check default-server** command.

The following example enables source IP check and set the default source IP to 192.1.1.1. In the example, a multicast-source IP entry is added, where VID is 1, group IP is 224.1.1.1, and source IP is 192.1.2.3.

```
DGS-3610# configure Terminal
DGS-3610(config)# ip igmp snooping source-check default-server 192.1.1.1
DGS-3610(config)# ip igmp snooping limit-ipmc vlan 1 address 224.1.1.1 server 192.1.2.3
DGS-3610(config)# end
```

15.2.13 Configuring Fast-Leave

In the configuration mode, set **igmp snooping fast-leave** by performing the following steps:

Command	Function
DGS-3610(config)# **ip igmp snooping fast-leave enable**	Enable the fast-leave function on the switch.
DGS-3610(config)# **end**	Return to the privileged mode.

You can disable the fast-leave function by using the **no ip igmp snooping fast–leave enable** command.

The following example enables the fast–leave function:

```
DGS-3610# configure Terminal
DGS-3610(config)# ip igmp snooping fast-leave enalbe
DGS-3610(config)# end
```

15.2.14 Configuring IGMP Snooping Suppression

In the configuration mode, set **igmp snooping suppression** by performing the following steps:

Command	Function
DGS-3610(config)# **ip igmp snooping suppression enable**	Enable the suppression function on the switch.
DGS-3610(config)# **end**	Return to the privileged mode.

You can disable the Suppression function by using the **no ip igmp snooping suppression enable** command.

The following example enables the Suppression function:

```
DGS-3610# configure Terminal
DGS-3610(config)# ip igmp snooping suppression enalbe
DGS-3610(config)# end
```

15.2.15 Configuring Static Members of IGMP Snooping

When igmp snooping is enabled, you can statically configure a port to receive a specific multicast flow, disregard the impact of various IGMP packets.

In the configuration mode, set the static member of IGMP Snooping by performing the following steps:

Command	Function
DGS-3610(config)# **ip igmp Snooping ivgl**	Enable IGMP Snooping and set it to the **IVGL** mode.
DGS-3610(config)# **ip igmp snooping vlan** *vlan-id* **static** *ip-addr* **interface** *[interface-id]*	Statically configure a port to receive a certain multicast flow. • *vlan-id*: vid of multicast flow • *ip-addr* : multicast address • *interface-id:* Interface ID
DGS-3610(config)# **end**	Return to the privileged mode.

Use **no ip igmp snooping vlan** *vlan-id* **static** *ip-addr* **interface** *interface-id* to delete the static configuration of multicast member.

This example configures static member of IGMP snooping:

```
DGS-3610# configure Terminal
DGS-3610(config)# ip igmp snooping vlan 1 static 224.1.1.1 interface GigabitEthernet 0/7
DGS-3610(config)# end
```

```
DGS-3610(config)# show ip igmp snooping gda
Abbr: M - mrouter
      D - dynamic
      S - static
VLAN  Address              Member ports
---- --------------   -----------------------------
1    224.1.1.1            GigabitEthernet 0/7(S)
```

15.2.16 Configuration IGMP Filtering

In some cases, you may need to make a certain port receive only a special batch of multicast data flows, and control the maximum number of groups permitted to be dynamically added under this port. IGMP Filtering meets this requirement.

You can apply one IGMP Profile to a port. If the port receives the IGMP Report packet, the switch will check if the multicast address the port wants to join is within the range of IGMP Profile. If yes, it is allowed to join, with subsequent processing performed later.

You can also configure the maximum number of groups to be added on one port. When it is beyond the range, the switch will no longer receive, or handle the IGMP Report packet.

In the configuration mode, set IGMP Filtering by performing the following steps:

Command	Function
DGS-3610(config)# **interface** *interface-id*	Enter the configuration interface.
DGS-3610(config-if)# **ip igmp snooping filter** *profile-number*	(Optional) apply the profile to this port. The profile number range is 1- 65535.
DGS-3610(config-if)# **ip igmp snooping max-groups** *number*	(Optional) the maximum number of groups permitted to be dynamically added to this port. The range is 0 – 4294967294.
DGS-3610(config-if)# **end**	Return to the privileged mode.

15.3 Viewing IGMP Snooping Information

Related to the information of IGMP snooping, please refer to the following information:

- Viewing Current Mode
- Viewing and Clearing IGMP snooping Statistics
- Viewing Router Interface Information
- Viewing Dynamic Forwarding Table
- Viewing Source Port Check Status
- Viewing IGMP Profile
- Viewing IGMP Filtering

15.3.1 Viewing Current Mode

In the privileged mode, use the following command to view the current working mode and global configuration of IGMP Snooping:

Command	Function
DGS-3610# **show ip igmp snooping**	View the current operation mode of IGMP Snooping and global configuration.

The following example shows to use the **show ip igmp snooping** command to view the IGMP Snooping configuration information:

```
DGS-3610# show ip igmp snooping
Igmp-snooping mode      : IVGL
SVGL vlan-id            : 1
SVGL profile number     : 0
Source check port       : Disabled
Query max respone time  : 10(Seconds)
```

15.3.2 Viewing and Clearing IGMP snooping Statistics

In the privileged mode, view and clear the IGMP Filtering statistics by using the following commands:

Command	Function
DGS-3610# **show ip igmp snooping statistics** [**vlan** *vlan-id*]	View the statistic information of IGMP Snooping
DGS-3610# **clear ip igmp snooping statistics**	Clear the statistic information of IGMP Snooping

The following example shows to use the **show ip igmp snooping statistics** command to view the router interface information of IGMP Snooping :

```
DGS-3610# show ip igmp snooping statistics
GROUP    Interface    Last report      Last leave    Last
                         time             time      reporter
--------------- ------------ ---------  ----------  ---------
224.1.1.2 VL1:Gi4/2   0d:0h:0m:7s     ----    192.168.9.250
                      Report pkts: 1           Leave pkts: 0
```

15.3.3 View Router Interface Information

In the privileged mode, view the IGMP Filtering router interface information by using the following command:

Command	Function
DGS-3610# **show ip igmp snooping mrouter**	View the route connection port information of IGMP Snooping

The following example shows to use the **show ip igmp snooping** command to view the IGMP Snooping router interface information:

```
DGS-3610# show ip igmp snooping mrouter
Vlan    Interface          State       IGMP profile number
----    --------            -------     -------------------
1   GigabitEthernet 0/7    static        1
1   GigabitEthernet 0/12   dynamic       0
```

15.3.4 Viewing Dynamic Forwarding Table

In the privileged mode, view the forwarding rule of each port in the multicast group, that is, the GDA table.

Command	Function
DGS-3610# **show ip igmp snooping gda-table**	Show the forwarding rule of each port in the multicast group

This example shows information of various multicast groups of GDA table and the information of all member ports of one multicast group:

```
DGS-3610# show ip igmp snooping gda-table
Abbr: M - mrouter
      D - dynamic
      S - static
VLAN  Address             Member ports
---------------------   -----------------------------------
1      224.1.1.1         GigabitEthernet 0/7(S)
```

15.3.5 Viewing Source Port Check Status

In the privileged mode, use the following command to view the current source port check status of IGMP Snooping:

Command	Function
DGS-3610# **show ip igmp snooping**	View the current operation mode of IGMP Snooping and global configuration.

15.3.6 Viewing IGMP Profile

In the privileged mode, view the IGMP Profile information by using the following command:

Command	Function
DGS-3610# **show ip igmp profile** *profile-number*	View the IGMP Profile information.

15.3.7 Viewing IGMP Filtering

In the privileged mode, view the IGMP Filtering configuring information by using the following command:

Command	Function
DGS-3610# **show ip igmp snooping interface** *interface-id*	View IGMP Filtering configuration information.

The following serves to view IGMP Filtering information.

```
DGS-3610# show ip igmp snooping interface GigabitEthernet 0/7
Interface         Filter Profile number     max-groups
----------       ---------------------    -----------
GigabitEthernet 0/7         1              4294967294
```

15.3.8 Configuring Other Restrictions of IGMP Snooping

The IGMP Snooping source port check needs to use filtering domain masks. For detailed definition of filtering domain masks, please see the chapter *“ACL Configuration*”. Address binding, source port check and ACL share the filtering domain masks. The total number of masks available depends on the specific products. As the number of filtering domain masks is limited, these three functions will influence each nother. Enable the address binding function needs to occupy two masks, enabling the source port check occupies two masks, and the usable masks for the ACL depend on whether these two kinds of functions are enabled. By default, the ACL can use 8 masks. If any one function of the address binding and source port check is enabled, then masks used for the ACL can be reduced two masks. If the address binding and source port check are concurrently enabled, then the number of usable masks for ACL is reduced by 4, and only four are left. Contrarily, if the ACL uses multiple masks and the number of left masks cannot meet the requirement of these two kinds of applications, then when enabling the address binding, source port check functions, the system will prompt the mask resources use-up information. When any one of the three functions cannot operate normally due to the mask restriction, it is advisable to realize the normal application of this function through reducing the mask occupancy of other two functions. For example, when three functions are concurrently enabled, enable the source port check, and it prompts that the mask will be used up, then disable the address binding function (deleting all address bindings) or delete the ACE of ACL occupying multiple masks, and the source port check can be enabled normally.

When the IGMP Snooping or setting router interface is enabled, if the source port check is enabled, then the source port check function fails due to inadequate mask resource. At this moment, the system prompts: source port check applying failed for hardware out of resources. In this case, you should release other resources of the masks, redisable and then enable source port check.

16 PIM Snooping Configuration

This chapter will describe how to configure the protocol independent multicast snooping on the DGS-3610 series. It will cover the content below:

- Understand the PIM snooping principle.
- Configure the PIM snooping by default.
- Guide and restriction the PIM snooping configuration.
- Configure the PIM snooping.

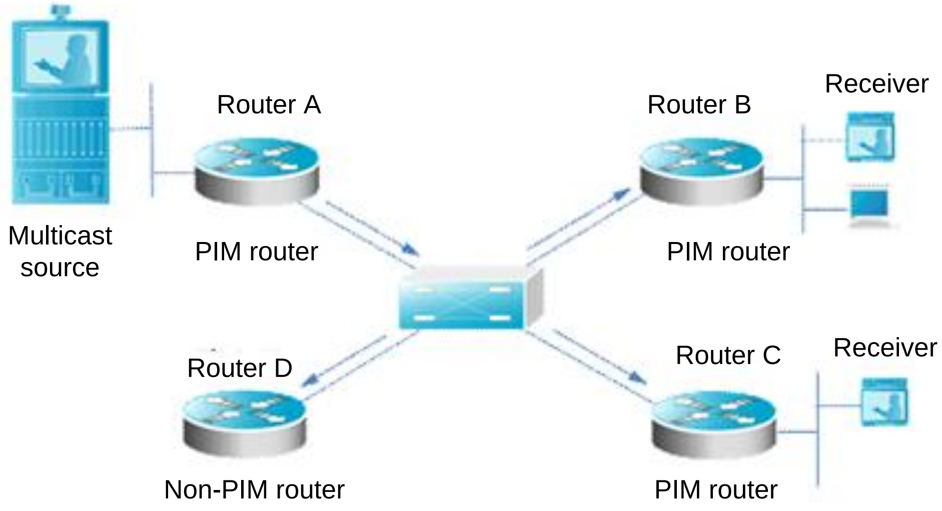
16.1 Understanding PIM Snooping Principle

Within the network that the L2 switches connect to several routers, the switches will flood the multicast data flow into all router ports even though the multicast function is not enabled in the downstream direction. When the PIM snooping is enabled, the switches will limit the multicast data to connect the ports of the multicast routers.

The figure below shows the multicast data flow flooding before the PIM snooping is enabled and the multicast data stream limit after the PIM snooping is enabled.

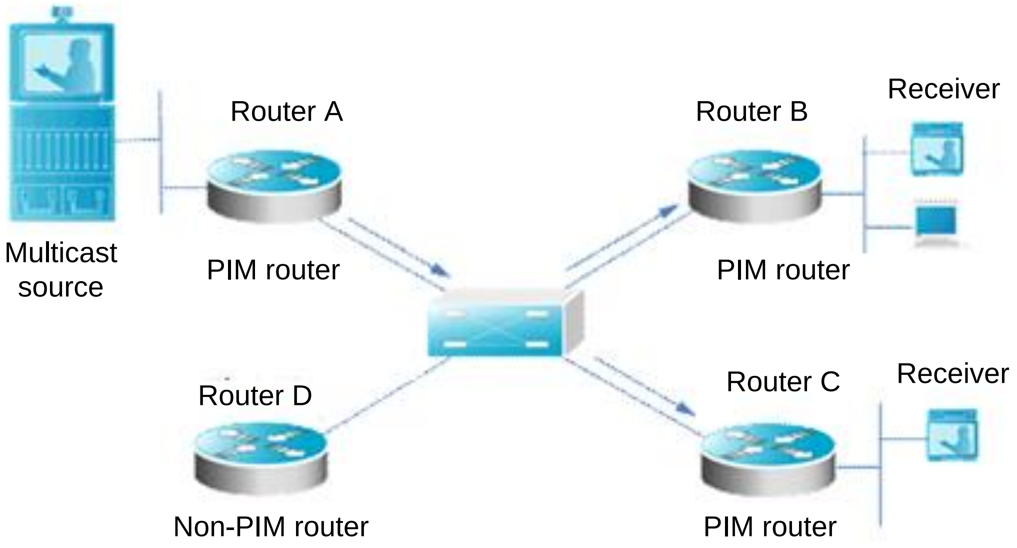
In the Figure 16-1, the multicast data will flow into all the ports of the switches if the PIM snooping is not enabled.

Figure 16-1 Multicast flow the PIM snooping is diabled



In the Figure 16-2, the multicast data only flows into the ports that connect to the multicast router B and C, but not flows into the router D.

Figure 16-2 Multicast flow after PIM Snooping is Enabled



16.2 Configuration of PIM Snooping by Default

By default, the PIM snooping is disabled.

16.3 Guiding and Limiting PIM Snooping Configuration

- The PIM snooping is applicable for PIM-DM and PIM-SM at the same time.
- The PIM snooping can be enabled or disabled on SVI individually.
- Only when the multicast route and PIM are enabled, the PIM snooping can produce actual effect on the forwarding of the multicast flow.
- The neighboring information of the PIM snooping will carry out the timeout processing according to the hold-time in the Hello message.
- The neighboring information of the PIM snooping will only be removed for the timeout, but the change of the port status has no effect on the neighboring under this port.

16.4 Configuring PIM Snooping

This section will describe how to configure the PIM snooping.

- Enable the PIM snooping globally.
- Enable the PIM snooping on SVI.

16.4.1 Enable PIM Snooping Globally

To enable the PIM snooping globally, execute the following tasks:

Command	Function
DGS-3610(config)# **ip pim snooping** DGS-3610(config)# **no ip pim snooping**	Enable the PIM snooping. Disable the PIM snooping.
DGS-3610(config)# **end**	Exit the configuration mode.
DGS-3610# **show ip pim snooping**	Check the configuration.

The following example will show how to enable and check the configuration globally.

```
DGS-3610(config)# ip pim snooping
DGS-3610(config)# end
DGS-3610# show ip pim snooping
```

16.4.2 Enable PIM Snooping on SVI

To enable the PIM snooping on SVI, execute the following tasks:

Command	Function
DGS-3610(config)# **interface vlan** *vlan_ID*	Select the VLAN interface.
DGS-3610(config)# **ip pim snooping** DGS-3610(config)# **no ip pim snooping**	Enable the PIM snooping. Disable the PIM snooping.
DGS-3610(config)# **end**	Exit the configuration mode.
DGS-3610# **show ip pim snooping**	Check the configuration.

The following example will show how to enable and check the configuration globally.

```
DGS-3610(config)# ip pim snooping
DGS-3610(config)# end
DGS-3610# show ip pim snooping
```

17 MSTP Configuration

17.1 MSTP Overview

17.1.1 STP and RSTP

17.1.1.1 STP and RSTP Overview

This device can support both the STP protocol and the RSTP protocol and comply with the IEEE 802.1D and IEEE 802.1w standards.

The STP protocol is applied to avoid the broadcast storm generated in the link loop and provide the link redundant backup protocol.

For the layer 2 Ethernet, there is only one active channel between two LANs. Otherwise, the broadcast storm will be produced. However, it is necessary to set up the redundant link to improve the reliability of the LAN. Furthermore, some channels should be in the backup status, so that the redundant link will be upgraded to the active status if the network failure occurs and the other link fails. It is obviously hard to control this process by manual, while the STP protocol can complete this work automatically. It enables a device in LAN to:

- Discover and activate an optimal tree-type topology of the LAN.
- Detect the failure and then restore it, automatically update the network topology, so that the possible optimal tree-type structure can be selected at any time.

The topology of the LAN is calculated by a set of bridge configuration parameters automatically set by administrators. These parameters can be used to span an optimal topology tree. The optimal solution can be implemented only when it is configured appropriately.

The RSTP protocol is completely compatible with the 802.1D STP protocol downward. In addition to such function as the preventing of loops and the provisioning of redundant links like conventional STP protocol, its most critical feature is “quick”. If the bridge of one LAN supports the RSTP protocol and is configured by administrators appropriately, it will only take no more than 1 second to re-span the topology tree once the network topology changes (it takes about 50s for traditional STP protocol).

17.1.1.2 Bridge Protocol Data Units (BPDU):

To span a stable tree-type topology, it should depend on the elements below:

- The unique bridge ID of each bridge consists of the bridge priority and the MAC address.
- The bridge to root path cost is short for the Root Path Cost.
- Each port ID consists of the port priority and port number.

The information required to establish the optimal tree-type topology is obtained by the switching BPDU (Bridge Protocol Data Units) among bridges. These frames take the multicast address 01-80-C2-00-00-00 (hex) as the destination address.

Each BPDU is comprised of the following elements:

- Root Bridge ID (the root bridge ID this bridge considers)
- Root Path cost (the Root Path cost of this bridge).
- Bridge ID (the bridge ID of this bridge).
- Message age (the live time of the packet)
- Port ID (the port ID that the port sends this packet).
- The time parameters of the Forward-Delay Time, the Hello Time and the Max-Age Time protocol.
- Other flag bits, such as those represent to detect the change of the network topology and the status of this port.

When one port of the bridge receives the BPDU with higher priority (the smaller bridge ID and less root path cost), this information will be stored at this port. At the same time, it will update and promulgate this information for all ports. If the BPDU with lower priority is received, the bridge will discard this information.

This mechanism makes the information with higher priority be spreaded in the whole network, and the exchange of the BPDU will obtain the following results:

- One bridge is taken as the Root Bridge in the network.
- Each bridge other than the root bridge will present a Root Port. Namely, it will provide the port to the Root Bridge with the shortest path.
- Each bridge will calculate the shortest path to the Root Bridge.
- Each LAN will present the Designated Bridge, which lies in the shortest path between this LAN and the root bridge. The port for connecting the Designated Bridge and the LAN is referred to as the Designated port.
- The Root port and the Designated port enter the Forwarding status.
- Other ports that will not span the tress will be in the Discarding status.

17.1.1.3 Bridge ID

In accordance with the prescription of the IEEE 802.1W standard, each bridge should present unique Bridge ID, which will be taken as the standard to select the Root Bridge in the algorithm of the spanning tree. The Bridge ID consists of 8 bytes, where, the latter 6 bytes is the **mac** address of this bridge, while the first 2 bytes is shown as the table below. Of which, the first 4 bits denote the priority, while the last 8 bits denotes the System ID for the use of subsequent extending protocol.. This value is 0 in the RSTP, so the priority of the bridge should be configured as the multiple of 4096.

	Priority value				**System ID**											
Bits	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
Value	32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

17.1.1.4 Spanning-Tree Timers

The following description has an effect on three timers of the performance for the whole spanning-tree.

- Hello timer: The time interval for forwarding the BUDU packets periodically.
- Forward-Delay timer: The time interval for the change of the port status. The time interval when the port switches to the learning from the listening, or to the forwarding from the learning if the RSTP protocol runs in the compatible STP protocol mode.
- Max-Age timer: The longest time for the BPDU packets. Once it is timeout, the packets will be discarded.

17.1.1.5 Port Roles and Port States

Each port will play a Port Role in the network and be used to represent different acts in the network topology.

- Root port: The port that provides the shortest path to the Root Bridge.
- Designated port: The port by which each LAN is connected to the root bridge.
- Alternate port: The alternate port of the root port which will change into the root port once the root port fails.
- Backup port: The backup port of the Designated port. If two ports are connected to one LAN for the bridge, the port with higher priority is the Designated port, while that with lower priority is the Backup port.
- Disable port: The port that is not in the active status. Namely, the port whose operation state is down is assigned to this role.

The roles of various ports are shown in following Figure 17-1, Figure 17-2 and Figure 17-3 :

R = Root port D = Designated port A = Alternate port B = Backup port

Unless otherwise stated, the priority of the port will be lowered from left to right.

Figure 17-1

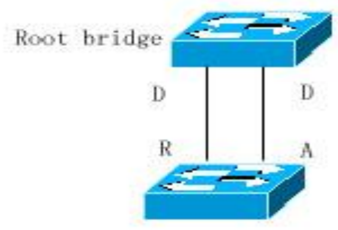


Figure 17-2

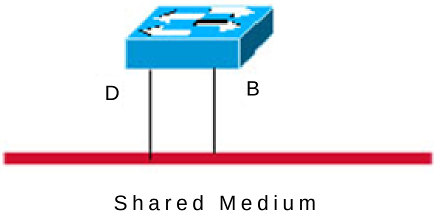
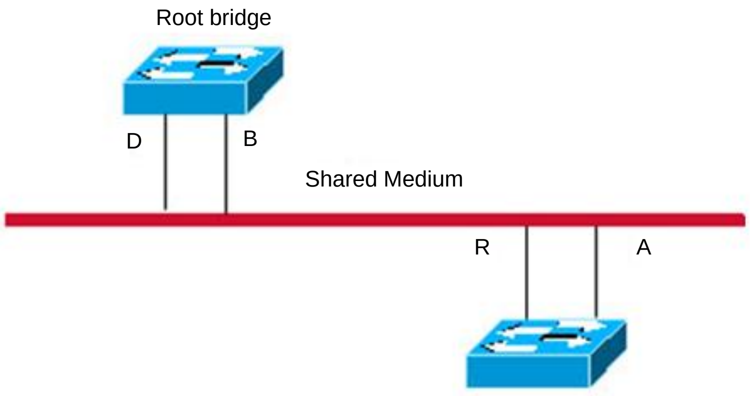


Figure 17-3



Each port takes three port states to indicate whether the data packet is forwarded, to control the topology of the whole spanning tree.

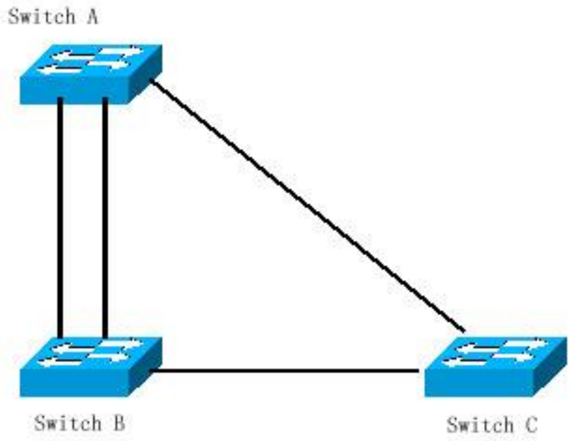
- Discarding: It will neither forward the received frame nor learn about the source Mac address.
- Learning: It will not forward the received frame, but learn about the source Mac address, so it is a transitional status.
- Forwarding: It will forward the received frame and learn about the source Mac address.

For the stable network topology, only the Root port and Designated port enter the Forwarding status, while other ports are only in the Discarding status.

17.1.1.6 Spanning of Network Topology Tree (Typical Application Solution)

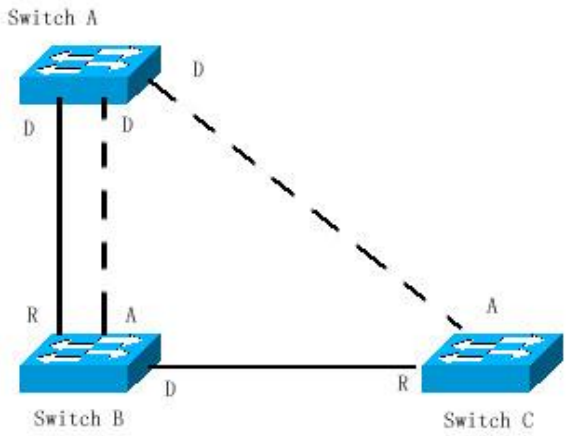
We now describe how the STP and RSTP protocol spans the mixed network topology to a tree-type structure. As is shown in Figure 17-4 below, the bridge IDs of the Switch A, B and C are assumed to be increasing. Namely, the Switch A presents the highest priority. There is the 1000M link between switch A and switch B, and the 100M link between the switch A and switch C, while it is the 10M link between switch B and switch C. The Switch A acts as the backbone switch of this network and implements the link redundancy for both Switch B and Switch C. Obviously, it will generat the broadcast storm if all these links are active.

Figure 17-4



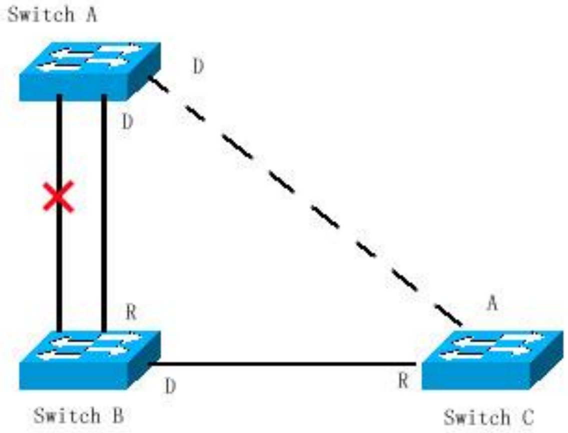
If all of three Switches enable the Spanning Tree protocol, they will select the root bridge as the Switch A by switching the BPDU. Once Switch B detects that two ports are connected to Switch A, it will select the port with the highest priority as the root port, while another one is selected as the Alternate port. While, Switch C detects that it can reach A in the B to A way or directly. However, the switch discovers that the Path cost in the B to A way is lower than that directly (For the Path cost corresponding to various paths, refer to table), so Switch C selects the port connected with B as the Root port, while selects that connected with A as the Alternate port. It will enter corresponding status of various ports to generate corresponding Figure 17-5 after the port roles are selected.

Figure 17-5



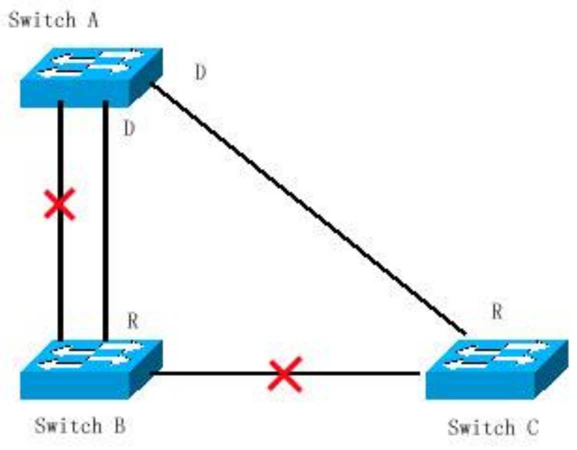
If the failure of the active path between Switch A and Switch B occurs, the backup link will take action immediately to generate corresponding Figure 17-6.

Figure 17-6



If the failure of the path between Switch B and Switch C occurs, the Switch C will switch the Alternate port to the Root port to generate the Figure 17-7.

Figure 17-7



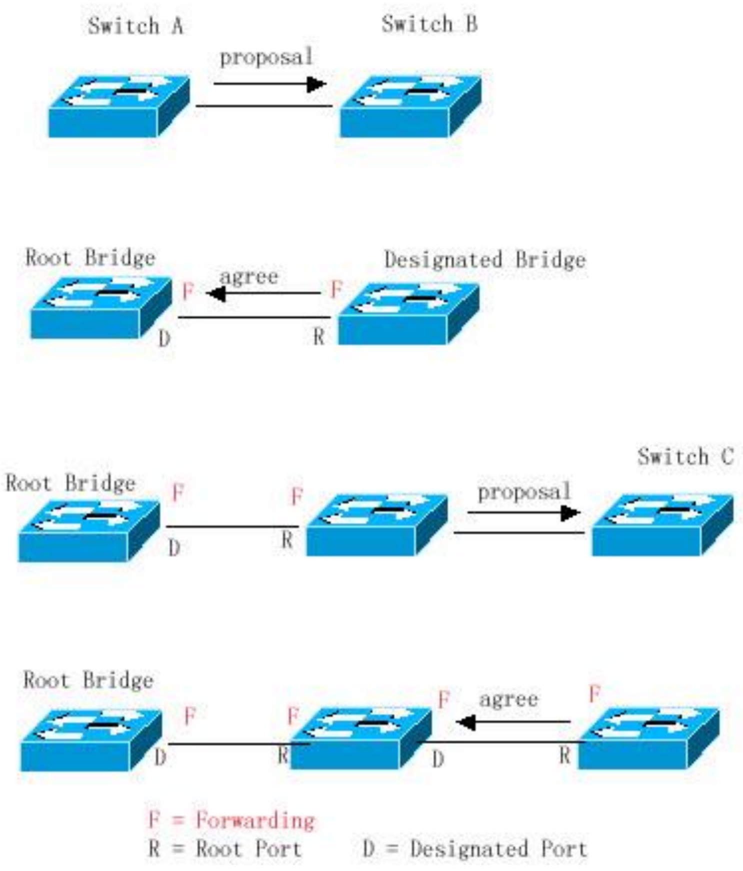
17.1.1.7 Quick Convergence of RSTP

We now introduce the special function of RSTP, which enables the “quick” forwarding of the port.

The STP protocol will carry out the forwarding after 30s since the port role is selected. Furthermore, the Root port and Designated port of each bridge will carry out the forwarding again after 30s, so it will take about 50s to stabilize the tree-type structure of the whole network topology.

The forwarding of the RSTP port is different. As is shown in Figure 17-8, the Switch A will send the “Proposa”l packet dedicated for the RSTP, the Switch B detects that the priority of Switch A is higher than itself, takes the Switch A as the root bridge and carries out the forwarding immediately after the port that receives the packet is the Root Port, and then sends the “Agree” packet to Switch A from Root Port. The Designated Port of Switch A is agreed and carries out the forwarding. Then, the Designated Port of Switch B sends the proposal message to deploy the spanning tree in turn. In theory, the RSTP can immediately restore the tree-type network structure to implement the quick convergence when the network topology changes.

Figure 17-8



Caution	Certain conditions must be met before the above "handshaking" process can take place, namely “Point-to-point Connect” must be used between ports. In order to maximize the power of you device, do not use non-point-to-point connection between devices.

Other than Figure 17-9, other schematics in this chapter are the point-to-point connection. The following lists the example figure of the Non point-to-point connection.

Example of Non Point-to-point Connection:

Figure 17-9

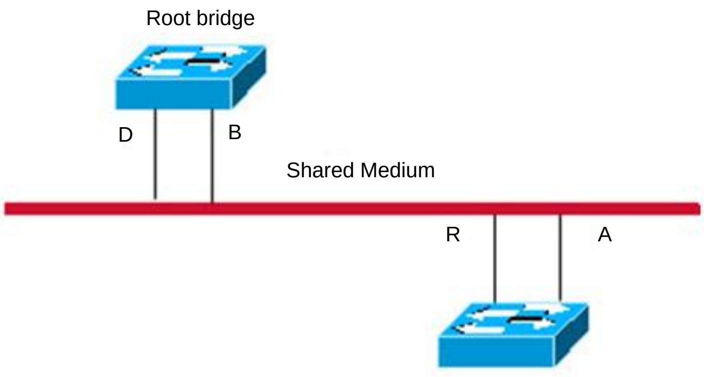
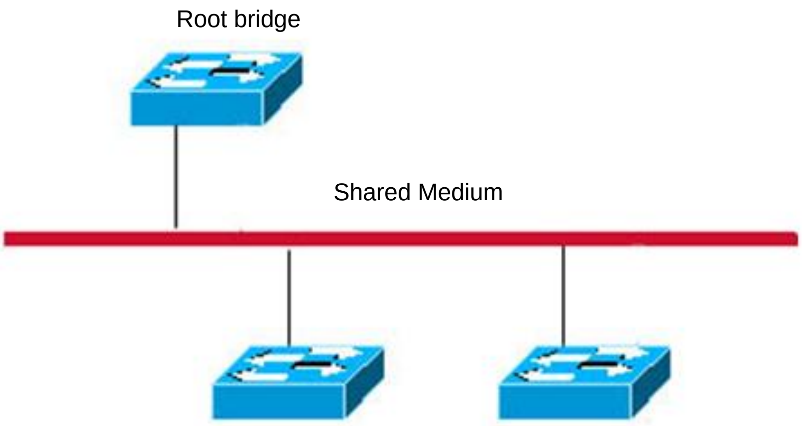
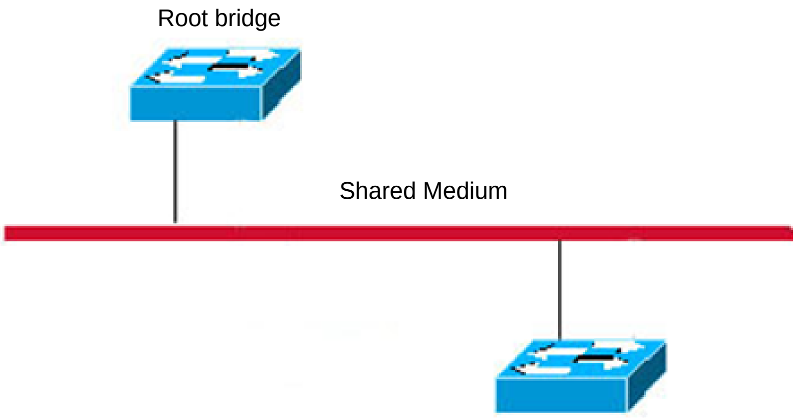


Figure 17-10



In addition, the following figure is a “point-to-point” connection and should be differentiated by users carefully.

Figure 17-11



17.1.1.8 Compatibility of RSTP and STP

The RSTP protocol is completely compatible with the STP protocol, and will automatically judge whether the bridge connected with supports the STP protocol or the RSTP protocol by the version number of received BPDU, It can only take the forwarding method of the STP to carry out the forwarding after 30s if it is connected with the STP bridges, so it can’t maximize the performance of the RSTP.

Furthermore, The mixture of the RSTP and the STP will suffer from the following problem. As is shown in Figure 17-12 the Switch A supports the RSTP protocol, while the Switch B only supports the STP protocol. What’s more, they are connected with each other, the Switch A will send the BPDU of the STP to be compatible with it once it detects that it is connected with the STP bridge. However, if it is replaced with the Switch C, which supports the RSTP protocol, but the Switch A still sends the BPDU of the STP, that causes the Switch C considers the STP is connected with itself. As a result, two RSTP-supported switches run by the STP protocol, which reduces the efficiency greatly.

For this reason, the RSTP protocol provides the protocol-migration function to send the RSTP BPDU forcibly. Once the Switch A sends the RSTP BPDU forcibly, the Switch C will detect the bridge connected with it supports the RSTP, so two devices can run by the RSTP protocol as shown in Figure 17-13.

Figure 17-12

Protocol Migration

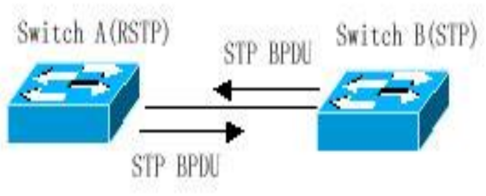
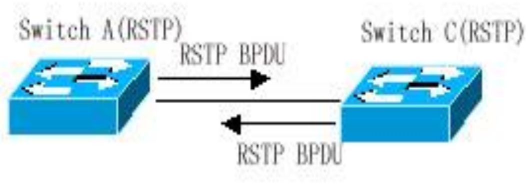


Figure 17-13



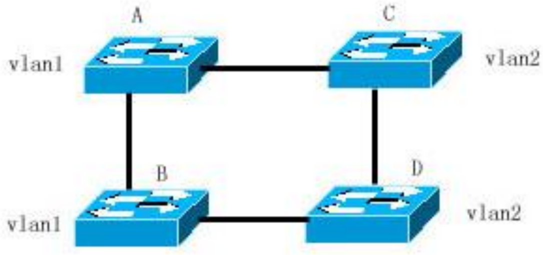
17.1.2 MSTP Overview

This device supports the MSTP, which is a new spanning-tree protocol derived from the traditional STP and RSTP and includes the quick FORWARDING mechanism of the RSTP itself.

For traditional spanning-tree protocol is not related to the VLAN, it will cause the following problem under specified network topology:

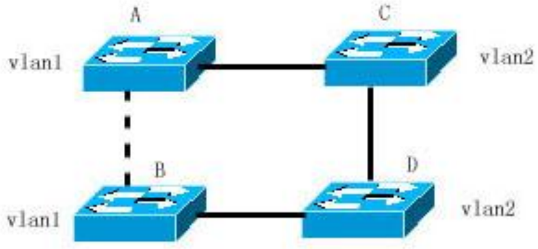
As shown in Figure 17-4, devices A and B are located in Vlan1, and devices C and D in Vlan2. They form a loop.

Figure 17-14



If the link from device A to devices C, D and B has a lower cost than the link from device A to device B, the link between devices A and B will be discarded (as shown in Figure 17-15). Packets in Vlan1 will not be forwarded because devices C and D do not contain Vlan1. This way, Vlan1 of device A cannot communicate with Vlan1 of device B.

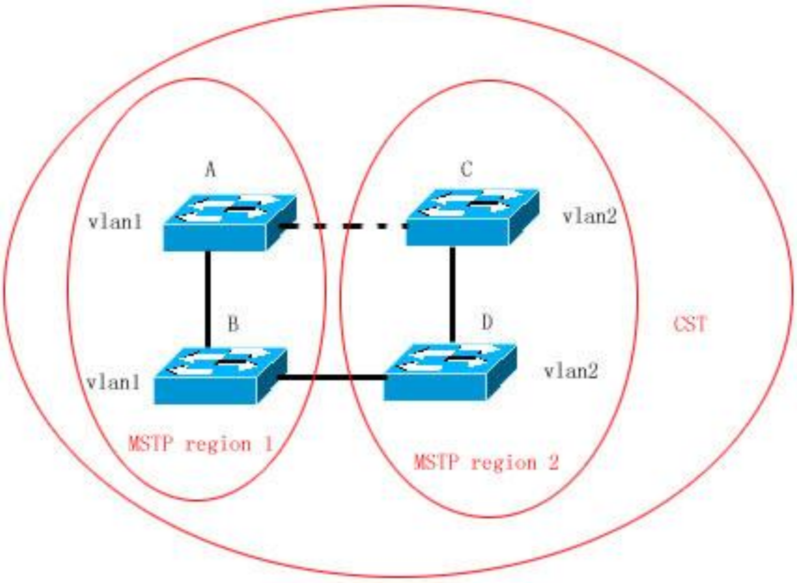
Figure 17-15



The MSTP is developed to solve this problem for it can partition one or more vlans of the switch into an Instance, so the switches with the same Instance configuration form a region (MST region) to run separate spanning tree (this internal spanning-tree is referred to as the IST). The combination of the MST region is equivalent to a large device, which executes the spanning tree algorithm with other MST region to obtain a common spanning tree, referred to as the common spanning tree (CST).

According to this algorithm, above network can form the topology as Figure 17-16: the devices A and B are within the MSTP Region 1 and no loop is produced in the MSTP Region 1, so there is no the path DISCARDING. Furthermore, it is the same in the MSTP Region 2 as that in the MSTP region 1. Then, the Region 1 and Region 2 are equivalent to two large devices respectively and there is no loop between them, so one path is discarded according to related configuration.

Figure 17-16



In this way, it prevents the form of loop and has no effect on the communication among the same vlans.

17.1.2.2 How to Partition MSTP region

According to above description, the MSTP Region should be partitioned rationally and the MST configuration information of the switch within the MSTP Region should be the same to make the MSTP play corresponding role.

The MST configuration information contains:

- MST configuration name (name): The string with up to 32 bytes is used to identify the MSTP Region.
- MST revision number: Use a modification value with 16 bits to identify the MSTP Region.
- MST instance-vlan table: Each device can create up to 64 Instances (id ranging from 1 to 64). Instance 0 always exists forcibly, so the system totally supports 65 instances. You can allocate 1-4094 Vlans for different Instances (0-64) as needed, and the unallocated vlans belong to instance 0 by default. In this way, each MSTI (MST instance) is a “Vlan group” and executes the spanning tree algorithm within the MSTI according to the MSTI information of the BPDU without the effect of the CIST and other MSTI.

You can use the global configuration command **spanning-tree mst configuration** to enter the MST configuration mode, so as to configure above information.

The MSTP BPDU carries above information. If the MST configuration information of the BPDU received by one device is the same as itself, it will consider that the device connects to this port is of the same MST Region as itself. Otherwise, it is considered to come from another Region.

We recommend you configure the corresponding table of the Instance-Vlan in the STP-closed mode, and then enable the MSTP to ensure the stability and convergence of the network topology.

17.1.2.3 Spanning Tree within MSTP region (IST)

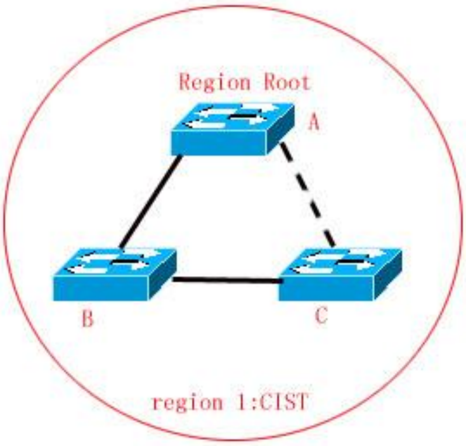
After the MSTP Region is partitioned, each Region will select separate root bridge of various instances and the port role of various ports for each device according to such parameters as the bridge priority and port priority. Finally, it will specify whether this port is FORWARDING or DISCARDING within this instance for the Port Role.

In this way, the IST (Internal Spanning Tree) is generated by the communication of the MSTP BPDU, and various Instances present separate spanning tree (MSTI). Where, the spanning tree corresponding to the Instance 0 is referred to as the CIST (Common Instance Spanning Tree). That is to say, each Instance provides each vlan group with a single network topology without loop.

As is shown in Figure below, the devices A, B and C form the loop within the region 1.

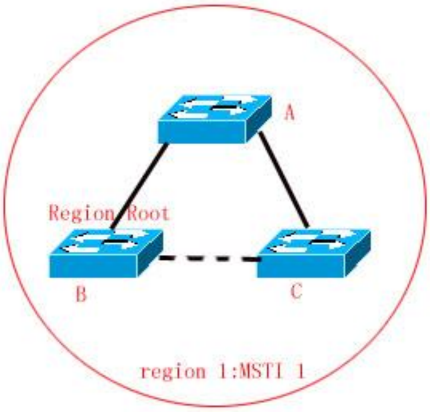
As is shown in Figure 17-17, device A with the highest priority is selected as the Region Root in the CIST (Instance 0). Then, the path between devices A and C are DISCARDING according to other parameters. Hence, for the vlan group of the Instance 0, only the path from switch A to B and device B to C is available, which breaks the loop of the vlan group.

Figure 17-17



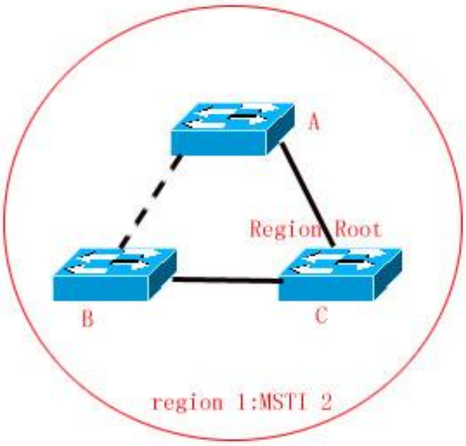
As is shown in Figure 17-18, switch B with the highest priority is selected as the Region Root in the MSTI 1 (Instance 1). Then, the link between switch B and C is DISCARDING according to other parameters. Hence, for the “Vlan group” of the instance 1, only the path from switch A to B and switch A to C is available, which breaks the loop of the “Vlan group”.

Figure 17-18



As is shown in Figure 17-19, switch C with the highest priority is selected as the Region Root in the MSTI 2 (Instance 2). Then, the link between switch A and B is DISCARDING according to other parameters. Hence, for the "Vlan group" of the instance 2, only the path from switch B to C and switch A to C is available, which breaks the loop of the "Vlan group".

Figure 17-19



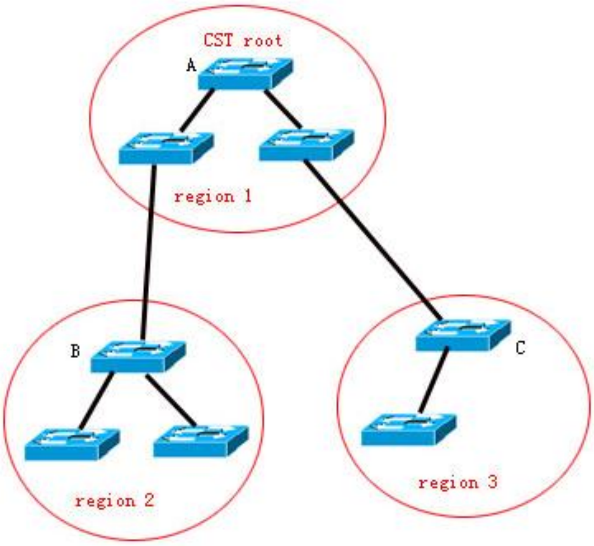
It's noted that the MSTP protocol doesn't concern with which Vlan the port is of, so users should configure corresponding Path cost and Priority for related port according to actual vlan configuration, to prevent the MSTP protocol from breaking the loop unexpected.

17.1.2.4 Spanning Tree between MSTP regions (CST)

For CST, each MSTP region is equivalent to a whole large-sized device, and different MSTP Regions also span a large-sized network topology tree, referred to as the CST (common spanning tree). As shown in Figure 17-20, for CST, device A with the smallest Bridge ID is selected as the root of the entire CST (CST Root) and the CIST Regional Root in this Region.

In Region 2, since Root Path Cost from device B to CST Root is the lowest one, device B is selected as the CIST Regional Root in this region. Similarly, device C is chosen as the CIST Regional Root in Region 3.

Figure 17-20



CIST Regional Root is not necessarily the device with the smallest Bridge ID in that region. It is the device in the region that has the lowest Root Path Cost to the CST Root.

At the same time, the Root Port of the CIST regional root takes a new Port Role for the MSTI, namely the "**Master port",** as the "outlet" of all instances, which is FORWARDING to all Instances. In order to make the topology more stable, we recommend each "outlet" for the Region to the CST root is only on one device of this Region as much as possible!

17.1.2.5 Hop Count

The IST and MSTI will not take the Message Age and Max Age to calculate whether the BPDU information is timeout, but the mechanism similar to the TTL of the IP message is used, namely the Hop Count.

You can set it by using the global configuration command **spanning-tree max-hops**. In the Region, starting from Region Root Bridge, Hop Count decreases by 1 every time when a device is passed until it is 0, which means the BPDU information is timeout. Devices discard BPDUs with the Hops value 0.

In order to be compatible with the STP and the RSTP, the MSTP still remains the message age and Max age mechanism.

17.1.2.6 Compatibility with MSTP, RSTP and STP Protocol

For the STP protocol, the MSTP will send the STP BPDU to be compatible with it like the RSTP. For detailed information, refer to the "*Compatibility of RSTP and STP*" section.

For the RSTP protocol, it will process the CIST part of the MSTP BPDU, so it is not necessary for the MSTP to send the RSTP BPDU to be compatible with it.

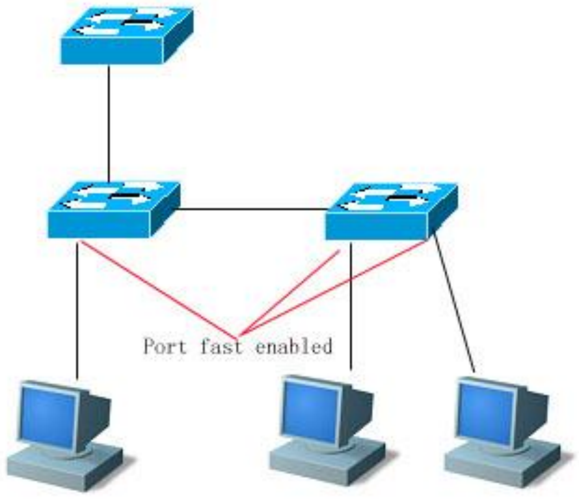
Each device that runs STP or RSTP is an independent Region, and does not form the same Region with any other device.

17.2 Overview of Optional Features of MSTP

17.2.1 Understanding Port Fast

If the port of the device is connected with the network terminal directly, this port can be set as the Port Fast and be Forwarding directly, by which to avoid the waiting process for the port to the Forwarding (If the port of the Port Fast is not configured, it needs to wait for 30s before the forwarding). The following figure indicates which ports of one device can be set as the Port Fast enabled.

Figure 17-21



If the BPDU is received from the port with the Port Fast set, its Port Fast Operational State is disabled. At this time, this port will execute the forwarding by normal STP algorithm.

17.2.2 Understanding BPDU Guard

The BPDU guard may be global enabled or execute enabled for single interface. There are some slightly difference between these two ways.

You can use the **spanning-tree portfast bpduguard default** command to enable the global BPDU guard enabled status in the privileged mode. In this status, if some interface opens the Port Fast and receives the BPDU, this port will enter the Error-disabled status to indicate the configuration error. At the same time, the whole port will be closed to show that some illegal users may add network devices in the network, which change the network topology.

You can also use the **spanning-tree bpduguard enable** command to open the BPDU guard of single interface in the interface configuration mode (it is not related to whether this port opens the Port Fast). Under this situation, it will enter the error-disabled status if this interface receives the BPDU.

17.2.3 Understanding BPDU Filter

The BPDU filter may be global enabled or enabled for single interface. There are some slightly difference between these two ways.

You can use the **spanning-tree portfast bpdufilter default** command to open the global BPDU filter enabled status in the privileged mode. In this status, the interface of the Port Fast enabled will not receive or transmit the BPDU, so the host that is connected with the Port Fast enabled ports directly will not receive the BPDU. If the interface of the Port Fast enabled makes the Port Fast operational status be disabled for it receives the BPDU, the BPDU filter will be failed automatically.

You can also use the **spanning-tree bpdufilter enable** command to set the BPDU filter enable of single interface in the interface configuration mode (it is not related to whether this port opens the Port Fast). Under this situation, this interface will not receive or transmit the BPDU, but execute the forwarding directly.

17.2.4 Understanding Tc-protection

Tc-protection can only be enabled or disabled globally. It is enabled by default.

When the corresponding function is enabled, only one delete operation is performed within a certain period of time (usually 4 seconds) following reception of TC-BPDU packet. At the same time, whether the TC-BPDU packets is received during this period of time is monitored. If TC-BPDU packets are received within this period of time, the device will perform one delete operation again when this period of time expires. This eliminates the need of frequently deleting MAC address entries and ARP entries.

17.2.5 Understanding TC Guard

The Tc-Protection function can ensure to reduce the dynamic MAC address and remove the ARP when the network produces a large number of tc packets. However, it will still produce much deletion operation when it suffers from the TC packets attack. Furthermore, the TC packet is spreaded and will have an effect on the whole network. We allow users to prohibit the spreading of the TC packet on the ports with the globally mode by using the TC Guard function. When one port receives the TC message, if the TC guard is configured globally or on a port, this port will shield the TC packet received or produced by this port, to prevent the TC packet spreading into other ports. In this way, it can effectively control the possible TC attack existed in the network, to ensure the stability of the network, especially on the L3 device. This function can avoid the interruption of the core routing caused by the vibration of the access layer device effectively.

17.2.6 Understanding BPDU Source MAC Check

The BPDU source MAC is checked in order to prevent malicious attack on the switch by sending BPDU packets manually to cause failure MSTP. When the switch of point-to-point connection to the remote is determined for a port, the BPDU source MAC check can be configured, so that only BPDU frames from the remote switch are received, while all other BPDU frames are discarded, preventing malicious attacks. You can configure corresponding MAC addresses for BPDU source MAC check for a specific port in the interface mode. Only one filtered MAC is allowed for one port. BPDU source MAC check can be disabled by using no bpdu src-mac-check, when the port does not receive any BPDU frame.

17.2.7 Understanding Illegal Length Filtering for BPDU

When the Ethernet length field of BPDU exceeds 1500, this BPDU frame is discarded in order to avoid receiving illegal BPDU packets.

17.2.8 Understanding Automatic Identification of Edge Ports

If the specified port doesn’t receive the BPDU sent by the downstream within a certain period of time (3 s), it will be considered that this port is connected with one network device, and this port will be set as the edge port to enter the Forwarding status directly. The port automatically identified as the edge port will be identified as the non edge port for it receives the BPDU automatically.

You can cancel the automatic identification function of the edge port by the **spanning-tree autoedge disabled** command.

This function is enabled by default.

Caution

When the automatic identification function of the edge port conflicts with the manual Port Fast, it will take the manual configuration as the standard.

This function will take action when the specified port and the downstream port carry out the quick negotiation forwarding, so the STP protocol doesn't support this function. At the same time, if the specified port is in the forwarding status, the configuration of the Autoedge for this port will not be valid. It will take effect during the quick re-negotiation, such as plug /unplug network cable.

If the port enables the BPUD Filter firstly, this port will carry out the Forwarding directly, but not be identified as the edge port automatically.

This function is only applicable for the specified port.

17.3 Configuring MSTP

17.3.1 Default Configuration of Spanning Tree

The following lists the default configuration of the Spanning Tree.

Item	Default value
Enable State	Disable, the STP is disabled.
STP MODE	MSTP
STP Priority	32768
STP port Priority	128
STP port cost	Automatically judged according to the port rate .
Hello Time	2 seconds
Forward-delay Time	15 seconds
Max-age Time	20 seconds
Default calculation method of the Path Cost	Long integer type
Tx-Hold-Count	3
Link-type	Automatically determined by the dual status of the port .
Maximum hop count	20
Corresponding relationship between vlan and instance	All VLANs belong to instance 0 Only instance 0 exists

You can restore the Spanning Tree parameter to its default configuration (not including disabled Span) by using the **spanning-tree reset** command.

17.3.2 Enable and Disable Spanning Tree Protocol

Once the Spanning-tree protocol is enabled, the device starts to run the spanning-tree protocol. By default, this device runs MSTP.

The Spanning-tree protocol is disabled on the device by default.

In the privileged mode, perform these steps to open the Spanning Tree protocol:

Command	Function
DGS-3610# **configure terminal**	Enter the global configuration mode.
DGS-3610(config)# **spanning-tree**	Enable the Spanning tree protocol.
DGS-3610(config)# **end**	Return to the privileged mode.
DGS-3610# **show spanning-tree**	Check the configuration entities.
DGS-3610# **copy running-config startup-config**	Save the configuration.

If you disable the Spanning Tree protocol, use the global configuration command **no spanning-tree** to set.

17.3.3 Configuring Mode of Spanning Tree

According to the 802.1-related protocol standard, it is not necessary for administrators to set much for three versions of Spanning Tree protocols such as the STP, RSTP and MSTP, and various versions will be compatible with one another naturally. However, considering that some manufacturers will not develop according to the standard completely, it may cause some compatibility problem. Hence, we provide a command configuration to facilitate administrators to switch to the lower version of the Spanning Tree mode and be compatible with it when they detects that this device is not compatible with that of other manufacturers.

Note: When you switch the MSTP mode to the RSTP or STP mode, all information related to MSTP Region will be cleared.

The default mode of the device is MSTP.

In the privileged mode, perform these steps to open the Spanning Tree protocol:

Command	Function
DGS-3610# **configure terminal**	Enter the global configuration mode.
DGS-3610(config)# **spanning-tree mode mstp/rstp/stp**	Switch the Spanning Tree mode.
DGS-3610(config)# **end**	Return to the privileged EXEC mode.
DGS-3610# **show spanning-tree**	Check the configuration entries.

Command	Function
DGS-3610# **copy running-config startup-config**	Save the configuration.

If you want to restore the default mode of the Spanning Tree protocol, use the global configuration command **no spanning-tree mode** to set.

17.3.4 Configuring Switch Priority

The setting of the device priority concerns with which device is the root of the whole network, as well as the topology of the whole network. It is recommended that administrators set the core device with higher priority (smaller value), which will facilitate the stability of the whole network. You can assign different device priorities for different instances, by which various instances can run separate spanning tree protocol. Only the priority of CIST (Instance 0) is related to the devices between different regions.

As mentioned in Bridge ID, there are 16 values for the priority, and all of them are multiples of 4096, which are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. The default value is 32768.

In the privileged mode, perform these steps to configure the device priority:

Command	Function
DGS-3610# **configure terminal**	Enter the global configuration mode.
DGS-3610(config)# **spanning-tree** [**mst** *instance-id*] **priority** *priority*	For the configuration of the device priority for different instances, it will configure the instance 0 if you don’t add the instance parameters. *instance-id*, whose range is 0-64. *priority*, whose value range is 0 – 61440 and is increasing by the integral multiple of 4096, 32768 by default.
DGS-3610(config)# **end**	Return to the privileged EXEC mode.
DGS-3610# **show running-config**	Check the configuration entries.
DGS-3610# **copy running-config startup-config**	Save the configuration.

If you want to restore the default value, use the global configuration command **no spanning-tree mst** *instance-id* **priority** to set.

17.3.5 Configuring Port Priority

When two ports are connected to the shared medium, the device will select one port with the higher priority (smaller value) to enter the forwarding status, and one with lower priority (greater value) to enter the discarding status. If two ports possess the same priority, the port with smaller port number will enter the forwarding status. You can assign different port priorities for different instances on one port, by which each instance can run separate spanning tree protocol.

Same as the device priority, it has 16 values, all a multiple of 16. They are 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240 respectively. The default value is 128.

In the privileged mode, perform these steps to configure the port priority:

Command	Function
DGS-3610# **configure terminal**	Enter the global configuration mode.
DGS-3610(config)# **interface** *interface-id*	Enter he configuration mode of this interface, the legal interface contains the physical port and the Aggregate Link.
DGS-3610(config-if)# **spanning-tree** [**mst** *instance-id*] **port-priority** *priority*	For the configuration of the port priority for different instances, it will configure the instance 0 if you don't add the instance parameters. instance-id, whose range is 0-64. priority, configure the priority of this interface and its value range is 0 – 240. Furthermore, it is increasing by the integral multiple of 16, 128 by default.
DGS-3610(config-if)# **end**	Return to the privileged mode.
DGS-3610# **show spanning-tree** [**mst** *instance-id*] **interface** *interface-id*	Check the configuration entries.
DGS-3610# **copy running-config startup-config**	Save the configuration.

If you want to restore to the default value, use the interface configuration command **no spanning-tree mst** *instance-id* **port-priority** to set.

17.3.6 Configuring Path Cost of the Port

Setting of Port Path Cost is related to the root port of the device because the device selects the root port with the smallest sum of Path Cost of the port to the root bridge. Its default value is calculated by The Media Speed of the interface automatically. The higher the media speed, the smaller the cost is. It is not necessary to be changed unless required by administrators especially, so the path cost calculated in this way is most scientific. You can assign different cost paths for different instances on one port, by which every instance can run independent spanning tree protocol.

In the privileged mode, perform these steps to configure the port path cost:

Command	Function
DGS-3610# **configure terminal**	Enter the global configuration mode.
DGS-3610(config)# **interface** *interface-id*	Enter the configuration mode of this interface, the legal interface contains the physical port and the Aggregate Link.
DGS-3610(config-if)# **spanning-tree** [**mst** *instance-id*] **cost** *cost*	For the configuration of the port priority for different instances, it will configure the instance 0 if you don't add the instance parameters. instance-id, whose range is 0-64. *cost*, Configure the cost for this port, whose value ranges is 1-200,000,000. The default value is calculated by the media rate of the interface automatically.
DGS-3610(config-if)# **end**	Return to the privileged EXEC mode.
DGS-3610# **show spanning-tree** [**mst** *instance-id*] **interface** *interface-id*	Check the configuration entities.
DGS-3610# **copy running-config startup-config**	Save the configuration.

If you want to restore to the default value, use the interface configuration command **no spanning-tree mst** *cost* to set.

17.3.7 Configuring Default Calculation Method of Path Cost (path cost method)

When this port Path Cost is the default value, the device will calculate the path cost of this port by the port rate. However, the IEEE 802.1d and the IEEE 802.1t specify different path cost values for the same media rate respectively. Where, the value range of the 802.1d is the short integer (1-65535), while the value range of the 802.1t is the long integer (1-200,000,000). Administrators should unify the path cost standard of the whole network. The default mode is the long integer (IEEE 802.1t Mode).

The following lists the path cost set for different media rate in two ways automatically.

Port Rate	Interface	IEEE 802.1d (short)	IEEE 802.1t (long)
10M	Common Port	100	2000000
	Aggregate Link	95	1900000
100M	Common Port	19	200000
	Aggregate Link	18	190000

Port Rate	Interface	IEEE 802.1d (short)	IEEE 802.1t (long)
1000M	Common Port	4	20000
	Aggregate Link	3	19000

In the privileged mode, perform these steps to configure the default calculation method of the port path cost:

Command	Function
DGS-3610# **configure terminal**	Enter the global configuration mode.
DGS-3610(config)# **spanning-tree pathcost method long**/**short**	Configure the default calculation method of the port path cost. The setting value is the long integer (long) or short integer (short), the long integer (long) by default.
DGS-3610(config)# **end**	Return to the privileged EXEC mode.
DGS-3610# **show running-config**	Check the configuration entries.
DGS-3610# **copy running-config startup-config**	Save the configuration.

If you want to restore to the default value, use the global configuration command **no spanning-tree pathcost method** to set.

17.3.8 Configuring Hello Time

Configure the time interval of sending the BPDU packets by device. The default value is 2s.

In the privilege mode, perform these steps to configure the Hello Time:

Command	Function
DGS-3610# **configure terminal**	Enter the global configuration mode.
DGS-3610(config)# **spanning-tree hello-time** *seconds*	Configure the hello_time, whose value range is 1-10s, 2s by default.
DGS-3610(config)# **end**	Return to the privileged mode.
DGS-3610# **show running-config**	Check the configuration entries.
DGS-3610# **copy running-config startup-config**	Save the configuration.

If you want to restore to the default value, use the global configuration command no spanning-tree hello-time to set.

17.3.9 Configuring Forward-Delay Time

Configure the time interval the port status changes. The default value is 15s.

In the privilege mode, perform these steps to configure the Forward-Delay Time:

Command	Function
DGS-3610# **configure terminal**	Enter the global configuration mode.
DGS-3610(config)# **spanning-tree forward-time** *seconds*	Configure the forward delay time, whose value range is 4-30s, 15s by default.
DGS-3610(config)# **end**	Return to the privileged EXEC mode.
DGS-3610# **show running-config**	Check the configuration entries.
DGS-3610# **copy running-config startup-config**	Save the configuration.

If you want to restore to the default value, use the global configuration command **no spanning-tree forward-time** to set.

17.3.10 Configuring Max-Age Time

Configure the longest time for the BPDU packets to be alive. The default value is 20s.

In the privilege mode, perform these steps to configure the Max-Age Time:

Command	Function
DGS-3610# **configure terminal**	Enter the global configuration mode.
DGS-3610(config)# **spanning-tree max-age** *seconds*	Configure the max age time, whose value range is 6-40s, 20s by default.
DGS-3610(config)# **end**	Return to the privileged EXEC mode.
DGS-3610# **show running-config**	Check the configuration entries.
DGS-3610# **copy running-config startup-config**	Save the configuration.

If you want to restore to the default value, use the global configuration command **no spanning-tree max-age** .

⚠ **Caution**

Each of Hello Time, Forward-Delay Time and Max-Age Time has a value range. There is constraint relationship among them, that is: 2*(Hello Time + 1.0 seconds) <= Max-Age Time <= 2*(Forward-Delay – 1.0 second). The configured three parameters should meet above condition. Otherwise, it may cause the topology instability.

17.3.11 Configuring Tx-Hold-Count

Configure the maximum count of the BPDU sent per second, 3 by default.

In the privileged mode, perform these steps to configure the Tx-Hold-Count:

Command	Function
DGS-3610# **configure terminal**	Enter the global configuration mode.
DGS-3610(config)# **spanning-tree tx-hold-count** *numbers*	Configure the maximum count of the BPDU sent per second, whose value range is 1-10, 3 by default.
DGS-3610(config)# **end**	Return to the privileged EXEC mode.
DGS-3610# **show running-config**	Check the configuration entries.
DGS-3610# **copy running-config startup-config**	Save the configuration.

If you want to restore to the default value, use the global configuration command **no spanning-tree tx-hold-count** to set.

17.3.12 Configuring Link-type

Configure whether the link-type of this port is the point-to-point connection, which concerns with whether the RSTP can be converged quickly. Refer to "*Fast Convergence of RSTP*". If you don't set this value, the device will set it according to the dual status of the port automatically, the full duplex port will set the link type as the **point-to-point,** while the half duplex is set as the **shared**. You can forcibly set the **link type** to determine whether the link of the port is the point-to-point connection.

In the privileged mode, perform these steps to configure the link type of the port:

Command	Function
DGS-3610# **configure terminal**	Enter the global configuration mode.
DGS-3610(config)# **interface** *interface-id*	Enter the interface configuration mode.
DGS-3610(config-if)# **spanning-tree link-type point-to-point**/**shared**	Configure the link type of the interface. The default value is to judge whether it is the point-to-point connection according to the duplex status of the port. The full duplex is the point-to-point connection, namely it can be quick FORWARDING.
DGS-3610(config-if)# **end**	Return to the privileged EXEC mode.
DGS-3610# **show running-config**	Check the configuration entries.
DGS-3610# **copy running-config startup-config**	Save the configuration.

If you want to restore to the default value, use the interface configuration command **no spanning-tree link-type** to set.

17.3.13 Configuring Protocol Migration Processing

This setting is to enable this port to execute the version check forcibly. For related description, refer to the *Compatibility of RSTP and STP*.

Command	Function
DGS-3610# **clear spanning-tree detected-protocols**	Forcibly check versions of all the ports
DGS-3610# **clear spanning-tree detected-protocols interface** *interface-id*	Execute the version check forcibly to a specific port.

17.3.14 Configuring MSTP Region

To have several devices in the same MSTP Region, you have to give these devices the same name, the same revision number, and the same Instance-Vlan table.

You can configure the vlans included in instances 0-64. The remaining vlans will be automatically allocated to instance 0. One vlan can only be of an instance.

We recommend you configure the corresponding table of the instance-vlan in the STP-closed mode, and then open the MSTP to ensure the stability and convergence of the network topology.

In the privileged mode, perform these steps to configure the MSTP region:

Command	Function
DGS-3610# **configure terminal**	Enter the global configuration mode.
DGS-3610(config)# **spanning-tree mst configuration**	Enter the MST configuration mode.
DGS-3610(config-mst)# **instance** *instance-id* **vlan** *vlan-range*	Add the vlan group to a MST instance *instance-id*, whose range is 0-64. *vlan-range,* whose range is 1-4094. For instance: The instance 1 vlan 2-200 is to add the vlan 2-200 to the instance 1. The instance 1 vlan 2,20,200 is to add the vlan 2-200 to the instance 1. In this way, you can use the **no** command to delete the vlan from the instance, and the deleted vlan will be

Command	Function
	transferred to the instance 0 automatically.
DGS-3610(config-mst)# **name** *name*	Specify the MST configuration name, this string can present up to 32 bytes.
DGS-3610(config-mst)# **revision** *version*	Specify the MST revision number, whose range is 0-65535. The default value is 0.
DGS-3610(config-mst)# **show**	Check the MST configuration entries.
DGS-3610(config-mst)# **end**	Return to the privileged EXEC mode.
DGS-3610# **copy running-config startup-config**	Save the configuration.

To restore the default MST Region Configuration, you can use the global configuration command **no spanning-tree mst configuration**. You can use the **no instance** *instance-id* to delete this instance. In this way, the **no name** and **no revision** can be used to restore the MST name and MST revision number to the default value respectively.

The following is the example of configuration:

```
DGS-3610(config)# spanning-tree mst configuration
DGS-3610(config-mst)# instance 1 vlan 10-20
DGS-3610(config-mst)# name region1
DGS-3610(config-mst)# revision 1
DGS-3610(config-mst)# show
Multi spanning tree protocol : Enable Name [region1]
Revision 1
Instance Vlans Mapped
-------- --------------------
0 1-9,21-4094
1 10-20
-------------------------------
DGS-3610(config-mst)# exit
DGS-3610(config)#
```

17.3.15 Configuring Maximum-Hop Count

Configure the Maximum-Hop Count to specify how many devices the BPDU within a region will pass through before it is discarded. It is valid for all instances.

In the privileged mode, perform these steps to configure the Maximum-Hop Count:

Command	Function
DGS-3610# **configure terminal**	Enter the global configuration mode.
DGS-3610(config)# **spanning-tree max-hops** *hop-count*	Configure the Maximum-Hop Count, whose range is 1-40, 20 by default.
DGS-3610(config)# **end**	Return to the privileged EXEC mode.

Command	Function
DGS-3610# **show running-config**	Check the configuration entries.
DGS-3610# **copy running-config startup-config**	Save the configuration.

If you want to restore to the default value, use the global configuration command **no spanning-tree max-hops** to set.

17.4 Configuring Optional Features of MSTP

17.4.1 Default Setting of Optional Features for Spanning Tree

All the optional features are disabled by default.

17.4.2 Enabling Port Fast

This port will execute the forwarding directly after the Port Fast is enabled. However, the Port Fast Operational State will be disabled because of the received BPDU. It can participate in the STP algorithm and execute the forwarding normally.

In the privileged mode, perform these steps to configure the **Port Fast**:

Command	Function
DGS-3610# **configure terminal**	Enter the global configuration mode.
DGS-3610(config)# **interface** *interface-id*	Enter the configuration mode of this interface, the legal interface contains the physical port and the Aggregate Link.
DGS-3610(config-if)# **spanning-tree portfast**	Enable the portfast of this interface.
DGS-3610(config-if)# **end**	Return to the privileged EXEC mode.
DGS-3610# **show spanning-tree interface** *interface-id* **portfast**	Check the configuration entries.
DGS-3610# **copy running-config startup-config**	Save the configuration.

If you want to close the Port Fast, use the **spanning-tree portfast disable** command to set in the interface configuration mode.

You can use the global configuration command **spanning-tree portfast default** to enable the portfast of all ports.

17.4.3 Enabling BPDU Guard

If the BPDU is received from this port, the enabled BPDU guard will enter the error-disabled status.

In the privileged mode, perform these steps to configure the BPDU guard:

Command	**Function**
DGS-3610# **configure terminal**	Enter the global configuration mode.
DGS-3610(config)# **spanning-tree portfast** **Bpduguard default**	Open the BPDU guard globally.
DGS-3610(config)# **interface** *interface-id*	Enter the configuration mode of this interface, the legal interface contains the physical port and the Aggregate Link.
DGS-3610(config-if)# **spanning-tree portfast**	Enable the portfast of this interface.
DGS-3610(config-if)# **end**	Return to the privileged EXEC mode.
DGS-3610# **show running-config**	Check the configuration entries.
DGS-3610# **copy running-config startup-config**	Save the configuration.

If you want to close the BPDU guard, use the global configuration command **no spanning-tree portfast bpduguard default** to set.

If you want to enable the BPDU guard for single interface, use the interface configuration command **spanning-tree bpduguard enable** to set, and use the **spanning-tree bpduguard disable** to close the BPDU guard.

17.4.4 Enabling BPDU Filter

Corresponding port will not be transmitted or receive the BPDU after the BPDU filter is enabled.

In the privilege mode, perform these steps to configure the BPDU Filter for the port:

Command	**Function**
DGS-3610# **configure terminal**	Enter the global configuration mode.
DGS-3610(config)# **spanning-tree portfast bpdufilter default**	Enable the BPDU filter globally.
DGS-3610(config)# **interface** *Interface-id*	Enter he configuration mode of this interface, the legal interface contains the physical port and the Aggregate Link.

Command	Function
DGS-3610(config-if)# **spanning-tree portfast**	Enable the portfast of this interface.
DGS-3610(config-if)# **end**	Return to the privileged EXEC mode.
DGS-3610# **show running-config**	Check the configuration entries.
DGS-3610# **copy running-config startup-config**	Save the configuration.

If you want to close the BPDU filter, use the global configuration command **no spanning-tree portfast bpdufilter default** to set.

If you want to open the BPDU filter for single interface, use the interface configuration command **spanning-tree bpdufilter enable** to set, and use the **spanning-tree bpdufilter disable** to disable the BPDU guard.

17.4.5 Enabling Tc_Protection

In the privileged mode, perform these steps to configure tc_protection:

Command	Function
DGS-3610# **configure terminal**	Enter the global configuration mode.
DGS-3610(config)# **spanning-tree tc-protection**	Enable tc-protection
DGS-3610(config)# **end**	Return to the privileged EXEC mode.
DGS-3610# **show running-config**	Check the configuration entries.
DGS-3610# **copy running-config startup-config**	Save the configuration.

To disable Tc_Protection, use the global configuration command **no spanning-tree tc-protection**.

17.4.6 Enabling TC Guard

It will enter the privilege mode and configure the global TC Guard according to the following steps.

Command	Function
DGS-3610# **configure terminal**	Enter the global configuration mode.
DGS-3610(config)# **spanning-tree tc-protection tc-guard**	Enable the global TC Guard.
DGS-3610(config)# **end**	Return to the privilege mode.

Command	Function
DGS-3610# **show running-config**	Check the configuration entities.
DGS-3610# **copy running-config startup-config**	Save the configuration.

It will enter the privilege mode and configure the TC Guard on the port according to the following steps

Command	Function
DGS-3610# **configure terminal**	Enter the global configuration mode.
DGS-3610(config)# **interface** *Interface-id*	Enter the configuration mode of this interface, and the legal interface includes the physical port and the Aggregate Link.
DGS-3610(config-if)# **spanning-tree tc-guard**	Enable the TC Guard of this interface.
DGS-3610(config-if)# **end**	Return to the privilege mode.
DGS-3610# **show running-config**	Check the configuration entities.
DGS-3610# **copy running-config startup-config**	Save the configuration.

17.4.7 Enabling the BPDU source MAC check

After the BPDU source MAC check is enabled, the switch accepts only the BPDU frames whose source MAC addresses are the specified MAC, and filters all the received other BPDU frames.

Enter the interface mode and perform the steps below to configure the BPDU source MAC check:

Command	Function
DGS-3610# **configure terminal**	Enter the global configuration mode.
DGS-3610(config)# **interface** *Interface-id*	Enter the configuration mode of this interface, and the legal interface includes the physical port and the Aggregate Link.
DGS-3610(config-if)#**bpdu src-mac-check** *H.H.H*	Enable the BPDU source MAC check
DGS-3610(config-if)# **end**	Return to the privilege mode.
DGS-3610# **show running-config**	Check the configuration entities.

Command	Function
DGS-3610# **copy running-config startup-config**	Save the configuration.

To disable the BPDU source MAC check, run **no bpdu src-mac-check** in the interface mode.

17.4.8 Disabling the Automatic Identification of Edge Ports

If a specified port has not received the BPDU in a certain time (3 seconds), the port is automatically recognized as an edge port. However, the Port Fast Operational State may be disabled due to the receiving if BPDU. This function is enabled by default.
In the privileged mode, you can set Autoedge by performing the following steps:

Command	Function
DGS-3610# **configure terminal**	Enter the global configuration mode.
DGS-3610(config)# **interface** *Interface-id*	Enter the configuration mode of this interface, and the legal interface includes the physical port and the Aggregate Link.
DGS-3610(config-if)# **spanning-tree autoedge**	Enable the autoedge of this interface.
DGS-3610(config-if)# **end**	Return to the privilege mode.
DGS-3610# **show spanning-tree interface** *interface-id*	Check the configuration entities.
DGS-3610# **copy running-config startup-config**	Save the configuration.

If you want to disable the Autoedge, use the **spanning-tree autoedge disabled** command to set in the interface configuration mode.

17.5 Showing MSTP Configuration and Status

MSTP provides the following show commands for viewing configuration information and runtime information. Functions of each command are depicted below:

Command	Meaning
DGS-3610# **show spanning-tree**	Show parameter information of MSTP and topology information of the spanning tree

Command	**Meaning**
DGS-3610# **show spanning-tree summary**	Show the each instance information and the forwarding status information of this port of MSTP
DGS-3610# **show spanning-tree mst configuration**	Show the configuration information of the MST domain.
DGS-3610# **show spanning-tree mst** *instance-id*	Show the MSTP information of this instance.
DGS-3610# **show spanning-tree mst** *instance-id* **interface** *interface-id*	Show the MSTP information of corresponding instance for specified interface.
DGS-3610# **show spanning-tree interface** *interface-id*	Show the MSTP information of all instances for specified interface.
DGS-3610# **show spanning-tree forward-time**	Show forward-time
DGS-3610# **show spanning-tree Hello time**	Show Hello time
DGS-3610# **show spanning-tree max-hops**	Show max-hops
DGS-3610# **show spanning-tree tx-hold-count**	Show tx-hold-count
DGS-3610# **show spanning-tree pathcost method**	Show pathcost method

18 SPAN Configuration

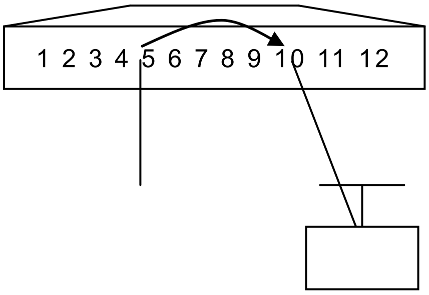
18.1 Overview

18.1.1 Understanding SPAN

You can copy the packets from one port to another port connected with a network analysis device or RMON analyzer by using the SPAN to analyze the communication on the port. The SPAN mirrors all the packets sent/received at a port to a physical port for analysis.

For example, all the frames on Gigabit port 5 are mirrored to Gigabit port 10, as shown in Figure 18-1. Although the network analyzer connected to port 10 is not directly connected to port 5, it can receive all the frames at port 5.

Figure 18-1 SPAN Configuration Example



Notwork Analyzer

Through the SPAN, you can monitor all the frames incoming/outgoing the source port, including the route input frames.

The SPAN does not affect the normal packet switching of the switch, except that it only copies the frames incoming/outgoing the source port to the destination port. However, a destination port with excessive traffic volume, for example, when one 100Mbps destination port monitors a 1000Mbps port, may cause frames to be dropped.

18.1.2 Precautions

- On DGS-3610 series products, enable the port mirroring. If the mirroring source port is configured with the tx direction and allowing the enabled mirroring destination port to switch, send a packet from the mirroring destination port, this packet will be forwarded to the mirroring source port. However, at this moment it couldn't be mirrored to the mirroring destination port (that is to say that the tx direction is not effective configured on the mirroring source port).

- For DGS-3610 series, SPAN supports the enabled mirroring destination port and allows the switching function.

18.2 SPAN Concepts and Terms

This section describes the concepts and terms related to SPAN configuration.

18.2.1 SPAN Session

One SPAN session is the combination of one destination port and source port. You can monitor the input, output, and bi-directional frames of single or multiple interfaces.

You can only configure one SPAN sessions. Switched port, routed port and AP can be configured as source port and destination port. The SPAN session does not affect the normal operation of the switch.

You can configure the SPAN session on one disabled port, but the SPAN does not take effect until you enable the destination and source ports. The **Show monitor session** *session number* command shows the operation status of the SPAN session. One SPAN session does not take effect immediately after power-on, but until the destination port becomes operable.

18.2.2 Frame Type

The SPAN session includes the following frame types:

- **Received frames**

Each received frame is copied to the destination port. In one SPAN session, you can monitor the input frames of one or multiple source ports. The inputted frames from the source port may be discarded due to some reasons, for example, port security, but this does not affect the function of the SPAN, and the frames are still sent to the destination port.

- **Transmitted frames**

All transmitted frames from the source port will be copied to the destination port. In one SPAN session, you can monitor the input frames of one or multiple source ports. The inputted frames to the source port from other ports may be discarded due to some reasons, This frame couldn't be sent to the destination port..The format of frames sent to the source port may be changed. For example, the frame pass through routing output from the source port, the source MAC of the frame, destination MAC, VLAN ID and TTL will be changed. Similarly, the format of the frame copied to the destination port may be changed.

- **Bi-directional frames**

It includes the two types of frames mentioned above. In one SPAN session, you can monitor the input and output frames of one or multiple source ports.

18.2.3 Source Port

The source port (also known as the monitored interface) is a switched port, routed port or AP. This port is monitored for network analysis. In the single SPAN session, you can monitor input, output and bi-directional frames. There is no restriction for the maximum number of the source ports.

A source port has the following features:

- It can be a switched port, routed port or AP.
- It cannot be a destination port at the same time.
- It can specify the input/output directions of the monitored frames.
- The source port and destination port can reside on the same VLAN or different VLANs.

18.2.4 Destination Port

The SPAN session has a destination port (also known as the monitoring port), which is used to receive the frame copies from the source port.

The destination port has the following features:

- It can be a Switched Port or Routed Port.
- When the SPAN session is activated, the destination port does not participate in the STP.

18.2.5 SPAN Traffic

You can use the SPAN to monitor all network communications, including multicast frames and BPDU frames.

18.2.6 Interfaces between the SPAN and Other Functions

The SPAN interacts with the following functions.

Spanning Tree Protocol (STP) — the destination port of SPAN participates in the STP.

18.2.7 Configuring SPAN

This section describes how to configure the SPAN on your switch, covering:

18.2.7.1 Configuring SPAN

Function	Default Configuration
SPAN status	Disabled

18.2.8 SPAN Configuration Guide

Please follow the rules below when configure the SPAN.

- The network analyzer should be connected to the monitoring interface.

The destination port can not be source port, and the source port can not be destination port.

You can configure one disabled port as a destination port or source port, but the SPAN function does not take effect until the destination port and source port have been enabled again.

The **no monitor session** *session_number* global configuration command allows you to delete the source or destination port from the SPAN session.

The SPAN destination port does not participate in the STP .

The destination port of SPAN participants STP.

When the SPAN is enabled, the configuration change has the following result.

- If you change the VLAN configuration of the source port, the configuration takes effect immediately.
- If you change the VLAN configuration of the destination port, the configuration takes effect immediately.
- If you have disabled the source port or destination port, the SPAN does not take effect.
- If you add one source or destination port to an AP, the configuration will cause the source port or destination port of the SPAN to be disappeared.

18.2.9 Creating a SPAN Session and Specifying the Monitoring Port and Monitored Port

Specify a SPAN session and the destination port (monitoring port0 and the source port (monitored port).

Command	Function
DGS-3610(config)# **monitor session** *session_number* **source interface** *interface-id* [,| -] {**both** | **rx** | **tx**}	Specify the source port. For *session_number*, specify the session number 1-128. For *interface-id*, specify the appropriate interface ID.
DGS-3610(config)# **monitor session** *session_number* **destination interface** *interface-id* {**switch**}	Specify the source port. For *session_number*, specify the session number 1-128. For *interface-id*, specify the appropriate interface ID. Adding the parameter **switch** will support the switching function of mirror destination port.

To delete the SPAN session, use the **no monitor session** *session_number* global configuration command. To delete the SPAN session, use the **no monitor session all** global configuration command. You can use the **no monitor session** *session_number* **source interface** *interface-id* global configuration command or the **no monitor session** *session_number* **destination interface** *interface-id* command to delete the source port or destination port.

The following example shows how to create one SPAN session: session 1. First, clear the configuration of the currently session 1, and then set to mirror the frames of port 1 to port 8. The **Show monitor session** privileged command allows you to verify your configuration.

```
DGS-3610(config)# no monitor session 1
DGS-3610(config)# monitor session 1 source interface gigabitEthernet 3/1 both
DGS-3610(config)# monitor session 1 destination interface gigabitEthernet 3/8
DGS-3610(config)# end
DGS-3610# show monitor session 1
sess-num: 1
src-intf:
GigabitEthernet 3/1 frame-type Both
dest-intf:
GigabitEthernet 3/8
```

18.2.10 Deleting a Port from the SPAN Session

Delete a port from a SPAN session:

Command	Function
DGS-3610(config)# **no monitor session** *session_number* **source interface** *interface-id* [,| -] [**both** | **rx** | **tx**]	Specify the deleted source port to . For *session_number 1-128*, specify the session number. For *interface-id*, specify the appropriate interface ID.

You can use the **no monitor session** *session_number* **source interface** *interface-id* global configuration command to delete the source port from a SPAN session. The following example shows how to delete port 1 from session 1 and verify your configuration.

```
DGS-3610(config)# no monitor session 1 source interface gigabitethernet 1/1 both
DGS-3610(config)# end
DGS-3610# show monitor session 1
sess-num: 1
dest-intf:
GigabitEthernet 3/8
```

18.3 Showing the SPAN Status

The show monitor privileged command allows you to show the current SPAN status. The following example illustrates how to show the current status of SPAN session 1 by using the **show monitor** privileged command.

```
DGS-3610# show monitor session 1
sess-num: 1
src-intf:
GigabitEthernet 3/1 frame-type Both
dest-intf:
GigabitEthernet 3/8
```

19 IP Address and Service Configuration

19.1 IP Addressing Configuration

19.1.1 IP Address Overview

IP address is made up of 32 binary bits and expressed in dotted decimal format for the convenience of writing and describing. When expressed in decimal format, the 32 binary bits are broken into four octets (1 octet = 8 bits). Each octet is separated by a period (dot)”. “in range from 0 to 255 (for example, 192.168.1.1). When the decimal format is used, the address is divided into four groups, each with 8 bits ranging 0~255. The groups are separated by ".". For example, "192.168.1.1" is an IP address in the decimal format.

An IP address is an address used to uniquely identify the inter-connection address on IP layer. The IP uses a 32-bit address field and divides into two parts: 1) network part; 2) local address part. The IP addresses in use can be divided into four categories according to the value in the first several bits of the network portion.

Category A, the highest-order bit is set to 0, has 7 bit denotes the network number, and 24 bit denotes the local address. .There are total 128 networks of category A .

			8 16 24 32
A type network	0	Network ID	Host ID

Category B, the two highest-order bits are set to “10”, has 14 bit denotes network number and 16 bit denotes the local address. .Thus, there are total 16,384 networks of category B .

			8	16 24 32
B type network	0	1	Network ID	Host ID

Category C, the three highest-order bits are set to “110”, has 22 bit denotes network number and 8 bit denotes the local address. .Thus, there are total 2,097,152 networks of category C

				8 16 24	32
C type network	1	1	0	Network ID	Host ID

For category D, the four highest-order bits are set to “1110”, other bits are used as multicast addresses.

					8 16 24 32
D type network	1	1	1	0	Multicast address

Note

No addresses are allowed with the four highest-order bits set to “1111”. These addresses, called "category E"-type addresses, are reserved.

During the period of network construction and IP address planning, it is essential to make IP address allocation according to network property. If you expect to connect your network to public network, turn to management office to apply for correct IP address allocation. In the region of China, you can put forward the application to China Internet Network Information Center (CNNIC). The highest organization is the Internet Corporation for Assigned Names and Numbers (ICANN) that is responsible for IP address allocation. If the network which is under constructed will be used as an internal private network, you do not need to apply for the IP address. It is better to assign special private network address instead of IP address assignment at random.

The following table lists these addresses which are reserved and available.

Class	Address Range	Status
Category A network	0.0.0.0	Reserved
	1.0.0.0~126.0.0.0	Available
	127.0.0.0	Reserved
Category B network	128.0.0.0~191.254.0.0	Available
	191.255.0.0	Reserved
Category C network	192.0.0.0	Reserved
	192.0.1.0~223.255.254.0	Available
	223.255.255.0	Reserved
Category D network	224.0.0.0~239.255.255.255	Available
Category E network	240.0.0.0~255.255.255.254	Reserved
	255.255.255.255	Multicast

There are three blocks of the IP address space reserved for private networks. These addresses are not used for the internet. In order to connect the private networks to Internet, It’s required to convert these private IP addresses to valid internet IP addresses. The private network addresses spaces are listed in the following table, which is defined in RFC 1918.

Class	IP Address Range	Network Numbers
Category A network	10.0.0.0~10.255.255.255	1 Category A networks
Category B network	172.16.0.0~172.31.255.255	16 Category B networks
Category C network	192.168.0.0~192.168.255.255	256 Category C networks

For the description of IP address, TCP/UDP port and other network number, please refer to document RFC 1166.

19.1.2 IP Address Configuration Task List

IP addressing configuration task list includes the following tasks, but only the first one is required. For others, they are optional to be executed according to the actual network requirement.

- Configuration of IP Addresses to the Interfaces (Required)
- Configuration of Address Resolution Protocol (ARP) (Optional)
- Configuration of IP address mapping to WAN Address (Optional)
- Disabling IP Routing (Optional)
- Configuration of Broadcast Packets Processing (Optional)

19.1.2.1 Configuration of IP Addresses to the Interfaces

Only if configured an IP address, the device is able to receive and send IP datagram. If an interface is configured IP address, it means that IP protocol is running on this interface.

To assign an IP address to a network interface, use the following command in interface configuration mode:

Command	Function
DGS-3610(config-if)# **ip address** *ip-address mask*	Set an IP address for an interface.
DGS-3610(config-if)# **no ip address**	Cancel the IP address configuration of an interface.

A mask is a 32-bit number, which helps you know which portion of the address identifies the network. For network masks, any address bits which have corresponding mask bits set to 1 represent the network ID, any address bits that have corresponding mask bits set to 0 represent the host ID. For example, the masks of Category A network is “255.0.0.0”. You can perform the subnet partition to a network by using network masks. The subnet partition is to take some of the bits from the host address as the part of subnetwork, it can reduce hosts capacity of the host and increase the number of networks. For this reason, the network masks are called subnet masks.

Note

Theoretically, bits of subnet masks can be any bits of the host addresses. Our product only supports continuous subnet masks from left to right which is started from network portion.

For the feature configuration related to the interface IP address, refer to the following tasks list. These tasks are taken as optional configuration and you can determine whether they are need to be configured according to the practical requirement.

- Configuring Multiple IP Addresses to the Interfaces

19.1.2.1.1 Configuring Multiple IP Addresses to the Interfaces

Our product supports multiple IP addresses configured on one interface. One of them is the primary IP address and others are secondary addresses. The secondary IP addresses can be theoretically configured to be unlimited, which can be configured freely. But between the secondary IP addresses and the primary IP, among the secondary IP addresses, the addresses must located in different networks. Secondary IP address is used frequently during the period of network building. For the following cases, it is considered that secondary IP address could be used.

- There might not be enough host addresses for a network. For example, a generally LAN needs a Category C network, which allows up to 254 hosts. However, when there are more than 254 hosts in the LAN, another category C network address is necessary since one category C network is not enough. Therefore, the router should be connected to two networks and multiple IP addresses should be configured.
- Many older networks were built using Level 2 bridges, and were not subnetted. The use of secondary addresses can make it easier to upgrade the network to a router-based network of IP layer. One IP address is configured in the equipment for each subnet.
- Two subnets of a single network might be separated by another network. You can create a subnets for the isolated network. By configuring secondary IP addresses, the separated subnets can be re-connected. Note that a subnet cannot be appeared on two or more than two interfaces in the router.

Note

Before configuring secondary IP addresses, you need to confirm that the primary IP address has been configured. If the secondary IP address is configured for a router in the network, the secondary IP address for the same network must be configured for other routers. If other devices have not been configured an IP address yet, you can configure the primary IP address for them.

To configure the secondary IP addresses to a network interface, use the following command in interface configuration mode:

Command	Function
DGS-3610(config-if)# **ip address** *ip-address mask* **secondary**	Set secondary IP addresses to an interface.

Command	**Function**
DGS-3610(config-if)# **no ip address** *ip-address* *mask* **secondary**	Cancel the configuration of the secondary IP addresses on an interface.

19.1.2.2 Configuration of Address Resolution Protocol (ARP)

For each IP network device in a LAN, it uses two addresses including local address and network address. 1) Local address is contained in the header of data link frame. Disputably, the correct term is "data link layer address". Since this local address is processed in the MAC sub-layer of data link layer, it is normally called MAC address, which represents IP network device in the LAN. 2) Network address represents the IP network devices in the Internet, and denotes the network which this device belongs to at the same time.

To implement the inter-communication with two IP devices on the LAN, it’s needed to know the 48-bits MAC address of the destination host. The procedure of acquiring the MAC address according to the IP address is called Address Resolution Protocol (ARP). There are two ways of address resolution: 1) Address Resolution Protocol (ARP); 2) Proxy Address Resolution Protocol (Proxy ARP). About the description of ARP, Proxy ARP and RARP, refer to RFC 826, RFC 1027, RFC 903.

ARP is used to bind together the IP and MAC Address. By an input of an IP address, ARP is able to locate the associated MAC address. Once the MAC address is known, the corresponding relationship between the IP address and the MAC address will be saved in the ARP buffer in the equipment. Based on the MAC address, IP devices can encapsulate the frame of data link layer and send the frame to the LAN. By default, IP and ARP encapsulations are the type of Ethernet II. However the frames can also be encapsulated into other types of Ethernet frame (for example, SNAP).

The principle of RARP is similar to ARP. With the input of an MAC address, RARP obtains the the associated IP address. RARP is configured on non-disks workstation in general.

Usually, you do not need to configure address resolution protocols on the router except the case in particular . Our product can manage the address resolution procedure by performing the following tasks.

- Configuring ARP Statically
- Setting ARP Encapsulations
- Setting ARP Timeout

19.1.2.2.1 Configuring ARP Statically

ARP provides the function of dynamic mapping from IP address to MAC address. It is not necessary to configure ARP statically in most cases. By Configuring ARP Statically, our product can respond to the ARP request which is not belonged to its own IP address.

To configure static ARP, execute the following command at global configuration mode:

Command	**Function**
DGS-3610(config)# **arp** *ip-address mac-address arp-type*	Define static ARP. where, arp-type can only support the arpa type currently.
DGS-3610(config)# **no arp** *ip-address*	Cancel the static ARP

19**.1.2.2.1 Setting ARP Encapsulations**

So far DGS-3610 series only supports ARP Ethernet II type for ARP encapsulations. It is also expressed as the ARPA keyword in our produt.

19**.1.2.2.1 ARP Timeout Setting**

ARP timeout setting only affects the address mapping from IP address to MAC address which is learned dynamically. The shorter the timeout, the truer the mapping table saved in the ARP cache, but the more network bandwidth occupied by the ARP. Hence the advantages and disadvantages should be weighted. Generally it is not necessary to configure the ARP timeout unless there is a special requirement.

To configure ARP timeout, execute the following command at interface configuration mode:

Command	**Function**
DGS-3610(config-if)# **arp timeout** *seconds*	Configure the ARP timeout with the range 0-2147483, where, 0 indicates it is not aged.
DGS-3610(config-if)# **no arp timeout**	Restore to default configuration

By default, timeout is 3600 seconds, that is, 1 hour.

19.1.2.3 Disabling IP Routing

IP routing function is enabled by default. Unless it is ensured that IP routing is not needed, you do not need to perform this command. Disabling IP routing will make the equipment lose all the routes and disables the route forwarding function.

To disable IP routing, use the following commands at global configuration mode:

Command	**Function**
DGS-3610(config)# **no ip routing**	Disable IP routing function.
DGS-3610(config)# **ip routing**	Enable IP routing function.

19.1.2.4 Broadcast Packets Processing Configuration

A broadcast packet is a data packet destined for all hosts on a particular physical network. Our product supports two kinds of broadcast packets: directed broadcasting and flooding broadcasting. A directed broadcast is a packet sent to all the hosts of a specific network and destination address of host part are all set to 1. While a flooded broadcast packet is sent to every network and 32-bits destination address are all set to 1. Broadcast packets are heavily used by some IP protocols, including very important Internet protocols. Therefore, how to control and use the broadcast packets is the basicl responsibility of a network administrator.

If IP network devices forward flooding broadcasts, it maybe cause a serious network overload to lead to the severity impact for the running of networks. This case is called broadcast storm. The router provides some protection to limit the broadcast storms within the local network so as to prevent the expending of thebroadcast storms. Due to the bridges and switches are located on Layer 2 network devices, they will forward and spread the broadcast storms.

The best solution to the broadcast storm problem is to specify a single broadcast address on each network, that is, directed broadcast, which requires IP protocols to use directed broadcast instead of flooding broadcast if possible.

For detailed description about broadcasting, please refer to RFC 919 and RFC 922.

How to process the broadcast packets, perform the following tasks according to the network requirement.

- Enabling Directed Network Broadcast to Physical Broadcast Translation
- Creating an IP Broadcast Address

19.1.2.4.1 Enabling Directed Broadcast to Physical Broadcast Translation

An IP directed broadcast packet refers to an IP packet of the IP subnet broadcast address. For instance, the packet with destination address 172.16.16.255 is a directed broadcast packet. However, the node that generates this packet is not a member of the destination subnet.

When the router without direct connection to destination subnet received the IP directed broadcast packet, it will process the directed broadcast packet like forwarding unicast packet. After the directed broadcast packet reaches a device that is directly connected to this subnet, the device converts the directed broadcast packet into a flooding broadcast packet (typically the broadcast packet whose destination IP address is all “1”), and then sends the packet to all the hosts in the destination subnet in the manner of link layer broadcast.

You can enable the translation function of the directed broadcasts to the physical broadcast on the specified interface. so that this interface can forward to the directed broadcasts within the directly-connected network. This command will only affect the final transmission of the directed broadcasts which arrived at the final destination subnet, while other directed broadcasts packets will be forwarded normally.

You can define an access list to control which directed broadcasts are forwarded on an interface. When an access list is defined, only those data packets permitted by the access list are eligible to be translated from directed broadcasts to physical broadcasts.

To configure the Directed Broadcast to Physical Broadcast translation, use the following command in interface configuration mode:

Command	Function
DGS-3610(config-if)# **ip directed-broadcast** [*access-list-number*]	Enable directed broadcast to physical broadcast translation on an interface.
DGS-3610(config-if)# **no ip directed-broadcast**	Cancel the translation

19.1.2.4.2 Creating an IP Broadcast Address

Currently, the destination address of the most popular broadcasts packets is an address consisting of all “1”, denotes as 255.255.255.255. Our product can defince to generate other broadcast packets of other address and receive all-type broadcast packets.

To set a different IP broadcast address other than 255.255.255.255, execute the following command in interface configuration mode:

Command	Function
DGS-3610(config-if)# **ip broadcast-address** *ip-address*	Create a new broadcast address
DGS-3610(config-if)# **no ip broadcast-address**	Cancel a new broadcast address

19.1.3 Monitoring and Maintaining IP Address

To monitor and maintain your network, perform the tasks described in the following sections.

- Clearing the information of Caches and Tables
- Displaying System and Network Status

19.1.3.1 Clearing the Information of Caches and Tables

You can remove all contents of a particular cache, table, or database, including following g three aspects: 1) Clearing ARP cache; 2) Clearing the mapping table from hostname to IP address; 3) Clearing the routing tables.

Command	**Function**
DGS-3610# **clear arp-cache**	Clear the ARP cache.
DGS-3610# **clear ip route** {*network* [*mask*] | *}	Clearing IP Routing Table

19.1.3.2 Displaying System and Network Status

You can show the contents of the IP routing table, cache, and database. Such information is very helpful in troubleshooting the network. You also can display the information about reachability of local equipment network and discover the routing path that the packets of your device are taking through the network.

Execute the following commands in privileged mode to display system and network statistics:

Command	**Function**
DGS-3610# **show arp**	Display the ARP table.
DGS-3610# **show ip arp**	Display the IP ARP cache.
DGS-3610# **show ip interface** [*interface-type interface-number*]	Show the interface IP information.
DGS-3610# **show ip route** [*network* [*mask*]]	Display the routing table
DGS-3610#**show ip route**	Display the current state of the routing table in summary form.
DGS-3610# **ping** *ip-address* [**length** *bytes*] [**ntimes** *times*] [**timeout** *seconds*]	Test network node reachability.

19.1.4 IP Addressing Configuration Examples

This chapter provides some IP address configuration examples as follows:

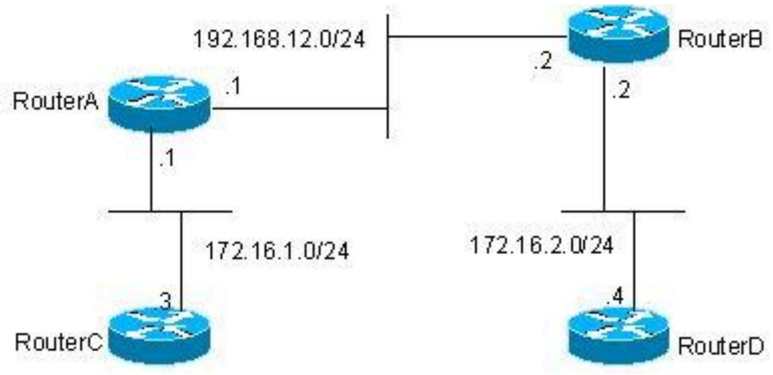
- □ Secondary IP Addressing Configuration Example

19.1.4.1 Secondary IP Address Configuration Example

- **Configuration requirements:**

The IP addresses allocation and network connections as shown in the following Figure 19-1.

Figure 19-1 Secondary IP address configuration example



It is required to configure RIP routing protocol, but the version can only be set as RIPv1, and display the routes of 172.16.2.0/24 on router C, and display routes of 172.16.1.0/24 on router D.

- **Detailed Configuration of the Routers:**

RIPv1 does not support none-category routes, which means masks are not carried in routing notification. The two subnets of 172.16.1.0/24 and 172.16.2.0/24 within the same network are separated by categoty C 192.168.12.0/2. Therefore router C and router D can not learn the detailed network information from each other according to the usual configuration. Based on the feature of RIP, if interface network and received route are located in the same network, the route must be set the same network mask to the interface network. Therefore you can configure the router A and router B to create a secondary network 172.16.3.0/24 on network 192.168.12.0/24, so as to re-connect these two separated subnets. It only describes the configuration of router A and router B as follow.

Configuration of Router A:

```
interface FastEthernet 0/0
ip address 172.16.3.1 255.255.255.0 secondary
ip address 192.168.12.1 255.255.255.0
!
interface FastEthernet 0/1
ip address 172.16.1.1 255.255.255.0
!
router rip
network 172.16.0.0
network 192.168.12.0
```

Configuration of Router B:

```
interface FastEthernet 0/0
ip address 172.16.3.2 255.255.255.0 secondary
ip address 192.168.12.2 255.255.255.0
!
interface FastEthernet 0/1
ip address 172.16.2.1 255.255.255.0
!
```

```
router rip
network 172.16.0.0
network 192.168.12.0
```

19.2 IP Service Configuration

19.2.1 IP Services Configuration Task List

IP service configuration includes the following tasks which are all optional. You can perform IP connection management according to the actual requirement.

19.2.2 IP ConnectionsManagement

The IP protocols stack offers lot of of services to control and manage IP connections. Internet Control Message Protocol (ICMP) provides many of these services. When there is any problem with the network, the router or access server will send an ICMP message to the host or other routers. For detailed information on ICMP, see RFC 792.

To manage various aspects of IP connections, perform the optional tasks described in the following sections:

- Enabling ICMP Protocol Unreachable Messages
- Enabling ICMP Redirect Messages
- Enabling ICMP Mask Reply Messages
- Setting the IP MTU
- Configuring IP Source Routing

19.2.2.1 Enabling ICMP Protocol Unreachable Messages

When the device receives a non-broadcast packet that the destination is itself, and this packet uses the IP protocol that the router cannot process, the router will send an ICMP protocol unreachable message to the source address. Similarly, if the router is unable to forward the packet because it knows of no route to the destination address, it sends an ICMP host unreachable message. This feature is enabled by default.

To re-enable this ICMP protocol unreachable message, use the following command in interface configuration mode:

Command	Function
DGS-3610(config-if)# **ip unreachables**	Enable the ICMP protocol unreachable and host unreachable messages.
DGS-3610(config-if)# **no ip unreachables**	Disable the ICMP protocol unreachable and host unreachable messages.

19.2.2.2 Enabling ICMP Redirect Messages

Routes are sometimes less than optimal it is possible for the device to be forced to resend a packet through the same interface on which it was received. If the router resends a packet through the same interface on which it was received, it sends an ICMP redirect message to the data resource to inform the data resource that the gateway reached to this destination address is another router in the same subnet. Therefore the data resource will transmit the packets based on the optimized path afterwards. This feature is enabled by default.

To enable the ICMP redirect messages execute the following command in interface configuration mode:

Command	Function
DGS-3610(config-if)# **ip redirects**	Enable the sending of ICMP redirect messages. It is enabled by default.
DGS-3610(config-if)# **no ip redirects**	Disable the sending of ICMP redirect messages.

19.2.2.3 Enabling ICMP Mask Reply Messages

Occasionally, network devices need to know the subnet mask for a particular subnetwork in the Internet. To obtain this information, such devices can send ICMP mask request messages. ICMP mask reply messages are sent in reply from devices that received the requested information. Our product can respond to ICMP mask request messages. This function is enabled by default.

To enable ICMP mask reply messages, use the following command in interface configuration mode:

Command	Function
DGS-3610(config-if)# **ip mask-reply**	Enable the mask reply messages.
DGS-3610(config-if)# **no ip mask-reply**	Disable the mask reply messages.

19.2.2.4 Setting the IP MTU

All interfaces have a default MTU (Maximum Transmission Unit) value. All the packets which are larger than the MTU have to be fragmented before sending. Otherwise it is unable to be forwarded on the interface.

Our product allows you to adjust the MTU on an interface. Changing the MTU value can affect the IP MTU value, and the IP MTU value will be modified automatically to match the new MTU. However, if ajust the value of the IP MTU, the MTU of the interface will not change with it..

Also, all device interfaces on a physical network must keep coherence with the MTU value for the same protocol.

To set the IP MTU value, use the following command in interface configuration mode:

Command	**Function**
DGS-3610(config-if)# **ip mtu** *bytes*	Set the MTU value with the range 68~1500.
DGS-3610(config-if)# **no ip mtu**	Restore the default setting

19.2.2.5 Configuring IP Source Routing

Our product supports IP source routing. When the router receives the IP dato packets, it will check the Strict Source Route, Loose Source Route and Record Route of the IP header. These options are described in RFC 791. If one of these options enabled in this data packet, it performs the appropriate reply action. If it detects a packet with an invalid option, an ICMP parameter problem message will be sent to the source of the packet and discards the packet. Our product supports IP source routing by default.

To enable IP source routing, execute the following command in interface configuration mode:

Command	**Function**
DGS-3610(config)# **ip source-route**	Enable IP source routing
DGS-3610(config)# **no ip source-route**	Disable IP surce routing

20 DHCP Configuration

20.1 Introduction to DHCP

DHCP (Dynamic Host Configuration Protocol), detailed in RFC 2131, provides configuration parameters for hosts over the Internet. DHCP is based on Client/Server working mode. The DHCP server assigns IP addresses for the hosts to be configured dynamically and provides host configuration parameters.

DHCP assigns IP address in three ways:

1. Assign automatically. The DHCP server assigns permanent IP addresses to the clients;
2. Assign dynamically. The DHCP server assigns IP addresses that will expire after a period of time to the clients (or the clients can release the addresses by themselves);
3. Configure manually. Network administrators specify IP addresses for the clients. Administrators can use DHCP to send a specified IP address to the client.

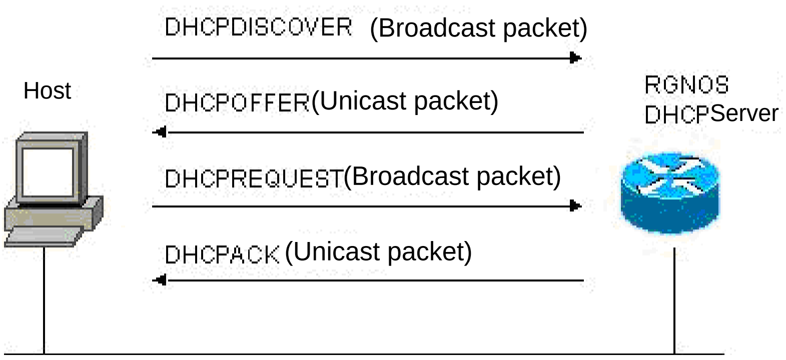
Among the three methods mentioned above, only dynamic assignment allows reuse of address that the client does not need any more.

The format of DHCP message is based on that of BOOTP (Bootstrap Protocol) message. hence, it is necessary for the device to be able to act as the BOOTP relay agent and interact with the BOOTP client and the DHCP server. The function of BOOTP relay agent eliminates the need of deploying a DHCP server in every physical network. DHCP is detailed in RFC 951 and RFC 1542.

20.2 Introduction to DHCP Server

The DHCP server of our company is implemented in strict accordance with RFC 2131. It is used to assign and manage IP addresses for the hosts. The basic flow of DHCP working is shown in Figure 20-1.

Figure 20-1


DHCPDISCOVER (Broadcast packet)
Host
DHCPOFFER(Unicast packet)
RGNOS
DHCPServer
DHCPREQUEST(Broadcast packet)
DHCPACK (Unicast packet)

Process of DHCP requesting an IP address:

1. The host sends a DHCPDISCOVER broadcast packet to locate a DHCP server in the network;
2. The DHCP server sends a DHCPOFFER unicast packet to the host, including IP address, MAC address, domain name and address lease period;
3. The host sends a DHCPREQUEST broadcast packet to formally request the server to assign the provided IP address;
4. The DHCP server sends a DHCPACK unicast packet to the host to confirm the request of the host.

Note

The DHCP client may receive DHCPOFFER packets from multiple DHCP servers, and accept any DHCPOFFER packet. However, the client usually accepts the first received DHCPOFFER packet only. The address specified in DHCPOFFER from the DHCP server is not necessarily the finally assigned address. Generally, the DHCP server reserves this address until the client sends a formal request.

A broadcast packet is used to formally request the DHCP server to assign an address, so that all the DHCP servers that send DHCPOFFER packets also receives this packet and release the IP address that is offered to the clients.

If the DHCPOFFER packet sent to the DHCP client contains invalid configuration parameters, the client sends a DHCPDECLINE packet to refuse the assigned configuration information.

During negotiation, if the DHCP client does not respond to the DHCPOFFER packet in time, the DHCP server will send a DHCPNAK message to the DHCP client, which will initiate the address request process again.

During network construction, using our DHCP server brings the following advantages:

- Decrease network access cost. Generally, access using static address assignment is costly, while access using dynamic address assignment costs less.

- Simplify configuration tasks and reduce network construction cost. Dynamic address assignment significantly simplifies equipment configuration, and even reduces deployment cost if devices are deployed in the places where there are no professionals.
- Centralized management. During configuration management on several subnets, any configuration parameter can be changed simply by modifying and updating configurations in the DHCP server.

20.3 Introduction to DHCP Client

The DHCP client enables devices to obtain IP addresses and other configuration parameters from the DHCP server automatically. The DHCP client brings the following advantages:

- Shorten device configuration and deployment time.
- Reduce the possibility of configuration error.
- Allow centralized management on IP address assignment for devices.

20.4 Introduction to DHCP Relay Agent

The DHCP relay agent forwards DHCP packets between the DHCP server and the client. When the DHCP client and the server are not located in the same subnet, a DHCP relay agent must be available for forwarding DHCP requests and response messages. Data forwarding by the DHCP relay agent is different from routing and forwarding in that transparent transmission is used for routing and forwarding where the device often does not modify the contents in the IP packet. However, upon receiving a DHCP message, the DHCP relay agent regenerates and forwards a DHCP message.

In the perspective of the DHCP client, the DHCP relay agent works like a DHCP server, I the perspective of the DHCP server, the DHCP relay agent works like a DHCP client.

20.5 Configuring DHCP

To configure DHCP, perform the following tasks, of which the first three configuration tasks are compulsory.

- Enabling DHCP Server and Relay Agent (required)
- Configuration of DHCP Excluded Addresses (required)
- Configuration of DHCP Address Pool (required)
- Binding Address Manually (optional)
- Configuring the times of the Ping packet (optional)
- Configuring Packet Ping Timeout (optional)
- Ethernet interface DHCP client configuration (optional)
- DHCP client configuration of the PPP encapsulation link (optional).
- DHCP client configuration of the RP encapsulation link (optional)

- DHCP client configuration of the HDLC encapsulation link (optional)

20.5.1 Enabling DHCP Server and Relay Agent

To enable the DHCP server and the relay agent, execute the following commands in the global configuration mode:

Command	Function
DGS-3610(config)# **service dhcp**	Enable the DHCP server and the DHCP relay agent
DGS-3610(config)# **no service dhcp**	Disable the DHCP server and the relay agent

20.5.2 Configuring DHCP Excluded Addresses

Unless otherwise configured, the DHCP server tries to assign all the subnet addresses defined in the address pool to the DHCP client. If you want to reserve some addresses, such as those that have been assigned to servers or devices, you must define clearly that these addresses cannot be assigned to clients.

To configure the addresses that cannot be assigned to clients, execute the following commands in the global configuration mode:

Command	Function
DGS-3610(config)# **ip dhcp excluded-address** *low-ip-address* [*high-ip-address*]	Define a range of IP addresses that the DHCP will not assign to clients
DGS-3610(config)# **no ip dhcp excluded-address** *low-ip-address* [*high-ip-address*]	Cancel address exclusion

A good practice in configuring the DHCP server is to prohibit DHCP from assigning any address that has been assigned specifically. This provides two advantages: 1) No address conflict will occur; 2) When DHCP assigns addresses, the time for detection is shortened and thus DHCP will perform assignment more efficiently.

20.5.3 Configuration of DHCP Address Pool

Address assignment by DHCP and each DHCP parameter sent to the client should be defined in the DHCP address pool. If no DHCP address pool is configured, addresses cannot be assigned to clients even when the DHCP server has been enabled. However, if the DHCP has been enabled, the DHCP relay agent is always working regardless of the DHCP address pool.

You can give a meaningful name that can be memorized easily to the DHCP address pool. The name of address pool contains characters and digits. Our producet allows you to define multiple address pools. The IP address of relay agent in the DHCP request packet is used to determine which address pool is used for address assignment.

- If the DHCP request packet does not contain the IP address of the relay agent, the address that is in the same subnet or network as the IP address of the interface that receives the DHCP request packet is assigned to the client. If no address pool is defined for this network segment, address assignment fails.
- If the DHCP request packet contains the IP address of the relay agent, the address that is in the same subnet or network as this address is assigned to the client. If no address pool is defined for this network segment, address assignment fails.

To configure a DHCP address pool, perform the following tasks as appropriate, of which the first three tasks are compulsory:

- Configure an address pool and enter its configuration mode (compulsory)
- Configure a subnet and its mask for the address pool (compulsory)
- Configure the default gateway for the client (compulsory)
- Configure the address lease period (optional)
- Configure the domain name of the client (optional)
- Configuring the domain name server (optional)
- Configure the NetBIOS WINS server (optional)
- Configure the NetBIOS node type for the client (optional)

20.5.4 Configuring Address Pool Name and Enter Its Configuration Mode

To configure an address pool name and enter the address pool configuration mode, execute the following command in the global configuration mode:

Command	Function
DGS-3610(config)# **ip dhcp pool** *dhcp-pool*	Configuring an address pool name and enter the address pool configuration mode

The address pool configuration mode is shown as “DGS-3610(dhcp-config)#”.

20.5.5 Configuring Client Boot File

The client boot file is a boot image file to be used when the client starts. The boot image file is often the operating system to be downloaded by the DHCP client.

To configure the boot file of the client, execute the following command in the address pool configuration mode:

Command	Function
DGS-3610(dhcp-config)# **bootfile** *filename*	Configure the name of the client boot file

20.5.6 Configuring Default Gateway for Client

The configured default gateway for the client will be used as the default gateway parameter that the server assigns to the client. The IP address of the default gateway must be in the same network as the IP address of the DHCP client.

To configure the default gateway of the client, execute the following command in the address pool configuration mode:

Command	Function
DGS-3610(dhcp-config)# **default-router** *address* [*address2…address8*]	Configure the default gateway

20.5.7 Configuring Address Lease Period

The lease for the address that the DHCP server assigns to the client is usually one day. The client should request to renew when the lease period is going to expire. Otherwise, this address cannot be used when the lease period expires.

To configure the address lease period, execute the following commands in the address pool configuration mode:

Command	Function
DGS-3610(dhcp-config)# **lease** {*days* [*hours*] [*minutes*] | **infinite**}	Configure the address lease period

20.5.8 Configuring Domain Name of Client

The domain name of the client can be specified, so that the domain name suffix will be automatically added to the incomplete host name to form a complete host name when the client accesses the network resources using the host name.

To configure the domain name of the client, execute the following command in the address pool configuration mode:

Command	Function
DGS-3610(dhcp-config)# **domain-name** *domain*	Configure the domain name

20.5.9 Configuring Domain Name Server

A DNS server should be specified for domain name resolution when the client accesses the network resources using a host name. To configure a domain name server available to the DHCP client, execute the following command in the address pool configuration mode:

Command	Function
DGS-3610(dhcp-config)# **dns-server** *address* [*address2…address8*]	Configure a DNS server

20.5.10 Configuring NetBIOS WINS Server

WINS is a domain name resolution service from Microsoft for the TCP/IP network that resolves NetNBIOS names to an IP addresses. The WINS server runs in Windows NT. After started, the WINS server will receive a registration request from the WINS client. When the WINS client is being shut down, it will send a name release message to the WINS server, so that the available computers in the WINS database and those in the network are kept consistent.

To configure a NetBIOS WINS server available to the DHCP client, execute the following command in the address pool configuration mode:

Command	Function
DGS-3610(dhcp-config)# **netbios-name-server** *address* [*address2…address8*]	Configure a DNS server

20.5.11 Configuring NetBIOS Node Type for Client

There are four types of NetBIOS nodes for the DHCP client: 1) Broadcast. The NetBIOS name is resolved in the broadcast mode; 2) Peer-to-peer. The WINS server is asked directly to resolve the NetBIOS name; 3) Mixed. First, the name is resolved in the broadcast mode, and then the WINS server is connected to resolve the name; 4) Hybrid. First the WINS server is asked directly to resolve the NetBIOS name. If there is no response, the NetBIOS name is resolved in the broadcast mode.

By default, the nodes in the Microsoft operating systems are of broadcast or hybrid type. If no WINS server is configured, the node is of broadcast type. If a WINS server is configured, the node is of hybrid type.

To configure the NetBIOS node type for the DHCP client, execute the following command in the address pool configuration mode:

Command	Function
DGS-3610(dhcp-config)# **netbios-node-type** *type*	Configure the NetBIOS node type

20.5.12 Configuring Network Number and Mask for DHCP Address Pool

To configure dynamic address binding, you must configure the subnet and its mask for the new address pool, so as to provide the DHCP server with an address space that can be assigned to clients. All the addresses in the address pool may be assigned to clients unless address exclusion is configured. The DHCP server assigns the addresses in the address pool in sequence. If an address already exists in the binding table or this address is detected to be already present in this network segment, the DHCP server will check the next address until it assigns a valid address.

To configure the subnet and its mask for the address pool, execute the following commands in the address pool configuration mode:

Command	Function
DGS-3610(dhcp-config)# **network** *network-number mask*	Configure the network number and mask for the DHCP address pool

Caution

For the DHCP dynamic address pool of our product, the assignment of the address takes the physical address of client and the client ID as the index, which means there should not be two leases for the same client in the DHCP dynamic address pool. If there is the redundant path on the network topology between the client and server (the client can reach servers by the direct path or by the relay path), it will cause the failure of address assignment occurs and may fail to assign the address.

To avoid above problem, it requires the network manager takes other methods to prevent the path redundancy from the client to server when the network is established, such as adjust the physical link or the network path.

20.5.13 Binding Address Manually

Address binding refers to the mapping relationship between the IP address and the MAC address of the client. There are two types of address binding: 1) Manual binding, namely a user define manually in the DHCP server database to statically map the IP address to the MAC address. Manual binding is actually a special address pool; 2) Dynamic binding, namely upon receiving a DHCP request, the DHCP server dynamically assigns an IP address in the address pool to the client, thus mapping the IP address to the MAC address.

To define manual address binding, you first need to define a host address pool for each manual binding, and then define the IP address and hardware address or client ID for the DHCP client. The MAC address is the hardware address. Generally, a client ID, instead of a MAC address, is defined for the Microsoft clients. The client ID contains network media type and MAC address. For the codes of media types, refer to description in RFC 1700 regarding “Address Resolution Protocol Parameters”. The code for Ethernet type is “01”.

To configure the manual address binding, execute the following commands in the address pool configuration mode:

Command	Function
DGS-3610(config)# **ip dhcp pool** *name*	Define the name of address pool and enter the DHCP configuration mode
DGS-3610(dhcp-config)# **host** *address*	Define an IP address for the client
DGS-3610(dhcp-config)# **hardware-address** *hardware-address type* DGS-3610(dhcp-config)# **client-identifier** *unique-identifier*	Define a hardware address for the client, such as aabb.bbbb.bb88 Define the client ID, such as 01aa.bbbb.bbbb.88
DGS-3610(dhcp-config)# **client-name** *name*	(Optional) Define the client name using standard ASCII characters. Don't include domain name in the client name. For example, if you define the mary host name, do not define as mary.rg.com

20.5.14 Configuring Number of Packet Ping

By default, when trying to assign an IP address in the address pool, the DHCP server will perform the Ping command twice on this address (one packet for each time) If there is no response to the Ping command, the DHCP server considers this address an idle address and assigns it to the DHCP client. If there is a response to the Ping command, the DHCP server considers that this address is in use and tries to assign another address to the DHCP client until an address is assigned successfully.

To configure the number of Ping packets, execute the following commands in the global configuration mode:

Command	Function
DGS-3610(config)# **ip dhcp ping packets** *number*	Configure the number of Ping packets before the DHCP server assigns an address. If it is set to 0, the Ping operation is not performed. The default value is 2.

20.5.15 Configuring Packet Ping Timeout

By default, this IP address is considered not existent if there is no response within 500 milliseconds following the Ping operation by the DHCP server. You can change the time for the server to wait for a response to the Ping operation by adjusting the Ping packet timeout.

To configure the Ping packet timeout, execute the following commands in the global configuration mode:

Command	Function
DGS-3610(config)# **ip dhcp ping timeout** *milliseconds*	Configure the Ping packet timeout for the DHCP server. The default value is 500ms.

20.5.16 Configuring DHCP Client over Ethernet Interface

Our product supports the Ethernet port to obtain a dynamically assigned IP address using DHCP. To configure the DHCP client for the Ethernet port, execute the following command in the interface configuration mode:

Command	Function
DGS-3610(config-if)# **ip address dhcp**	Configure as obtaining an IP address using DHCP

20.5.17 Configuring DHCP Client on PPP Encapsulated Link

Our product supports the PPP-encapsulated port to obtain a dynamically assigned IP address throug DHCP. To configure the DHCP client, execute the following command in the interface configuration mode:

Command	Function
DGS-3610(config-if)# **ip address dhcp**	Configure as obtaining an IP address using DHCP

20.5.18 Configuring DHCP Client on FR Encapsulated Link

Our product supports the FR-encapsulated port to obtain a dynamically assigned IP address using DHCP. To configure the DHCP client, execute the following command in the interface configuration mode:

Command	Function
DGS-3610(config-if)# **ip address dhcp**	Configure as obtaining an IP address using DHCP

20.5.19 Configuring DHCP Client on HDLC Encapsulated Link

Our product supports the HDLC-encapsulated port to obtain a dynamically assigned IP address using DHCP. To configure the DHCP client, execute the following command in the interface configuration mode:

Command	**Function**
DGS-3610(config-if)# **ip address dhcp**	Configure to obtain an IP address via DHCP

20.6 Monitoring and Maintaining Information

20.6.1 Monitoring and Maintaining DHCP Server

Three types of commands are available for monitoring and maintaining the DHCP server:

1. Clear commands, used to clear such information as DHCP address binding, address conflict and server statistics status;
2. Debug commands, used to output necessary debugging information. Such commands are mainly used to diagnose and clear faults;
3. Show commands, used to show information about DHCP.

Our product provides three clear commands. To clear information, execute the following commands in the command execution mode:

Command	**Function**
DGS-3610# **clear ip dhcp binding** { *address* | *****}	Clear DHCP address binding information
DGS-3610# **clear ip dhcp conflict** { *address* | *}	Clear DHCP address conflict information
DGS-3610# **clear ip dhcp server statistics**	Clear DHCP server statistics status

To debug the DHCP server, execute the following command in the command execution mode:

Command	**Function**
DGS-3610# **debug ip dhcp server** [events | **packet**]	Debug the DHCP server

To show the working status of the DHCP server, execute the following commands in the command execution mode:

Command	**Function**
DGS-3610# **show ip dhcp binding** [*address*]	Show DHCP address binding information
DGS-3610# **show ip dhcp conflict**	Show DHCP address conflict information
DGS-3610# **show ip dhcp server statistics**	Show DHCP server statistics information

20.6.2 Monitoring and Maintaining DHCP Client

There are two types of commands for monitoring and maintaining the DHCP client. The following operations can be performed on the client:

1. Debug commands, used to output necessary debugging information. Such commands are mainly used to diagnose and clear faults.
2. Show commands, used to show information about DHCP.

To debug the DHCP client, execute the following command in the command execution mode:

Command	**Function**
DGS-3610# **debug ip dhcp client**	Debug the DHCP client

To show information about the lease that the DHCP client obtains, execute the following command in the command execution mode:

Command	**Function**
DGS-3610# **show dhcp lease**	Show information about DHCP lease

20.7 Configuration Examples

This section provides three configuration examples:

- Address Pool Configuration Example
- Manual Binding Configuration
- DHCP Client Configuration

20.7.1 Address Pool Configuration Example

In the following configuration, the address pool net172 is defined, the network segment of the address pool is 172.16.1.0/24, the default gateway is 172.16.16.254, the domain name is rg.com, the domain name server is 172.16.1.253, the WINS server is 172.16.1.252, the NetBIOS node is of hybrid type, and the address lease period is 30 days. In this address pool, all the addresses other than 172.16.1.2~172.16.1.100 can be assigned.

```
ip dhcp excluded-address 172.16.1.2 172.16.1.100
```

```
!
ip dhcp pool net172
network 172.16.1.0 255.255.255.0
default-router 172.16.1.254
domain-name rg.com
dns-server 172.16.1.253
netbios-name-server 172.16.1.252
netbios-node-type h-node
lease 30
```

20.7.2 Manual Binding Configuration

In the following configuration, the IP address assigned to the DHCP client with the MAC address 00d0.df34.32a3 is 172.16.1.101, the mask is 255.255.255.0, the host name is Billy.rg.com, the default gateway is 172.16.1.254, the WINS server is 172.16.1.252, and the NetBIOS node is of the hybrid type.

```
ip dhcp pool Billy
host 172.16.1.101 255.255.255.0
hardware-address 00d0.df34.32a3 ethernet
client-name Billy
default-router 172.16.1.254
domain-name rg.com
dns-server 172.16.1.253
netbios-name-server 172.16.1.252
netbios-node-type h-node
```

20.7.3 DHCP Client Configuration

In the following configuration, the device interface FastEthernet 0/0 is automatically assigned an address by DHCP.

```
interface FastEthernet0/0
ip address dhcp
```

21 DHCP Relay Configuration

21.1 Overview

21.1.1 Understanding DHCP

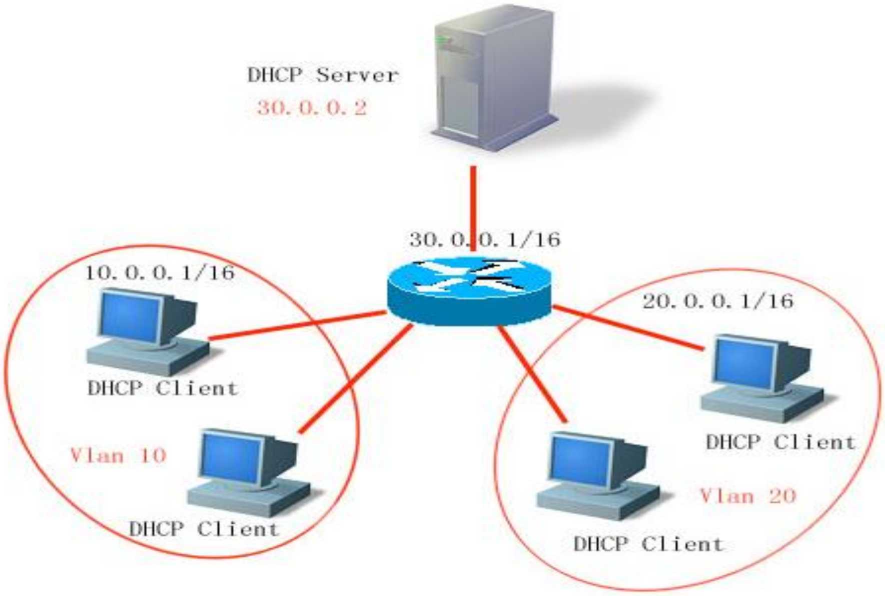
The DHCP is widely used to dynamically allocate the reusable network resources, for example, IP address.

The DHCP Client sends the DHCP DISCOVER broadcast packets to the DHCP Server. After the DHCP Server receives DHCP DISCOVER packets, it allocates resources to the Client, for example, IP address according to the appropriate policy, and sends the DHCP OFFER packets. After the DHCP Client receives the DHCP OFFER packets, it checks if the resources are available. If resources are available, it sends the DHCP REQUEST packets. If not, it sends the DHCP DISCOVER packets. When the server receives the DHCP REQUEST packets, it checks if the IP addresses (or other limited resources) can be allocated. If yes, it sends the DHCP ACK packets. If not, it sends the DHCP NAK packets. When the DHCP Client receives the DHCP ACK packets, it starts to use the resources allocated by the server. If it receives the DHCP NAK, it may re-send the DHCP DISCOVER packets to request for another IP address.

21.1.2 Understanding DHCP Relay Agent

The DHCP request packets have the destination IP address of 255.255.255.255. This type of packets is only forwarded inside the subnet and is not to be forwarded by the devices. For dynamic IP address allocation across network segments, the DHCP Relay Agent is created. It encapsulates the received DHCP request packets into IP unicast packets and forwards them to the DHCP Server. At the same time, it forwards the received DHCP response packets to the DHCP Client. This way, the DHCP Relay Agent works as a transit station, which is responsible for communicating with the DHCP Client and DHCP Server on different network segments. Therefore, one DHCP Server in a LAN can implement the dynamic IP management for all network segments, that is, a dynamic DHCP IP management in the Client - Relay Agent - Server mode.

Figure 21-1



VLAN 10 and VLAN 20 correspond to the 10.0.0.1/16 and 20.0.0.1/16 networks respectively, while the DHCP Server is located on the 30.0.0.1/16 network. To have a dynamic IP management on the 10.0.0.1/16 and 20.0.0.1/16 networks through the DHCP Server at 30.0.0.2, just enable the DHCP Relay Agent on the device that functions as the gateway, and specify the DHCP Server IP as 30.0.0.2.

21.1.3 Understanding DHCP Relay Agent Information(option 82)

According to the definitions in RFC3046, when a relay device performs DHCP relay, the network information of DHCP client can be indicated in detail by adding an option, so that the server can assign users with IP addresses for different privileges. RFC3046 specifies that the option is numbered 82, so it is also called option82. This option can be divided into several sub-options. Currently, the sub-options in frequent use are Circuit ID and Remote ID.

Relay agent information option82: This option can be used without running other protocol modules. During DHCP relay, the device forms option82 information according to the entity port that receives the DHCP request and the physical address information of the device itself, and uploads the option82 information to the server. The option is in the following format:

Figure 21-1

Agent Circuit ID

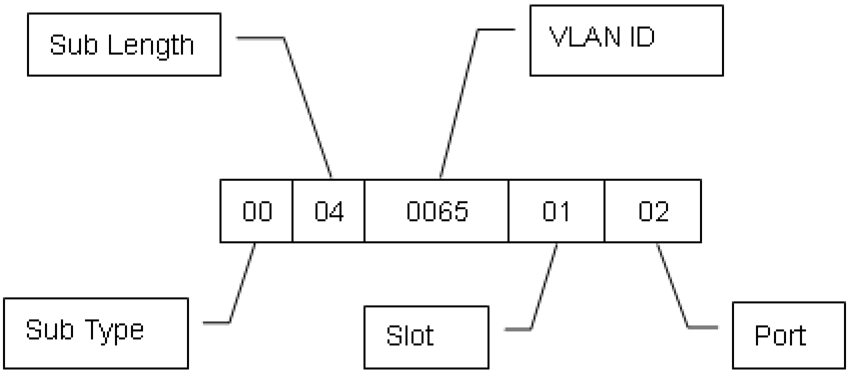
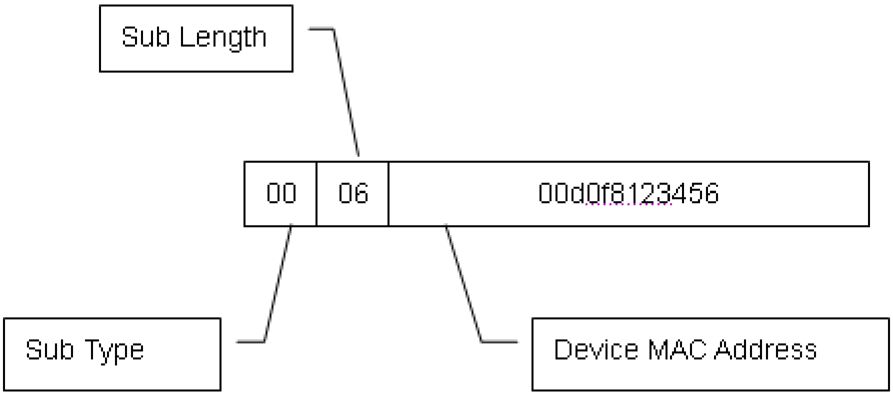


Figure 21-2

Agent Remote ID



21.1.4 Understanding DHCP relay Check Server-id Function

When DHCP is used, generally multiple DHCP servers will be available for each network for the purpose of backup, so that the network will continue to work even if a server fails. During the four interaction processes of DHCP acquisition, a server has been selected when the DHCP client sends a DHCP request. Here, the packet of the request includes an option of server-id. In some particular application circumstances, we need to enable this option for relay in order to reduce load on the network server. In this way, the request packet is only sent to the server in this option, instead of to every configured DHCP server. This is the DHCP check server-id function.

21.2 Configuring DHCP

21.2.1 Configuring DHCP Relay Agent

In the global configuration mode, configure the DHCP relay agent by performing the following steps.

Command	**Function**
DGS-3610(config)# **service dhcp**	Enable the DHCP agent
DGS-3610(config)# **no service dhcp**	Disable the DHCP agent

21.2.2 Configuring the DHCP Server IP Address

After you have configured the IP address of the DHCP Server, the DHCP request packets received by the device will be forwarded to it. At the same time, the DHCP response received from the Server will also be forwarded to the Client.

The DHCP server address can either be globally or on the layer 3 interface. In each configuration mode, up to 20 server addresses can be configured. When the DHCP requests are received from an interface, the DHCP server of the interface is first used. If no server address is configured on the interface, the DHCP server globally configured will be used.

To configure the DHCP server address, please perform the following steps:

Command	**Function**
DGS-3610(config)# **IP helper-address** *A.B.C.D*	Add a global DHCP server address
DGS-3610(config-if)# **IP helper-address** *A.B.C.D*	Add the DHCP server address of an interface. This command must be set under the layer 3 interface.
DGS-3610(config)# **no IP helper-address** *A.B.C.D*	Delete a global DHCP server address
DGS-3610(config-if)# **no IP helper-address** *A.B.C.D*	Delete the DHCP server address of an interface

21.2.3 Configuring DHCP option dot1x

Description in understanding the DHCP Relay Agent Information shows that we can configure **ip dhcp relay information option dot1x** to enable the option dot1x function of DHCP relay when it is required to assign users with different privilege IPs according to different user privileges. When this function is enabled, the device will work with 802.1x to add corresponding option information to the server when it relays. This function should be used with the dot1x function.

In the global configuration mode, configure DHCP option dot1x by performing the following steps:

Command	**Function**
DGS-3610(config)# **ip dhcp relay information option dot1x**	Enable the DHCP option dot1x function
DGS-3610(config)# **no ip dhcp relay information option dot1x**	Disable the DHCP option dot1x function

21.2.4 Configuring DHCP option dot1x access-group

In the option dot1x application scheme, the device needs to restrict the unauthorized IP or the IP with low privilege to access certain IP addresses, and restrict the access between users with low privileges. To do so, configure the command **ip dhcp relay information option dot1x access-group** *acl-name*. Here the ACL defined by *acl-name* must be configured in advance. It is used to filter some contents and prohibit unauthorized users from accessing each other. In addition, ACL associated here is applied to all the ports on the device. This ACL has not default ACE and is not conflicted with ACLs associated with other interfaces. For example:

Assign a type of IP addresses for all the unauthorized users, namely 192.168.3.2-192.168.3.254, 192.168.4.2-192.168.4.254, and 192.168.5.2-192.168.5.254. 192.168.3.1, 192.168.4.1, and 192.168.5.1 are gateway addresses that are not assigned to users. This way, an unauthorized user uses one of the 192.168.3.x-5.x addresses to access the Web portal for downloading client software. Therefore, the device should be configured as follows:

```
DGS-3610# config
DGS-3610(config)# ip access-list extended DenyAccessEachOtherOfUnauthrize
DGS-3610(config-ext-nacl)# permit ip any host 192.168.3.1      //Packet that can be sent to the gateway
DGS-3610(config-ext-nacl)# permit ip any host 192.168.4.1
DGS-3610(config-ext-nacl)# permit ip any host 192.168.5.1
DGS-3610(config-ext-nacl)# permit ip host 192.168.3.1 any
```

//Allow communication of packets with IP address as the gateway address

```
DGS-3610(config-ext-nacl)# permit ip host 192.168.4.1 any
DGS-3610(config-ext-nacl)# permit ip host 192.168.5.1 any
DGS-3610(config-ext-nacl)# deny ip 192.168.3.0 0.0.0.255 192.168.3.0 0.0.0.255
```

//Prohibit unauthorized users from accessing each other

```
DGS-3610(config-ext-nacl)# deny ip 192.168.3.0  0.0.0.255  192.168.4.0  0.0.0.255
DGS-3610(config-ext-nacl)# deny ip 192.168.3.0  0.0.0.255  192.168.5.0  0.0.0.255
DGS-3610(config-ext-nacl)# deny ip 192.168.4.0  0.0.0.255  192.168.4.0  0.0.0.255
DGS-3610(config-ext-nacl)# deny ip 192.168.4.0  0.0.0.255  192.168.5.0  0.0.0.255
DGS-3610(config-ext-nacl)# deny ip 192.168.5.0  0.0.0.255  192.168.5.0  0.0.0.255
DGS-3610(config-ext-nacl)# deny ip 192.168.5.0  0.0.0.255  192.168.3.0  0.0.0.255
DGS-3610(config-ext-nacl)# deny ip 192.168.5.0  0.0.0.255  192.168.4.0  0.0.0.255
DGS-3610(config-ext-nacl)# exit
```

Then, apply the command to the global interfaces using the command **ip dhcp relay information option dot1x access-group** *DenyAccessEachOtherOfUnauthrize*.

In the global configuration mode, configure **DHCP option dot1x access-group** by performing the following steps:

Command	Function
DGS-3610(config)# **ip dhcp relay information option dot1x access-group** *acl-name*	Apply DHCP option dot1x acl
DGS-3610(config)# **no ip dhcp relay information option dot1x access-group** *acl-name*	Cancel the applied DHCP option dot1x acl.

21.2.5 Configuring DHCP option 82

When the **ip dhcp relay information option82** command is configured, the device adds **option** in the format as described in Understanding **DHCP Relay Agent Information** to the server during DHCP relay.

In the global configuration mode, configure DHCP option82 by performing the following steps:

Command	Function
DGS-3610(config)# **ip dhcp relay information option82**	Enable the DHCP option82 function
DGS-3610(config)# **no ip dhcp relay information option82**	Disable the DHCP option82 function.

21.2.6 Configuring DHCP relay check server-id

After the **ip dhcp relay check** *server-id* command is configured, the device resolves DHCP SERVER-ID option upon receiving DHCP relay. If this option is not empty, it sends a request to this server only, instead of other configured servers.

In the global configuration mode, configure **DHCP relay check** *server-id* function by performing the following steps:

Command	Function
DGS-3610(config)# **ip dhcp relay check server-id**	Enable the DHCP relay check server-di function

Command	**Function**
DGS-3610(config)# **no ip dhcp relay check server-id**	Disable the DHCP relay check server-id function

21.2.7 Configuring DHCP relay suppression

After the **ip dhcp relay suppression** command is configured, the interface configured with DHCP relay suppression does not translate the received DHCP boardcast request as unicast relay. The normally broadcast forwarding will not perform the suppression.

In the global configuration mode, configure the function by performing the following steps:

Command	**Function**
DGS-3610(config)# **ip dhcp relay suppresson**	Enable the DHCP relay suppresson function
DGS-3610(config)# **no ip dhcp relay suppresson**	Disable the DHCP relay suppresson function

21.2.8 DHCP Configuration Example

The following commands enable the dhcp relay function and add two groups of server addresses:

```
DGS-3610# configure  terminal
DGS-3610(config)# service dhcp                         //Enable the dhcp relay function
DGS-3610(config)# ip helper-address 192.18.100.1     //Add a global server address
DGS-3610(config)# ip helper-address192.18.100.2      //Add a global server address
DGS-3610(config)# interface GigabitEthernet 0/3
DGS-3610(config-if)# ip helper-address 192.18.200.1 //Add an interface server address
DGS-3610(config-if)# ip helper-address 192.18.200.2 // Add an interface server address
DGS-3610(config-if)# end
```

21.3 Other Precautions on DHCP Relay Configuration

For layer 2 network device, you must enable at least one of the option dot1x, dynamic address binding and option82 functions when the cross-management vlan relay function is required. Otherwise, only the relay function of management VLAN can be enabled for the layer 2 device.

21.3.1 Precautions on DHCP option dot1x Configuration

1. This command works only when the configuration related to AAA/802.1x is correct.
2. When this scheme is adopted, the IP authorization of the DHCP mode of 802.1x should be enabled.
3. This command cannot be used together the **dhcp option82** command because they are conflicted.
4. When the IP authorization of the DHCP mode of 802.1x is enabled, MAC + IP will also be bound. Therefore, IP authorization and DHCP dynamic binding function cannot be enabled at the same time.

21.3.2 Precautions on DHCP option82 Configuration

The DHCP option82 function and the **dhcp option dot1x** function cannot be used at the same time because they are conflicted.

21.4 Showing DHCP Configuration

Show the DHCP configuration using the **show running-config** command in the privilege mode.

```
DGS-3610# show running-config
Building configuration...
Current configuration : 1464 bytes
version v 10.1.00(1), Release(11758)(Fri Mar 30 12:53:11 CST 2007 -nprd
hostname DGS-3610
vlan 1
ip helper-address 192.18.100.1
ip helper-address 192.18.100.2
ip dhcp relay information option dot1x
interface GigabitEthernet 0/1
interface GigabitEthernet 0/2
interface GigabitEthernet 0/3
no switchport
ip helper-address 192.168.200.1
ip helper-address 192.168.200.2
interface VLAN 1
ip address 192.168.193.91 255.255.255.0
line con 0
exec-timeout 0 0
line vty 0
exec-timeout 0 0
login
password 7 0137
line vty 1 2
login
```

```
password 7 0137
line vty 3 4
login
end
```

22 DNS Configuration

22.1 DNS Overview

Each IP address may present a host name, which consists of one or more strings, and it is separated by the decimal between the strings. For the host name, it is not necessary to remember the IP address of each IP device, but remember the meaningful host name. This is the function the DNS protocol should implement.

There are two methods to map to the IP address from the host name: 1) Static Mapping, each device is equipped with the mapping from the host to the IP address, various devices maintain their mapping table individually and only provide for the use of the device itself; 2) Dynamic Mapping, establish a set of the domain name system (DNS), only dedicated DNS server is equipped with the mapping from the host to the IP address, it is necessary for the network to use the device for the host name communication. Firstly, it is necessary to query the IP address corresponding to the host from the DNS server.

The process that the IP address which corresponds to the host name by the host name is referred to as the domain name resolution (or host name resolution). The DGS-3610 series support the host name resolution locally or by the DNS. During the resolution of domain name, the static method may be used firstly. If it fails, use the dynamic method instead. Some frequently used domain names can be put into the resolution list of static domain names. In this way, the efficiency of domain name resolution can increase considerably.

22.2 Configuring Domain Name Resolution

22.2.1 Default Configuration of DNS

The default configurations of DNS are as follows:

Attribute	Default value
Enable/disable the DNS resolution service	Enable
IP address of DNS server	Void
Static Host List	Void
Maximum number of DNS servers	6

22.2.2 Enabling DNS Resolution Service

This section describes how to enable the DNS resolution service.

Command	Function
DGS-3610(config)# **ip Domain-lookup**	Enable the function of DNS resolution.

The command **no ip domain-lookup** is used to disable the function of DNS resolution.

```
DGS-3610(config)# ip domain-lookup
```

22.2.3 Configuring DNS Server

This section describes how to configure the DNS server. The dynamic domain name resolution can be carried out only when the DNS Server is configured.

The command **ip name-server** [*ip-address*] can be used to remove the DNS server. Where, the parameter **ip-address** indicates the specified DNS server to be removed. If this parameter is omitted, all of the DNS servers will be removed.

Command	Function
DGS-3610(config)# **ip name-server** *ip-address*	Add the IP address of the DNS Server. The device will add a DNS Server when this Command is executed every time. If the domain name can't be obtained from the first Server, the device will attempt to send the DNS request to the subsequent several Servers until the correct response is received.The system can support six DNS server at most.

22.2.4 Configuring Mapping between Host Name and IP Address Statically

This section describes how to configure the mapping from the host name to the IP address. The switch maintains a corresponding table of the host names and the IP addresses, which is also referred to as the mapping table from the host name to the IP address. The contents of the mapping table from the host name to the IP address comes from the manual configuration and the dynamic learning. If it is not possible to learn dynamically, the manual configuration is required.

Command	Function
DGS-3610(config)# **ip host** *host-name ip-address*	Configuring the mapping between the host name and IP address manually

This command with the parameter **no** can be used to remove the mapping between the host name and IP address.

22.2.5 Clearing Cache Table of Dynamic Host Names

This section describes how to clear the cache table of dynamic host names. If the command **clear host** or **clear host** * is entered, the dynamic cache table will be cleared. Otherwise, only the entries of specified domain names will be cleared.

Command	Function
DGS-3610# **clear host** [*word*]	Clear the cache table of dynamic host names. The host names configured statically will not be removed.

22.2.6 Showing Domain Name Resolution Information

This section describes how to display relevant configuration information of DNS.

Command	Function
DGS-3610# **show hosts**	View related parameters of the DNS.

```
DGS-3610# show hosts
DNS name server   :
192.168.5.134   static
    host               type       address
www.163.com            static      192.168.5.243
www.dlink.com.tw         dynamic     192.168.5.123
```

22.2.7 Application examples

Ping the host with specified domain name:

```
DGS-3610# ping www.dlink.com.tw
Resolving host[www.dlink.com.tw]……
Sending 5,100-byte ICMP Echos to 192.168.5.123,
timeout is 2000 milliseconds.
!!!!!
Success rate is 100 percent(5/5)
Minimum = 1ms Maximum = 1ms, Average = 1ms
```

23 NTP Configuration

23.1 Unerstanding NTP

Network Time Protocol (NTP) is a protocol for the time synchronization of network devices. It is designed to synchronize the network devices with the server or clock source, to provide high accurate time correction (less than one millisecond on the LAN an dozens of milliseconds on the WAN, compared with the standard time), and to prevent from attack by the means of encryption and confirmation.

To provide accurate time, NTP needs precise time source, which should be the Coordinated Universal Time (UTC). The NTP may obtain the time source of UTC from the atom clock, the observatory, the satellite or the Internet. Thus, accurate and reliable time source is available.

To prevent the time server from malicious destroying, an Authentication mechanism is used by the NTP to check whether the request of time correcting really comes from the declared server, and check the returning path of data. This mechanism provides protection of anti-interference.

As a simplified version of NTP, SNTP has the identical message format. The difference is that SNTP simplifies the algorithm of time correction and neglects many possible factors resulting in errors. Therefore, SNTP is not as good as NTP in respect of precision. The SNTP does not support the security authentication mechanism. The switch supports the NTP for the client at present, that is, the time can be synchronized according to the time server.

23.2 Configuring NTP

This chapter describes how to configure the NTP client in the system implementation.

- Configuring Global Security Authentication Mechanism for the NTP
- Configuring Global Authentication Key for the NTP
- Configuring Global Trusted Key ID for the NTP
- Configuring NTP Server
- Disabling receiving NTP Packets on the Interface
- Enabling/Disabling NTP Function
- Configuring Real Time Synchronization for NTP

23.2.1 Configuring Global Security Authentication Mechanism for the NTP

The NTP client of DGS-3610 series supports encrypting communication with the server by means of key encryption.

There are two steps to configure the NTP client to communicate with the server by means of encryption: Step 1, complete relevant settings for global security authentication and global key for the NTP client; Step 2, complete the trusted key settings for the communication server. The global security settings of NTP should be done in Step 1, however, the authentication key should be set also for corresponding server if encrypting communication with the server is to be initiated.

By default, the client does not use the global security authentication mechanism. If the security authentication mechanism is not used, the communication will not be encrypted. However, only the setting of global security authentication does not mean that the encryption is used to implement the communication between the server and client. The other global key must also be configured and the encrypted key must be set for the server before the encrypted communication with the server can be initiated.

To configure the global security authentication mechanism, run the following commands in the global configuration mode:

Command	Function
ntp authenticate	Configure global security authentication mechanism for the NTP.
no ntp authenticate	Disable global security authentication mechanism for the NTP.

The packet is verified by the trusted key, which is specified by the command **ntp authentication-key** or **ntp trusted-key**.

23.2.2 Configuring Global Authentication Key for the NTP

The next step to configure the global security authentication for the NTP is to set the global authentication key.

During the configuration of global authentication key, each key is identified by a unique key-id. The customer can use the command **ntp trusted-key** to set the key corresponding to the key-id as a global trusted key.

To specify a global authentication key, run the following commands in the global configuration mode:

Command	Function
ntp authentication-key *key-id* **md5** *key-string* [*enc-type*]	Specify a global authentication key for the NTP. *key-id*: 1-4294967295 *key-string*: its length is not limited. *enc-type*: there are two types: 0 and 7.
no ntp authentication-key *key-id* **md5** *key-string* [*enc-type*]	Remove a global authentication key for the NTP.

The configuration of global authentication key does not mean the key is effective; therefore, the key must be configured as global trusted key before using it.

Caution The current version in DGS-3610 series can support the authentication key up to 1024 and only one key can be set for each server for secure communication.

23.2.3 Configuring Global Trusted Key ID for the NTP

The last step to configure the global security authentication is to set a global authentication key as a global trusted key. Only by this trusted key the user can send encrypted data and check the validity of the message.

To specify a global trusted key, run the following commands in the global configuration mode:

Command	Function
ntp trusted-key *key-id*	Configure a global trusted key ID for the NTP.
no ntp trusted-key *key-id*	Remove a global trusted key ID for the NTP.

The above-mentioned three steps of settings are the first procedure to implement security authentication mechanism. To initiate real encrypted communication with client server, a trusted key must be set for corresponding server.

Caution When a global authentication key is removed, its all trusted information are removed.

23.2.4 Configuring NTP Server

No NTP server is configured by default. DGS-3610 series's client system supports simultaneous interaction with up to 20 NTP servers, and one authentication key can be set for each server to initiate encrypted communication with the server.(after relevant settings of global authentication and key are completed)

NTP version 3 is the default version of communication with the server. Meantime, the source interface can be configured to send the NTP message, and the NTP message from relevant server can only be received on the sending interface.

To configure an NTP server, run the following commands in the global configuration mode:

Command	**Function**
ntp server *ip-addr* [**version** *version*][**source** *if-name number*][**key** *keyid*][**prefer**]	Configure an NTP server. *version* (the version numer of NTP): 1-3 *if-name* (interface type): Aggregateport, Dialer GigabitEthernet, Loopback, Multilink, Null, Tunnel, Virtual-ppp, Virtual-template and Vlan type. *keyid*: 1-4294967295
no ntp server *ip-addr*	Remove an NTP server.

Only when the global security authentication and key setting mechanisms are completed, and the trusted key for communicating with server is set, can the encrypted communication with the server be initiated. In order to implement the encrypted communication, the same trusted key is needed on the server.

23.2.5 Disabling receiving NTP Packets on the Interface

The function of this command is to disable the receiving messages on relevant interfaces.

By default, the NTP messages received on any interface are available to the client for clock synchronization. By setting this function, the NTP messages received on relevant interfaces can be shielded.

⚠ **Caution**

If an interface can be set for this command, it must be the interface that can be set for its IP to send and receive messages. This command cannot be run on other interfaces.

To disable receiving NTP messages on the interface, run the following commands in the interface configuration model:

Command	**Function**
interface *interface-type number*	Enter the interface configuration mode.
ntp disable	Disable the function of receiving NTP messages on the interface.

To enable the function of receiving NTP messages on the interface, use the command **no ntp disable** in the interface mode.

23.2.6 Enabling/Disabling NTP Function

The function of command **no ntp** is to disable the NTP synchronization service, stop the time synchronization, and clear relevant information of NTP configuration.

The NTP function is disabled by default, but may be enabled as long as the NTP server or NTP security authentication mechanism is configured.

To disable the NTP, run the following commands in the global configuration mode:

Command	Function
no ntp	Disable the NTP function.
ntp authenticate or **ntp server** *ip-addr* [**version** *version*][**source** *if-name number*][**key** *keyid*][**prefer**]	Enable the NTP function.

23.2.7 Configuring Real Time Synchronization for NTP

For higher accuracy, the interaction of eight messages will be completed consecutively between the client and server during the first synchronization. In subsequent synchronization, the time interval of NTP synchronization is one minute, that is, from the end of this synchronization to the automatic initiation of next clock synchronization. When the users want to implement real time synchronization manually, this command can be used.

To implement NTP real time synchronization, run the following commands in the global configuration mode:

Command	Function
ntp synchronize	Enable real time synchronization.
no ntp synchronize	Disable real time synchronization.

DGS-3610 series client system is set to conduct next synchronization in 30 minutes after the completion of each synchronization. Real time synchronization will be triggered when new servers are added and when the NTP clients stop synchronization. There is no effect to use the command during synchronization.

Both the command to disable real time synchronization and the command to disable the NTP can stop the clock synchronization (during the synchronization) or disable the clock synchronization (between processes of synchronization). The difference is that the latter can not only disable the NTP synchronization function, but also clear relevant NTP configuration information.

23.3 Display of NTP Information

23.3.1 Debugging the NTP

If you want to debug the NTP function, this command may be used to output necessary debugging information for troubleshooting.

To debug the NTP function, run the following commands in the privilege mode:

Command	Function
debug ntp	Enable the debugging function.
no debug ntp	Disable the debugging function.

23.3.2 Showing NTP Information

In the privilege mode, the command **show ntp status** can be used to display the current NTP information.

To display the NTP function, run the following command in the privilege mode:

Command	Function
show ntp status	Show the current NTP information.

Only when relevant communication server is configured, can this command be used to print the display information.

```
Switch# show ntp status
Clock is synchronized, stratum 9, reference is 192.168.217.100
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**18
reference time is AF3CF6AE.3BF8CB56 (20:55:10.000 UTC Mon Mar 1 1993)
clock offset is 32.97540 sec, root delay is 0.00000 sec
root dispersion is 0.00003 msec, peer dispersion is 0.00003 msec
```

Note: the starum indicates the level of current clock, reference indicates the address of server used for synchronization, freq indicates the clock frequency of current system, precision indicates the precision of current system clock, reference time indicates the UTC time of reference clock on the synchronization server, clock offset indicates the offset of current clock, root delay indicates the delay of current clock, root dispersion indicates the precision of top server, peer dispersion indicates the precision of synchronization server.

23.4 Configuration Examples

In the following configuration, there is an NTP server specified as the master in the network, relevant authentication mechanism is enabled, a key with the key-id of 6 and the key-string of wooooop is configured as the trusted key for the server. To configure the DGS-3610 series client so that it is synchronized for the time with the NTP server on the network, it can be configured as follows: enable security authentication, configure a key which is the same as that on the NTP server, set this NTP server on the network as the synchronization server, and begin to synchronize the time.

```
DGS-3610(config)# no ntp
DGS-3610(config)# ntp authentication-key 6 md5 wooooop
DGS-3610(config)# ntp authenticate
DGS-3610(config)# ntp trusted-key 6
DGS-3610(config)# ntp server 192.168.210.222 key 6
DGS-3610(config)# ntp synchronize
DGS-3610(config)# interface gigabitEthernet 0/1
DGS-3610(config-if)# ntp disable
DGS-3610(config-if)# no ntp disable
```

24 UDP-Helper Configuration

24.1 UDP-Helper Configuration

24.1.1 UDP-Helper Overview

The main function of UDP-Helper is to implement the relay and forward of UDP broadcast message. By configuring the destination server requiring forwarding, the UDP broadcast messages can be converted into unicast messages which are sent to the specified destination server. This destination server plass the role of a relay.

When the UDP-Helper is enabled, the destination UDP port number of received broadcast packets will be identified. If this number matches the port number to be forwarded, the destination IP address of packets will be modified as the IP address of the specified destination server, and the specified destination server will be sent by means of unicast.

When enabling the UDP-Helper, the broadcast packets of Ports 69, 53, 37, 137, 138 and 49 are relayed and forwarded by default.

Note The relay of BOOTP/DHCP broadcast message is implemented through the UDP Port 67 and 68 by the DHCP Relay module; therefore, the two ports can not be configured as the relay port of UDP-Helper.

24.2 Configuring UDP-Helper

24.2.1 Default Configuration of UDP-Helper

Table 24-1 Default Configuration of UDP-Helper

Attribute	Default value
Function of relay and forwarding	Off
UDP port number for relay and forwarding	When enabling the UDP-Helper, the UDP broadcast packets of Ports 69, 53, 37, 137, 138 and 49 are relayed and forwarded by default.
Destination Server for relay and forwarding	None

24.2.2 Enable the Function of Relay and Forwarding for UDP-Helper

Command	**Function**
DGS-3610(config)# **udp-helper enable**	The Command **udp-helper enable** is used to enable the function of relay and forward for UDP broadcast packet. This function is disabled by default.

The command **no udp-helper enable** is used to disable the function of relay and forwarding for the UDP.

Note

1. The function of relay and forwarding is disabled by default.
2. When enabling the function of relay and forward for UDP broadcast packets, the broadcast packets of UDP Ports 69, 53, 37, 137, 138 and 49 are relayed and forwarded by default.
3. When the function of relay and forward for UDP broadcast is disabled, all of the configured UDP ports including the default ports are cancelled.

24.2.3 Configuring Destination Server for Relay and Forward

Command	**Function**
DGS-3610(config-if)# **ip helper-address** *IP-address*	Configure the destination server to which the UDP broadcast packets are relayed and forwarded. By default, it is not configured.

The command **no ip helper-address** can be used to remove the destination server of relay and forwarding.

Note

1. At most 20 destination servers can be configured for one interface.
2. If the destination server for relay and forwarding is configured on a specified interface, when the UDP-Helper is enabled, the broadcast messages of specified UDP port received from this interface will be sent to the destination server configured for this interface by means of unicast.

24.2.4 Configuring UDP Port Requiring Relay and Forwarding

Command	Function
DGS-3610(config)# **ip forward-protocol udp** *ID*	Configure the UDP port requiring delay and forwarding. If only the UDP parameter is specified, the default port will be relayed and forwarded, otherwise, the port can be configured upon necessary. When enabling the UDP-Helper, the broadcast packets of Ports 69, 53, 37, 137, 138 and 49 are relayed and forwarded by default.

The command **no ip forward-protocol udp port** can be used to disable the UDP ports requiring relay and forwarding.

Note

- Only when the function of relay and forwarding is enabled for the UDP-Helper and the destination server is configured for the relay and forwarding, can the UDP port requiring relay and forward be configured. Otherwise, the error prompts will appear.
- When the function of UDP relay and forward is enabled, the function of forwarding the broadcast UDP packets from the default ports 69, 53, 37, 137, 138 and 49 will be enabled right now without any configuration from the user.
- At most 256 UDP ports requiring relay and forwarding are supported by the device.
- Two ways can be used to configure the default ports, for example, the configuration of the commands **ip forward-protocol udp domain** and **ip forward-protocol udp** *53* are the same.

25 SNMP Configuration

25.1 SNMP Related Information

25.1.1 Overview

As the abbreviation of Simple Network Manger Protocol, SNMP has been a network management standard (RFC1157) since the August, 1988. So far, the SNMP is supported by many manufacturers and becomes the actual network management standard. It is applicable to the situation of interconnecting multiple systems from different manufacturers. The network administrator can use the SNMP to query the information, configure the network, locate the failure and plan the capacity for the node on the network. The network supervision and administration are the basic function of SNMP.

As a protocol in the application layer, the SNMP adopts the client machine/server mode, including three parts as follows:

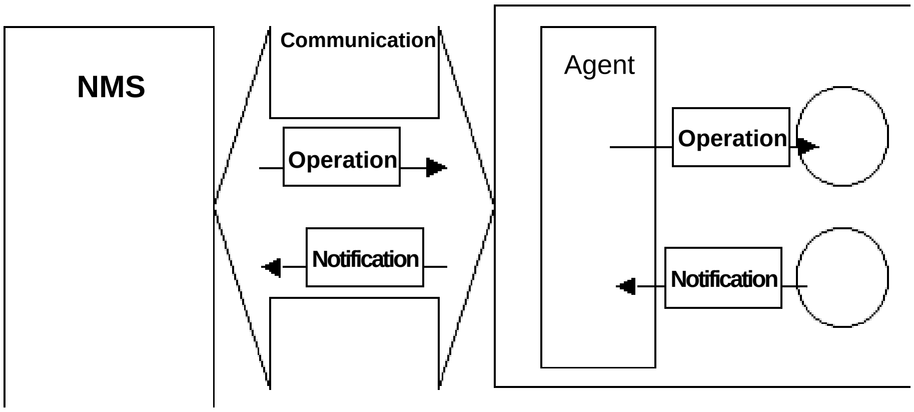
- SNMP network manager
- SNMP agent
- MIB (management information base)

The SNMP network manager is a system to control and monitor the network using the SNMP, and also referred to as NMS (Network Management System). HP OpenView, CiscoView and CiscoWorks 2000 are the typical network management platforms running on the NMS. D-Link has developed a suit of software (D-View) for network management for its own network devices. These typical network management software are convenient to monitor and manage the network devices.

The SNMP Agent is the software running on the managed devices. It receives, processes and responds the messages of monitoring and controlling from the NMS, and also sends some messages to the NMS.

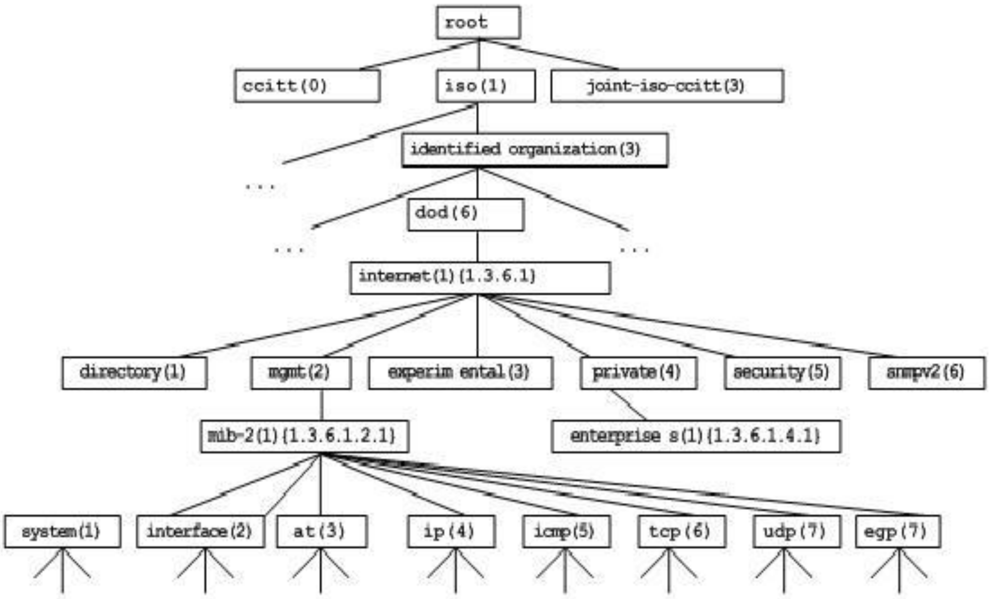
The relation of the NMS and Agent can be indicated as follows:

Figure 25-1 Relation diagram between the NMS and agent



The MIB (Management Information Base) is a virtual information base for network management. There are large volumes of information for the managed network equipment. In order to uniquely identify a specific management unit in the SNMP message, the tree hierarchy is used to by the MIB to describe the management units in the network management equipment. The node in the tree indicates a specific management unit. Take the following figure of MIB as an example to name the objectives in the tree. To identify a specific management unit system in the network equipment uniquely, a series of numbers can be used. For instance, the number string {1.3.6.1.2.1.1} is the object identifier of management unit, so the MIB is the set of object identifiers in the network equipment.

Figure 25-2 MIB tree hierarchy



25.1.2 SNMP Protocol Versions

This software supports these SNMP versions:

- SNMPv1: the first formal version of the Simple Network Management Protocol, which is defined in RFC1157.
- SNMPv2C: The community-based Administrative Framework for SNMPv2, an Experimental Internet Protocol defined in RFC1901.
- SNMPv3: Through authenticating and encrypting packets, some security features can be provided as follows:
  1. Ensuring that the data are not tampered during transmission.
  2. Ensuring that the data sends from a valid data source.
  3. Encrypting packets to ensure the data confidentiality.

Both the SNMPv1 and SNMPv2C adopt a community-based framework of security. The managers' operations on MIB are confined by the host IP addresses and Community string.

SNMPv2C adds a GetBulk operating mechanism and is able to get more detailed error information for management stations. The GetBulk can obtain all the information from the table at a time or obtain a great volume of data, to reduce the request-response times. The SNMPv2C improved error-processing capability includes expanded error codes that distinguish different kinds of error conditions; these conditions are only reported through a single error code in SNMPv1. Now, the error type can be distinguished through the error code. Because the management workstation of SNMPv1 and the same of SNMPv2C can exist simultaneously, so an SNMP agent must be able to recognize both SNMPv1 and SNMPv2C messages, and return correct version's messages.

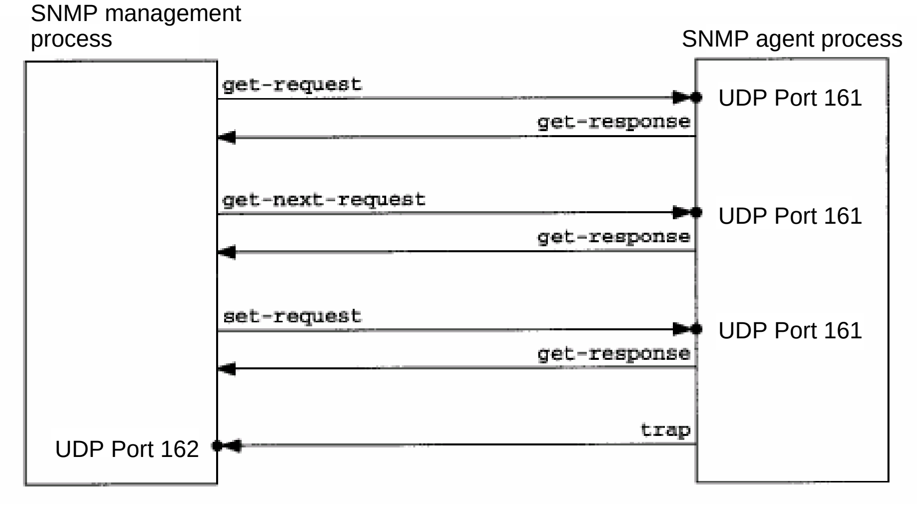
25.1.3 SNMP Management Operations

In the interaction information between the NMS and Agent in SNMP, six types of operations are defined:

1. Get-request operation: the NMS gets one or more parameter values from the Agent.
2. Get-next-request operation: the NMS gets next parameter value of one or more parameters from the Agent.
3. Get-bulk operation: the NMS gets a bulk of parameter values from the Agent.
4. Set-request operation: the NMS sets one or more parameter values for the Agent.
5. Get-response operation: the Agent returns one or more parameter values, as the response of the Agent to any of the above 3 operations for the NMS.
6. Trap operation: the Agent proactively sends messages to notify events occurring to the NMS.

The first four packets are sent from the NMS to the Agent, and the last two packets are sent from the Agent to the NMS (Note: the SNMPv1 does not support the Get-bulk operation). These operations are described in the following figure:

Figure 25-3 Packet Types in SNMP



The Port 161 of UDP is used by the first three operations sent from the NMS to the Agent and the response operation of the Agent.The Port 162 of UDP is used by the Trap operation sent from the Agent.

25.1.4 SNMP Security

Both SNMPv1 and SNMPv2 use the community string to identify whether it is entitled to use the MIB objects. In order to manage the equipment, the community string of NMS must be identical to a community string defined in the equipment.

A community string can have one of these attributes:

- Read-only: Gives read authorization to authorized management workstations to all variables in MIB.
- Read-write: Gives read-write authorization of all variables in MIB for accessing to authorized management stations.

Having evolved from SNMPv2, SNMPv3 can determine a security mechanism to data by selecting different security models and security levels; there are three types of security models: SNMPv1, SNMPv2C and SNMPv3.

The table below describes the supported security models and security levels.

Security Model	Level	Authentication	Encryption	Description
SNMPv1	noAuthNoPriv	Community string	None	Ensures the data validity through Community string.
SNMPv2c	noAuthNoPriv	Community string	None	Ensures the data validity through Community string.

Security Model	Level	Authentication	Encryption	Description
SNMPv3	noAuthNoPriv	User Name	None	Ensures the data validity through User Name.
SNMPv3	authNoPriv	MD5 or SHA	None	Provides an authentication mechanism based on HMAC-MD5 or HMAC-SHA.
SNMPv3	authPriv	MD5 or SHA	DES	Provides an authentication mechanism based on HMAC-MD5 or HMAC-SHA. Provides an encryption mechanism based on CBC-DES.
SNMPv2c	noAuthNoPriv	Community string	None	Ensures the data confidentiality through Community string.
SNMPv3	noAuthNoPriv	User Name	None	Ensures the data confidentiality through User Name.
SNMPv3	authNoPriv	MD5 or SHA	None	Provides an authentication mechanism based on HMAC-MD5 or HMAC-SHA.
SNMPv3	authPriv	MD5 or SHA	DES	Provides an authentication mechanism based on HMAC-MD5 or HMAC-SHA. Provides an encryption mechanism based on CBC-DES.

25.1.5 SNMP Engine ID

The engine ID is designed to identify an SNMP engine uniquely. SNMP engine ID within a management domain, a SNMP engine ID is the unique and unambiguous identifier of a SNMP engine. So every SNMPV3 entity has a unique engine identifier named SNMPEngineID.

SNMP Engine ID is an OCTET STRING, the length is 5~32 bytes the format of Engine ID is defined in RFC3411:

- The first four bytes are assigned with the private enterprise number in HEX by IANA.
- The fifth bytes indicates how the rest (6th and following octets) are formatted.

  0: Reserved

  1: The following 4 bytes are for IPv4 address

2: The following 16 bytes are for IPv6 address

3: The following 6 bytes are for MAC address

4: Texts, assigned by product providers, 27 octets at most

5: Hexadecimal number, assigned by product providers, 27 bytes at most

6-127: Reserved

128-255: Special Form assigned by product providers

25.2 SNMP Configuration

The configuration of the SNMP is completed in the global mode of network devices. It is required to enter the global configuration mode first to make SNMP configuration.

25.2.1 Setting the Community String and Access Authority

The community-based security scheme is adopted by SNMPv1/SNMPv2C. The SNMP only receives the management operations from the same community-string. The SNMP packets not matching the community string to the network equipment will be discarded instead of responded. The community-string serves as the password between the NMS and Agent.

- Configure the access list association to manage only the NMS of the specified IP addresses.
- Set the community operation authorities as ReadOnly or ReadWrite.
- Specify the name of view used for view-based management. By default, no view is configured, allow access to all MIB objects
- Indicate the IP address of managers who can use this community string. If it is not indicated, the IP address of managers using this community string will not be confined. By default, the IP address of managers using this community string is not confined.

To configure the SNMP community string, run the following command in the global configuration mode:

Command	Function
DGS-3610(config)# **snmp-server community** *string* [**view** *view-name*] [**ro** | **rw**] **[host** *host-ip*] [*num*]	Set the community string and the authority.

One or more commands can be used to specify multiple different community strings, so that the network equipment can be managed by the NMS with different authority. To remove the community name and its access authority, run the command **no snmp-server community** in the global mode.

25.2.2 Configuring MIB Views and Groups

You can decide whether a MIB object allowed by a SNMP view or not through the access-control model based on SNMP view, only the MIB objects allowed by the SNMP view can be accessed. For accessing control, we always specify a user to associate with a SNMP group, the associate the SNMP group with a SNMP view. Any user in the same SNMP group has the same access authority.

- Including view and excluding view can be set.
- Read only view and writable view can be set for a group of users.
- For the SNMPv3 users, it is possible to specify the safety level and whether the authentication or encryption is necessary.

To configure the MIB views and groups, run the following commands in the global configuration mode:

Command	Function
DGS-3610(config)# **snmp-server view** *view-name oid-tree* {**include | exclude**}	Create an MIB view to including or excluding associated MIB objects.
DGS-3610(config)# **snmp-server group** *groupname* {**v1** | **v2c** |**v3** {**auth** | **noauth** | **priv**}} [**read** *readview*] [**write** *writeview*] [**access** {*num* | *name*}]	Create a group and associate it with the view.

You can delete a view by using the **no snmp-server view** *view-name* command, or delete a sub-tree from the view by using the **no snmp-server view** *view-name oid-tree* command. You can also delete a group by using the **no snmp-server group** *groupname* command.

25.2.3 Configuring SNMP Users

You can implement the security management through the security model user based, first the user information should be configured for the management user based . Only valid users of NMS can communicate with the SNMP agent.

For the SNMPv3 users, specify the security level, authentication algorithm (MD5 or SHA), authentication password, encryption algorithm (only DES now) and encryption password.

To configure the SNMP user, run the following commands in the global configuration mode:

Command	Function
DGS-3610(config)# **snmp-server user** *username roupname* {**v1 | v2 | v3** [**encrypted**] [**auth** { **md5|sha** } *auth-password*] [**priv des56** *priv-password*] }	Set the information for the user.

To remove the specified user, the **no snmp-server user** *username groupname* command can be used.

25.2.4 Configuring SNMP Host Address

In special cases, Agent may actively send messages to NMS. To configure NMS host address that the Agent actively sends messages to, execute the following commands in the global configuration mode:

Command	**Function**
DGS-3610(config)# **snmp-server host** *host-addr* **traps** [**vrf** *vrfname*] [**version {1|2c |3 [auth | noauth | priv**]} *community-string [udp-port port-num] [***type***]*	Set the address of SNMP host, host port, message type, community string (user name in SNMPv3) and security level (supported only be SNMPv3).

25.2.5 Configuring SNMP Agent Parameters

You can configure the basic parameters for the Agent of SNMP, including the contact method of the device, location and sequential number. The NMS gets to know the contact, location and more information of the device by accessing those parameters of the device.

To configure the SNMP agent parameters, run the following commands in the global configuration mode:

Command	**Function**
DGS-3610(config)# **snmp-server contact** *text*	Configure the contact method of the system
DGS-3610(config)# **snmp-server location** *text*	Configure the location of the system
DGS-3610(config)# **snmp-server chassis-id** *number*	Configure the sequential number of the system

25.2.6 Defining Maximum Packet Length of SNMP Agent

In order to reduce the impact on the bandwidth, user can configure the maximum size of packet allowed by SNMP agent. Run the following command in the global configuration mode:

Command	**Function**
DGS-3610(config)# **snmp-server packetsize** *byte-count*	Set the maximum size of packet allowed by SNMP agent.

25.2.7 Shielding SNMP Agent

The SNMP agent service is a service provided by the product of our company. It's enabled by default. When the agent service is not required, the snmp agent unction and related configuration information can be shielded through running following steps; To shield the snmp agent function, perform the following command in the global configuration mode:

Command	Function
DGS-3610(config)# **no snmp-server**	Shield the SNMP agent service.

25.2.8 Disable SNMP Agent

Our product provides a different command from the shield command to disable the SNMP agent. This command will act on all of the SNMP services instead of shielding the configuration information for the agent. To disable the SNMP agent service, run the following command in the global configuration mode:

Command	Function
DGS-3610(config)# **no enable service snmp-agent**	Disable the SNMP agent service.

25.2.9 Configuring Agent to Send Trap to NMS Initiatively

Trap is the message automatically sent by Agent to NMS unsolicited, and is used to report some urgent and important events. By default it is not allowed for Agent to send Traps. To enable it, run the following command in the global configuration mode:

Command	Function
DGS-3610(config)# **snmp-server enable traps** [*type*] [*option*]	Allow Agent to sent trap initiatively.
DGS-3610(config)# **no snmp-server enable traps** [*type*] [*option*]	Forbid Agent to sent trap initiatively.

25.2.10 Configuration of Link Trap Policy

Whether to send the LinkTrap for the interface can be configured according to the interface in the equipment. When this function is enabled, if the Link status of the interface changes, the SNMP will send out the LinkTrap. Otherwise, it will not send. By default, this function is enabled.

Command	Function
DGS-3610(config)# **interface** *interface-id*	Enter the interface configuration mode.

Command	Function
DGS-3610(config-if)# **no snmp-server enable traps**	Enable or disable the function to send the link trap for the interface.

No link trap will be sent for the interface according to the following configuration.

```
DGS-3610(config)# interface gigabitEthernet 1/1
DGS-3610(config-if)# no snmp trap link-status
```

25.2.11 Configuring Message Sending Operation Parameters

It is possible to specify the parameters for Agent to send Trap messages by executing the following commands:

Command	Function
DGS-3610(config)# **snmp-server trap-source** *interface*	Specify the source interface for sending Trap messages.
DGS-3610(config)# **snmp-server queue-length** *length*	Specify the length of each Trap message queue.
DGS-3610(config)# **snmp-server trap-timeout** *seconds*	Specify the interval for sending Trap messages.

25.3 SNMP Monitoring and Maintenance

25.3.1 Checking Current SNMP Status

To monitor the SNMP status and troubleshoot SNMP configurations, our product provides the monitoring commands for SNMP, with which it is possible to easily view the SNMP status of the current network device. In the privileged user mode, execute **show snmp** to view the current SNMP status.

```
DGS-3610# show snmp
Chassis: 1234567890 0987654321
Contact: wugb@i-net.com.cn
Location: fuzhou
2381 SNMP packets input
5 Bad SNMP version errors
6 Unknown community name
0 Illegal operation for community name supplied
0 Encoding errors
9325 Number of requested variables
0 Number of altered variables
31 Get-request PDUs
2339 Get-next PDUs
```

```
0 Set-request PDUs
2406 SNMP packets output
0 Too big errors (Maximum packet size 1500)
4 No such name errors
0 Bad values errors
0 General errors
2370 Get-response PDUs
36 SNMP trap PDUs
SNMP global trap: disabled
SNMP logging: enabled
SNMP agent: enabled
```

The above statistical messages are explained as follows:

Showing Information	Description
Bad SNMP version errors	SNMP version is incorrect
Unknown community name	The community name is not known
Illegal operation for community name supplied	Illegal operation
Encoding errors	Code error
Get-request PDUs	Get-request packet
Get-next PDUs	Get-next packet
Set-request PDUs	Set-request packet
Too big errors (Maximum packet size 1500)	Too large response packet
No such name errors	No specified managed unit existed
Bad values errors	Wrong value type specified
General errors	General error
Get-response PDUs	Get-response packet
SNMP trap PDUs	SNMP trap packet

25.3.2 Checking MIB Objects Supported by Current SNMP Agent

To check the MIB objects supported by the current agent, run the command **show snmp mib** in the privileged user mode:

```
DGS-3610# show snmp mib
sysDescr
sysObjectID
sysUpTime
sysContact
sysName
sysLocation
sysServices
sysORLastChange
snmpInPkts
```

```
snmpOutPkts
snmpInBadVersions
snmpInBadCommunityNames
snmpInBadCommunityUses
snmpInASNParseErrs
snmpInTooBigs
snmpInNoSuchNames
snmpInBadValues
snmpInReadOnlys
snmpInGenErrs
snmpInTotalReqVars
snmpInTotalSetVars
snmpInGetRequests
snmpInGetNexts
snmpInSetRequests
snmpInGetResponses
snmpInTraps
snmpOutTooBigs
snmpOutNoSuchNames
snmpOutBadValues
snmpOutGenErrs
snmpOutGetRequests
snmpOutGetNexts
snmpOutSetRequests
snmpOutGetResponses
snmpOutTraps
snmpEnableAuthenTraps
snmpSilentDrops
snmpProxyDrops
entPhysicalEntry
entPhysicalEntry.entPhysicalIndex
entPhysicalEntry.entPhysicalDescr
entPhysicalEntry.entPhysicalVendorType
entPhysicalEntry.entPhysicalContainedIn
entPhysicalEntry.entPhysicalClass
entPhysicalEntry.entPhysicalParentRelPos
entPhysicalEntry.entPhysicalName
entPhysicalEntry.entPhysicalHardwareRev
entPhysicalEntry.entPhysicalFirmwareRev
entPhysicalEntry.entPhysicalSoftwareRev
entPhysicalEntry.entPhysicalSerialNum
entPhysicalEntry.entPhysicalMfgName
entPhysicalEntry.entPhysicalModelName
entPhysicalEntry.entPhysicalAlias
entPhysicalEntry.entPhysicalAssetID
entPhysicalEntry.entPhysicalIsFRU
entPhysicalContainsEntry
entPhysicalContainsEntry.entPhysicalChildIndex
entLastChangeTime
```

25.3.3 Viewing SNMP User

To view the SNMP users configured on the current agent, run the command **show snmp user** in the privileged user mode:

```
DGS-3610# show snmp user
User name: test
Engine ID: 8000131103000000000000
storage-type: permanent    active
Security level: auth priv
Auth protocol: SHA
Priv protocol: DES
Group-name: g1
```

25.3.4 Viewing SNMP View and Group

To view the group configured on the current agent, run the command **show snmp group** in the privileged user mode:

```
DGS-3610# show snmp group
groupname: g1
securityModel: v3
securityLevel:authPriv
readview: default
writeview: default
notifyview:
groupname: public
securityModel: v1
securityLevel:noAuthNoPriv
readview: default
writeview: default
notifyview:
groupname: public
securityModel: v2c
securityLevel:noAuthNoPriv
readview: default
writeview: default
notifyview:
```

To view the view configured on the current agent, run the command **show snmp view** in the privileged user mode:

```
DGS-3610# show snmp view
default(include) 1.3.6.1
test-view(include) 1.3.6.1.2.1
```

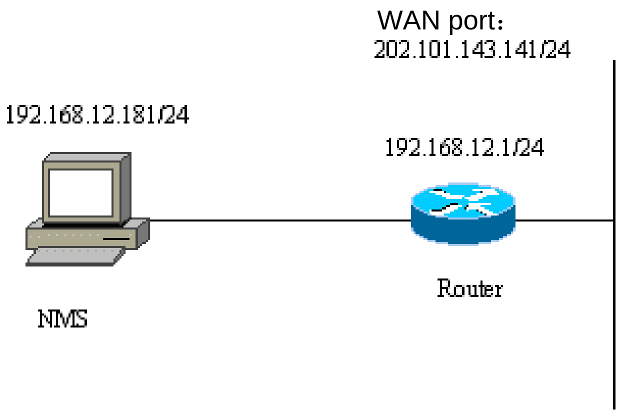
25.4 SNMP Configuration Example

- **Configuration requirement**

In the figure, the router is connected with the network management station (NMS) via the Ethernet. The IP addresses of NMS and the router are 192.168.12.181 and 192.168.12.1

respectively. A network management software (taking HP OpenView as an example) is running on the NMS.

Figure 25-4 Typical Networking Diagram of SNMP



- **Detailed configuration of the network device**

Enable the SNMP agent service:

```
DGS-3610(config)# snmp-server community public RO
```

As long as the above command is configured in the global configuration mode, the SNMP agent service is enabled on the network device, and then the NMS can monitor the SNMP for the network device. However, just read-only authority is configured; the NMS can not modify the router's configuration but monitor its running. Other configurations are optional.

If the read-write function is required, it can be configured as follows:

```
DGS-3610(config)# snmp-server community private RW
```

Followings are basic agent parameters to configure the SNMP of network device. The NMS can get basic system information of the router via these parameters. This configuration is optional:

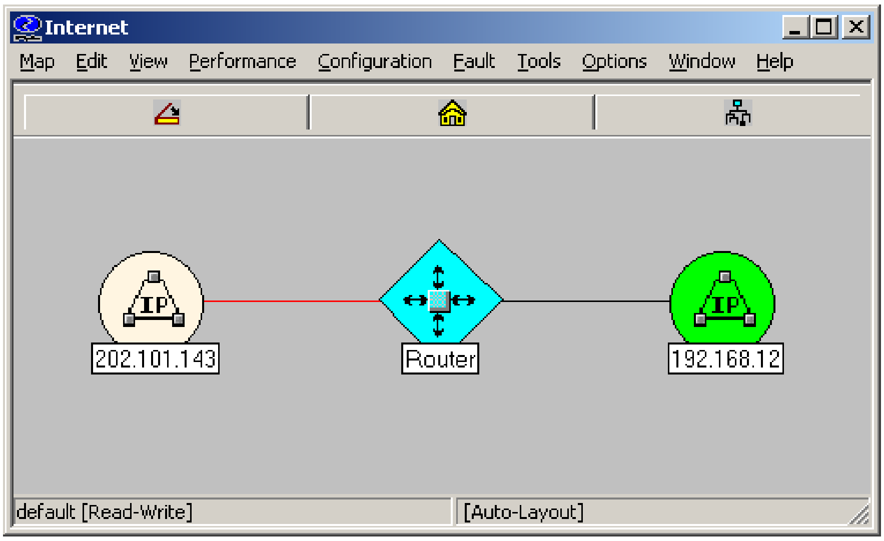
```
DGS-3610(config)# snmp-server location fuzhou
DGS-3610(config)# snmp-server contact wugb@i-net.com.cn
DGS-3610(config)# snmp-server chassis-id 1234567890
0987654321
```

The following configuration is optional; the network device is allowed to send some Trap messages to the NMS proactively.

```
DGS-3610(config)# snmp-server enable traps
DGS-3610(config)# snmp-server host 192.168.12.181 public
```

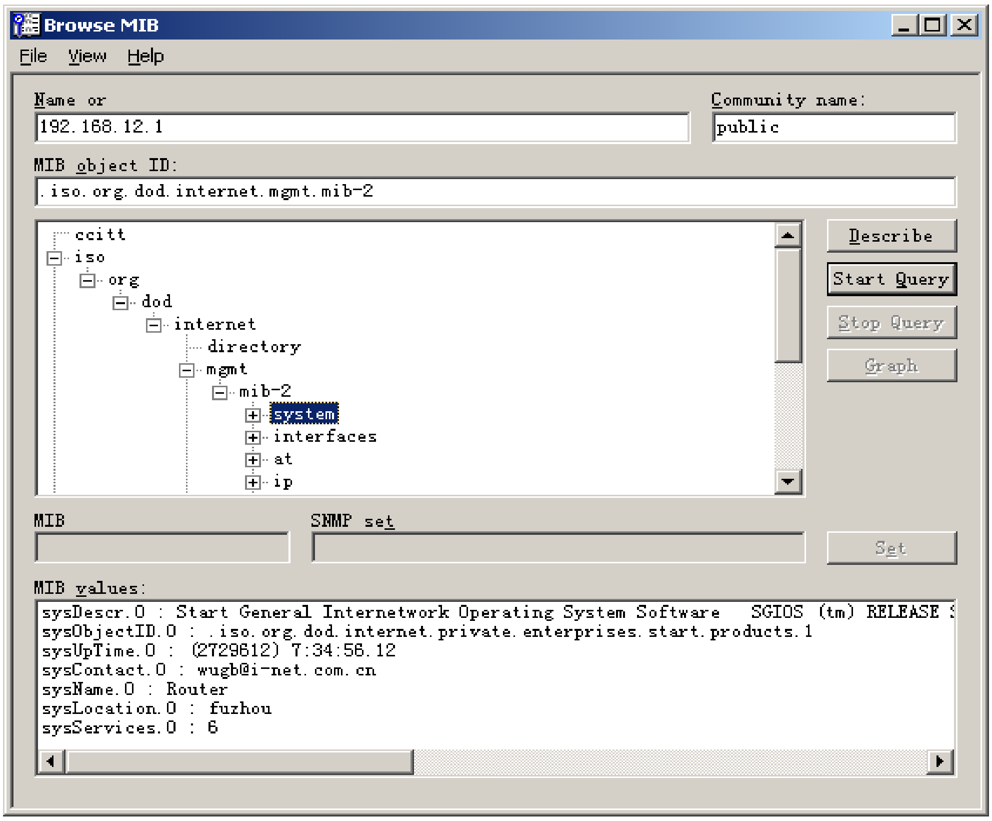
The SNMP agent is configured for the router by the above configuration. Then, the NMS can monitor and manage the router. Take HP OpenView as an example and a network topology is coming into being as follows:

Figure 25-5 Network topology diagram



Now it is possible to query or set the managed units in the network device. Click the TOOL->SNMP MIB Brower menu on the HP OpenView to display the following dialog box. Enter the IP address 192.168.12.1 in the Name field, and input **public** in the Community Name field. Select the specific managed unit of the MIB, such as the **system** in the diagram below. Click Start Query to initiate MIB query for the network device. The results are displayed in the MIB Values pane of the dialog box.

Figure 25-6 Interface of MIB query



Name or: 192. 168. 12. 1

Community name: public

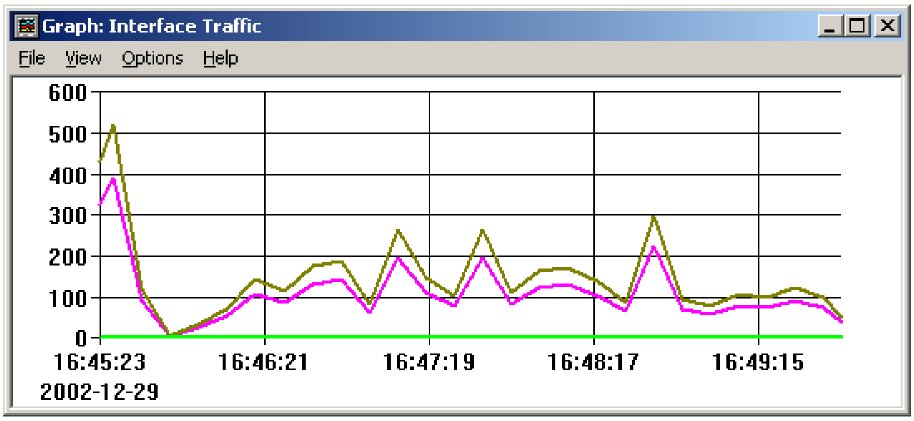
MIB object ID: . iso. org. dod. internet. mgmt. mib-2

MIB values:

```
sysDescr.0 : Start General Internetwork Operating System Software   SGIOS (tm) RELEASE S
sysObjectID.0 : .iso.org.dod.internet.private.enterprises.start.products.1
sysUpTime.0 :  (2729612) 7:34:56.12
sysContact.0 : wugb@i-net.com.cn
sysName.0 : Router
sysLocation.0 : fuzhou
sysServices.0 : 6
```

HP OpenView has powerful function for the network management. For example, the traffic statistics of network interface can be expressed in the form of graph. For the other functions of SNMP, see the document of network management software.

Figure 25-7 Statistics graph of interface traffic



25.4.2 Example of SNMP Access List Association Control

DGS-3610 series allows the setting of access list association mode. Only the NMS allowed in the access list can monitor and manage Agent through SNMP. This may limit NMS's accesses to the network device and improve the SNMP security.

In the global configuration mode:

```
DGS-3610(config)# access-list 1 permit 192.168.12.181
DGS-3610(config)# snmp-server community public RO 1
```

Now, only the host with IP address 192.168.12.181 can monitor and manage network devices through SNMP.

25.4.3 SNMPv3 Related Configuration Examples

The following configuration allows the SNMPv3 manager to set and view the management variables under the MIB-2 (1.3.6.1.2.1) by using the v3user as the user name through the authentication + encryption mode. The MD5 is used as the encryption method and the MD5-Auth is used as the authentication password. The DES is used for encryption and the encryption key is Des-Priv. Meantime, it is allowed to send Trap to 192.168.65.199 in the format of SNMPv3. Use v3user as the user name to send Trap in the mode of authentication and encryption. The authentication method is MD5 and the authentication password is MD5-Auth. The DES is used for encryption and the encryption key is Des-Priv.

```
DGS-3610(config)# snmp-server view v3userview 1.3.6.1.2.1 include
DGS-3610(config)# snmp-server group v3usergroup v3 priv read v3userview write v3userview
DGS-3610(config)# snmp-server user v3user v3usergroup v3 auth md5 md5-auth priv des56
des-priv
```

```
DGS-3610(config)# snmp-server host 192.168.65.199 traps version 3 priv v3user
```

26 Configuration of RMON

26.1 Overview

RMON (Remote Monitoring) is a standard monitoring specification of IETF (Internet Engineering Task Force). It can be used to exchange the network monitoring data among various network monitors and console systems. In the RMON, detectors can be placed on the network nodes, and the NMS determines which information is reported by these detectors, for example, the monitored statistics and the time buckets for collecting history. The network device such as the switch or router acts as a node on the network. The information of current node can be monitored by means of the RMON.

There are three stages in the development of RMON. The first stage is the remote monitoring of Ethernet. In the second stage introduces the token ring which is referred to as the token ring remote monitoring module. The third stage is known as RMON2, which develops the RMON to a high level of protocol monitor.

The first stage of RMON (known as RMON1) contains nine groups. All of them are optional (not mandatory), but some groups should be supported by the other groups.

The switch implements the contents of Group 1, 2 , 3 and 9: the statistics, history, alarm and event.

26.1.1 Statistics

Statistics is the first group in RMON. It measures the basic statistics information of each monitored subnet. At present, only the Ethernet interfaces of network devices can be monitored and measured.This group contains a statistics of Ethernet, including the discarded packets, broadcast packets, CRC errors, size block, conflicts and etc.

26.1.2 History

History is the second group in RMON. It collects the network statistics information regularly and keeps them for processing later on. This group contains two subgroups:

1. The subgroup HistoryControl is used to set such control information as sampling time interval and sampling data source.
2. The subgroup EthernetHistory provides history data about the network section, error packets, broadcast packets, utilization, number of collision and other statistics for the administrator.

26.1.3 Alarm

Alarm is the third group in RMON. It monitors a specific management information base (MIB) object at the specified interval. When the value of this MIB object is higher than the predefined upper limit or lower than the predefined lower limit, an alarm will be triggered. The alarm is handled as an event by means of recording the log or sending SNMP Trap.

26.1.4 Event

Event is the ninth group in RMON. It determines to generate a log entry or a SNMP Trap when an event is generated due to alarms.

26.2 List of RMON Configuration Tasks

26.2.1 Configuring Statistics

One of these commands can be used to add a statistic entry.

Command	Function
DGS-3610(config-if)# **rmon collection stats** *index* [**owner** *ownername*]	Add a statistic entry.
DGS-3610(config-if)# **no rmon collection stats** *index*	Remove a statistic entry.

Caution The current version of our product supports only the statistics of Ethernet interface. The index value should be an integer between 1-65535. At present, at most 100 statistic entries can be configured at the same time.

26.2.2 Configuring History Control

One of these commands can be used to add an entry for history control.

Command	Function
DGS-3610(config-if)# **rmon collection history** *index* [**owner** *ownername*] [**buckets** *bucket-number*] [**interval** *seconds*]	Add an entry of history control.
DGS-3610(config-if)# **no rmon collection history** ***i****ndex*	Remove an entry of history control.

Caution The current version of our product supports only the records of Ethernet. The index value should be within 1-65535. At most 10 control entry can be configured.

Bucket-number: the control entry specifies the used data source and time interval. Each sampling interval should be sampled once. The sampling results are saved. The Bucket-number specifies the maximum number of sampling. When the maximum is reached for the sampling records, the new one will overwrite the earliest one. The value range of Bucket-number is 1-65535. Its default value is 10.

Interval: the time interval of sampling. Its default value is 1800 seconds, and its value range is 1-3600.

26.2.3 Configuring Alarm and Event

One of these command can be used to configure the alarm form:

Command	Function
DGS-3610(config)# **rmon alarm** *number variable interval* {**absolute | delta**} **rising-threshold** *value* [*event-number*] **falling-threshold** *value* [*event-number*] [**owner** *ownername*]	Add an entry of history control.
DGS-3610(config)# **rmon event** *number* [**log**] [**trap** *community*] [**description** *description-string*]	Add an entry of Event.
DGS-3610(config)# **no rmon alarm** *number*	Remove an alarm.
DGS-3610(config)# **no rmon event** *number*	Remove an event.

Number: the index of alarm form (event form) with the range of 1-65535.

Variable: the variable monitored by the alarm form. The variable must be an integer.

Interval: the time interval of sampling. Its range is 1-4294967295.

The keyword Absolute indicates each sampling value compared with the high and low limits. The keyword Delta indicates the difference with previous sampling value compared with the high and low limits.

Value defines the values of high limit and low limit.

Event-number: when the value exceeds the high or low limit, the event with the index of Event-number will be triggered.

The keyword Log indicates the action triggered by the event is to record the event.

The keyword Trap indicates the action is to send the Trap message to the NMS when the event is triggered.

Community: the community name when sending the Trap.

description-string: the description of the event.

26.2.4 Showing RMON status

Command	**Function**
DGS-3610(config)# **show rmon alarms**	Show the Alarm
DGS-3610(config)# **show rmon events**	Show the Event
DGS-3610(config)# **show rmon history**	Show the History
DGS-3610(config)# **show rmon statistics**	Show the Statistics

26.3 RMON Configuration Examples

26.3.1 Example of Configuring Statistics

If you want to get the statistics of Ethernet Port 3 , use the following commands:

```
DGS-3610(config)# interface gigabitEthernet 0/3
DGS-3610(config-if)# rmon collection stats 1 owner zhangsan
```

26.3.2 Example of Configuring History

Use the following commands if you want to get the statistics of Ethernet Port 3 every 10 minutes:

```
DGS-3610(config)# interface gigabitEthernet 0/3
DGS-3610(config-if)# rmon collection history 1 owner zhangsan interval 600
```

26.3.3 Example of Configuring Alarm and Event

For example, you want to configure the alarm function for a statistical MIB variable. The following example shows you how to set the alarm function to the instance ifInNUcastPkts.6 (number of non-unicast frames received on port 6; the ID of the instance is 1.3.6.1.2.1.2.2.1.12.6) in **IfEntry** table of MIB-II. The specific function is as follows: the switch checks the changes to the number of non-unicast frames received on port 6 every 30 seconds. If 20 or more than 20 non-unicast frames are added than last check (30 seconds earlier), or only 10 or less than 10 are added, the alarm will be triggered, and event 1 is triggered to do corresponding operations (record it into the log and send the Trap with "community" name as "rmon"). The "description" of the event is "ifInNUcastPkts is too much"). The "owner" of the alarm and the event entry is "zhangsan".

```
DGS-3610(config)# rmon alarm 10 1.3.6.1.2.1.2.2.1.12.6 30 delta rising-threshold 20 1
falling-threshold 10 1 owner zhangsan
DGS-3610(config)# rmon event 1 log trap rmon description "ifInNUcastPkts is too much "
owner zhangsan
```

26.3.4 Example of Showing rmon Status

26.3.4.1 show rmon alarms

```
DGS-3610# show rmon alarms
Alarm : 1
Interval : 1
Variable : 1.3.6.1.2.1.4.2.0
Sample type : absolute
Last value : 64
Startup alarm : 3
Rising threshold : 10
Falling threshold : 22
Rising event : 0
Falling event : 0
Owner : zhangsan
```

26.3.4.2 show rmon events

```
DGS-3610# show rmon events
Event : 1
Description : firstevent
Event type : log-and-trap
Community : public
Last time sent : 0d:0h:0m:0s
Owner : zhangsan
Log : 1
Log time : 0d:0h:37m:47s
Log description : ipttl
Log : 2
Log time : 0d:0h:38m:56s
Log description : ipttl
```

26.3.4.3 show rmon history

```
DGS-3610# show rmon history
Entry : 1
Data source : Gi1/1
Buckets requested : 65535
Buckets granted : 10
Interval : 1
Owner : zhangsan
Sample : 198
Interval start : 0d:0h:15m:0s
DropEvents : 0
Octets : 67988
```

```
Pkts : 726
BroadcastPkts : 502
MulticastPkts : 189
CRCAlignErrors : 0
UndersizePkts : 0
OversizePkts : 0
Fragments : 0
Jabbers : 0
Collisions : 0
Utilization : 0
```

26.3.4.4 show rmon statistics

```
DGS-3610# show rmon statistics
Statistics : 1
Data source : Gi1/1
DropEvents : 0
Octets : 1884085
Pkts : 3096
BroadcastPkts : 161
MulticastPkts : 97
CRCAlignErrors : 0
UndersizePkts : 0
OversizePkts : 1200
Fragments : 0
Jabbers : 0
Collisions : 0
Pkts64Octets : 128
Pkts65to127Octets : 336
Pkts128to255Octets : 229
Pkts256to511Octets : 3
Pkts512to1023Octets : 0
Pkts1024to1518Octets : 1200
Owner : zhangsan
```

27 RIP Routing Protocol Configuration

27.1 RIP Overview

The RIP (Routing Information Protocol) is a relatively old routing protocol, which is widely used in small or homogeneous networks. The RIP uses the distance-vector algorithm, and so is a distance-vector protocol. The RIP is defined in the RFC 1058 document.

The RIP exchanges the routing information by using the UDP packets, with the UDP port number to be 520. Usually, the RIPv1 packets are broadcast packets, while the RIPv2 packets are multicast packets, with the multicast addresses to be 224.0.0.9. The RIP sends update packets at the intervals of 30 seconds. If the router does not receive the route update packets from the other end within 180 seconds, it will mark all the routes from that router as unreachable. If the router still does not receive the update packets within 120 seconds, it will delete such routes from the routing table.

The RIP measures the distance to the destination in hops, know as route metrics. In the RIP, the router has zero hop to the network to which it is directly connected. The network that is reachable by one router is one hop away, and so on. The unreachable networks have hops of 16.

The device that runs the RIP routing protocol can learn the default routes from the neighbors or generate their own default routes. When any of the following condition is met, the DGS-3610 series will generate the default route and advertise it to the neighbor router:

- IP Default-network is configured.
- The default routes or static default routes learnt by the routing protocol are incorporated into the RIP routing protocols.

The RIP will send the update packets to the port of the specified network. If the network is not associated with the RIP routing process, the interface will not be notified to any update packets. The RIP is available in two versions: RIPv1 and RIPv2. The RIPv2 supports plain-text authentication, MD5 cryptographic text and variable length subnet mask.

To avoid a loop route, the RIP uses the following means:

- Split Horizon
- Poison Reverse
- Holddown time

For other feature applications of the RIP, see the *IP Routing “Protocol Independent” Feature Configuration* chapter.

27.2 RIP Configuration Task List

To configure the RIP, perform the following tasks. The first two tasks are required, while other tasks are optional. You should determine whether to perform the optional tasks according to your specific needs.

- Create the RIP routing process (required)
- Configuring Packet Unicast for the RIP (required)
- Configuring Split Horizon (optional)
- Defining the RIP Version (optional)
- Disable automatic route convergence (optional)
- Adjusting the RIP Timer (optional)
- Configuring the RIP Route Source Address Verification (optional)
- Control of RIP interface status (optional)

For the following topics, see the *IP Routing “Protocol Independent” Feature Configuration* chapter.

- Filtering the RIP route information
- VLSMs (for RIPv2)

27.2.1 Create the RIP routing process

For the router to run the RIP, you must first create the RIP routing process and define the network associated with the RIP routing process.

To create the RIP routing process, execute the following commands in the global configuration mode:

Command	Function
DGS-3610(config)# **router rip**	Create the RIP routing process
DGS-3610(config-router)# **network** *network-number*	Define the associated network

Note

There are two meanings for the associated network defined by the command Network:

1. RIP only notifies the router information of associated network to the outside.
2. RIP only notifies the router information to the interfaces belonging to the associated network.

27.2.2 Configuration of Packet Unicast for the RIP

The RIP is usually a broadcast protocol. If the RIP routing information needs to be transmitted via the non-broadcast networks, you need to configure the router so that it supports the RIP to advertise the route update packets via unicast.

To configure the packet update notification via unicast for the RIP, execute the following commands in the RIP routing process configuration mode:

Command	Function
DGS-3610(conf-router)# **neighbor** *ip-address*	Configure the packet unicast notification for the RIP

By using this command, you can also control which port is allowed to notify the RIP route update packets, restrict a interface from notifying the broadcast route update packets. You need to configure the **passive-interface** command in the routing process configuration mode. For the related description about the route information advertisement restriction, see the "*Route Filtering Configuration*" section in the *IP Routing Protocol Independent Feature Configuration* chapter.

Note

When you configure the FR and X.25, if the address mapping has specified the Broadcast keyword, you do not need to configure the **neighbor**. The function of the **Neighbor** command is largely reflected in reducing broadcast packets and route filtering.

27.2.3 Configuration of Split Horizon

When multiple devices are connected to the IP broadcast type network and the distance-vector routing protocol is run, the split horizon mechanism must be used to avoid loop routes. Split horizon can prevent the router from advertising some route information to the port from which it learns such information. This behavior optimizes the route information exchange between multiple routers.

However, split horizon may cause the failure of some routers to learn all the routes, for a non-broadcast multi-access network (for example, frame relay, X.25 network). In this case, you may need to disable split horizon. If a port is configured with an IP address, you also need to pay attention to the split horizon problem.

To enable or disable split horizon, execute the following commands in the interface configuration mode:

Command	Function
DGS-3610(config-if)# **no ip split-horizon**	Disable split horizon

Command	**Function**
DGS-3610(config-if)# **ip split-horizon**	Enable split horizon

The default of all the interface are configured as enabling split horizon.

27.2.4 Defining the RIP Version

Our product supports RIP version 1 and version 2, where RIPv2 supports authentication, key management, route convergence, CIDR and VLSMs. For the information about the key management and VLSMs, see the *IP Routing "Protocol Independent" Feature Configuration* chapter.

By default, our product can receive RIPv1 and RIPv2 packets, but it can only send RIPv1 packets. You can configure to receive and send only the packets of RIPv1 or only those of RIPv2.

To configure the specified version packets to be received and sent, execute the following commands in the routing process configuration mode:

Command	**Function**
DGS-3610(config-router)# **version** {**1** | **2**}	Defining the RIP Version

The above command allows the software to only receive or send the packets of the specified version. If needed, you can modify the default behavior of every port.

To configure a port to send the packets of only a specified version, execute the following commands in the interface configuration mode:

Command	**Function**
DGS-3610(config-if)# **ip rip send version 1**	Specify the packets only send the RIPv1
DGS-3610(config-if)# **ip rip send version 2**	Specify the packets only send the RIPv2
DGS-3610(config-if)# **ip rip send version 1 2**	Specify the packets only send the RIPv1 and RIPv2

To configure a interface to receive the packets of which version, execute the following commands in the interface configuration mode:

Command	**Function**
DGS-3610(config-if)# **ip rip receive version 1**	Specify the packets only receive the RIPv1
DGS-3610(config-if)# **ip rip receive version 2**	Specify the packets only receive the RIPv2
DGS-3610(config-if)# **ip rip receive version 1 2**	Specify the packets only receive the RIPv1 and RIPv2

27.2.5 Disable automatic route summary

The automatic route summary of the RIP is the process to automatically summarize them into classful network routers when subnet routes pass through classful network borders. By default, the RIPv2 will automatically perform route summary, while the RIPv1 does not support this feature.

The automatic route summary function of the RIPv2 enhances the scalability and effectiveness of the network. If there are any summarized routes, the sub-routes contained in them cannot be seen in the routing table. This greatly reduces the size of the routing table.

It is more efficient to advertise the summarized routes than the separate routes. There are the following factors:

- In looking up the RIP database, the summarized routes will receive preferential treatment;
- In looking up the RIP database, any sub-routes will be ignored, thus reducing the processing time.

Sometimes, you want to learn the specific sub-net routes, rather than only see the summarized network routers, you should disable the automatic route summary function.

To configure automatic route summary, execute the following commands in the RIP routing process mode:

Command	Function
DGS-3610(config-router)# **no auto-summary**	Disable automatic route summary
DGS-3610(config-router)# **auto-summary**	Enable automatic route summary

After disabling the automatic summary, the interface-level summary can be configured. Execute following commands to configure the address and sub-net route summary under certain interface:

Command	Function
DGS-3610(config-if)# **ip summary-address rip** *ip-address ip-network-mask*	Configure the interface-level route summary
DGS-3610(config-if)# **no ip summary-address rip** *ip-address ip-network-mask*	Cancel the interface-level route summary

27.2.6 Configuring RIP Authentication

The RIPv1 does not support authentication. If the device is configured with the RIPv2 routing protocol, you can configure authentication at the appropriate interface.

The key chain defines the set of the keys that can be used by the interface. If no key chain is configured, no authentication will be performed even if a key chain is applied to the interface.

Oure product supports two RIP authentication modes: plain-text authentication and MD5 authentication. The default is plain-text authentication.

To configure RIP authentication, execute the following commands in the interface configuration mode:

Command	**Function**
DGS-3610(config-if)# **ip rip authentication key-chain** *key-chain-name*	Apply the key chain and enable RIP authentication
DGS-3610(config-if)# **ip rip authentication mode** {**text** | **md5**}	Configure the RIP authentication for the interface Mode: plain-text or MD5

27.2.7 Adjusting the RIP Timer

The RIP provides the timer adjustment function, which allows you to adjust the timer so that the RIP routing protocol can run in a better way. You can adjust the following timers:

Route update timer: It defines the intervals in seconds at which the router sends the update packets;

Route invalid timer: It defines the time in seconds after which the routes in the routing table will become invalid if not updated;

Route clearing timer: It defines the time in seconds after which the routes in the routing table will be cleared from the routing table;

By adjusting the above timers, you can accelerate the summary and fault recovery of the routing protocol. To adjust the RIP timers, execute the following commands in the RIP routing process configuration mode:

Command	**Function**
DGS-3610(config-router)# **timers basic** *update invalid flush*	Adjust the RIP timers

By default, the update interval is 30 seconds, the invalid period is 180 seconds, and the clearing (flush) period is 120 seconds.

Note

The routers connected in the same network must have the same RIP timers.

27.2.8 Configuring the RIP Route Source Address Validation

By default, the RIP will validate the source addresses of the incoming route update packets. If the source address of a packet is invalid, the RIP will discard that packet. Determining the validity of the source address is determine if the source IP address is on the same network as the IP address of the interface. No validation will be performed if the IP address interface is not numbered.

To configure route source address validation, execute the following commands in the RIP routing process configuration mode:

Command	**Function**
DGS-3610(config-router)# **no validate-update-source**	Disable source address validation
DGS-3610(config-router)# **validate-update-source**	Enable source address validation

27.2.9 Control of RIP interface status

In some condition, it is necessary to configure the RIP operation flexibly. If you only hope the device to learn the RIP route, but not carry out the RIP route notification, you can configure the passive interface. Or, if you hope to configure the status of some interface individually, you can use the command to control the sending or receiving of the RIP message for specified interface by using the command.

To configure some interface as the passive mode, execute the following command in the RIP route process configuration mode:

Command	**Function**
DGS-3610(config-router)# **passive-interface** {**default** | *interface-type interface-num*}	Configure the passive interface.
DGS-3610(config-router)#**no passive-interface** {**default** | *interface-type interface-num*}	Cancel the passive interface.

Note

After the passive interface receives the RIP request, it will not carry out the response. However, after it receives the non RIP (such as the route diagnosis program) request, it will carry out the message, for these request programs hope to understand the route condition of all devices.

To forbid or allow some interface to receive the RIP packet, execute the following command in the interface configuration mode:

Command	Function
DGS-3610(config-if)# **no ip rip receive enable**	Forbid the interface to receive the RIP packet.
DGS-3610(config-if)# **ip rip receive enable**	Allow the interface to receive the RIP packet.

To disable or allow some interface to receive the RIP message, execute the following command in the interface configuration mode:

Command	Function
DGS-3610(config-if)# **no ip rip send enable**	Forbid the interface to send the RIP message.
DGS-3610(config-if)# **ip rip send enable**	Allow the interface to send the RIP message.

27.3 RIP Configuration Examples

This section provides two RIP configuration examples:

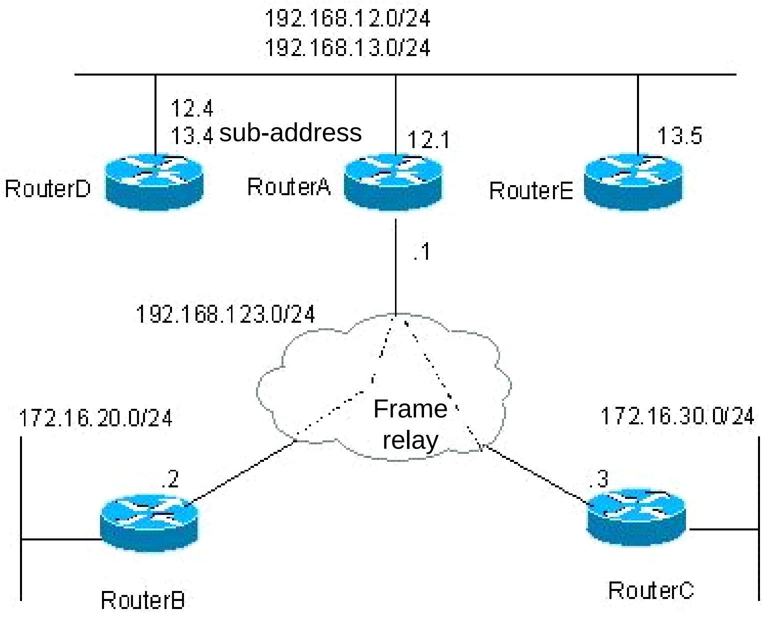
- Example of Configuring Split Horizon
- Example of configuring RIP unicast update packets

27.3.1 Example of Configuring Split Horizon

- **Configuration requirements:**

There are five devices. Where, RouterA, RouterD and RouterE are connected via the Ethernet; RouterA, RouterB and RouterC are connected via the frame relay. Figure 27-1shows IP address distribution and equipment connection, where RouterD is configured with a sub-address.

Figure 27-1 Example of Configuring RIP Split Horizon



The route should be configured to achieve the following purposes: 1) All routers run the RIP routing protocol; 2) RouterB and RouterC can learn the network segment routes advertised; 3) RouterE can learn the routes of the 192.168.12.0/24 network segment.

- **Detailed configuration of devices**

In this example, to achieve the above purposes, RouterA and RouterD must have split horizon disabled. Otherwise, RouterA will not notify the routes advertised by RouterB to RouterC. Neither will RouterD advertise the 192.168.12.0 network segment to RouterE. Detailed configurations of each device are listed as follows.

Configuration of Device A:

# Configuring Ethernet port

```
interface FastEthernet0/0
ip address 192.168.12.1 255.255.255.0
```

# Configure the WAN port

```
interface Serial1/0
ip address 192.168.123.1 255.255.255.0
encapsulation frame-relay
no ip split-horizon
```

# Configuring RIP route protocol

```
router rip
version 2
network 192.168.12.0
network 192.168.123.0
```

Configuration of Device B:

#Configuring Ethernet port

```
interface FastEthernet0/0
ip address 172.16.20.1 255.255.255.0
```

#Configure the WAN port

```
interface Serial1/0
ip address 192.168.123.2 255.255.255.0
encapsulation frame-relay
```

#Configuring RIP route protocol

```
router rip
version 2
network 172.16.0.0
network 192.168.123.0
no auto-summary
```

Configuration of Device C:

# Configuring Ethernet port

```
interface FastEthernet0/0
ip address 172.16.30.1 255.255.255.0
```

# Configure the WAN port

```
interface Serial1/0
ip address 192.168.123.3 255.255.255.0
encapsulation frame-relay
```

# Configuring RIP route protocol

```
router rip
version 2
network 172.16.0.0
network 192.168.123.0
no auto-summary
```

Configuration of Device D:

# Configuring Ethernet port

```
interface FastEthernet0/0
ip address 192.168.12.4 255.255.255.0
ip address 192.168.13.4 255.255.255.0 secondary
no ip split-horizon
```

# Configuring RIP route protocol

```
router rip
version 2
network 192.168.12.0
network 192.168.13.0
```

Configuration of Device E:

# Configuring Ethernet port

```
interface FastEthernet0/0
ip address 192.168.13.5 255.255.255.0
```

# Configuring RIP route protocol

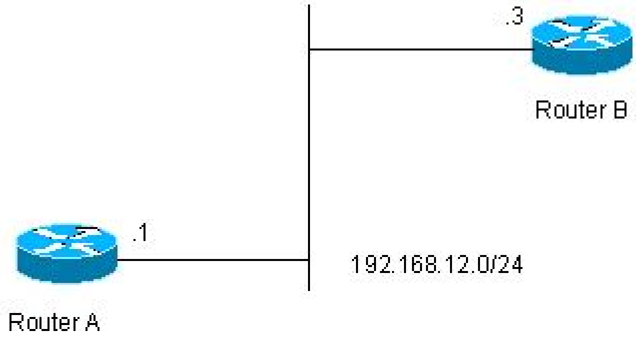
```
router rip
version 2
network 192.168.13.0
```

27.3.2 Example of Configuring RIP Authentication

- **Configuration requirements:**

Two routers are connected via the Ethernet and run the RIP routing protocol, with the MD5 authentication used. The connection diagram of the devices and the assignment of IP addresses are shown in Figure 27-2.

Figure 27-2 Example of Configuring RIP Authentication



Router A must send RIP packets with the authentication key of keya and can receive the RIP packets whose authentication keys are keya and keyb. Router B sends the RIP packets with the authentication key of keyb and can receive the RIP packets of the authentication keys of keya and keyb.

- **Detailed configuration of devices**

Configuration of Device A:

#Configure the key chain

```
key chain ripkey
key 1
key-string keya
accept-lifetime 00:00:00 Dec 3 2000 infinite
send-lifetime 00:00:00 Dec 4 2000 infinite
key 2
```

```
key-string keyb
accept-lifetime 00:00:00 Dec 3 2000 infinite
send-lifetime 00:00:00 Dec 4 2000 infinite
```

# Configuring Ethernet interface

```
interface FastEthernet0/0
ip address 192.168.12.1 255.255.255.0
ip rip authentication mode md5
ip rip authentication key-chain ripkey
```

# Configuring RIP route protocol

```
router rip
version 2
network 192.168.12.0
```

Configuration of Device B:

# Configure the key chain

```
key chain ripkey
key 1
key-string keyb
accept-lifetime 00:00:00 Dec 3 2000 infinite
send-lifetime 00:00:00 Dec 4 2000 00:00:00 Dec 5 2000
key 2
key-string keya
accept-lifetime 00:00:00 Dec 3 2000 infinite
send-lifetime 00:00:00 Dec 4 2000 infinite
```

# Configuring Ethernet port

```
interface FastEthernet0/0
ip address 192.168.12.2 255.255.255.0
ip rip authentication mode md5
ip rip authentication key-chain ripkey
```

# Configuring RIP route protocol

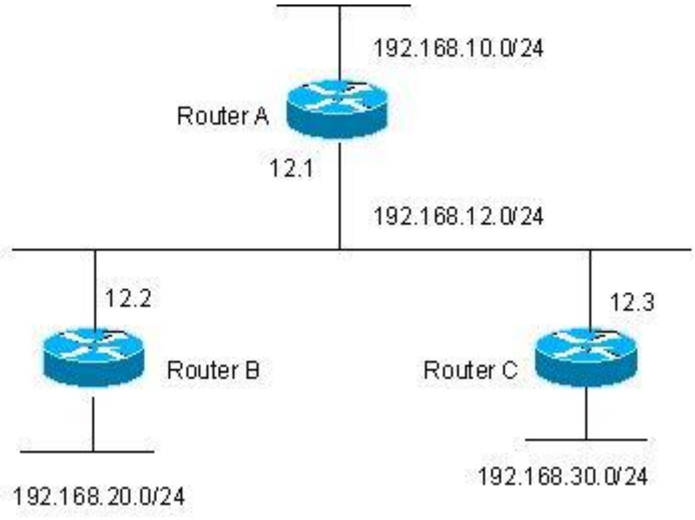
```
router rip
version 2
network 192.168.12.0
```

27.3.3 Example of Configuring Packet Unicast for the RIP

- **Configuration requirements:**

All the three devices are connected on the LAN, and all run the RIP routing protocol. Figure 27-3 shows the IP address allocation and connection of the equipment.

Figure 27-3 Example of Configuring Packet Unicast for the RIP



Following are to be implemented via the configuration of RIP packet unicast:

1. Router A can learn the route of notification from Router C.

2. Router C cannot learn the route of notification from Router A.

- **Detailed configuration of devices**

To achieve the above purposes, RIP packet unicast must be configured at router A.

Configuration of Device A

# Configuring Ethernet port

```
interface FastEthernet0/0
ip address 192.168.12.1 255.255.255.0
```

#Configure the loopback port

```
interface Loopback0
ip address 192.168.10.1 255.255.255.0
```

# Configuring RIP route protocol

```
router rip
version 2
network 192.168.12.0
network 192.168.10.0
passive-interface FastEthernet0/0
neighbor 192.168.12.2
```

Configuration of Device B:

# Configuring Ethernet interface

```
interface FastEthernet0/0
ip address 192.168.12.2 255.255.255.0
```

#Configure the loopback port

```
interface Loopback0
ip address 192.168.20.1 255.255.255.0
```

# Configuring RIP route protocol

```
router rip
version 2
network 192.168.12.0
network 192.168.20.0
```

Configuration of Device C:

# Configuring Ethernet interface

```
interface FastEthernet0/0
ip address 192.168.12.3 255.255.255.0
```

#Configure the loopback port

```
interface Loopback0
ip address 192.168.30.1 255.255.255.0
```

# Configuring RIP route protocol

```
router rip
version 2
network 192.168.12.0
network 192.168.30.0
```

28 OSPF Routing Protocol Configuration

28.1 OSPF Overview

OSPF (Open Shortest Path First) is an internal gateway routing protocol based on link status as developed by IETF OSPF work group. OSPF is a routing protocol specially configured for IP and directly runs on the IP layer. Its protocol number is 89 and it performs OSPF packet switching through multicast, with the multicast address 224.0.0.5 (all OSPF routers) and 224.0.0.6 (specified routers).

The link status algorithm is an algorithm totally different from Huffman vector algorithm (distance vector algorithm). The RIP is a traditional routing protocol that uses the Huffman vector algorithm, while the OSPF routing protocol is the typical implementation of the link status algorithm. Compared with the RIP routing protocol, the OSPF uses a different algorithm, and also introduces the new concepts such as route update authentication, VLSMs, and route summary. Even if the RIPv2 has made great improvements, and can support the features such as route update authentication and VLSM, the RIP protocol still has two fatal weaknesses: 1) small summary speed; 2) limited network size, with the maximum hot count no more than 16. The OSPF is developed to overcome these weaknesses of the RIP so that the IGP can also be adequate for large or complicated network environments.

The OSPF routing protocol establishes and calculates the shortest path of every target network by using the link status algorithm. This algorithm is complicated. The following briefly describes how the status algorithm works:

- In the initialization stage, the device will generate the link status notification, in which includes all link statuses of this router.
- All devices switch the link status information in the multicast way, and each of the devices will copy the received update message of the link status to the local database as well as transmit it to other routers.
- When every router has a complete link status database, the device uses the Dijkstra algorithm to calculate the shortest path tree for all target networks. The results include target network, next-hop address, and cost, which are the key parts of the IP routing table.

If there is no link cost or network change, the OSPF will become quiet. If any changes occur on the network, the OSPF notifies the changes via the link status, but only the changed ones. The devices involved in the changes will have the Dijkstra algorithm run again, with a new shortest path tree created.

A group of devices running the OSPF routing protocol form the autonomous domain system of the OSPF route domain. An autonomous domain system consists of all the routers that are controlled and managed by one organization. Within the autonomous domain system, only one IGP routing protocol is run. However, between multiple such systems, the BGP routing protocol is used for route information exchange. Different autonomous domain systems can use the same IGP routing protocol. If connection to the Internet is needed, every autonomous system needs to request the related organization for the autonomous system number.

When the OSPF route domain is large, the hierarchical structure is usually used. In other words, the OSPF route domain is divided into several areas, which are connected via a backbone area. Every non-backbone area must be directly connected with this backbone area.

There are three roles for the devices in the OSPF routing domain according to their deployment position:

1. Area Internal Routers, all interface networks of this router are of this area;
2. ABR (Area Border Router): The interfaced networks of this device belong at least to two areas, one of which must be the backbone area;
3. ASBR (Autonomous System Boundary Routers): It is the device between which the OSPF route domain exchanges the external route domain.

Our prpduct implements the OSPF by fully complying with the OSPF v2 defined in RFC 2328. The main features of the OSPF implemented by our product are described as below:

- Support the multiple processing, up to 64 OSPF processing running at the same time;
- Support the VRF, It can be run the OSPF based on different VRF;
- Stub area——The definition of the sub area is fully supported;
- Route redistribution——Redistribution among the RIP, ISIS and BGP and the filtering redistribution are implemented;
- Authentication——Supporting plain-text or MD5 authentication between neighbors;
- Virtual links——Supporting virtual links;
- Supporting VLSMs
- Area division
- NSSA (Not So Stubby Area), as defined in RFC 1587;

Caution

Currently, our product does not support the following functions, but will support them in future versions;

OSPF line on-demand support, as defined in RFC 1793;

Function of OSPF Graceful Restart, as defined in RFC 3623 and RFC 4167;

Module of PE-CE OSPF routing in the network of BGP/MPLS VPN, as defined in RFC 4576 and RFC4577;

OSPF fast summary;

28.2 OSPF Configuration Task List

The configuration of OSPF should be cooperated with various devices (including internal devices, area boundary routers and autonomous system boundary routers). When no configuration is performed, the defaults are used for various parameters of the routers. In this case, Both sending and receiving packets do not need authentication, and the interface does not belong to any devision of the autonomous system. When you change the default parameters, you must ensure that the devices have the same configuration settings.

To configure the OSPF, you must perform the following tasks. Among them, activating the OSPF is required, while others are optional, but may be required for particular applications. The steps to configure the OSPF routing protocols are described as below:

- Creating the OSPF routing process (required)
- Configuring the OSPF interface parameters (optional)
- Configuring the OSPF to accommodate different physical networks (optional)
- Configuring the OSPF area parameters (optional)
- Configuring the OSPF NSSA area (optional)
- Configuring the route summary between OSPF areas (optional)
- Configuring route summary when routes are injected to the OSPF (optional)
- Creating the virtual connections (optional)
- Creating the default routes (optional)
- Using the Loopback address as the route ID (optional)
- Changing the OSPF default management distance (optional)
- Configuring the route calculation timer (optional)
- LSA pacing (optional)
- Route selection configuration (optional)
- Configuring whether to check the MTU value when the interface receives the database description packets (optional)
- Configuring to prohibit an interface from sending the OSPF interface parameters (optional)

The default OSPF configuration is shown as below:

Interface parameters	Interface cost: none is preset LSA retransmit interval: 5 seconds. LSA transmit delay: 1 second. hello packet transmit interval : 10 seconds (30 seconds for non-broadcast networks) Failure time of adjacent routers: 4 times the hello interval. Priority: Authentication type: 0 (No authentication). Authentication password: No password specified.
Area	Authentication type : 0 (No authentication). Default cost of summary routing in Stub or NSSA area: 1 Inter-area summary scope: Undefined Stub area: Undefined NSSA: Undefined
Virtual Link	No virtual link is defined. The default parameters of the virtual link are as below: LSA retransmit interval: 5 seconds. LSA transmit delay: 1 second. hello packet interval: 10 seconds. Failure time of adjacent routers: 4 times the hello interval. Authentication type: No authentication. Authentication password: No password specified.
Automatic cost calculation	Enabled;; Default automatic cost is 100Mbps;
Default route generation	Disabled; The default metric will be 1 and the type is type-2.
Default metric **(Default metric)**	The default metric used to redistribute the other routing protocols;
Management Distance	Intra-area route information: 110 Inter-area route information: 110 External route information: 110
Database filter	Disabled. All interfaces can receive the status update message.
Neighbor change log	Enabled
Neighbor	None
Neighbor database filter **Disabled.**	Disabled, outputting LSAs are sent to all the neighbors;

network area **(network area)**	None
Device ID	Undefined; the OSPF protocol does not run by default
Route summarization **(summary-address)**	Undefined
Changing LSAs Group Pacing	240 seconds
Timers shortest path first (SPF)	The time between the receipt of the topology changes and SPF-holdtime: 5 seconds . The least interval between two calculating operations: 10 seconds
Optimal path rule used to calculate the external routes	Adopting the rules defined in RFC1583

28.2.1 Creating the OSPF Routing Process

This is to create the OSPF routing process and define the range of the IP addresses associated with the OSPF routing process and the OSPF area to which these IP addresses belong. The OSPF routing process only sends and receives the OSPF packets at the interface within the IP address range and notifies the link status of the interface to the outside. Currently, we support 64 OSPF routing processes.

To create the OSPF routing process, you can perform the following steps:

Command	Meaning
DGS-3610# **configure terminal**	Enter the global configuration mode.
DGS-3610(config)# **ip routing**	Enable the IP routing (if disabled)
DGS-3610(config)# **router ospf** *process_id*	Enable OSPF and enter OSPF configuration mode.
DGS-3610(config-router)# **network** *address wildcard-mask* **area** *area-id*	Define an IP address range for an area.
DGS-3610(config-router)# **end**	Return to the privileged EXEC mode.
DGS-3610# **show ip protocol**	Display the routing protocol that is running currently.
DGS-3610# **write**	Save the configuration.

To disable the OSPF protocol, use the **no router ospf** [*process-id*] command. The example shows how to enable the OSPF protocol:

```
DGS-3610(config)# router ospf 1
DGS-3610(config-router)# network 192.168.0.0 255.255.255.0 area 0
```

```
DGS-3610(config-router)# end
```

28.2.2 Configuring the OSPF Interface Parameters

The OSPF allows you to change some particular interface parameters. You can set such parameters as needed. It should be noted that some parameters must be set to match those of the adjacent router of the interface. These parameters are set via the ip ospf hello-interval, ip ospf dead-interval, ip ospf authentication, ip ospf authentication-key and ip ospf message-digest-key. When you use these commands, you should make sure that the adjacent routers have the same configuration.

To configure the OSPF interface parameters, execute the following commands in the interface configuration mode:

Command	Meaning
DGS-3610# **configure terminal**	Enter the global configuration mode.
DGS-3610(config)# **ip routing**	Enable the routing function (if disabled)
DGS-3610(config)# **interface** *[interface-id]*	Enter the interface configuration mode.
DGS-3610(config-if)# **ip ospf cost** *cost-value*	(Optional) Define the interface cost
DGS-3610(config)# **ip ospf retransmit-interval** *seconds*	(Optional) Set the link status retransmission interval;
DGS-3610(config)# **ip ospf transmit-delay** *seconds*	(Optional) Set the transmit estimated time for the link status update packets;
DGS-3610(config)# **ip ospf hello-interval** *seconds*	(Optional) Set the sending interval of hello packet. For the nodes of the whole network, this value should be the same.
DGS-3610(config)# **ip ospf dead-interval** *seconds*	(Optional) Set the dead interval for the adjacent device, which must be the same for all the nodes of the entire network;
DGS-3610(config)# **ip ospf priority** *number*	(Optional) The priority is used to select the dispatched devices (DR) and backup dispatched devices (BDR).
DGS-3610(config)# **ip ospf authentication [message-digest | null]**	(Optional) Set the authentication method on the network interface.
DGS-3610(config)# **ip ospf authentication-key** *key*	(Optional) Configure the key for text authentication of the interface
DGS-3610(config-if)#**ip ospf message-digest-key** *keyid* **md5** *key*	(Optional) Configure the key for MD5 authentication of the interface

Command	**Meaning**
DGS-3610(config-if)#**ip ospf database-filter all out**	(Optional) Prevent the interfaces from flooding the LSAs packets. By default, OSPF floods new LSAs over all interfaces in the same area, except the interface on which the LSA arrives.
DGS-3610(config-if)#**End**	Return to the privileged EXEC mode.
DGS-3610#**show ip ospf** [*process-id*] **interface** [*interface-id*]	Display the routing protocol that is running currently.
DGS-3610# **write**	(Optional) Save the configuration.

You can use the **no** form of the above commands to cancel the original configuration or restore the configuration to the default.

28.2.3 Configuring the OSPF to Accommodate Different Physical Networks

According to the transmission nature of different media, the OSPF divides the networks into three types:

- Broadcast network (Ethernet, token network, and FDDI)
- Non-broadcast network (frame relay, X.25)
- Point-to-point network (HDLC, PPP, and SLIP)

The non-broadcast networks include two sub-types according to the operation modes of the OSPF:

1. One is the type of Non-broadcast Multi-access (NBMA) network. The NBMA requires direct communication all routers interconnected. Only fully meshed network connection can meet this requirement. If the SVC (for example, X.25) connection is used, this requirement can be met. However, if the PVC (for example, frame relay) networking is used, there will be some difficulty in meeting this requirement. The operation of the OSPF on the NBMA network is similar to that on the broadcast network: One Designated Router must be elected and this router is to advertise the link status of the NBMA network.
2. The second is the point-to-multipoint network type. If the network topology is not a fully meshed non-broadcast network, you need to set the network type of the interface to the point-to-multipoint network type for the OSPF. In a point-to-multipoint network type, the OSPF takes the connections between all routers as point-to-point links, so it does not involve the election of the designated router.

Whatever the default network type of the interface, you must set it to the broadcast network type. For example, you can set the non-broadcast multi-access network (frame relay, X.25) to be a broadcast network. This spares the step to configure the neighbor when you configure the OSPF routing process. By using the X.25 map and Frame-relay map commands, you can allow X.25 and frame relay to have the broadcast capability, so that the OSPF can see the networks like X.25 and frame relay as the broadcast networks.

The point-to-multipoint network interface can be seen as the marked point-to-point interface of one or multiple neighbors. When the OSPF is configured as the point-to-multipoint network type, multiple host routes will be created. The point-to-multipoint network has the following advantages over the NBMA network:

- Easy configuration, no needing to configure the neighbors, neither election of the designated router;
- Small cost, no needing the fully meshed topology

To configure the network type, execute the following commands in the interface configuration mode:

Command	**Function**
DGS-3610(config-if)# **ip ospf network {broadcast | non-broadcast | point-to-point | {point-to-multipoint [non-broadcast]} }**	Configure the OSPF network type

For different link encapsulation types, the default network type is shown as below:

- Point-to-point network type
- PPP, SLIP, frame relay point-to-point sub-interface, X.25 point-to-point sub-interface encapsulation
- NBMA (non-broadcast) network type
  Frame relay, X.25 encapsulation (except point-to-point sub-interface)
- Broadcast network type
  Ethernet encapsulation
- The default type is not the point-to-multipoint network type

It should be noted that the types of networks at both sides should be consistent with each other for the configuration. Otherwise, the neighbor Full may appear and the calculation of the routing is incorrect.

28.2.3.2 Configuring Point-to-Multipoint, Broadcast Network

When routers are connected via X.25 and frame relay networks, if the network is not a fully meshed network or you do not want the election of the designated router, you can set the OSPF interface network type as the point-to-multipoint type. Since the point-to-multipoint network takes the link as a point-to-point link, multiple host routes will be created. In addition, all the neighbors have the same cost in the point-to-multiple networks. If you want to make different neighbors have different costs, you can set them by using the neighbor command.

To configure the point-to-multipoint network type, execute the following commands in the interface configuration mode:

Command	**Function**
DGS-3610(config-if)# **ip ospf network point-to-multipoint**	Configure the point-to-multipoint network type for an interface
DGS-3610(config-if)# **exit**	Exit to the global configuration mode
DGS-3610(config)# **router ospf 1**	Enter the routing process configuration mode
DGS-3610(config-router)# **neighbor ip-address cost** *cost*	Specify the cost of the neighbor (optional)

Note

Although the OSPF point-to-multipoint network is a non-broadcast network, it can allow non-broadcast networks to have broadcast capability by using the frame relay, X.25 mapping manual configuration or self-learning. Therefore, you do not need to specify neighbors when you configure the point-to-multipoint network type.

28.2.3.3 Configuring Non-broadcast Network

When the OSPF works in the non-broadcast network, you can configure it to the NBMA or the point-to-multipoint non-broadcast type. Since it cannot dynamically discover neighbors without the broadcast capability, you must manually configure neighbors for the OSPF working in the non-broadcast network.

Considering the following conditions, you can configure the NBMA network type:

1. When a non-broadcast network has the fully meshed topology;
2. You can set a broadcast network as the NBMA network type to reduce the generation of the broadcast packets and save the network bandwidth, and also avoid arbitrary reception and transmission of routers by some degree. The configuration of the NBMA network should specify the neighbor. For there is the choice to specify the routers, you should determine which router is taken as specified one. For this reason, it is necessary for you to configure the priority. If the priority is higher, it is more possible to become the specified router.

To configure the NBMA network type, execute the following commands in the interface configuration mode:

Command	**Function**
DGS-3610(config-if)# **ip ospf network non-broadcast**	Specify the network type of the interface to be the NBMA type
DGS-3610(config-if)# **exit**	Exit to the global configuration mode
DGS-3610(config)# **router ospf 1**	Enter the routing process configuration mode

Command	Function
DGS-3610(config-router)# **neighbor** *ip-address* [**priority** *number*] [**poll-interval** *seconds*]	Specify the neighbor and designate its priority and round robin interval of hello.

In a non-broadcast network, if it cannot ensure that any two routers are in direct connection, the better solution is to set the network type of the OSPF to the point-to-multipoint non-broadcast network type.

Whether in a point-to-multipoint broadcast or non-broadcast network, all the neighbors have the same cost, which is the value set by using the ip ospf cost command. However, the bandwidths of the neighbors may be actually different, so the costs should be different. Therefore, you can specify the necessary cost for each neighbor by using the neighbor command. This only applies to the interfaces of the point-to-multipoint type (broadcast or non-broadcast).

To configure the point-to-multipoint type for the interfaces in a non-broadcast network, execute the following commands in the interface configuration mode:

Command	Function
DGS-3610(config-if)# **ip ospf network point-to-multipoint non-broadcast**	Specify the network type of the interface to be the point-to-multipoint non-broadcast type
DGS-3610(config-if)# **exit**	Exit to the global configuration mode
DGS-3610(config)# **router ospf 1**	Enter the routing process configuration mode
DGS-3610(config-router)# **neighbor** *ip-address* [**cost** number]	Specify the neighbor and specify the cost to the neighbor

Pay attention to step 4. If you have not specified the cost for the neighbors, the costs referenced by the ip ospf cost command in the interface configuration mode will be used.

28.2.3.4 Configuring Broadcast Network Type

It is necessary for the OSPF broadcast network to select the designated routers (DR) and backup designated router (BDR). And the designated routers will notify the link status of this network to the outer networks. All of the routers keep the neighbor relationship. However, all of routers only keep the adjacent relationship with the designated routers and backup designated routers. That is to say, each router only switches the link status data packet with the designated routers and backup designated routers, and the designated routers notify all routers, so that each router can keep the consistent link status database.

You can control the election result of the routers by setting the OSPF priority parameter. However, the parameter does not take effect immediately and affect the current designated router. It takes effect only in the new round of election. The unique condition to carry out new selection of the designated routers is that the OSPF neighbor doesn’t receive the Hello message from the designated routers within specified time and it is considered that the router is down.

To configure the broadcast network type, execute the following commands in the interface configuration mode:

Command	Function
DGS-3610(config-if)# **ip ospf network broadcast**	Specify the type of the interface to be the broadcast network type
DGS-3610(config-if)# **ip ospf priority** *priority*	(Optional) Specify the priority of the interface

28.2.4 Configuring the OSPF Area Parameters

To configure area authentication, stub area, and default route total cost, you need to implement this through configuring the area commands.

Area authentication is configured to avoid the learning of non-authenticated and invalid routers and the notificaion of invalid routes to the non-authentication route. In the broadcast network, area authentication can also prevent non-authentication routers from becoming the designated routers to ensure that the stability and intrusion prevention of the routing system.

When an area is the leaf area of the OSPF route domain, which means that the area does not act as the transit area, neither does it injects external routes to the OSPF routing area, you can configure the area as a stub area. The stub area routers can only learn about three routes, namely, 1) Routes in the stub area, 2) Other area routes, and 3) Default routes advertised by the border router in the stub area. For there is no much external routing, the route table of the stub area routers is small and it can save the resource of routers, so the stub area routers may be low- or middle-level of routers. To further reduce the Link Status Advertisements (LSA) sent to the stub areas, you can configure an area as the full stub area (configured with the no-summary option). The routers in a full stub area can learn two types of routes: 1) routes in the stub area; 2) default routes advertised by the border router in the stub area. The configuration of the full stub area allows the OSPF to occupy the minimized router resources, increasing the network transmission efficiency.

If the routers in a stub area can learn multiple default routes, you need to set the costs of the default routes (by using the area default-cost command), so that they first use the specified default route.

You should pay attention to the following when you configure the STUB area:

- The backbone area cannot be configured as a STUB area, and the STUB area cannot be used as the transmission area of the virtual links.
- To set an area as the STUB area, all the routers in the area must be configured with this attribute.

- There is no ASBR in stub areas. In other words, the routes outside an autonomous system cannot be transmitted in the area.

To configure the OSPF area parameters, execute the following commands in the routing process configuration mode:

Command	Function
DGS-3610(config-router)#**area** *area-id* **authentication**	Set plain-text authentication as the authentication mode for the area
DGS-3610(config-router)#**area** *area-id* **authentication message-digest**	Set MD5 authentication as the authentication mode for the area
DGS-3610(config-router)#**area** *area-id* **stub [no-summary]**	Set the area as a stub area **no-summary:** Set the area as a stub area to prevent the ABR between areas from sending summary-LSAs to the stub area
DGS-3610(config-router)#**area** *area-id* **default-cost** *cost*	Configure the cost of the default route sent to the stub area

Note

For authentication configuration, you still need to configure the authentication parameters at the interface. See "*Configuring the OSPF Interface Parameters*" section in this chapter. You must configure the stub area on all the devices in the area. To configure a full stub area, you still have to configure the full stub area parameters on the border device of the stub area in addition to the basic configuration of stub area. You do not need to change the configuration of other routers.

28.2.5 Configuring OSPF NSSA

The NSSA (Not-So-Stubby Area) is an expansion of the OSPF STUB area. The NSSA also reduces the consumption of the resources of the routers by preventing the Category 5 LSA (AS-external-LSA) from flooding the NSSA. However, unlike the STUB area, the NSSA can inject some routes outside the autonomous region to the route selection area of the OSPF.

Through redistribution, the NSSA allows the external routes of autonomous system type 7 to the NSSA. These external LSAs of type 7 will be converted into the LSAs of type 5 at the border router of the NSSA and flooded to the entire autonomous system. During this process, the external routes can be summarized and filtered.

You should pay attention to the following when you configure the NSSA:

- The backbone area cannot be configured as a NSSA, and the NSSA cannot be used as the transmission area of the virtual links.
- To set an area as the NSSA, all the devices connected to the NSSA must be configured with the NSSA attributes by using the area nssa command.

To configure an area as the NSSA, execute the following commands in the routing process configuration mode:

Command	Function
DGS-3610(config-router)# **area** *area-id* **nssa** [**no-redistribution**] [**no-summary**] [**default-information-originate**[**metric** *metric*][**metric-type** [**1** | **2**]]]	(Optional) Define a NSSA
DGS-3610(config-router)#**area** *area-id* **default-cost** *cost*	Configure the cost of the default route sent to the NSSA

The *default-information-originate parameter* is used to generate the default Type-7 LSA. This option varies slightly between the ARR and ASBR of the NSSA. On the ABR, whether there is a default route or not in the routing table, the Type-7 LSA default route will be created. On the other hand, this is only created when there is a default route in the routing table on ASBR.

The no-redistribution parameter allows other external routes introduced by using the redistribute commands via the OSPF on the ASBR not to be distributed to the NSSA. This option is usually used when the router in the NSSA is both an ASBR and an ABR to prevent external routes from entering the NSSA.

To further reduce the LSAs sent to the NSSA, you can configure the no-summary attribute on the ABR to prevent the ABR from sending the summary LSAs (Type-3 LSA) to the NSSA.

In addition, the area default-cost is used on the ABR connected to the NSSA. This command configures the cost of the default route sent by the border router to the NSSA. By default, the cost of the default route sent to the NSSA is 1.

28.2.6 Configuring the Route Summary between OSPF Areas

The ABR (Area Border Router) have at least two interfaces that belong to different areas, one of which must be the backbone area. The ABR acts as the pivot in the OSPF routing area, and it can advertise the routes of one area to another. If the route network addresses are continual in the area, the border router can advertise only one summary route to other areas. The route summary between areas greatly reduces the size of the routing table and improves the efficiency of the network.

To configure the route summary between areas, execute the following commands in the routing process configuration mode:

Command	Function
DGS-3610(config-router)# **area** *area-id* **range** *ip-address mask* [**advertise** | **not-advertise**]	Configure the summary route of the area

Note

If route summary is configured, the detailed routes in this area will not be advertised by the ABR to other areas.

28.2.7 Configuring Route Summary When Routes Are Injected to the OSPF

When the routes are redistributed from other routing process to the OSPF routing process, every route is advertised to the OSPF router as a separate link status. If the injected route is a continuous address space, the autonomous area border router can advertise only one summary route, thus reducing the size of the routing table.

To configure the external route summary, execute the following commands in the routing process configuration mode:

Command	Function
DGS-3610(config-router)# **summary-address** *ip-address mask*[**not-advertise | tag** *tag-id* **|**]	Configure the external summary route

28.2.8 Creating the Virtual Connections

In the OSPF routing area, the OSPF route updates between none-backbone areas are exchanged via the backbone area, to which all the areas are connected. If the backbone area is disconnected, you need to configure the virtual connection to connect the backbone area. Otherwise, the network communication will fail. If physical connection cannot be ensured due to the restriction of the network topology, you can also meet this requirement by creating the virtual connections.

Virtual connections should be created between two ABRs. The common area of the ABRs become the transmit areas. The stub areas and NSSA areas cannot be used as the transit area. The virtual connections can be seen as a logical connection channel established between two ABRs via the transit area. On both its ends must be ABRs and configuration must be performed on both ends. The virtual connection is identified by the router-id number of the peer router. The area that provides the two ends of a virtual connection with an internal non-backbone area route is referred to as the transit area, whose number must be specified at configuration.

The virtual connections will be activated after the route in the transit area has been calculated (that is, the route to the other router). You can see it as a point-to-point connection, on which most parameters of the interface can be configured, like a physical interface, for example, hello-interval and dead-interval.

The “logical channel” means that the multiple routers running the OSPF between the two ABRs only forward packets (If the destination addresses of the protocol packets are not these routers, the packets are transparent to them and are simply forwarded as common IP packets), and the ABRs exchange route information directly. The route information means the Type-3 LSAs generated by the ABR, and the synchronization mode in the area is not changed as a result.

To create the virtual connection, execute the following commands in the routing process configuration mode:

Command	Function
DGS-3610(config-router)# **area** *area-id* **virtual-link** *router-id* [[**hello-interval** *seconds*]| [**retransmit-interval** *seconds*] |[**transmit-delay** *seconds*]|[**dead-interval** *seconds*]| [**authentication** [**message-digest | null**] |[[**authentication-key** *key* | **message-digest-key** *keyid* **md5** *key*]]]	Create a virtual connection

It should be noted that: If the autonomous system is divided into more than one area, one of the areas must be the backbone area, to which the other areas must be connected directly or logically. Also, the backbone area must be in good connection.

Note

The router-id is the ID of the OSPF neighbor device. If you are not sure of the value of the router-id, you can use the show ip ospf neighbor command to verify it. How to manually configure the router-id, Please refer to the chapter of "*Using the Loopback Address as the Route ID*".

28.2.9 Creating the Default Routes

An ASBR can be forced to generate a default route, which is injected to the OSPF routing area. If one router is forced to generate the default route, it will become the ASBR automatically. However, the ASBR will not automatically generate the default route.

To force the ASBR to generate the default route, execute the following commands in the routing process configuration mode:

Command	Function
DGS-3610(config-router)# **default-information originate [always] [metric** *metric-value*] **[metric-type** *type-value*] **[route-map** *map-name*]	Configure to generate the default route

Note

When the stub area is configured, the ABR will generate the default route automatically, and notifies it to all routers within the stub area.

28.2.10 Using the Loopback address as the route ID

The OSPF routing process always uses the largest interface IP address as the device ID. If the interface is disabled or the IP address does not exist, the OSPF routing process must calculate the device ID again and send all the route information to the neighbor.

If the loopback (local loop address) is configured, the routing process will select the IP address of the loopback interface as the device ID. If there are multiple loopback interfaces, the largest IP address is selected as the device ID. Since the loopback address always exists, this enhances the stability of the routing table.

To configure the loopback address, execute the following commands in the global configuration mode:

Command	Function
DGS-3610(config)# **interface loopback 1**	Create the loopback interface
DGS-3610(config-if)# **ip address** *ip-address mask*	Configure the Loopback IP address

Note

If the OSPF route process has elected the general-interface IP address as the route ID, at this case, to configure the loopback port does not lead to the re-elect the ID by the OSPF process.

28.2.11 Changing the OSPF Default Management Distance

The management distance of a route represents the credibility of the source of the route. The management distance ranges from 0 to 255. The greater this value, the smaller the credibility of the source of the route.

The OSPF of our product has three types of routes, whose management distances are all 110 by default: intra-area, inter-area, and external. A route belongs to an area is referred to as the intra-area route, and a route to another area is referred to as the inter-area route. A route to another area (learnt through redistribution) is known as the external route.

To change the OSPF management distance, execute the following commands in the routing process configuration mode:

Command	Function
DGS-3610(config-router)#**distance ospf** {[**inter-area** *dist1*] [**inter-area** *dist2*] [**external** *dist3*]}	Change the OSPF management distance

28.2.12 Configuring the Route Calculation Timer

When the OSPF routing process receives the route topology change notification, it runs the SPF for route calculation after some time of delay. This delay can be configured, and you can also configure the minimum intervals between two SPF calculations.

To configure the OSPF route calculation timer, execute the following commands in the routing process configuration mode:

Command	Function
DGS-3610(config-router)#**timers spf spf-delay spf-holdtime**	Configure the route calculation timer

28.2.13 Changing LSAs Group Pacing

The OSPF LSA group pacing characteristic allows the switch to group OSPF LSAs and pace the refreshing, check, and aging functions for more efficient use of the devie. The default is 4 minutes. This parameter needs not to be adjusted often. The optimum group pacing interval is inversely proportional to the number of LSAs that need to be calculated. For example, if you have approximately 10,000 LSAs in the database, decreasing the pacing interval would be better. If the switch has a small database (40 to 100 LSAs), increasing the pacing interval to 10 to 20 minutes might be better. To configure OSPF LSA pacing, follow these steps in the privileged mode:

Execute the following commands in the routing process configuration mode:

Command	Meaning
DGS-3610# **configure terminal**	Enter the global configuration mode.
DGS-3610(config)# **router ospf 1**	Enable OSPF and enter OSPF route configuration mode.
DGS-3610(config-router)# **timers lsa-group-pacing** *seconds*	(Optional) Change the LSAs group pacing.
DGS-3610(config-router)# **End**	Return to the privileged EXEC mode.
DGS-3610# **show running-config**	Verify whether the content is correct.
DGS-3610# **write**	(Optional) Save the configuration.

To restore the default value, use the **no timers lsa-group-pacing** in **the** router configuration mode.

28.2.14 Configuring Route Selection

OSPF calculates the destination based on the Cost, where the route with the least Cost is the shortest route. The default route cost is based on network bandwidth. When you configure the OSPF router, you can set the link cost according to the factors such as link bandwidth, delay or economic cost. The lower its cost, the higher the possibility of that link to be selected as the route. If route summarization takes place, the summarized cost of all the links is taken as the cost of the summarized information.

Routing configuration includes two parts. In the first place, you set the reference value for the bandwidth generated cost. This value and the interface bandwidth value are used to create the default cost. In the second place, you can set the respective metric of each interface by using the ip ospf cost command, so that the default metric is not effective for the interface. For example, the default reference value is 100 Mbps, and an Ethernet interface has the bandwidth of 10Mbps. Other example, the bandwidth is 100Mbps, the bandwidth of an Ethernet interface is 10Mbps, this interface will have the default metric of 100/10 + 0.5 ≈ 10.

The interface cost is selected in the following way in the protocol. The set interface has the highest priority. If you have set an interface cost, the set value is taken as the interface cost. If you did not set one while the automatic cost generation function is enabled, the interface cost is calculated automatically. If the function is disabled, the default of 10 is taken as the interface cost.

The configuration process is shown as below:

Command	Meaning
DGS-3610# **configure terminal**	Enter the global configuration mode.
DGS-3610(config)# **router ospf 1**	Enable OSPF and enter OSPF route configuration mode.
DGS-3610(config-router)#**auto-cost reference-bandwidth** *ref-bw*	(Optional) Set the default cost based on the bandwidth on an interface.
DGS-3610(config-router)# **end**	Return to the privileged EXEC mode.
DGS-3610# **show ip protocols**	Display the routing protocol that is running currently.
DGS-3610# **write**	(Optional) Save the configuration.

To disable route cost, use the **no ip ospf cost** or **auto-cost** command.

28.2.15 Configuring whether to check the MTU value when the interface receives the database description packets

When the OSPF receives the database description packet, it will check whether the MTU interface is the same with its own. If the interface indicated in the received database description packet has a MTU greater than that of the receiving interface, the neighborhood relationship cannot be established. In this case, you can disable MTU check as a solution. To disable the MTU check of an interface, you can execute the following command in the interface mode;

Command	Meaning
DGS-3610(config-if)# **ip ospf mtu-ignore**	Configure to not check the MTU value when the interface receives the database description packets

By default, the MTU check is enabled.

28.2.16 Configuring to prohibit an interface from sending the OSPF interface parameters

To prevent other devices in the network from dynamically learning the route information of the device , you can set the specified network interface of the device as a passive interface by using the passive-interface command. This prohibits the OSPF packets from sending at the interface.

In the privileged mode, you can configure the passive interface by performing the following steps:

Command	Meaning
DGS-3610# **configure terminal**	Enter the global configuration mode.
DGS-3610(config)# **router ospf 1**	Enter the routing protocol configuration mode (currently RIP and OSPF are supported)
DGS-3610(config-router)# **passive-interface** *interface-name*	(Optional) Set the specified interface as passive interface.
DGS-3610(config-router)# **passive-interface default**	(Optional) Set all the network interfaces as passive
DGS-3610(config-router)# **end**	Return to the privileged EXEC mode.
DGS-3610# **write**	Save the configuration.

By default, all interfaces are allowed to receive/send the OSPF packets. To re-enable the network interface to send the route information, you can use the **no passive-interface** *interface-id* command. To set all network interfaces, use the keyword **default.**

28.2.17 OSPF TRAP Sending Configuration

The protocol defines several types of the OSPF TRAP, such TRAP information is used to send the TRAP information to snmp-server when part of the network configuration changes and some OPSF event occurs for the network management. In the global configuration mode, you can enable the TRAP sending switch of OSPF by the following steps:

Command	Meaning
DGS-3610# **configure terminal**	Enter the global configuration mode.
DGS-3610(config)# **snmp-server host** *host-ip* **version** *version-no string* **[ospf]**	Configure the snmp-server to receive the TRAP. host-ip refers to the address corresponding to the server. version-no refers to the snmp version corresponding to the server. String is usually the communication authentication code of snmp, which is generally public. The optional parameter ospf refers to snmp-server receive the OSPF TRAP (by default, the server receives all types of TRAPs).
DGS-3610(config-router)# **snmp-server enable traps ospf**	Enable the sending switch of OSPF TRAP
DGS-3610(config-router)# **end**	Return to the privileged EXEC mode.
DGS-3610# **write**	Save the configuration.

By default, the device will not send the TRAP information to any snmp-server. At present, our product can only control the sending condition of all OSPF TRAPs by this switch, but can not accurately control whether it will send the specified type of the OSPF TRAP.

28.3 Monitoring and Maintaining OSPF

You can show the data such as the routing table, cache, and database of the OSPF. The following table lists some of that data that can be shown for your reference.

Command	Meaning
DGS-3610# **show ip ospf** [*process-id*]	Show the general information of the OSPF protocol for corresponding processes. It will display all processes if the process number is not specified.

Command	Meaning
DGS-3610# **show ip ospf** [*process-id*] [*area-id*] database	OSPF database information Can show the information of each type of LSAs for specified processes. area-id: It specifies the area on which the LSA is to show. For a class 5 LSA, the area filtering does not work.
DGS-3610# **show ip ospf** [*process-id*] [*area-id*] **database** [**adv-router** *ip-address*]	
DGS-3610# **show ip ospf** [*process-id*] [*area-id*] **database** [**self-originate**]	
DGS-3610# **show ip ospf** [*process-id*] [*area-id*] **database** [**database-summary**]	
DGS-3610# **show ip ospf** [*process-id*] [*area-id*] **database** [**router**] **[link-state-id**]	
DGS-3610# **show ip ospf** [*process-id*] [*area-id*] **database** [**router**] [**adv-router** *ip-address*]	
DGS-3610# **show ip ospf** [*process-id*] [*area-id*] **database** [**router**] [**self-originate**]	
DGS-3610# **show ip ospf** [*process-id*] [*area-id*] **database** [**network**][**link-state-id]**	
DGS-3610# **show ip ospf** [*process-id*] [*area-id*] **database** [**network**] [**link-state-id] [adv-router** *ip-address*]	
DGS-3610# **show ip ospf** [*process-id*] [*area-id*] **database** [**network**][**link-state-id**] [**self-originate**]	
DGS-3610# **show ip ospf** [*process-id*] [*area-id*] **database** [**summary**] **[link-state-id**]	
DGS-3610# **show ip ospf** [*process-id*] [*area-id*] **database** [**summary**] [**link-state-id]** [**adv-router** *ip-address*]	
DGS-3610# **show ip ospf** [*process-id*] [*area-id*] **database** [**summary**] [**link-state-id**] [**self-originate**]	
DGS-3610# **show ip ospf** [*process-id*] [*area-id*] **database** [**asbr-summary**] **[link-state-id]**	
DGS-3610# **show ip ospf** [*process-id*] [*area-id*] **database** [**asbr-summary**] [**link-state-id**] [**adv-router** *ip-address*]	

Command	**Meaning**
DGS-3610# **show ip ospf** [*process-id*] [*area-id*] **database** [**asbr-summary**] [**link-state-id**] [**self-originate**]	
DGS-3610# **show ip ospf** [*process-id*] [*area-id*] **database** [**external**] [**link-state-id]**	
DGS-3610# **show ip ospf** [*process-id*] [*area-id*] **database** [**external**] [**link-state-id]** [**adv-router** *ip-address*]	
DGS-3610# **show ip ospf** [*process-id*] [*area-id*] **database** [**external**] [**link-state-id**] [**self-originate**]	
DGS-3610# **show ip ospf** [*process-id*] [*area-id*] **database** [**nssa-external**] [**link-state-id**]	
DGS-3610# **show ip ospf** [*process-id*] [*area-id*] **database** [**nssa-external]** [**link-state-id**] [**adv-router** *ip-address*]	
DGS-3610# **show ip ospf** [*process-id* [*area-id*] **database**[**nssa-external**] [**link-state-id**][**self-originate**]	
DGS-3610# **show ip ospf** [*process-id*] **border-routers**	Show the route information when specified processes reach to the ABR and ASBR.
DGS-3610# **show ip ospf interface** [*interface-name*]	Show the information on the OSPF interface
DGS-3610# **show ip ospf** [*process-id*] **neighbor**[*interface-name*] [*neighbor-id*] **[detail]**	The interface information of adjacent routers interface-name: The local interface ID connected to the neighbor neighbor-id: The router ID of neighbor
DGS-3610# **show ip ospf**[*process-id*] **virtual-links**	View the virtual connection information of specified processes.

For the explanations of the commands, see *IP Routing Protocol Configuration Command Reference*. There are the following common monitoring and maintenance commands:

1. Show the status of the OSPF neighbor

Use the **show ip ospf** [*process-id*] **neighbor** to show all neighbor information of the OSPF process, including the status of neighbor, role, router ID and IP address.

```
DGS-3610# show ip ospf neighbor
OSPF process 1:
Neighbor ID      Pri State    Dead Time    Address:     Interface
```

```
10.10.10.50 1    Full/DR      00:00:38     10.10.10.50  eth0/0
OSPF process 100:
Neighbor ID      Pri State    Dead Time    Address I    nterface
10.10.11.50 1    Full/Backup  00:00:31     10.10.11.50  eth0/1
DGS-3610# show ip ospf 1 neighbor
OSPF process 1:
Neighbor ID      Pri State    Dead Time    Address:     Interface
10.10.10.50 1    Full/DR      00:00:38     10.10.10.50  eth0
DGS-3610# show ip ospf 100 neighbor
OSPF process 100:
Neighbor ID      Pri State    Dead Time    Address:     Interface
10.10.11.50 1    Full/Backup  00:00:31     10.10.11.50  eth1
```

2. Show the OSPF interface status

The following message shows that the F0/1 port belongs to area 0 of the OSPF, and the device ID is 172.16.120.1. The network type is “BROADCAST”-broadcast type. You must pay special attention to the parameters such as Area, Network Type, Hello and Dead. If these parameters are different from the neighbor, no neighborhood relationship will be established.

```
DGS-3610# sh ip ospf interface fastEthernet 1/0
FastEthernet 1/0 is up, line protocol is up
Internet Address 192.168.1.1/24, Ifindex: 2 Area 0.0.0.0, MTU 1500
Matching network config: 192.168.1.0/24
Process ID 1, Router ID 192.168.1.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 192.168.1.1, Interface Address 192.168.1.1
Backup Designated Router (ID) 192.168.1.2, Interface Address 192.168.1.2
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:04
Neighbor Count is 1, Adjacent neighbor count is 1
Crypt Sequence Number is 30
Hello received 972 sent 990, DD received 3 sent 4
LS-Req received 1 sent 1, LS-Upd received 10 sent 26
LS-Ack received 25 sent 7, Discarded 0
```

3. Show the information of the OSPF routing process

The following command shows the route ID, device type, area information, area summary, and other related information.

```
DGS-3610# show ip ospf
 Routing Process "ospf 1" with ID 1.1.1.1
 Process uptime is 4 minutes
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583Compatibility flag is enabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 This router is an ASBR (injecting external routing information)
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 LsaGroupPacing: 240 secs
 Number of incomming current DD exchange neighbors 0/5
 Number of outgoing current DD exchange neighbors 0/5
 Number of external LSA 4. Checksum 0x0278E0
 Number of opaque AS LSA 0. Checksum 0x000000
 Number of non-default external LSA 4
 External LSA database is unlimited.
 Number of LSA originated 6
 Number of LSA received 2
 Log Neighbor Adjency Changes : Enabled
 Number of areas attached to this router: 1
 Area 0 (BACKBONE)
 Number of interfaces in this area is 1(1)
 Number of fully adjacent neighbors in this area is 1
 Area has no authentication
 SPF algorithm last executed 00:01:26.640 ago
 SPF algorithm executed 4 times
 Number of LSA 3. Checksum 0x0204bf

 Routing Process "ospf 20" with ID 2.2.2.2
 Process uptime is 4 minutes
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583Compatibility flag is enabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 LsaGroupPacing: 240 secs
 Number of incomming current DD exchange neighbors 0/5
 Number of outgoing current DD exchange neighbors 0/5
 Number of external LSA 0. Checksum 0x000000
 Number of opaque AS LSA 0. Checksum 0x000000
 Number of non-default external LSA 0
 External LSA database is unlimited.
 Number of LSA originated 0
 Number of LSA received 0
 Log Neighbor Adjency Changes : Enabled
 Number of areas attached to this router: 0
```

28.4 OSPF Configuration Examples

Seven OSPF configuration examples are provided in this chapter:

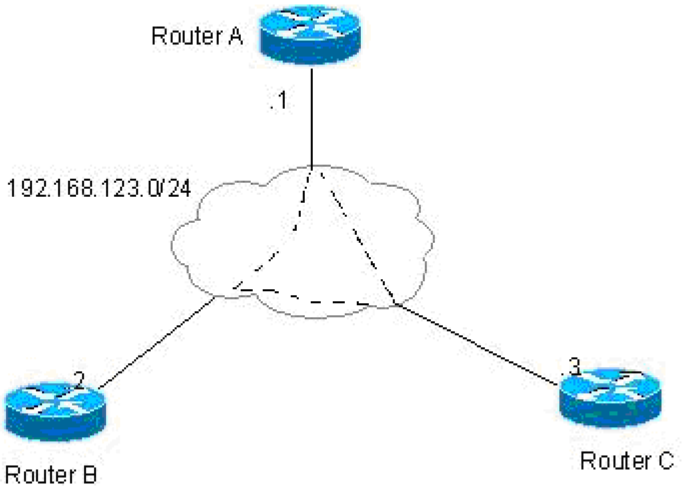
- Example of configuring the OSPF NBMA network type
- Example of configuring the OSPF point-to-multipoint board network type
- Example of configuring OSPF authentication
- Example of configuring route summary
- OSPF ABR, ASBR Configuration Examples
- Example of configuring OSPF stub area
- Example of configuring OSPF virtual connection

28.4.1 Example of configuring the OSPF NBMA network type

- **Configuration requirements:**

The three devices must be fully connected in a meshed network via frame relay. Each device has only one frame relay line, which has the same bandwidth and PVC rate. Figure 28-1 shows the IP address allocation and connection of the device.

Figure 28-1 Example of configuring the OSPF NBMA network type



Requirement: 1) The NBMA network type is configured among device A, B and C, 2) The device A is the designated router, and the device B is the backup designated device, 3) All networks are of one area.

- **Concrete Configuration of Routers**

Since the OSPF has no special configuration, it will automatically discover the neighbors via multicast. If the interface is configured with the NBMA network type, the interface will not send the OSPF multicast packets, so you need to specify the IP address of the neighbor.

Configuration of Device A:

#Configure the WAN port

```
interface Serial 1/0
ip address 192.168.123.1 255.255.255.0
encapsulation frame-relay
ip ospf network non-broadcast
ip ospf priority 10
```

# Configure the OSPF routing protocol to minimize the cost to the router B.

```
router ospf 1
network 192.168.123.0 0.0.0.255 area 0
neighbor 192.168.123.2     priority 5
neighbor 192.168.123.3
```

Configuration of Device B:

#Configure the WAN port

```
interface Serial 1/0
ip address 192.168.123.2 255.255.255.0
encapsulation frame-relay
ip ospf network non-broadcast
ip ospf priority 5
```

#Configuring OSPF routing protocol

```
router ospf 1
network 192.168.123.0 0.0.0.255 area 0
neighbor 192.168.123.1 priority 10
neighbor 192.168.123.3
```

Configuration of Device C:

#Configure the WAN port

```
interface Serial 1/0
ip address 192.168.123.3 255.255.255.0
encapsulation frame-relay
ip ospf network non-broadcast
```

#Configuring OSPF routing protocol

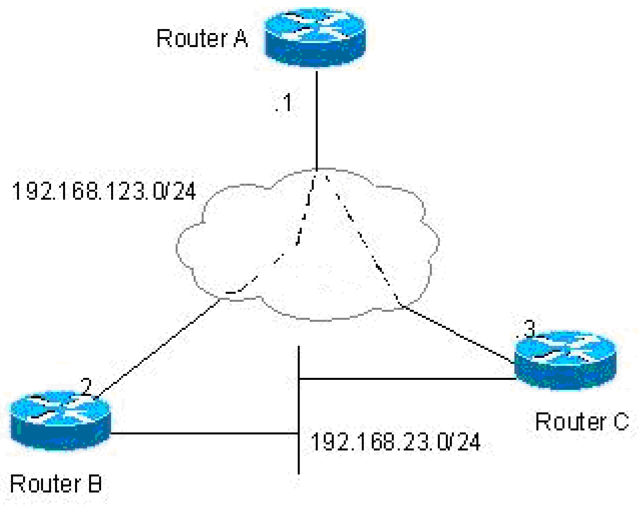
```
router ospf 1
network 192.168.123.0 0.0.0.255 area 0
neighbor 192.168.123.1 10
neighbor 192.168.123.2 5
```

28.4.2 Example of configuring the OSPF point-to-multipoint board network type

- **Configuration requirements:**

The three routers must be fully interconnected via frame relay. Each device has only one frame relay line, which has the same bandwidth and PVC rate. Figure 28-2 shows the IP address allocation and connection of the device .

Figure 28-2 Example of Configuring the OSPF Point-to-Multipoint Network Type



Requirements: 1) The point-to-multipoint network should be configured among devices A, B, and C.

- **Concrete Configuration of Devices**

If the interface is configured with the point-to-multipoint network type, the point-to-multipoint network type does not have the process to elect the specified router. The OSPF operation has similar action as the point-to-multipoint network type.

Configuration of Device A:

#Configuring Ethernet interface

```
interface FastEthernet 0/0
ip address 192.168.12.1 255.255.255.0
```

#Configure the WAN port

```
interface Serial 1/0
ip address 192.168.123.1 255.255.255.0
encapsulation frame-relay
ip ospf network point-to-multipoint
router ospf 1
network 192.168.23.0 0.0.0.255 area 0
network 192.168.123.0 0.0.0.255 area 0
```

Configuration of Device B:

#Configuring Ethernet interface

```
interface FastEthernet 0/0
ip address 192.168.23.2 255.255.255.0
```

#Configure the WAN port

```
interface Serial 1/0
```

```
ip address 192.168.123.2 255.255.255.0
encapsulation frame-relay
ip ospf network point-to-multipoint
```

#Configuring OSPF routing protocol

```
router ospf 1
network 192.168.23.0 0.0.0.255 area 0
network 192.168.123.0 0.0.0.255 area 0
```

Configuration of Device C:

#Configuring Ethernet interface

```
interface FastEthernet 0/0
ip address 192.168.23.3 255.255.255.0
```

#Configure the WAN port

```
interface Serial 1/0
ip address 192.168.123.3 255.255.255.0
encapsulation frame-relay
ip ospf network point-to-multipoint
```

#Configuring OSPF routing protocol

```
router ospf 1
network 192.168.23.0 0.0.0.255 area 0
network 192.168.123.0 0.0.0.255 area 0
```

The above configuration has another assumption:

From device A to the 192.168.23.0/24 target network, router B is the first choice. To achieve preferred routing, you must set the cost of the neighbor when you configure the neighbor.

The following commands can be configured in the device A:

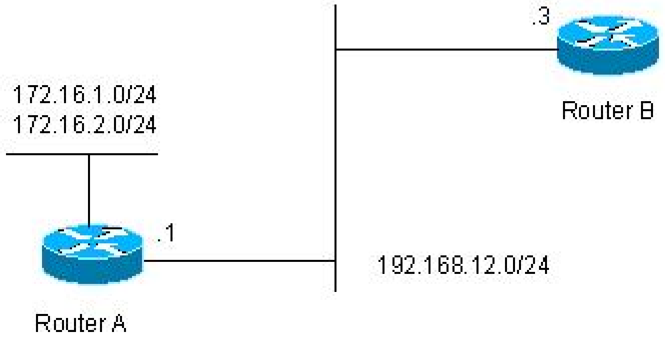
```
router ospf 1
neighbor 192.168.123.2 cost 100
neighbor 192.168.123.3 cost 200
```

28.4.3 Example of configuring OSPF authentication

- **Configuration requirements:**

Two devices are connected via the Ethernet and run the OSPF routing protocol, with the MD5 authentication used. The connection diagram among devices and the assignment of IP addresses are shown as in Figure 28-3.

Figure 28-3 Example of configuring OSPF authentication



- **Concrete Configuration of Devices**

The authentication configuration of the OSPF involves two parts:

2. Specifying the authentication mode of the area in the routing configuration mode;
3. Configuring the authentication method and key in the interface.

If both the area authentication and interface authentication are configured, the interface authentication shall be applied.

Configuration of Device A:

#Configuring Ethernet interface

```
interface FastEthernet0/0
ip address 192.168.12.1 255.255.255.0
ip ospf message-digest-key 1 md5 hello
```

#Configuring OSPF routing protocol

```
router ospf 1
network 192.168.12.0 0.0.0.255 area 0
area 0 authentication message-digest
```

Configuration of Device B:

#Configuring Ethernet interface

```
interface FastEthernet0/0
ip address 192.168.12.2 255.255.255.0
ip ospf message-digest-key 1 md5 hello
```

#Configuring OSPF routing protocol

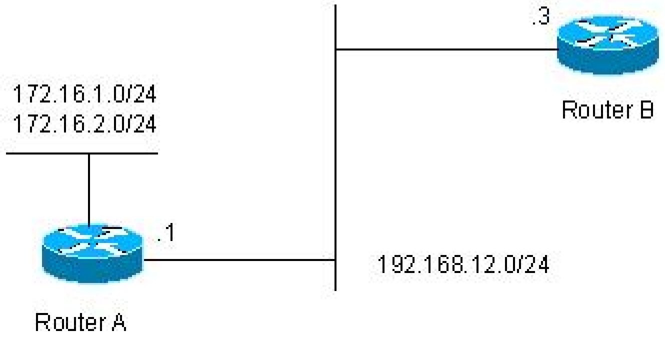
```
router ospf 1
network 192.168.12.0 0.0.0.255 area 0
area 0 authentication message-digest
```

28.4.4 Example of configuring route summary

- **Configuration requirements:**

The two devices are connected via Ethernet. Figure 28-4 shows the IP address allocation and connection of the equipment.

Figure 28-4 Example of configuring OSPF route summary



Requirements: 1) Both devices run the OSPF routing protocol. The 192.168.12.0/24 network belongs to area 0, while the 172.16.1.0/24 and 172.16.2.0/24 networks belong to area 10; 2) Router A is configured so that router A only advertises the 172.16.0.0/22 route, but not the 172.16.1.0/24 and 172.16.2.0/24.

- **Concrete Configuration of Devices**

You need to configure the OSPF area route summary on Router A. Please note that the area route summary can be configured only on the area border router.

Configuration of Device A:

#Configuring Ethernet interface

```
interface FastEthernet0/0
ip address 192.168.12.1 255.255.255.0
```

#Configure the two ports on the Ethernet card

```
interface FastEthernet1/0
ip address 172.16.1.1 255.255.255.0
interface FastEthernet1/1
ip address 172.16.2.1 255.255.255.0
```

#Configuring OSPF routing protocol

```
router ospf 1
network 192.168.12.0 0.0.0.255 area 0
network 172.16.1.0 0.0.0.255 area 10
network 172.16.2.0 0.0.0.255 area 10
area 10 range 172.16.0.0 255.255.252.0
```

Configuration of Device B:

#Configuring Ethernet interface

```
interface FastEthernet0/0
ip address 192.168.12.2 255.255.255.0
```

#Configuring OSPF routing protocol

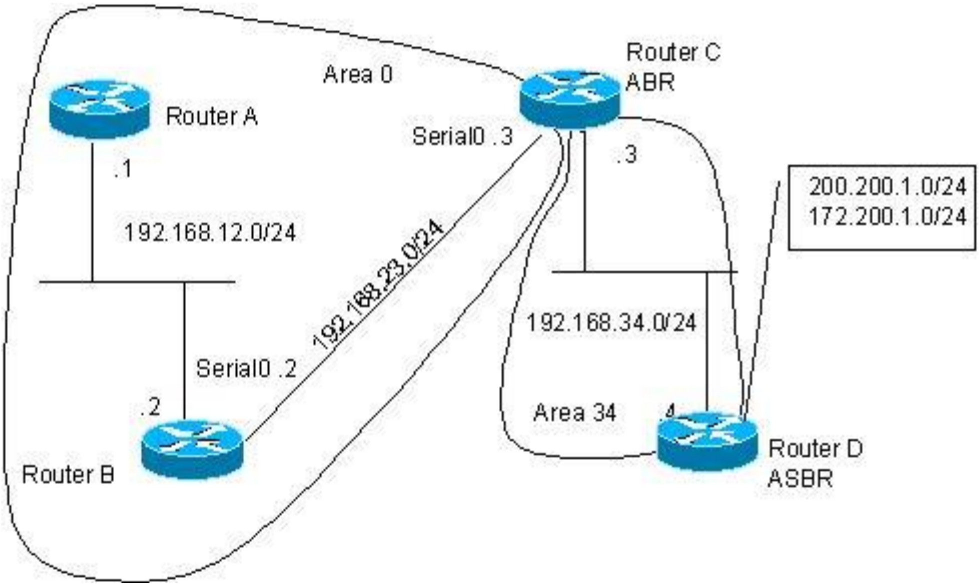
```
router ospf 1
network 192.168.12.0 0.0.0.255 area 0
```

28.4.5 OSPF ABR, ASBR Configuration Examples

- **Configuration requirements:**

Four devices form an OSPF routing area. Networks 192.168.12.0/24 and 192.168.23.0/24 belong to area 0, while network 192.168.34.0/24 belongs to area 34. Figure 28-5 shows the IP address allocation and connection of the equipment.

Figure 28-5 Example of configuring OSPF ABR and ASBR



As is shown in above figure, the device A and device B are of the area internal device s, the device C is of the ABRs, and the device D is of the ASBRs. 200.200.1.0/24 and 172.200.1.0/24 are the networks outside the OSPF routing area. Configure various devices so that all OSPF routers can learn the external routes, which must carry the “34” tag and be Type-I.

- **Concrete Configuration of Devices**

When the OSPF redistributes the routes of other sources, the default type is type II and it does not carry any tag.

Configuration of Device A:

#Configuring Ethernet interface

```
interface FastEthernet0/0
ip address 192.168.12.1 255.255.255.0
```

#Configuring OSPF routing protocol

```
router ospf 1
network 192.168.12.0 0.0.0.255 area 0
```

Configuration of Device B:

#Configuring Ethernet interface

```
interface FastEthernet0/0
ip address 192.168.12.2 255.255.255.0
```

#Configure the WAN port

```
interface Serial 1/0
ip address 192.168.23.2 255.255.255.0
```

#Configuring OSPF routing protocol

```
router ospf 1
network 192.168.12.0 0.0.0.255 area 0
network 192.168.23.0 0.0.0.255 area 0
```

Configuration of Device C:

#Configuring Ethernet interface

```
interface FastEthernet 0/0
ip address 192.168.34.3 255.255.255.0
```

#Configure the WAN port

```
interface Serial 1/0
ip address 192.168.23.3 255.255.255.0
```

Configuring OSPF routing protocol

```
router ospf 1
network 192.168.23.0 0.0.0.255 area 0
network 192.168.34.0 0.0.0.255 area 34
```

Configuration of Device D:

#Configuring Ethernet interface

```
interface FastEthernet 0/0
ip address 192.168.34.4 255.255.255.0
```

#Configure the ports on the Ethernet card

```
interface FastEthernet 1/0
ip address 200.200.1.1 255.255.255.0
interface FastEthernet 1/1
ip address 172.200.1.1 255.255.255.0
```

#Configure the OSPF routing protocol to redistribute the RIP route

```
router ospf 1
network 192.168.34.0 0.0.0.255 area 34
redistribute rip metric-type 1 subnets tag 34
```

#Configuring RIP routing protocol

```
router rip
network 200.200.1.0
network 172.200.1.0
```

On Device B, you can see the OSPF generates the following routes. Please note that the external route type becomes “E1”.

```
O E1 200.200.1.0/24 [110/85] via 192.168.23.3, 00:00:33, Serial1/0
O IA 192.168.34.0/24 [110/65] via 192.168.23.3, 00:00:33, Serial1/0
O E1     172.200.1.0 [110/85] via 192.168.23.3, 00:00:33, Serial1/0
```

On Device B, you can see the link status database as shown below. Please note that the tag of the external link has become “34”.

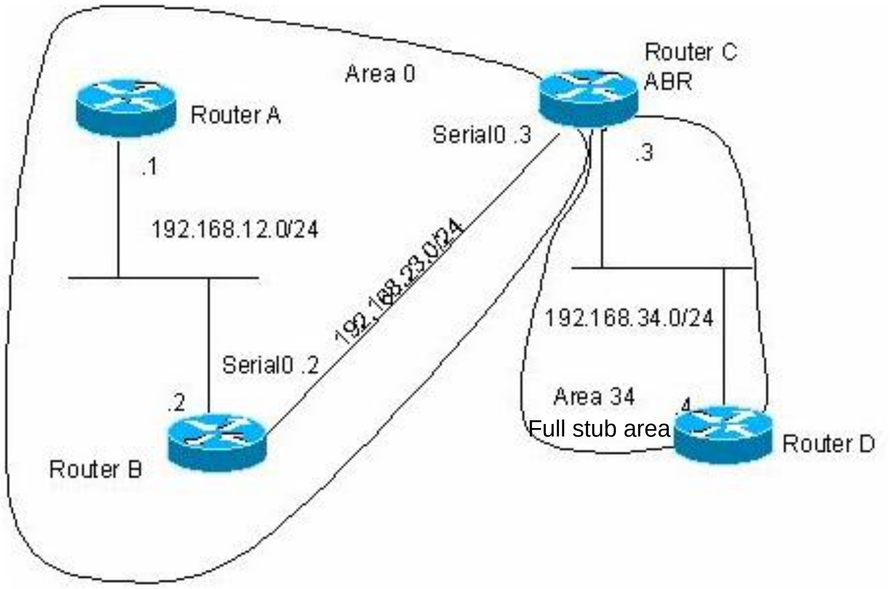
```
RouterB#show ip ospf 1 database
OSPF Router with ID (1.1.1.1) (Process ID 1)
Router Link States (Area 0.0.0.0)
Link ID       ADV Router     Age  Seq#      CkSum  Link count
1.1.1.1       1.1.1.1       2    0x80000011 0x6f39 2
3.3.3.3       3.3.3.3       120  0x80000002 0x26ac 1
Network Link States (Area 0.0.0.0)
Link ID       ADV Router     Age  Seq#      CkSum
192.88.88.27   1.1.1.1       120  0x80000001 0x5366
Summary Link States (Area 0.0.0.0)
Link ID       ADV Router     Age  Seq#      CkSum  Route
10.0.0.0       1.1.1.1       2    0x80000003 0x350d 10.0.0.0/24
100.0.0.0      1.1.1.1       2    0x8000000c 0x1ecb 100.0.0.0/16
Router Link States (Area 0.0.0.1 [NSSA])
Link ID       ADV Router     Age  Seq#      CkSum  Link count
1.1.1.1       1.1.1.1       2    0x80000001 0x91a2 1
Summary Link States (Area 0.0.0.1 [NSSA])
Link ID       ADV Router     Age  Seq#      CkSum  Route
100.0.0.0      1.1.1.1       2    0x80000001 0x52a4 100.0.0.0/16
192.88.88.0     1.1.1.1       2    0x80000001 0xbb2d 192.88.88.0/24
NSSA-external Link States (Area 0.0.0.1 [NSSA])
Link ID       ADV Router     Age  Seq#      CkSum  Route            Tag
20.0.0.0       1.1.1.1       1    0x80000001 0x033c E2 20.0.0.0/24    0
100.0.0.0      1.1.1.1       1    0x80000001 0x9469 E2 100.0.0.0/28    0
AS External Link States
Link ID       ADV Router     Age  Seq#      CkSum  Route            Tag
20.0.0.0       1.1.1.1       380  0x8000000a 0x7627 E2 20.0.0.0/24    0
100.0.0.0      1.1.1.1       620  0x8000000a 0x0854 E2 100.0.0.0/28    0
```

28.4.6 Example of configuring OSPF stub area

- **Configuration requirements:**

Four devices form an OSPF routing area. Networks 192.168.12.0/24 and 192.168.23.0/24 belong to area 0, while network 192.168.34.0/24 belongs to area 34. Figure 28-6 shows the IP address allocation and connection of the equipment.

Figure 28-6 Example of configuring OSPF stub area



The device is that only the OSPF default route and the network routes of the local area can be seen in the routing table of RouterD.

- **Concrete Configuration of Devices**

Only the devices in the full stub area can have their routing tables simplified to eliminate the external and inter-area routes. The stub area must be configured on all the devices in the area. In order to show the inter-area routing in the device D, the device C advertises a 192.168.30.0/24 network.

The configuration of Device A:

#Configuring Ethernet interface

```
interface FastEthernet0/0
ip address 192.168.12.1 255.255.255.0
```

#Configuring OSPF routing protocol

```
router ospf 1
network 192.168.12.0 0.0.0.255 area 0
```

Configuration of Device B:

# Configuring Ethernet interface

```
interface FastEthernet0/0
ip address 192.168.12.2 255.255.255.0
```

#Configure the WAN port

```
interface Serial1/0
ip address 192.168.23.2 255.255.255.0
```

#Configuring OSPF routing protocol

```
router ospf 1
network 192.168.12.0 0.0.0.255 area 0
network 192.168.23.0 0.0.0.255 area 0
```

Configuration of Device C:

#Configuring Ethernet interface

```
interface FastEthernet0/0
ip address 192.168.34.3 255.255.255.0
```

#Configure the WAN port

```
interface Serial1/0
ip address 192.168.23.3 255.255.255.0
```

#Add a network

```
interface Dialer10
ip address 192.168.30.1 255.255.255.0
```

Configuring OSPF routing protocol

```
router ospf 1
network 192.168.23.0 0.0.0.255 area 0
network 192.168.34.0 0.0.0.255 area 34
network 192.168.30.0 0.0.0.255 area 34
area 34 stub no-summary
```

Configuration of Device D:

#Configuring Ethernet interface

```
interface FastEthernet0/0
ip address 192.168.34.4 255.255.255.0
```

#Configuring OSPF routing protocol

```
router ospf 1
network 192.168.34.0 0.0.0.255 area 34
area 34 stub
```

The route generated in the device D by the ospf is shown as follows:

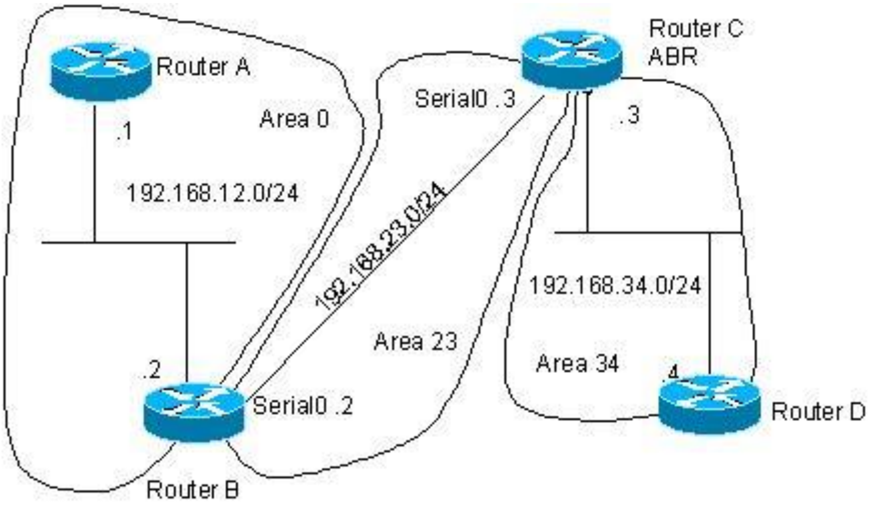
```
O 192.168.30.0/24 [110/1786] via 192.168.34.3, 00:00:03, FastEthernet0/0
O*IA 0.0.0.0/0 [110/2] via 192.168.34.3, 00:00:03, FastEthernet0/0
```

28.4.7 Example of configuring OSPF virtual connection

- **Configuration requirements:**

Four devices form an OSPF routing area. Networks 192.168.12.0/24 belongs to area 0, network 192.168.23.0/24 to area 23, while network 192.168.34.0/24 belongs to area 34. Figure 28-7 shows the IP address allocation and connection of the device.

Figure 28-7 Example of configuring OSPF virtual connection



The purpose is to allow device D to learn the routes of 192.168.12.0/24 and 192.168.23.0/24.

- **Concrete Configuration of Devices**

The OSPF routing area consists of multiple sub-areas, each of which must be connected to the backbone area (area 0) directly. If there is no direct connection, a virtual link must be created to ensure logical connection to the backbone area. Otherwise, the sub-areas are not in connection. The virtual connection must be configured on the ABR.

The configuration of device A:

#Configuring Ethernet interface

```
interface FastEthernet0/0
ip address 192.168.12.1 255.255.255.0
```

#Configure the OSPF routing protocol

```
router ospf 1
network 192.168.12.0 0.0.0.255 area 0
```

The configuration of device B:

#Configuring Ethernet interface

```
interface FastEthernet0/0
ip address 192.168.12.2 255.255.255.0
```

#Configure the WAN port

```
interface Serial1/0
ip address 192.168.23.2 255.255.255.0
```

#Add the loopback IP address and take it as the ID of the OSPF router.

```
interface Loopback2
ip address 2.2.2.2 255.255.255.0
```

#Configuring OSPF route protocol

```
router ospf 1
network 192.168.12.0 0.0.0.255 area 0
network 192.168.23.0 0.0.0.255 area 23
area 23 virtual-link 3.3.3.3
```

Configuration of device C:

#Configuring Ethernet interface

```
interface FastEthernet0/0
ip address 192.168.34.3 255.255.255.0
```

#Configure the WAN port

```
interface Serial1/0
ip address 192.168.23.3 255.255.255.0
```

#Add the loopback IP address and take it as the ID of the OSPF router.

```
interface Loopback2
ip address 3.3.3.3 255.255.255.0
```

#Configuring OSPF route protocol

```
router ospf 1
network 192.168.23.0 0.0.0.255 area 23
network 192.168.34.0 0.0.0.255 area 34
area 23 virtual-link 2.2.2.2
```

Configuration of device D:

#Configuring Ethernet interface

```
interface FastEthernet0/0
ip address 192.168.34.4 255.255.255.0
```

#Configuring OSPF route protocol

```
router ospf 1
network 192.168.34.0 0.0.0.255 area 34
```

The route generated in the device D by the ospf is shown as follows:

```
O IA 192.168.12.0/24 [110/66] via 192.168.34.3, 00:00:10, FastEthernet0/0
O IA 192.168.23.0/24 [110/65] via 192.168.34.3, 00:00:25, FastEthernet0/0
```

29 BGP Configuration

The BGP (Border Gateway Protocol) is an EGP (Exterior Gateway Protocol) to communicate with the routers of different autonomous systems, whose main function is to switch the network availability information among different Autonomous Systems (AS) and eliminate the routing lookback by the protocol mechanism itself.

The BGP takes the TCP protocol as the transmission protocol and ensures the transmission reliability of the BGP by the reliable transmission TCP mechanism.

The router which operates the BGP protocol is referred to as the BGP Speaker, and the BGP Speakers which set up the BGP session connection are referred to as the BGP Peers.

Two modes can be used to establish the BGP peers among BGP Speakers, such as IBGP (Internal BGP) and EBGP (External BGP). The IBGP refers to establish the BGP connection within the same AS, while the EBGP refers to establish the BGP connection among different ASs. In a word, the function of two connections is that the EBGP is to switch the route information among different ASs, while the IBGP is to carry out the transition of route information within this AS.

The BGP protocol of this product presents such characteristics as follows:

- BGP-4 Supported
- Path Attribute Supported
  - ✓ ORIGN Attribute
  - ✓ AS_PATH Attribute
  - ✓ NEXT_HOP Attribute
  - ✓ MULTI_EXIT_DISC Attribute
  - ✓ LOCAL-PREFERENCE Attribute
  - ✓ ATOMIC_AGGREGATE Attribute
  - ✓ AGGREGATOR Attribute
  - ✓ COMMUNITY Attribute
  - ✓ ORIGINATOR_ID Attribute
  - ✓ CLUSTER_LIST Attribute
- BGP Peer Groups Supported
- Loopback Interface Supported
- MD5 Authentication of TCP Supported
- Synchronization of BGP and IGP Supported

- BGP Route Aggregate Supported
- BGP Route Dampening Supported
- BGP Routing Reflector Supported
- AS Confederation Supported
- BGP Soft Reset Supported

29.1 Operating BGP Protocol

To operate the BGP function, execute the following operations in the privileged mode:

Command	Meaning
Router# **configure terminal**	Enter into the global configuration mode.
Router(config)# **ip routing**	Enable the routing function (if the switch is disabled)
Router(config)# **router bgp** *as-number*	Enable the BGP and configure this AS number to enter into the BGP configuration mode. The range of AS-number is 1~65535.
Router(config-router)# **bgp router-id** *router-id*	(Optional) Configure the ID used when this switch runs the BGP protocol.
Router(config-router)# **end**	Return to the privileged EXEC mode.
Router# **show run**	Show current configuration.
Router# copy running-config startup-config	Save the configuration.

Use the **no router bgp** command to close the **BGP.**

29.2 Default Configuration of BGP

In this product, it will not enable the BGP protocol by default.

After the BGP protocol is enabled, the default configuration of the BGP is shown as follows:

Router ID		To configure the Loopback interface, select the maximal one from the Loopback interface addresses. Otherwise, select the maximal interface address from the direct-connected interface.
Synchronization of BGP and IGP		Enabled
Generation of Default Route		Off
Allowed Hops of EBGP	Status	Off
	Multi-hops of EBGP	255

TCP MD5 Authentication Used		Off
Timer	Keepalive Time	60seconds
	Holdtime	180seconds
	ConnectRetry Time	120seconds
	AdvInterval(IBGP)	15seconds
	AdvInterval(EBGP)	30seconds
Path Attribute	MED	0
	LOCAL_PREF	100
Route Aggregate		Off
Routing Dampening	Status	Off
	Suppress Limit	2000
	Half-life-time	15minutes
	Reuse Limit	750
	Max-suppress-time	4*half-life-time
Route Reflector	Status	Off
	Cluster ID	Undefined
	Route among reflection clients	Enabled
AS Confederation		Off
Soft Reset		Off
Management Distance	External-distance	20
	Internal-distance	200
	Local-distance	200

29.3 Inject Route Information to BGP Protocol

The route information of the GBP is empty when it operates at just. Two measures can be taken to inject the route information to the BGP:

Manually inject the route information to the BGP by the Network commands.

Inject the route information to the BGP from the IGP by the interaction with the IGP protocol.

The BGP will issue the injected route information to its neighbors. This section will describe the manual injection of the route information. For the injection of the route information from the IGP, refer to the *Configuration of BGP and IGP Interaction* in related section.

To inject the network information advertised by the BGP Speaker to its BGP Speaker by means of the Network commands by manual, execute the following operations in the BGP configuration mode:

Command	**Meaning**
Router(config-router)# **network** *network-number* **mask** *network-mask* [**route-map** *map-tag*]	(Optional) Configure the network to inject the BGP routing table within this AS.

Use the **no network** *network-number* **mask** *network-mask* command to cancel the network to be sent. If it is necessary to cancel the used route-map, configure it again by using the Route-map Not Added option. If the configured network information is of standard class A, class B or class C network address, the mask option of this command may not be used.

The BGP4+ supports the IPv6 routing, and this command can be used to configure the route information of IPv6 in address-family ipv6.

Caution

1. The **network** command is used to inject the route of IGP into the route table of BGP, and the advertised Networks may be direct-connected route, static route and dynamic route.
2. For the external gateway protocol (EGP), the **network** command indicates the network to be advertised, which is different from the internal gateway protocol (IGP, such as OSPF and RIP). The latter uses the **network** commands to determine where the routing update will be sent to.

Sometimes, we hope some route of IGP is optimal, and the route information of EBGP is not used, so the configuration command **network backdoor** can be used to perform this function. Execute the following operations in the BGP configuration mode:

Command	**Meaning**
Router(config-router)# **network** *network-number* **mask** *network-mask* **backdoor**	(Optional) Indicate to transmit the availability information by the backdoor route.

Use the **no network** *network-number* **mask** *network-mask* **backdoor** command to cancel the indicated backdoor network information.

Caution

By default, the management distance of the network information learned about from the BGP Speakers which establish the EBGP connection is 20. Set the management distance of such network information by the **network backdoor** as 200.

Hence, the identical network information learned from the IGP presents higher priority. These networks learned from the IGP are considered as the backdoor network, and will not be advertised.

29.4 Configuring BGP Peer (Group) and Its Parameters

For the BGP is an external gateway protocol (EGP), it is necessary for the BGP Speakers to know who is their peer (BGP Peer).

It is mentioned in the overview of the BGP protocol that two modes can be used to set up the connection relationship among BGP Speakers, such as IBGP (Internal BGP) and EBGP (External BGP). It will judge which connection mode will be established among BGP Speakers by the AS of BGP Peer and that of the BGP Speakers.

Under normal condition, it is required to establish direct connection among BGP Speakers in a physical way for the EBGP connection. However, the BGP Speakers which establish the IBGP connection may be in any place within the AS.

To configure the BGP peer, Execute the following operations in the BGP configuration mode:

Command	Meaning
Router(config-router)# **neighbor** {*address*|*peer-group-name*} **remote-as** *as-number*	Configure the BGP peer. *Address* indicates the ip addresses of the bgp peer. *Peer-group-name* indicates the name of the bgp peer-group. The range of *as-number* is 1~65535.

Use the **no neighbor** {*address*|*peer-group-name*} to delete one peer or the peer group.

For the BGP Speakers, the configuration information of several peers (including the executed routing strategy) is identical. To simplify the configuration and improve the efficiency, it is recommended to use the BGP peer group.

To configure the BGP peer, Execute the following operations in the BGP configuration mode:

Command	Meaning
Router(config-router)# **neighbor** *peer-group-name* **peer-group**	(Optional) Create the BGP peer group.
Router(config-router)# **neighbor** *address* **peer-group***peer-group-name*	(Optional) Set the BGP peer as the member of the BGP peer group.
Router(config-router)# **neighbor** *peer-group-name* **remote-as** *as-number*	(Optional) Configure the peer group of BGP. The range of *as-number* is 1~65535.

Use the **no neighbor** *address* **peer-group** to delete some member of the peer group.

Use the **no neighbor** *peer-group-name* **peer-group** to delete the whole peer group.

Use the **no neighbor** *peer-group-name* **remote-as** to delete all members of the peer group and the AS number of the peer group.

To configure the peer of the BGP Speakers or the optional parameter of the peer group, Execute the following operations in the BGP configuration mode:

Command	**Meaning**
DGS-3610(config-router)# **neighbor** *{address* | *peer-group-name}* **update-source** *interface*	(Optional) Configure the network interfaces to establish the BGP Session with specified BGP peer (groups).
Router(config-router)# **neighbor** {*address* | *peer-group-name*} **ebgp-multihop** [*ttl*]	(Optional) Allow to establish the BGP Session among non-direct-connected EBGP peer (group). The range of TTL is 1~255, the EBGP is 1 hop by default, and the IBGP is 255 hops by default.
Router(config-router)# **neighbor**{*address* | *peer-group-name*} **password** *string*	(Optional) Enable the TCP MD5 authentication when the connection is established among specified BGP peer (group), and configure the password.
Router(config-router)# **neighbor** {*address* | *peer-group-name*} **times** *keepalive holdtime*	(Optional) Configure the Keepalive and Holdtime value to establish the connection among specified BGP peer (group). The range of the *keepalive is* 1~65535 seconds, 60 seconds by default. The range of the *holdtime is* 1~65535 seconds, 180 seconds by default.
Router(config-router)# **neighbor** {*address* | *peer-group-name*} **advertisemet-interval** *seconds*	(Optional) Configure the minimal time interval to send the routing update to specified BGP peer (group). The range of advertisement-interval is 1~600 seconds, the IBGP peer is 15 seconds by default, and the EBGP peer is 30 seconds by default.
Router(config-router)# **neighbor** {*address* | *peer-group-name*} **default-originate** [**route-map** *map-tag*]	(Optional) Configure to send the default route to specified BGP peer (group).
Router(config-router)# **neighbor** {*address* | *peer-group-name*} **next-hop-self**	(Optional) Configure to set the next route information as this BGP speaker when the route is distributed to specified BGP peer (group).
Router(config-router)# **neighbor** {*address* | *peer-group-name*} **remove-private-as**	(Optional) Configure to delete the private AS number in the AS path attribute when distributing the route information to the EBGP peer (group).
Router(config-router)# **neighbor** {*address* | *peer-group-name*}**send -community**	(Optional) Configure to send the community attribute to specified BGP peer (group).

Command	**Meaning**
Router(config-router)# **neighbor** {*address* | *peer-group-name*} **maximum-prefix** *maximum* [**warning-only**]	(Optional) Limit the number of the route information received from specified BGP peer (group).
Router(config-router)# **neighbor** {*address* | *peer-group-name*} **distribute-list** *access-list-name* {**in** | **out**}	(Optional) Configure to implement the routing strategy according to the access list when the route information is received from and sent to specified BGP peer (group).
Router(config-router)# **neighbor** {*address* | *peer-group-name*} **prefix-list** *prefix-list-name* {**in** | **out**}	(Optional) Configure to implement the routing strategy according to the prefix list when the route information is received from and sent to specified BGP peer (group).
Router(config-router)# **neighbor** {*address* | *peer-group-name*} **route-map** *map-tag* {**in** | **out**}	(Optional) Configure to implement the routing strategy according to the route-map when the route information is received from and sent to specified BGP peer (group).
Router(config-router)# **neighbor** {*address* | *peer-group-name*} **filter-list** *path-list-name* {**in** | **out**}	(Optional) Configure to implement the routing strategy according to the AS path list when the route information is received from and sent to specified BGP peer (group).
Router(config-router)# **neighbor** {*address* | *peer-group-name*} **unsuppress-map** *map-tag*	(Optional) Configure to selectively advertise the route information suppressed by the **aggregate-address** command previously when it is distributed to specified BGP peer.
Router(config-router)# **neighbor** {*address* | *peer-group-name*} **soft-reconfiguration inbound**	(Optional) Restart the BGP session and reserve the unchanged route information sent by the BGP peer (group).
Router(config-router)# **neighbor** {*address* | *peer-group-name*} **route-reflector-client**	(Optional) Configure this switch as the route reflector and specify its client.
Router(config-router)# **neighbor** {*address* | *peer-group-name*} **shutdown**	(Optional) Shut down the BGP peer (group).

Use the **no** mode of above commands to disable the configured content.

If one peer is not configured with the **remote-as**, each of its members can use the **neighbor remote-as** command to configure it independently.

By default, each member of the peer group will inherit all configurations of the peer group. However, each member is allowed to configure the optional configurations which have no effect on the output update independently, to replace the unified configuration of the peer group.

Caution

Each memberof the peer is allowed to configure the optional independently for replacing the unified configuration of it. But the information independently configured does not contain the updated configuration information effected on the output. That is to say, Each member of the peer group will inherit following configuration for the peer groups: **remote-as, update-source, local-as, reconnect-interval , times, advertisemet-interval, default-originate, next-hop-self, password remove-private-as, send-community , distribute-list out, filter-list out, prefix-list out, route-map out, unspress-map, route-reflector-client.**

Use the commane neighbor update-source to select the effective interface to establish the connection of TCP. The important role of this command is to provice Loopback interface for using, so as to the connection reached to the IBGP Speaker is more stable.

By default, it's required to phisically direct-connect with for the BGP Peers to establish the connection with EBGP. You can use **neighbor ebgp-multihop** command to establish the EBGP peers among the non-direct-connection External BGP Speakers.

Caution

For prevent the route loop and vibration, It is necessary to present the non-default routing to reach the opposite party among EBGP peers established the connection with BGP which multi-hop is needed..

For the sake of the security, you can set the authentication for the BGP peers (group) which will establish the connection, the authentication uses the MD5 algorithm. The authentication password set for the BGP peer should be identical. The process to enable the MD5 authentication in BGP is shown as follows:

Command	Meaning
Router(config-router)# **neighbor** {*address* | *peer-group-name*} **password** *string*	When the BGP connection with the BGP peer is established, use this command to enable the TCP MD5 authentication and set the password.

Use the **no neighbor** {*ip-address* **|** *peer-group-name*} **password** command to disable the MD5 authentication set among the BGP peer (group).

Use the **neighbor shutdown** command to disable the valid connection established with the peer (group) immediately, and delete all route information related to the peer (group).

Caution

To disable the connection established with specified peer (group) and reserve the configuration information set for this specified peer (group), use the **neighbor shutdown** command. If such configuration information is not required again, use the **no neighbor** [**peer-group**] command.

29.5 Configuring Management Policy for BGP

Once the routing policy (including the **distribute-list**, **neighbor route-map**, **neighbor prefix-list and neighbor filter-list)** changes at any time, it is necessary to take effective measure to implement new route policies. Traditional measure is to close it and reestablish new BGP connection.

This product supports to implement new routing policy without the close of the BGP session connection by the configuration of the soft reset for BGP effectively.

To facilitate the description of the BGP soft reset, the following will refer to the route policy which has an effect on the input route information as the input route policy (such as the In-route-map and In-dist-list), and that has an effect on the output route information as the output route strategy (such as the Out-route-map and Out-dist-list).

If the output routing policy changes, execute the following operations in the BGP configuration mode:

Command	Meaning
Router(config-router)# **clear ip bgp** {* | **neighbor** *address* | **peer-group** *peer-group-name* | **external**} **soft out**	For the soft reset BGP connection, it is not necessary to restart the BGP Session and activate the implement of the route policy.

If the input route policy changes, its operation will be more complicated than that of the output route policy: For the implement of the output routing policy is based on the route information table of this BGP Speaker. The implement of the input routing policy is based on the route information received from the BGP Peer. To reduce the memory consumption, the local BGP Speaker will not remain the original route information received from BGP Peers.

If it is necessary to modify the input routing policy, the common method is to save the original route information for each specified BGP peer in this BGP Speaker by the **neighbor soft-reconfiguration inbound** command, so as to provide the original foundation of the route information to modify the input route policy in the future.

At present, there is a standard implement method referred to as the Route Refresh Performance, which can support to modify the route policy without the storage of the original route information. This product supports the route refreshing performance.

If the input route policy changes, execute the following operations in the BGP configuration mode:

Command	Meaning
Router(config-router)# **neighbor** {*address* | *peer-group-name*} **soft-reconfiguration inbound**	(Optional) Restart the BGP session and reserve the unchanged route information sent by the BGP peer (group). Execution of this command will consume more memory. If both parties support the route refreshing performance, it is not necessary to execute this command.
Router(config-router)# **clear ip bgp** {* | **neighbor** *address* | **peer-group** *peer-group-name* | **external**} **soft in**	For the soft reset BGP connection, it is not necessary to restart the BGP Session and activate the implement of the route policy.

You can judge whether the BGP peer supports the route refreshing performance by the **show ip bgp neighbors** command. If it is supported, you need to execute the **neighbor soft-reconfiguration inbound** command when the input route policy changes.

29.6 Configuring Synchronization between BGP and IGP

For it will pass through this AS and reach another AS, the route information will be advertised to another AS only when it can ensure that all routers within this AS learn about this route information. Otherwise, if some routers (operate the IGP protocol) within this AS don’t learn about this route information, the data message may be discarded for these routers don’t know this routing when the data message passes through this AS, namely, it will cause the route black hole.

The ensuring of all routers within this AS learn about the route information out of this AS is referred to as the synchronization of BGP and IGP. The simple implement method of the synchronization is that the BGP Speakers redistribute all of the routes learned out by the BGP protocol to the IGP, to ensure the routers within the AS learn about such route information.

The synchronization mechanism of BGP can be cancelled under two conditions:

1. There is no the route information which pass through this AS (In general, this AS is an end AS).
2. All routers within this AS operate the BGP protocol and the full connection relationship is established among all BGP Speakers (The adjacent relationship is established between any two BGP Speakers).

Caution By default, the synchronization is enabled. However, to ensure the quick convergence of the route information, it is recommended to cancel the synchronization mechanism if possible.

To cancel the synchronization mechanism of BGP speakers, execute the following operations in the BGP configuration mode:

Command	**Meaning**
Router(config-router)# **noSynchronization**	(Optional) Cancel the synchronization of BGP and IGP.

Execute the **synchronization** command to enable the synchronization mechanism.

29.7 Configuring Interaction between BGP and IGP

To configure to inject the route information generated by the IGP protocol into the BGP, execute the following operations in the BGP configuration mode:

Command	**Meaning**
Router(config-router)# **redistribute** [**connected** | **ospf** | **rip** | **static | isis**] [**route-map** *map-tag*]	(Optional) Reassign the route information generated by other route protocols.

29.8 Configuration Timer of BGP

The BGP uses the Kepalive timer to maintain the effective connection with the peers, and takes the Hldtime timer to judge whether the peers are effective. By default, the value of the Kepalive timer is 60s, and the value of the Holdtime timer is 180s. When the BGP connection is established between BGP Speakers, both parties will negotiate with the Holdtime and that with smaller value will be selected. While, the selection of the Keepalive timer is based on the smaller one between 1/3 of the negotiated Holdtime and the configured Keepalive.

To adjust the value of the BGP timer based on all peers, execute the following operations in the BGP configuration mode:

Command	**Meaning**
Router(config-router)# **timers bgp** *keepalive holdtime*	(Optional) Adjust the keepalive and holdtime value of BGP based on all peers. The range of the *keepalive is* 1~65535 seconds, and 60 seconds by default. The range of the *holdtime is* 1~65535s, 180s by default.

Of course, you can adjust the value of the BGP timer based on specified peers, and execute the following operations in the BGP configuration mode:

Command	**Meaning**
Router(config-router)# **neighbor** {*address* | *peer-group-name*} **times** *keepalive holdtime*	(Optional) Configure the Keepalive and Holdtime value to establish the connection with specified BGP peer (group). The range of the keepalive is 1~65535s, 60s by default. The range of the holdtime *is* 1~65535s, 180s by default.

Use the **no** option of corresponding commands to clear the value of configured timer.

29.9 Configuring Path Attribute for BGP

29.9.1 AS_PATH Attribute Related Configuration

The BGP can control the distribution of the route information in three ways:

- IP Address, you can carry out it by using the **neighbor distribute-list** and **neighbor prefix-list** commands.
- AS_PATH Attribute, refer to the description in this section.
- COMMUNITY Attribute, refer to the COMMUNITY Attribute Related Configuration.

You can use the AS path-based Access Control List to control the distribution of the route information. Of which, the AS path-based Access Control List will use Regular Expression to resolute the AS path.

To configure the AS path-based distribution of the route information, execute the following operations in the privileged mode:

Command	**Meaning**
Router# **configure terminal**	Enter into the global configuration mode.
Router(config)# **ip as-path access-list** *path-list-name* {**permit** | **deny**} *as-regular-expression*	(Optional) Define an AS path list.
Router(config)# **ip routing**	Enable the route function (if disabled)
Router(config)# **router bgp** *as-number*	Enable the BGP and configure this AS number to enter into the BGP configuration mode.
Router(config-router)# **neighbor** {*address* | *peer-group-name*} **filter-list** *path-list-name* {**in** | **out**}	(Optional) Configure to implement the route strategy according to the AS path list when the route information is received from and sent to specified BGP peer (group).

Command	Meaning
Router(config-router)# **neighbor** {*address* | *peer-group-name*} **route-map** *map-tag* {**in** | **out**}	(Optional) Configure to implement the route policy according to the route-map when the route information is received from and sent to specified BGP peer (group). In the route-map configuration mode, you can use the **match as-path** to operate the AS path attribute by the AS path list, or take the **set as-path** to operate the AS attribute value directly.

The BGP will not take the length of the AS path into account when it selects the optimal path according to the implement of the standard (RFC1771). In general, the shorter the length of the AS path, the higher the path priority is. Hence, we take the length of the AS path when we select the optimal path. You can determine whether it is necessary to take the length of the AS path into account when you select the optimal path according to the actual condition.

If you don't hope take the length of the AS path into account when you select the optimal path, execute the following operations in the BGP configuration mode:

Command	Meaning
Router(config-router)# **bgp bestpath as-path ignore**	(Optional) Allow the BGP to compare with the length of the AS path when the optimal path is selected.

Caution

Within the whole AS, whether all BGP Speakers takes the length of the AS path into account will be consistent when the optimal path is selected. Otherwise, the optimal path information selected by various BGP Speakers will not be consistent with each other.

29.9.2 NEXT_HOP Attribute Related Configuration

To set the next hop as this BGP Speaker when the route is sent to the specified BGP peer, you can use the **neighbor next-hop-self** command, which mainly provides for the use of the non-mesh networks (such as frame relay and X.25). Execute the following operations in the BGP configuration mode:

Command	Meaning
Router(config-router)# **neighbor** {*address* | *peer-group-name*} **next-hop-self**	(Optional) Configure to set the next route information as this BGP speaker when the route is distributed to specified BGP peer (group).

You can also modify the next hop of specified path by the **set next-hop** command of Route-map.

Caution	This command is not recommended to use under the full mesh network environment (such as Ethernet), for this command will cause the extra hops of the message and increase unnecessary overhead.

29.9.3 MULTI_EXIT_DISC Attribute Related Configuration

The BGP takes the MED value as the foundation to compare with the priority of the path learned from the EBGP Peers. The smaller the MED value, the higher the priority of the path is.

By default, it will only compare with the MED value for the path of the peers from the same AS when the optimal path is selected. If you hope to compare with the MED value for the path of the peers from different AS's, execute the following operations in the BGP configuration mode:

Command	Meaning
Router(config-router)# **bgp always-compare-med**	(Optional) Allow to compare with the MED value for the path of different AS's.

By default, it will not compare with the MED value for the path of the peers for other AS's within the AS association when the optimal path is selected. If you hope to compare with the MED value for the path of the peers from different AS confederations, execute the following operations in the BGP :configuration mode

Command	Meaning
Router(config-router)# **bgp bestpath med confed**	(Optional) Allow to compare with the MED value for the path of the peers from other ASs within the confederation.

By default, if the path whose MED attribute is not set is received, The MED value of this path will be taken as 0. For the smaller the MED value, the higher the priority of the path is, the MED value of this path reaches the highest priority. If you hope the MED attribute for the path whose MED attribute is not set presents the lowest priority, execute the following operations in the BGP configuration mode:

Command	Meaning
Router(config-router)# **bgp bestpath med missing-as-worst**	(Optional) Set the priority of the path whose MED attribute is not set as the lowest.

By default, they will be compared with each other according to the sequence the paths are received when the optimal path is selected. If you hope to compare with the path of the peers from the same AS firstly, execute the following operations in the BGP configuration mode:

Command	Meaning
Router(config-router)# **bgp deterministic-med**	(Optional) Allow to compare with the path of the peers from the same AS firstly. By default, they will be compared with by the received sequence, the later received path will be compared with firstly.

29.9.4 LOCAL_PREF Attribute Related Configuration

The BGP takes the LOCAL_PREF as the foundation to compare with the priority of the path learned from the IBGP Peers. The larger the LOCAL_PREF value, the higher the priority of the path is.

The BGP Speakers will add the local preference when they send the received external route to the IBGP Peers. To modify the local preference, execute the following operations in the BGP configuration mode:

Command	Meaning
Router(config-router)# **bgp default local-preference** *value*	(Optional) Change the default local preference. The range of the value is 0~4294967295, 100 by default.

You can also modify the local preference of specified path by the **set local-preference** command of Route-map.

29.9.5 COMMUNITY Attribute Related Configuration

COMMUNITY Attribute is another method to control the distribution of the route information.

The community is a set of the destinations. The purpose of the definition for the community attribute is to implement the community-based routing strategy, so as to simplify the configuration to control the distribution of the route information in the BGP Speakers.

Each destination may be of more than one community, and the manager of the AS can define which community the destination is of.

By default, all destinations are of the Internet community, carried in the community attribute of the path.

At present, total for four common community attribute values are predefined:

- **Internet**: Indicate the Internet community, and all paths are of this community.
- **no-export**: Indicate this path will not be issued to the \BGP peers.
- **no-export**: Indicate this path will not be issued to the BGP peers.

- **local-as**: Indicate this path will not be issued to out of this AS. When the confederation is configured, this path will not be issued to other autonomous systems or sub autonomous systems.

You can control the receiving, priority and distribution of the route information by the community attribute.

The BGP Speakers can set, add or modify the community attribute value when they learn about, issue or redistribute the route. The aggregated path includes the community attribute of all aggregated paths when the route aggregate is carried out.

To configure the community attribute-based distribution of the route information, execute the following operations in the privileged mode:

Command	**Meaning**
Router# **configure terminal**	Enter into the global configuration mode.
Router(config)# **ip community-list standard** *community-list-name* {**permit** | **deny**} *community-number*	(Optional) Create the community list. The *community-list-name* is the name of the community list. The community-number is the concrete value of the community list, which may be one of the value you specified within 1~4,294,967,200, or the well-known community attribute such as internet, local-AS, no-advertise and no-export.
Router(config)# **ip routing**	Enable the routing function (if disabled)
Router(config)# **router bgp** *as-number*	Enable the BGP and configure this AS number to enter into the BGP configuration mode.
Router(config-router)# **neighbor** {*address* | *peer-group-name*} **send-community**	(Optional) Configure to send the community attribute to specified BGP peer (group).
Router(config-router)# **neighbor** {*address* | *peer-group-name*} **route-map** *map-tag* {**in** | **out**}	(Optional) Configure to implement the route strategy according to the route-map when the route information is received from and sent to specified BGP peer (group). In the route-map configuration mode, you can use the **match community-list [exact]** and **set community-list delete** to operate the community attribute by the community list, or take the **set community** command to operate the community attribute value directly.

29.9.6 Other Related Configuration

By default, if two paths with full identical path attributes are received from different EBGP Peers during the selection of the optimal path, we will select the optimal path according to the path received sequence. You can select the path with smaller Router ID as the optimal path by configuring the following commands.

Command	Meaning
Router(config-router)# **bgp bestpath compare-routerid**	(Optional) Allow the BGP to compare with the router ID when the optimal path is selected.

29.10 Selection of Optimal Path for BGP

The selection of the optimal route is an important part of the BGP protocol. The following will describe the selection process of the BGP route protocol in details:

1. If the route table item is invalid, it will not participate in the selection of the optimal route.

Caution

The invalid table item includes the items the next hop can not be reached and the vibrated table items.

2. Select the route with the maximal weight.
3. If else, select the route with high LOCAL_PREF attribute value.
4. If else, select the route generated by this BGP speaker.
   The route generated by this BGP speaker includes that generated by the network command, the redistribute command and the aggregate command.
5. If else, select the route with the shortest AS length.
6. If else, select the route with the lowest ORIGIN attribute value.
7. If else, select the route with the smallest MED value.
8. If else, the priority of the EBGP path is higher than that of the route of the IBGP path and the AS confederation, and the priority for the IBGP path and the AS confederation is identical.
9. If else, select the routing with the smallest IGP metric to reach the next hop.
10. If else, select the route which advertises that the router ID of the BGP speaker for this route is small.

Caution

Above is the optical process of the route by default configuration. You can change the selection process of the route by the CLI command. For instance, you can use the **bgp bestpath as-path ignore** command to make the step 5 in the optimal process of the route invalid.

29.11 Configuring Route Aggregate for BGP

For the BGP-4 supports CIDR, it allows to create the aggregate table item to reduce the BGP route table. Of course, only when there is valid path within the aggregate scope, the BGP aggregate table item will be added to the BGP route table.

To configure the BGP route aggregate, execute the following operations in the BGP configuration mode:

Command	Meaning
Router(config-router)# **aggregate-address** *address mask*	(Optional) Configure the aggregate address.
Router(config-router)# **aggregate-address** *address mask* **as-set**	(Optional) Configure the aggregate address, and remain the AS path information of the path within the scope of the aggregate address.
Router(config-router)# **aggregate-address** *address mask* **summary-only**	(Optional) Configure the aggregate address and only advertise the aggregated path.
Router(config-router)# **aggregate-address** *address mask* **as-set summary-only**	(Optional) Configure the aggregate address, and remain the AS path information of the path within the scope of the aggregate address. At the same time, only the aggregated path is advertised.

Use the **no** mode of above commands to disable the configured content.

⚠ **Caution** By default, the BGP will advertise all path information both before and after aggregation. If you only hope to advertise the aggregated path information, use the **aggregate-address summary-only** command.

29.12 Configuring Route Reflector for BGP

To speed up the convergence of the route information, all BGP Speakers within one AS will usually establish the full connection relationship (The adjacent relationship is established between any two BGP Speakers). If the BGP Speakers within the AS is too much, it will increase the resource overhead of the BGP Speakers, raise the workload and complexity of the task assignment for the network manager and reduce the network expansibility capacity.

For this reason, two measures such as the route reflector and AS confederation are proposed to reduce the connections of the IBGP peers within AS.

The route reflector is a measure to reduce the connections of the IBGP peer within the AS. One BGP Speaker is set as the route reflector, which divides the IBGP peer within this AS into two types, such as client and non-client.

The rule to implement the route reflector within the AS is shown as follows:

- Configure the route reflector and specify its client, so the route reflector and other clients form a cluster. The route reflector establishes the connection relationship with clients.
- The clients of the route reflector within one cluster should not establish the connection relationship with other BGP Speakers of other clusters.
- Within AS, the full connection relationship is established among the IBGP peer of non-clients. Where, the IBGP peer of non-clients includes the following conditions: among several route reflectors within one cluster, among the route reflector within the cluster and the BGP Speakers which don’t participate in the route reflector function out of the cluster (In general, the BGP Speakers don’t support the route reflector function), among the route reflector within the cluster and the route reflector of other cluster.

The processing rule when the route reflector receives one route is shown as follows:

- The route update received from the EBGP Speaker will be sent to all clients and non-clients.
- The route update received from the clients will be sent to other clients and all non-clients.
- The route update received from the IBGP non-clients will be sent to all its clients.

To configure the BGP route reflector, execute the following operations in the BGP configuration mode:

Command	**Meaning**
Router(config-router)# **neighbor** {*address* | *peer-group-name*} **route-reflector-client**	(Optional) Configure this product as the route reflector and specify its clients.

In general, one group is only configured with one route reflector. In this case, the Router ID of the route reflector can be used to identify this cluster. To increase the redundancy, you can set more than one route reflector within this cluster. In this case, you must configure the cluster ID, so that one route reflector can identify the route update from other route reflectors of this cluster.

Caution

To set several route reflectors for one cluster, it is necessary for you to configure a cluster ID for this cluster.

To configure the cluster ID of the BGP, execute the following operations in the BGP configuration mode:

Command	**Meaning**
Router(config-router)# **bgp cluster-id** *cluster-id*	(Optional) Configure the cluster ID of the route reflector.

In general, it is not necessary to establish the connection relationship between the clients of the route reflector within the cluster, and the route reflector will reflect the route among clients. However, if the full connection relationship is established for all clients, the function for the route reflector to reflect the client route can be cancelled.

To cancel the function of reflecting the client route, execute the following operations in the BGP configuration mode:

Command	Meaning
Router(config-router)# **no bgp client-to-client reflection**	(Optional) Cancel the route reflector among clients.

29.13 Configuring Route Dampening for BGP

The route changes between the validity and invalidity is referred to as the route flap. The route flap usually causes the unstable route to be transmitted on Internet, which will result in the instability of the network. The BGP route dampening is a measure to reduce the route flap, which will reduce the possible route flap by monitoring the route information of EBGP Peers.

The route dampening of BGP uses the following glossaries:

- Route Flap, the route changes between validity and invalidity.
- Penalty: For each route flap, enable the BGP Speakers of the route dampening to add one penalty for this route, which will be accumulated to exceed the suppress limit.
- Suppress Limit: When the penalty of the route exceeds this value, this route will be suppressed.
- Half-life-time: The time passed through when the penalty is reduced to half of its value.
- Reuse Limit: When the penalty of the route is lower than this value, the route suppression is released.
- Max-suppress-time: The maximal time the route can be suppressed.

The brief description of the route dampening processing: For one route flap, the BGP Speakers carry out one penalty for this route (Accumulated to the penalty). Once the penalty value reaches the suppress limit, the route will be suppressed. When the half-life-time reaches, the penalty value is reduced to half of its value. Once the penalty value is reduced to the reuse limit, the route will be activated again. The maximal time the route is suppressed is the maximal suppress time.

To configure the route dampening of the BGP, execute the following operations in the BGP configuration mode:

Command	Meaning
Router(config-router)# **bgp dampening**	Enable the Route dampening of the BGP.

Command	**Meaning**
Router(config-router)# **bgp dampening** *half-life-time reuse suppress max-suppress-time*	(Optional) Configure the parameters of the route dampening. half-life-time(1-45minutes), 15minutes by default. reuse (1-20000), 750 by default. suppress (1-20000), 2000 by default. max-supress-time (1-255minutes), 4*half-life-time by default.

If it is necessary to monitor the route dampening information, execute the following operations in the privileged mode:

Command	**Meaning**
Router# **show ip bgp dampening flap-statistics**	Show the flap statistics information of all routers.
Router# **show ip bgp dampening dampened-paths**	Show the dampened statistics information.

To clear the route dampened information or clear the dampened route, execute the following operations in the BGP configuration mode:

Command	**Meaning**
Router# **clear ip bgp flap-statistics**	Clear the flap statistics information of all un-dampened route.
Router# **clear ip bgp flap-statistics** *address mask*	Clear the flap statistics information of specified route (excluding the dampened route).
Router# **clear ip bgp dampening** [*address mask*]	Clear the flap statistics information of all routes, and release the suppressed routes.

29.14 Configuring AS Confederation for BGP

The confederation is a measure to reduce the connections of the IBGP peer within the AS.

One AS is divided into several sub ASs and one unified confederation ID (namely, confederation AS number) is set to constitute these sub ASs into a confederation. For the external confederation, the whole confederation is still considered as one AS, and only the confederation AS number is visible for the external network. Within the confederation, the full IBGP peer connection is still established among the BGP Speakers within the sub AS, and the EBGP connection is established among the BGP Speakers within the sub AS. Although the EBGP connection is established among BGP Speakers within the sub AS, the path attribute information of NEXT_HOP, MED and LOCAL_PREF retains constant when the information is exchanged.

To implement the AS confederation, execute the following operations in the BGP configuration mode:

Command	Meaning
Router(config-router)# **bgp confederation identifier** *as-number*	Configure the AS confederation number. The range of *as-number* is 1~65535.
Router(config-router)# **bgp confederation peers** *as-numbe* [*as-number..*]	Configure other sub AS numbers within the AS confederation. The range of *as-number* is 1~65535.

Use the **no** mode of above commands to disable the configured content.

29.15 Configuring Management Distance for BGP

The management distance indicates the reliability of the route information resource, whose range is 1-255. The larger the value of the management distance, the lower the reliability is.

The BGP sets different management distances for various information sources learned, such as External-distance, Internal-distance and Local-distance.

- External-distance: The management distance of route learned from the EBGP Peers.
- Internal-distance: The management distance of route learned from the IBGP Peers.
- Local-distance: The management distance of route learned from the Peers, but it is considered that the optimal one can be learned from the IGP. In general, these routes are indicated by the Network Backdoor command.

To modify the management distance of the BGP protocol, execute the following operations in the BGP configuration mode:

Command	Meaning
Router(config-router)# **distance bgp** *external-distance internal-distance local-distance*	(Optional) Configure the management distance of BGP. The range of the distance is 1-255. For the default configuration: *external-distance* 20 *internal-distance* 200 *local-distance* 200

Use the **no** command to restore the default management distance of the BGP protocol.

Caution

It is not recommended to change the management distance of the BGP route. If it is necessary to change, please keep it in mind that:

1. The External-distance should be lower than the management distance of other IGP route protocol (OSPF and RIP).
2. The Internal-distance and Local-distance should be higher than the management distance of other IGP route protocol.

29.16 Monitoring of BGP

You can use the monitoring of the BGP to read the route table, buffer and database of the BGP. Execute the following operations in the privileged mode:

Command	Meaning
Router# **show ip bgp**	Show all BGP route information.
Router# **show ip bgp** {*network* | *network-mask* } [**longer-prefixes**]	Show the BGP route information of the specified destination.
Router# **show ip bgp prefix-list** *prefix-list-name*	Show the BGP route information of specified destination which matches with the prefix list.
Router# **show ip bgp community** [**exact**] *community-number*	Show the BGP route information included with specified community value.
Router# **show ip bgp community-list** *community-lister-number* [**exact**]	Show the BGP route information which matches with specified community list.
Router# **show ip bgp filter-list** *path-list-number*	Show the BGP route information which matches with specified AS path list.
Router# **show ip bgp regexp** *as-regular-expression*	Show the BGP route information of specified regular expression which matches with the AS path attribute.
Router# **show ip bgp dampened-paths**	Show the suppressed flap statistics information.
Router# **show ip bgp flap-statistics**	Show the flap statistics information of all routes with the flap record.
Router# **show ip bgp neighbors** [*address*] [**received-routes** | **routes** | **advertised-routes** | **flap-statistics** | **dampened-routes**]	Show the information of the BGP peer.
Router# **show ip bgp summary**	Briefly show the configuration of the BGP Router itself and the information of the peer.
Router# **show ip bgp peer-group** [*peer-group-name*]	Show the configuration information of the BGP peer group.

29.17 Protocol Independent Configuration

29.17.1 route-map Configuration

The BGP protocol applies the Route-map policy on a large scale. For the configuration of the Route-map policy, refer to the *Protocol Independent Configuration* part in this manual.

29.17.2 Regular Expression Configuration

The regular expression is the formula to match the string according to a certain template. The regular expression is used to evaluate the text data and return a true or false value. That is to say, whether the expression can describe this data correctly.

29.17.2.1 Description of Control Characters for Regular Expression

The BGP path attribute uses the regular expression. Here will briefly describe the use of the special characters for the regular expression:

Characters	Signs	Special Meanings
Period	**.**	Match with any single character.
Asterisk	*****	Match with none or any sequence of the strings.
Plus	**+**	Match with one or any sequence of the strings.
Interrogation Mark	**?**	Match with none or one sign of strings.
Plus Sign	**^**	Match with the start of strings.
Dollar	**$**	Match with the end of strings.
Underlining	_	Match with the comma, bracket, the start and end of strings and blank.
Square Brackets	**[]**	Match with the single character within specified scope.

29.17.2.2 Application Example of Regular Expression

At present, the equipment **show ip bgp** presents the content below:

```
DGS-3610# show ip bgp
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Status Network           Next Hop     Metric  LocPrf  Path
------ ------------------  ---------------   --------  --------  -------------------
*>  211.21.21.0/24    110.110.110.10  0     1000   200 300
*>  211.21.23.0/24    110.110.110.10  0     1000   200 300
*>  211.21.25.0/24    110.110.110.10  0     1000   300
*>  211.21.26.0/24    110.110.110.10  0      1000   300
*> 1.1.1.0/24       192.168.88.250  444         0   606
*> 179.98.0.0       192.168.88.250  444         0   606
*> 192.92.86.0      192.168.88.250  8883        0   606
*> 192.168.88.0     192.168.88.250  444         0   606
*> 200.200.200.0    192.168.88.250  777         0   606
```

At present, use the regular expression in the **show** command. The effect is shown as follows:

```
DGS-3610# show ip bgp regexp __300__
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Status Network       Next Hop          Metric  LocPrf  Path
------ ------------------  ---------------   ---------  ---------  -------------------
*>  211.21.21.0/24  110.110.110.10  0     1000   200 300
*>  211.21.23.0/24  110.110.110.10  0     1000   200 300
*>  211.21.25.0/24  110.110.110.10  0     1000   300
*>  211.21.26.0/24  110.110.110.10  0     1000   300
```

29.18 BGP Configuration Examples

The following lists the BGP configuration.

29.18.1 Configuring BGP Neighbor

The following will show how to configure the BGP neighbor. Use the **neighbor remote-as** command to configure the BGP neighbor. The concrete configuration is shown as follows:

router bgp 109

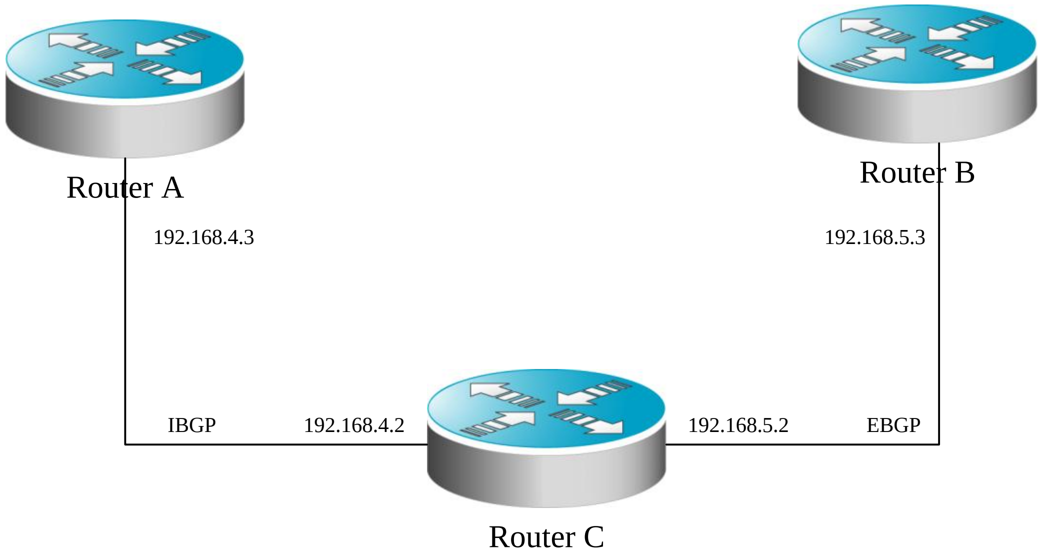
neighbor 131.108.200.1 remote-as 167

neighbor 131.108.234.2 remote-as 109

neighbor 150.136.64.19 remote-as 99

Configure one IBGP peer 131.108.234.2 and two EBGP peers such as 131.108.200.1 and 150.136.64.19.

The following is an example to configure the bgp neighbor. For the relationship among routers and the assignment of the IP addresses, refer to the schematics.



In this example, the bgp configuration of various devices is shown as follows:

Configuration of Device A:

```
!
router bgp 100
 neighbor 192.168.4.2 remote-as 100
```

Configuration of Device B:

```
!
router bgp 100
 neighbor 192.168.4.3 remote-as 100
 neighbor 192.168.5.3 remote-as 200
```

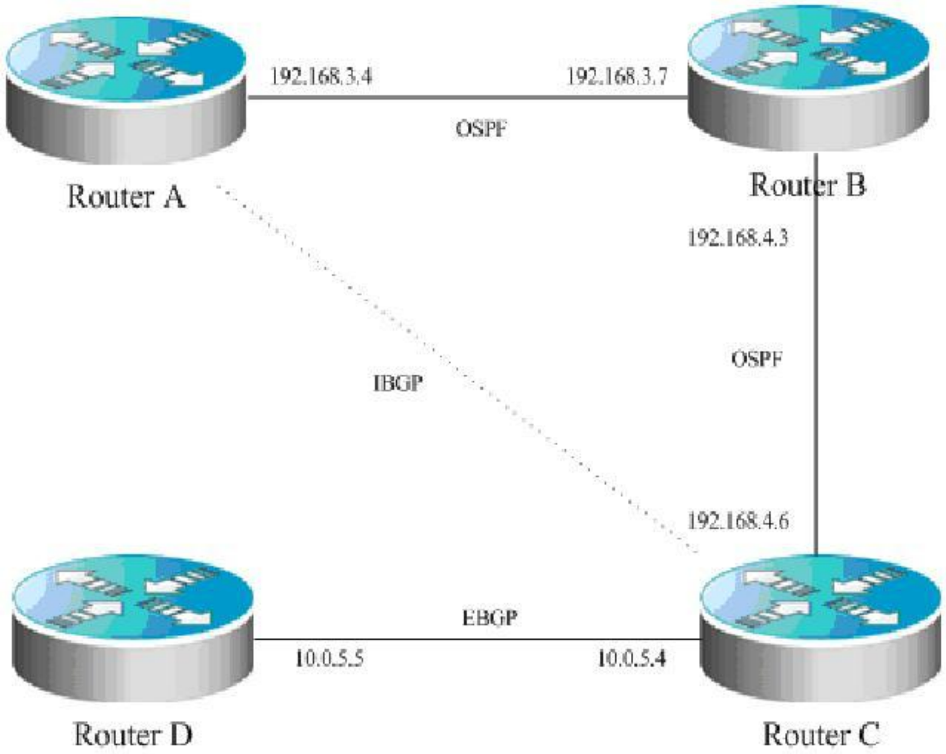
Configuration of Device C:

```
!
router bgp 200
 neighbor 192.168.5.2 remote-as 100
```

29.18.2 Configuring BGP Synchronization

Use the **synchronization** command to configure the use synchronization in the BGP routing configuration mode, and use the **no synchronization** command to cancel the configured synchronization.

Describe the function of synchronization, the relationship among equipments and the assignment of the IP addresses is shown as the schematics by the following configuration example:



In the schematics, there is a route p in the router A, which is sent to router C by the IBGP neighbor relationship. If the router C is configured with the BGP synchronization, it is necessary for the router C to wait for the IGP (this example uses the OSPF protocol) to receive the same route information p, so as to send the route p to the EBGP neighbor router D. If the router C is configured asynchronously, it is not necessary for the BGP to wait for the IGP to receive the route p, so as to send the route p to the EBGP neighbor router D.

29.18.3 Configuring Neighbors to Use aspath Filter

Configure the **as-path access-list** used for the filter in the configuration mode firstly. The configuration command is **ip as-path access-list**. Enter into the route configuration mode of the BGP after configuration, and use the **neighbor filter-list** command to apply the configured **as-path access-list** among the **neighbors** of the BGP, and carry out the **as-path** filter among the **neighbors**.

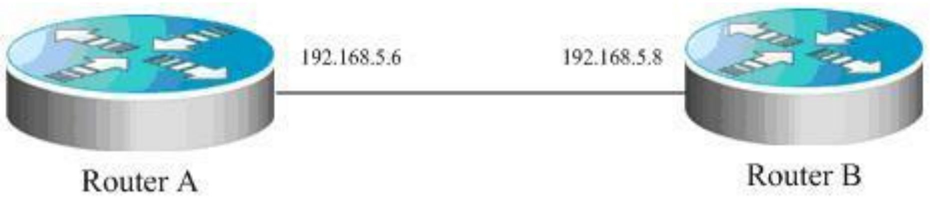
The detailed configurations are as below:

```
router bgp 200
neighbor 193.1.12.10 remote-as 100
neighbor 193.1.12.10 filter-list 2 out
neighbor 193.1.12.10 filter-list 3 in
ip as-path access-list 2 permit _200$
ip as-path access-list 2 permit ^100$
ip as-path access-list 3 deny _690$
ip as-path access-list 3 permit .*
```

This configuration indicates that only the route which passes through the **as-path access-list** *2* to filter can be advertised to the neighbor 193.1.12.10, and the advertised route from the neighbor 193.1.12.10 can be received only when it is filtered by the **as-path access-list** *3.*

Following is a configuration example, the relationship between the devices and the alloctioan of Ip address is shown:

Figure 29-3



Use the as-path to filter on the router A.

The configurations of all the devices are as below:

The configuration of Router A:

```
!
ip as-path access-list 4 deny ^300_
ip as-path access-list 4 permit .*
ip as-path access-list 5 deny ^450_65_
ip as-path access-list 5 permit .*
!
router bgp 100
bgp log-neighbor-changes
neighbor 192.168.5.8 remote-as 200
neighbor 192.168.5.8 filter-list 5 in
neighbor 192.168.5.8 filter-list 4 out
```

The configuration of Router B:

```
!
router bgp 200
bgp log-neighbor-changes
neighbor 192.168.5.6 remote-as 100
```

29.18.4 Configuring Aggregate Route

Use the **aggregate-address** command to configure the aggregate route in the route configuration mode. Once any route is within the configured range of routes, this aggregate route of the BGP will take into effect.

The concrete configuration is shown as follows:

```
router bgp 100
aggregate-address 193.0.0.0 255.0.0.0
```

Configure one aggregate route:

```
router bgp 100
aggregate-address 193.0.0.0 255.0.0.0 as-set
```

The **as-path** segment of aggregated route is an collection of **as**:

```
router bgp 100
aggregate-address 193.0.0.0 255.0.0.0 summary-only
```

The aggregated route will not be advertised

29.18.5 Configuring Confederation

When configuration of confederation, it is necessary to use the **bgp confederation identifier** command to configure the AS number for the external connection, and use the **bgp confederation peers** command to configure other confederation members.

The concrete configuration is shown as follows:

```
router bgp 6003
bgp confederation identifier 666
bgp confederation peers 6001 6002
neighbor 171.69.232.57 remote-as 6001
neighbor 171.69.232.55 remote-as 6002
neighbor 200.200.200.200 remote-as 701
```

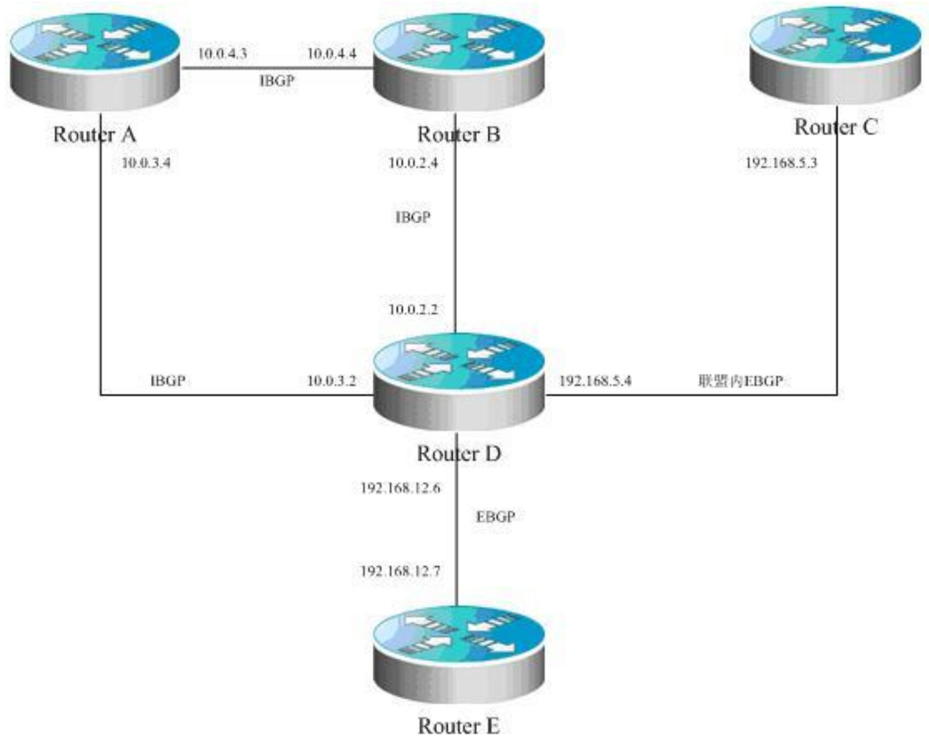
The configuration of peer 200.200.200.200 out of the confederation is shown as follows:

```
router bgp 701
neighbor 171.69.232.56 remote-as 666
neighbor 200,200,200,205 remote-as 701
```

For the configuration, the first device is of the confederation, while the second device is not of the confederation, so they are of the EBGP neighbor relationship.

Following is a configuration example, the relationship between the devices and the alloctioan of Ip address is shown:

Figure 29-4



The configurations of all the devices in this example are as below:

The configuration of Router A:

```
!
router bgp 65530
bgp confederation identifier 100
bgp confederation peers 65531
bgp log-neighbor-changes
neighbor 10.0.3.2 remote-as 65530
neighbor 10.0.4.4 remote-as 65530
```

The configuration of Router B:

```
!
router bgp 65530
bgp confederation identifier 100
bgp log-neighbor-changes
neighbor 192.168.5.4 remote-as 65530
```

The configuration of Router C:

```
!
router bgp 65531
bgp confederation identifier 100
bgp confederation peers 65530
bgp log-neighbor-changes
```

```
neighbor 10.0.3.2 remote-as 65530

neighbor 10.0.4.4 remote-as 65530
```

The configuration of Router D:

```
!

router bgp 65530

bgp confederation identifier 100

bgp confederation peers 65531

bgp log-neighbor-changes

neighbor 10.0.2.4 remote-as 65530

neighbor 10.0.3.4 remote-as 65530

neighbor 192.168.5.3 remote-as 65531

neighbor 192.168.12.7 remote-as 200
```

The configuration of Router E:

```
!

router bgp 200

bgp log-neighbor-changes

neighbor 192.168.12.6 remote-as 100
```

29.18.6 Configuring Route Reflector

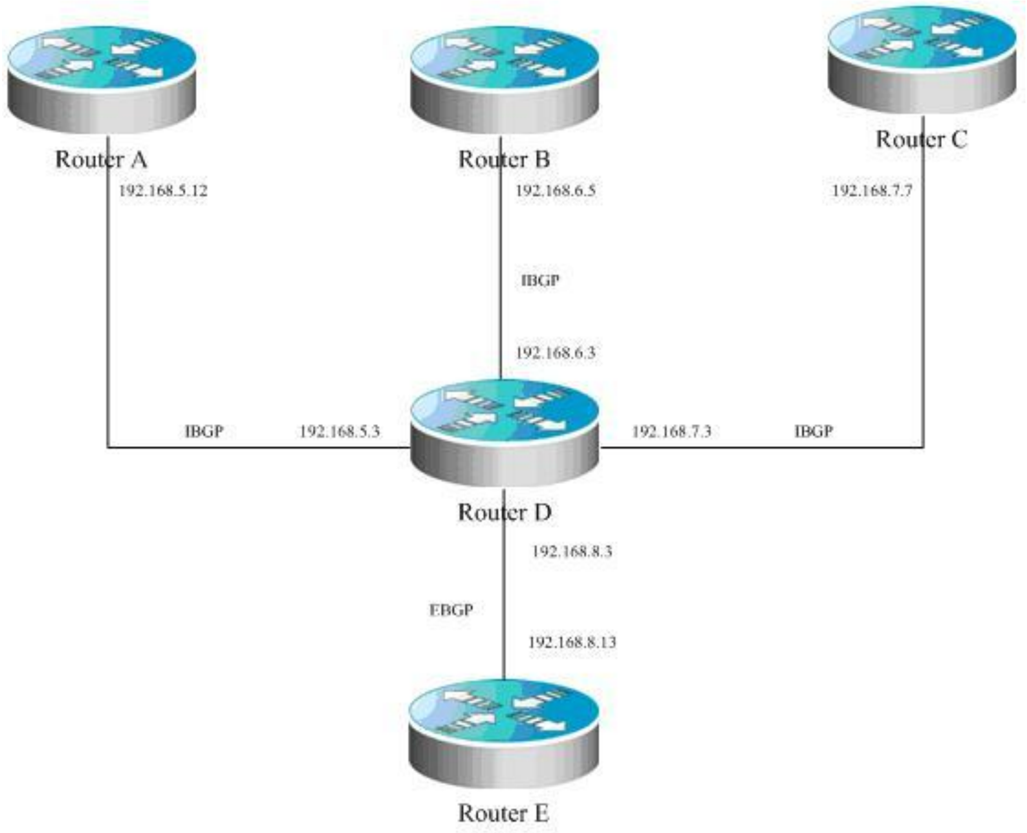
When the route reflector is configured, it is necessary to use the **bgp client-to-client reflection** command to enable the route reflection function of the equipment. If there are more than one route reflector within one cluster, use the **bgp** *cluster-id* command to configure the cluster ID of the reflector, and use the **neighbor** *A.B.C.D* **route-reflector-client** command to add the Peer to the client of the route reflection.

The concrete configuration is shown as follows:

```
router bgp 601
bgp cluster-id 200.200.200.200
neighbor 171.69.232.56 remote-as 601
neighbor 200,200,200,205 remote-as 701
neighbor 171.69.232.56 route-reflector-client
```

Following is example of a configured Route Reflector of bgp, the relationship between the devices and the alloctioan of Ip address is shown:

Figure 29-5



In this example, the router D is a route reflector. The configurations of all the devices in this example are as below:

The configuration of Router A:

```
!
router bgp 100
bgp log-neighbor-changes
neighbor 192.168.5.3 remote-as 100
neighbor 192.168.5.3 description route-reflector server
```

The configuration of Router B:

```
!
router bgp 100
bgp log-neighbor-changes
neighbor 192.168.6.3 remote-as 100
neighbor 192.168.6.3 description route-reflector server
```

The configuration of Router C:

```
!
router bgp 100
bgp log-neighbor-changes
neighbor 192.168.7.3 remote-as 100
neighbor 192.168.7.3 description not the route-reflector server
```

The configuration of Router D:

```
!
router bgp 100
bgp log-neighbor-changes
neighbor 192.168.5.12 remote-as 100
neighbor 192.168.5.12 description route-reflector client
neighbor 192.168.5.12 route-reflector-client
neighbor 192.168.6.5 remote-as 100
neighbor 192.168.6.5 description route-reflector client
neighbor 192.168.6.5 route-reflector-client
neighbor 192.168.7.7 remote-as 100
neighbor 192.168.7.7 description not the route-reflector client
neighbor 192.168.8.13 remote-as 200
```

The configuration of Router E:

```
!
router bgp 500
bgp log-neighbor-changes
neighbor 192.168.8.3 remote-as 100
```

29.18.7 Configuring peergroup

Here will take the configuration of **peergroup** for IBGP and EBGP as an example.

29.18.7.1 Configuring IBGP peergroup

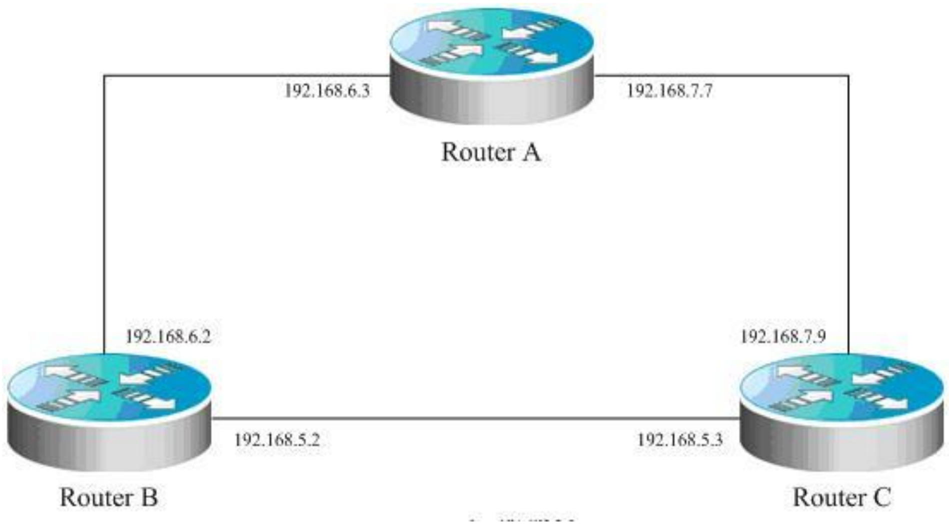
Use the **neighbor internal peer-group** command to create a **peer-group** firstly, configure the **peergroup internal** with **remote-as**, and the **peergroup** with other options, and take the **neighbor** *A.B.C.D* **peer-group internal** command to add the peer A.B.C.D into **peergroup internal**.

The configuration commands are as below:

```
router bgp 100
neighbor internal peer-group
neighbor internal remote-as 100
neighbor internal update-source loopback 0
neighbor internal route-map set-med out
neighbor internal filter-list 1 out
neighbor internal filter-list 2 in
neighbor 171.69.232.53 peer-group internal
neighbor 171.69.232.54 peer-group internal
neighbor 171.69.232.55 peer-group internal
neighbor 171.69.232.55 filter-list 3 in
```

Following is example of a configuring peer-group of ibgp. the relationship between the devices and the alloctioan of Ip address is shown:

Figure 29-6



The configuration of Router A:

```
!
router bgp 100
bgp log-neighbor-changes
neighbor ibgp-group peer-group
neighbor ibgp-group description peer in the same as
neighbor 192.168.6.2 remote-as 100
neighbor 192.168.6.2 peer-group ibgp-group
neighbor 192.168.6.2 description one peer in the ibgp-group
neighbor 192.168.7.9 remote-as 100
neighbor 192.168.7.9 peer-group ibgp-group
```

The configuration of Router B:

```
!
router bgp 100
bgp log-neighbor-changes
neighbor ibgp-peer peer-group
neighbor ibgp-peer remote-as 100
neighbor ibgp-peer route-map ibgp-rmap out
neighbor 192.168.5.3 peer-group ibgp-peer
neighbor 192.168.5.3 route-map set-localpref in
neighbor 192.168.6.3 peer-group ibgp-peer
```

The configuration of Router C:

```
!
router bgp 100
bgp log-neighbor-changes
neighbor ibgp-group peer-group
neighbor 192.168.5.2 remote-as 100
neighbor 192.168.5.2 peer-group ibgp-group
neighbor 192.168.7.7 remote-as 100
neighbor 192.168.7.7 peer-group ibgp-group
```

29.18.7.2 Configuring EBGP peergroup

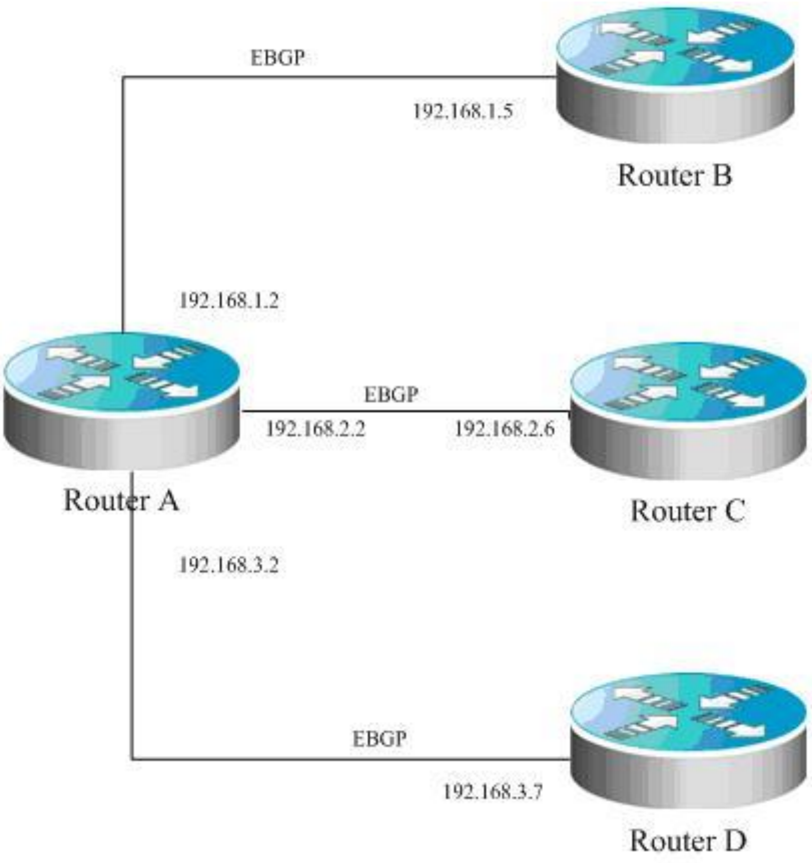
Use the **neighbor** *A.B.C.D* **remote-as** *num* command to configure an **ebgp peer,** firstly, take the **neighbor external peer-group** command to create a **peergroup** with the name **external**, and then apply the **neighbor** *A.B.C.D* **peer-group internal** command to add the peer A.B.C.D into the **peergroup internal**.

Following is an example of the specific configuration:

```
router bgp 100
neighbor external-peers peer-group
neighbor external-peers route-map set-metric out
neighbor external-peers filter-list 99 out
neighbor external-peers filter-list 101 in
neighbor 171.69.232.90 remote-as 200
neighbor 171.69.232.90 peer-group external-peers
neighbor 171.69.232.100 remote-as 300
neighbor 171.69.232.100 peer-group external-peers
neighbor 171.69.232.110 remote-as 400
neighbor 171.69.232.110 peer-group external-peers
neighbor 171.69.232.110 filter-list 400 in
```

Following is a simple diagram, the configuration of peer-group:

Figure 29-7



The relationship between the devices and the allocation of ip address are shown below:

The configuration of Router A:

```
!
router bgp 100
bgp log-neighbor-changes
neighbor ebgp-group peer-group
neighbor ebgp-group distribute-list 2 in
neighbor ebgp-group route-map set-med out
neighbor 192.168.1.5 remote-as 200
neighbor 192.168.1.5 peer-group ebgp-group
neighbor 192.168.2.6 remote-as 300
neighbor 192.168.2.6 peer-group ebgp-group
neighbor 192.168.2.6 distribute-list 3 in
neighbor 192.168.3.7 remote-as 400
neighbor 192.168.3.7 peer-group ebgp-group
!
```

The configuration of Router B:

```
!
router bgp 200
bgp log-neighbor-changes
neighbor 192.168.1.2 remote-as 100
!
```

The configuration of Router C:

```
!
router bgp 300
bgp log-neighbor-changes
neighbor 192.168.2.2 remote-as 100
!
```

The configuration of Router D:

```
!
router bgp 400
bgp log-neighbor-changes
neighbor 192.168.3.2 remote-as 100
!
```

29.18.8 Configuring TCP MD5 Code

Use the CLI command **neighbor password** to configure the TCP MD5 code information for the BGP connection in the BGP configuration mode.

The configuration format is shown as follows:

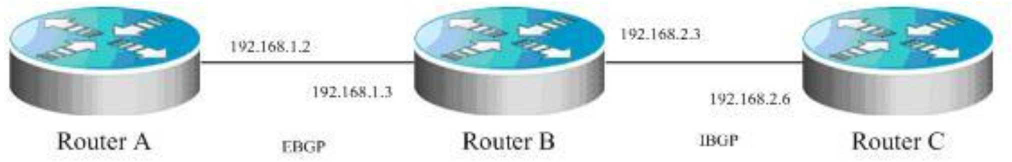
```
router bgp 100
neighbor 171.69.232.54 remote-as 110
neighbor 171.69.232.54 password peerpassword
```

Here configures the *password* of peer 171.69.232.54 as *peerpassword.*

Here configure the password of peer 171.69.232.54 as peerpassword.

In the following topology, the configurations of MD5 on each router are as below:

Figure 29-8



The relationship between the routers is: the as the router A located is 100, the as the router B and router C is 200, the usage of ip address shown in the figure. The relationship between Router A and Router B is the relation of ebgp neighbour, the password of md5 used is ebgp.The relationship between Router B and Router C is the relation of ibgp neighbour, the password of md5 used is ibgp.

The configuration of Router A:

```
!
router bgp 100
bgp log-neighbor-changes
neighbor 192.168.1.3 remote-as 200
eighbor 192.168.1.3 password ebgp
!
```

The configuration of Router B:

```
!
router bgp 200
bgp log-neighbor-changes
neighbor 192.168.1.2 remote-as 100
neighbor 192.168.1.2 password ebgp
neighbor 192.168.2.6 remote-as 200
neighbor 192.168.2.6 password ibgp
!
```

The configuration of Router C:

```
!
router bgp 200
bgp log-neighbor-changes
neighbor 192.168.2.3 remote-as 200
neighbor 192.168.2.3 password ibgp
!
```

30 Protocol-Independent Configuration

30.1 IP Route Configuration

30.1.1 Configuring Static Routes

Static routes are manually configured so that the packets to the specified destination network go through the specified route. When our product cannot learn the routes of some destination networks, it becomes critical to configure static routes. It is a common practice to configure a default route for the packets that do not have a definite route.

To configure static routes, execute the following commands in the global configuration mode:

Command	Function
DGS-3610(config)# **ip route** [**vrf** *vrf_name*] *network mask* {*ip-address* | *interface-type interface-number* } [*distance*] [**tag** *tag*] [**permanent**]	Configure static routes
DGS-3610(config)# **no ip route** *network mask*	Delet Static Route
DGS-3610(config)# **ip static route-limit** *number*	Specify the maximum number of static routes
DGS-3610(config)# **no ip static route-limit**	Restore the default maximum number of static routes

For the example of configuring static routes, see "*Example that Dynamic Routes Override Static Routes*" in this chapter.

If they are not deleted, our product will always retain the static routes. However, you can replace the static routes with the better routes learnt by the dynamic routing protocols. Better routes mean that they have smaller distances. All routes including the static ones carry the parameter of the management distance. The following table shows the management distances of various sources of our product:

Route source	Default management distance
Directly connected networks	0
Static route	1

Route source	Default management distance
OSPF route	110
RIP route	120
Unreachable route	255

The static routes to the ports can be advertised by such dynamic routing protocols as RIP and OSPF, no matter whether static route redistribution is configured in the routing protocols. These static routes can be advertised by the dynamic routing protocols. Since they point to specific ports and they are deemed as directly-connected port networks in the routing table, so they loose the attributes as static routes. However, if only the static routes pointing to ports are defined but the network is not defined by using the Network command in the routing process, the dynamic routing protocol will not advertise the static route, unless the static route redistribution command is used.

When a port is “down”, all routes to that port will disappear from the routing table. In addition, when our product fails to find the forwarding route to the next-hop address, the static route will also disappear from the routing table.

When the specified VRF static routes are added to the corresponding VRF, if the egress is specified at the same time, but the VRF of the egress does not match the specified VRF, the addition will fail. If no VRF is specified, it is added to the global routing table by default.

The maximum number of static routes is 1000 by default. If the number of static routes configured exceeds the specified upper limit, they will not be automatically deleted, but the addition will fail.

30.1.2 Configuring Default Routes

Not all devices have a complete overall network routing table. To allow every device to route all packets, it is a common practice that the powerful core network is provided with a complete routing table, while the other devices have a default route set to this core router. Default routes can be transmitted by the dynamic routing protocols, and can also be manually configured on every router.

Default routes can be generated in two ways: 1) manual configuration. For details, see “*Configuring Static Routes*” in the last section; 2) manually configuring the default network.

Most internal gateway routing protocols have a mechanism that transmits the default route to the entire routing domain. The device that needs to transmit the default route must have a default route. The transmission of the default route in this section applies only to the RIP routing protocol. The RIP always notifies the “0.0.0.0” network as the default route to the routing domain. For how the OSPF routing protocol generates and transmits the default routes, see the related chapter of the “*OSPF Routing Protocol Configuration Guide*”.

To general static routes, execute the following commands in the global configuration mode:

Command	Function
DGS-3610(config)# **ip default-network** network	Configure the default network
DGS-3610(config)# **no ip default-network** network	Delete the default network

Note

To generate the default routes by using the **default-network** command, only the following two conditions must be met: 1) The default network is not a directly-connected port network, but is reachable in the routing table. Under the same condition, the RIP can also transmit the default route. Alternatively, there is another way to do so, that is, by configuring the default static route or learning the 0.0.0.0/0 router via other routing protocols.

If the router has a default route, whether learnt by the dynamic routing protocol or manually configured, when you use the **show ip route** command, the “gateway of last resort” in the routing table will show the information of the last gateway. A routing table may have multiple routes as alterative default routes, but only the best default route becomes the “gateway of last resort”.

30.1.3 Configuring the Number of Equivalent Routes

If the load balancing function is needed, you can set the number of equivalent routes for control. An equivalent route is an alternative path to the same destination address. When there is only one equivalent route, one destination address can be configured with only one route, and the load balancing function is cancelled.

To configure the number of equivalent routes, execute the following commands in the global configuration mode. The **no** form of this command restores the default number of equivalent routes.

Command	Function
maximum-paths [*number*]	Configure the number of equivalent routes (1-100)

30.2 Route Redistribution

30.2.1 Configuring Route Redistribution

To support the routers to run multiple routing protocol processes, our product provides the function for redistributing the route information from one routing process to another routing process. For example, you can redistribute the routes in the OSPF routing area to the RIP routing area , or those in the RIP routing area to the OSPF routing area. Routes can be redistributed among all the IP routing protocols.

In route redistribution, the route maps are often used to enforce conditional control over the mutual route redistribution between two routers.

The following four tables contain the list of tasks for configuring route redistribution, including four parts:

1. Define the redistribution route map, which consists of many policy-based routes arranged in the order of the sequence numbers. When a policy is matched, the execution quits the route map;
2. Define the matching rule or condition for each policy of the route map;
3. Define the operation performed if the match rule is met.
4. Apply the route map in the routing process. Although the route map is a “protocol-dependent” feature, but different routing protocols have different **match** and **set** commands.

To define the redistribution route map, execute the following commands in the global configuration mode:

Command	Function
DGS-3610(config)# **route-map** *route-map-name* [**permit** | **deny**] *sequence*	Define the route map *sequence* : 0-65535
DGS-3610(config)# **no route-map** *route-map-name* {[**permit** | **deny**] *sequence*}	Delete the route map

When you configure the rules for a route map, you can execute one or multiple match or set commands. If there is no match command, all will be matched. If there is no set command, not any action will be taken.

To define the matching conditions for the rules, execute the following commands in the route map configuration mode:

Command	Function
Route(config-route-map)# **match interface** *interface-type interface-number*	Match the next-hop interface of the route *interface-type*: Aggregateport, Dialer, GigabitEthernet, Loopback, Multilink, Null, Tunnel, Virtual-ppp, Virtual-template, Vlan
Route(config-route-map)# **match ip address** *Access-list-number* [*…**access**-list-number*]	Match the address in the access list *Access-list-number: 1-199, 1300-2699,*

Command	**Function**
Route(config-route-map)# **match ip next-hop** *access-list-number* [*…access-list-number*]	Match the next-hop address in the access list *access-list-number* : *1-199*, *1300-2699,*
Route(config-route-map)# **match ip route-source** *access-list-number* [*…access-list-number*]	Match the route source address in the access list
Route(config-route-map)# **match metric** *Metric*	Match the metric of the route *Metric* : 0—4294967295
Route(config-route-map)# **match route-type** {**local** | **internal** | **external** [**level-1** | **level-2**]}	Match the type of the route
DGS-3610(config-route-map)# **match tag** *tag*	Match the tag of the route *tag* : 0—4294967295

To define the operation after matching, execute the following commands in the route map configuration mode:

Command	**Function**
DGS-3610(config-route-map)# **set level** {**stub-area** | **backbone** | **level-1** | **level-1-2** | **level-2**}	Specify the area of route inputted
DGS-3610(config-route-map)# **set metric** *metric*	Set the metric for route redistribution
DGS-3610(config-route-map)# **set metric** [+ *metric-value* | **-** *metric-value* | *metric-value*]	Set the type for route redistribution
DGS-3610(config-route-map)# **set tag** *tag*	Set the tag for route redistribution
DGS-3610(config-route-map)# **set next-hop** *next-hop*	Set the next hop for route redistribution *next-hop:* Next-hop IP address

To redistribute routes from one routing area to another and control route redistribution, execute the following commands in the routing process configuration mode:

Command	**Function**
DGS-3610(config-router)# **redistribute** *protocol* [**metric** *metric*]] [**route-map** *route-map-name*]	Set route redistribution *Protocol* (protocol type): bgp, connected, isis, rip, static
DGS-3610(config-router)# **default-metric** *metric*	Set the default metric for all redistributed routes (OSPF RIP) *metric* : 0-16777214 If no default metric is set for it, the *metric is* 20 and type is Type-2 by default.

At route redistribution, it is not necessary to convert the metric of one routing protocol into that of another routing protocol, since different routing protocols use distinctively different measurement methods. The RIP metric calculation is based on the hops, while the OSPF metric calculation is based on the bandwidth, so their metrics are not comparable. However, a symbolic metric must be set for route redistribution. Otherwise, route redistribution will fail.

Note

When the route redistribution is configured in the OSPF routing process, the metric of 20 is allocated to the redistributed routes with the type of Type-2 by default. This type belongs to the least credible route of the OSPF.

Route redistribution may easily cause loops, so you must be very careful in using them.

30.2.2 Configuration of Route Filtering

Route filtering is the process to control the incoming/outgoing routes so that the router only learns the necessary and predictable routes, and only advertise the necessary and predictable routes to the external necessary and predictable routes. The divulgence and chaos of the routes may affect the running of the network. Particularly for telecom operators and financial service networks, it is essential to configure route filtering.

30.2.2.1 Controlling the LSA

To prevent other routers or routing protocols from dynamically learning one or more route message, you can configure the control over the LSA to prevent the specified route update.

To prevent the LSA, execute the following commands in the routing process configuration mode:

Command	Function
DGS-3610(config-router)# **distribute-list** {[*access-list-number* | *access-list-name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] | **gateway** *prefix-list-name*} **out** [*interface-type interface-number*]	Allow or not allow some LSAs to be sent according to the access list rule. **Prefix:** This keyword specifies the prefix list for filtering the routes. The prefix list should be separately configured by using the ip prefix-list command. **Gateway:** Use the prefix list to filter the outgoing routes according to the source of the routes. Those filtered will not be sent.

Command	**Function**
DGS-3610(config-router)# **no distribute-list** {[*access-list-number* | *access-list-name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] | **gateway** *prefix-list-name* } **out** [*interface-type interface-number* | *protocol*]	Cancel the prevention of the LSA

Note

When you configure the OSPF, you cannot specify the interface and the features are only applicable to the external routes of the OSPF routing area.

30.2.2.2 Controlling Route Update Processing

To avoid processing the some specified routes of the incoming route update packets, you can configure this feature. This feature does not apply to the OSPF routing protocol.

To control route update processing, execute the following commands in the routing process configuration mode:

Command	**Function**
DGS-3610(config-router)# **distribute-list** {[*access-list-number* | *access-list-name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] | **gateway** *prefix-list-name*} **in** [*interface-type interface-number*]	Allow or deny the reception of the routes distributed according to the access list rule. **Prefix:** This keyword specifies the prefix list for filtering the routes. The prefix list should be separately configured by using the ip prefix-list command. **Gateway:** Use the prefix list to filter the routes distributed according to the source of the routes.
DGS-3610(config-router)# **no distribute-list** {[*access-list-number* | *name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] | **gateway** *prefix-list-name* } **in** [*interface-type interface-number*]	Cancel the control over route update processing

30.2.3 Configuration Examples:

30.2.3.1 Example of Static Route Redistribution

- **Configuration requirements:**

One device exchanges route information with other devices via the RIP. In addition, there are three static routes. The RIP is only allowed to redistribute the two routes of 172.16.1.0/24 and 192.168.1.0/24.

- **Configuration of the Routers:**

This is a common route filtering configuration example in practice, by configuring the distribute list. Additionally, note that the following configuration does not specify the metric for the redistributed route, so the redistributed route is a static route. The RIP will automatically distribute the metric. In the RIP configuration, the version must be specified and the route summary must be disabled, since the access list allows the 172.16.1.0/24 route. If the RIP is to advertise this route, it must first support the classless routes, and the route cannot be summarized to the 172.16.0.0/16 network when doing so.

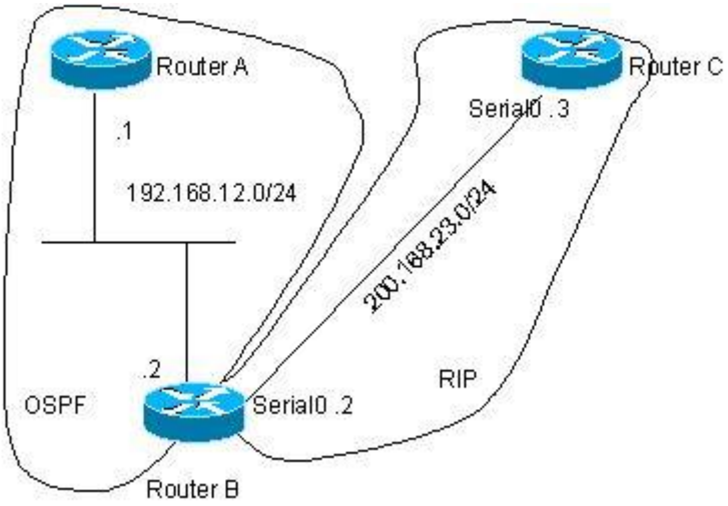
```
DGS-3610(config)# ip route 172.16.1.0 255.255.255.0 172.200.1.2
DGS-3610(config)# ip route 192.168.1.0 255.255.255.0 172.200.1.2
DGS-3610(config)# ip route 192.168.2.0 255.255.255.0 172.200.1.4
!
DGS-3610(config)# router rip
DGS-3610(config-router)# version 2
DGS-3610(config-router)# redistribute static
DGS-3610(config-router)# network 192.168.34.0
DGS-3610(config-router)# distribute-list 10 out static
DGS-3610(config-router)# no auto-summary
!
DGS-3610(config)# access-list 10 permit 192.168.1.0
DGS-3610(config)# access-list 10 permit 172.16.1.0
```

30.2.3.2 Example of RIP&OSPF Redistribution

- **Configuration requirements:**

There are three routers. Figure 30-1 shows the connection of the equipment. Router A belongs to the OSPF routing area, router C belongs to the RIP routing area, and router B is connected to two routing areas. Router A also advertises the two routers of 192.168.10.0/24 and 192.168.100.1/32, and router C also advertises the network routers of 200.168.3.0/24 and 200.168.30.0/24.

Figure 30-1 Example of RIP&OSPF Redistribution



The OSPF only redistributes the routes in the RIP routing area and the route type is Type-1. The RIP only redistributes the 192.168.10.0/24 route in the OSPF routing area and its metric is 3.

- **The Specific Configuration of the routers**

When the routing protocols redistribute routes among them, the simple route filtering can be controlled by the distribute list. However, different attributes must be set for different routes, and this is not possible for the distribute list, so the route map must be configured for control. The route map provides more control functions than the distribute list, and it is more complex to configure. Therefore, do not use the route map if possible for simple configuration of the router. The following example does not use the route map.

Configuration of router A:

```
DGS-3610(config)# interface gigabitEthernet 0/0
DGS-3610(config-if)# ip address 192.168.10.1 255.255.255.0
DGS-3610(config)# interface loopback 1
DGS-3610(config-if)# ip address 192.168.100.1 255.255.255.0
DGS-3610(config-if)# no ip directed-broadcast
!
DGS-3610(config)# interface gigabitEthernet 0/1
DGS-3610(config-if)# ip address 192.168.12.55 255.255.255.0
!
DGS-3610(config)# router ospf 1
DGS-3610(config-router)# network 192.168.10.0 0.0.0.255 area 0
DGS-3610(config-router)# network 192.168.12.0 0.0.0.255 area 0
DGS-3610(config-router)# network 192.168.100.0 0.0.0.255 area 0
```

Configuration of router B:

```
DGS-3610(config)# interface gigabitEthernet 0/0
DGS-3610(config-if)# ip address 192.168.12.5 255.255.255.0
!
DGS-3610(config)# interface Serial 1/0
```

```
DGS-3610(config-if)# ip address 200.168.23.2 255.255.255.0
```

#Configure OSPF and set the redistribution route type

```
DGS-3610(config)# router ospf
DGS-3610(config-router)# redistribute rip metric 100 metric-type 1 subnets
DGS-3610(config-router)# network 192.168.12.0 0.0.0.255 area 0
```

#Configure the RIP and use the distribute list to filter the redistributed routes

```
DGS-3610(config)# router rip
DGS-3610(config-router)# redistribute ospf metric 2
DGS-3610(config-router)# network 200.168.23.0
DGS-3610(config-router)# distribute-list 10 out ospf
DGS-3610(config-router)# no auto-summary
```

#Define an access list

DGS-3610(config)# **access-list** *10* **per**

```
mit 192.168.10.0
```

Configuration of router C:

```
DGS-3610(config)# interface gigabitEthernet 0/0
DGS-3610(config-if)# ip address 200.168.30.1 255.255.255.0
!
DGS-3610(config)# interface gigabitEthernet 0/1
DGS-3610(config-if)# ip address 200.168.3.1 255.255.255.0
!
DGS-3610(config)# interface Serial 1/0
DGS-3610(config-if)# ip address 200.168.23.3 255.255.255.0
DGS-3610(config)# router rip
DGS-3610(config-router)# network 200.168.23.0
DGS-3610(config-router)# network 200.168.3.0
DGS-3610(config-router)# network 200.168.30.0
```

OSPF routes found by router A:

```
O E1 200.168.30.0/24 [110/101] via 192.168.12.5, 00:04:07, FastEthernet0/1
O E1 200.168.3.0/24 [110/101] via 192.168.12.5, 00:04:07, FastEthernet0/1
```

RIP routes found by Router C:

```
R   192.168.10.0/24 [120/2] via 200.168.23.2, 00:00:00, Serial1/0
```

30.2.3.3 Example of Configuring the Route Map

The route map can be configured very flexibly to be used on the route redistribution and policy-based routing. No matter how the route map is used, the configuration principle is the same, except that different command sets are used. Even if it is used on the route redistribution, different routing protocols can use different commands with the route map.

In the following example, the OSPF routing protocol redistributes only the RIP routes whose hops are 4. In the OSPF routing area, the type of the routes is external route type-1, the initial metric is 40, and the route tag is 40.

```
!
DGS-3610(config)# router ospf
DGS-3610(config-router)# redistribute rip subnets route-map redrip
DGS-3610(config-router)# network 192.168.12.0 0.0.0.255 area 0
!
DGS-3610(config)# access-list 20 permit 200.168.23.0
!
DGS-3610(config)# route-map redrip permit 10
DGS-3610(config-route-map)# match metric 4
DGS-3610(config-route-map)# set metric 40
DGS-3610(config-route-map)# set metric-type type-1
DGS-3610(config-route-map)# set tag 40
!
```

In the following configuration example, the RIP routing protocol redistributes only the OSPF routes whose tag is and initial metric is 10.

```
DGS-3610(config)# router rip
DGS-3610(config-router)# version 2
DGS-3610(config-router)# redistribute ospf route-map redospf
DGS-3610(config-router)# network 200.168.23.0
!
DGS-3610(config)# route-map redospf permit 10
DGS-3610(config-route-map)# match tag 10
DGS-3610(config-route-map)# set metric 10
!
```

30.3 Configuring Switch Fast Forwarding ECMP/WCMP Policy

In the switch, when the hardware forwards and stores ECMP/WCMP routes, load-balance policies are also involved. When the route has multiple next hops, the hardware can select a next hop according to the policy set. The switch will select different fields of the packets as the keyword according to our settings, and send them to the hash as input (there are two algorithm available) to select the appropriate hop. The appropriate packet characteristic fields and hash algorithm should be selected to make more balanced egress traffic volume of the packets.

30.3.1 Selecting Hash Keyword

You can set the packet hash keyword as the combination of source IP, destination IP, TCP/UDP port number, and user-define (udf). UDF is 1-128, used as the seed value for hash calculation. Among various keywords, SIP is required, while others are optional. Various possible combinations are listed as below:

- SIP
- SIP+DIP
- SIP+TCP/UDP port
- port
- SIP+UDF

- SIP+DIP+TCP/UDP port
- SIP+DIP+UDF
- SIP + TCP/UDP port +UDF
- SIP + DIP+TCP/UDP port +UDF

The default keyword has only SIP.

30.3.2 Selecting the Hash Algorithm

There are two hash algorithms available:

CRC32_Upper	Select the upper bits of the crc32 to determine the next hop
CRC32_Lower	Select the lower bits of the crc32 to determine the next hop

These two kinds of algorithms have different effects for different types of packets. For example, the CRC32_Upper has a good effect on the IP addresses that have the same upper bits but different lower bits. On the other hand, the CRC32_Upper has a good effect on the IP addresses that have the same lower bits but different higher bits.

The default hash algorithm is CRC32_Upper.

30.3.3 Configuration Commands

Command	Function
DGS-3610(config)# **ip ref ecmp load-balance {[crc32_lower | crc32_upper] [dip] [port] [udf** *number*]}	Use any combination of DIP, Port and UDF for the generation of the Key. And select CRC32_Lower or CRC32_Upper as a Hash algorithm.
DGS-3610(config)# **no ip ref ecmp load-balance {[crc32_lower | crc32 upper] [dip] [port] [udf***number*]}	The **no** command will remove the keyword carried as part of the Key based on the system stored setting. For example, the system stored settings are SIP + DIP + Port. After the **no ip ref ecmp route dip port** command is executed, the component of the Key is only the SIP. If the member following the **no** command is not in the system stored setting, the execution of this command will not experience an error.

30.3.4 Configuration Examples

The following configures the hash algorithm as CRC32_Lower, and selects the key of the packet as SIP + DIP+TCP/UDP port +UDF:

```
DGS-3610(config)#ip ref ecmp load-balance crc32_lower dip port udf 50
```

31 Policy-Based Routing Configuration

Policy-based routing is a packet forwarding mechanism more flexible than the routing based on the target network. If policy-based routing is used, the router will determine how to process the packets to be routed according to the route map, which determines the next-hop router of the packets.

To use the policy-based routing, you must specify the route map for it and create the route map. A route map consists of multiple polices, each of which defines one or multiple matching rules and corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy. For the configuration of the route map, see the protocol-independent command configuration guide.

To configure policy-based routing, perform the following steps:

1. Define the route map, which consists of many policy-based routes arranged in the order of thei sequence numbers. When a policy is matched, the execution quits the route map;

   To define the redistribution route map, execute the following commands in the global configuration mode:

Command	Function
DGS-3610(config)# **route-map** *route-map-name* [**permit** | **deny**] *sequence*	Define the route map
DGS-3610(config)# **no route-map** *route-map-name* {[**permit** | **deny**] *sequence*}	Delete the route map

2. Define the matching rule or condition for eacy policy of the route map;

   To define the matching rules for the policies, execute the following commands in the route map configuration mode:

Command	**Function**
DGS-3610(config-route-map)# **match ip address** *access-list-number*	Match the address in the access list
DGS-3610(config-route-map)# **match length** *min* *max*	Match the length of the packet

3. Define the operation performed if the match rule is met.

   To define the operation after matching, execute the following commands in the route map configuration mode:

Command	**Function**
DGS-3610(config-route-map)# **set ip default next-hop** *ip-address*[*weight*][*ip-address*[*weight*]]	Set the next-hop IP address of the packets, if the routing table does not contain any definite routes
DGS-3610(config-route-map)# **set ip next-hop** *ip-address* [*weight*][*ip-address*[*weight*]]	Set the next-hop IP address of the packets
DGS-3610(config-route-map)# **set interface** *intf_name*	Set the egress
DGS-3610(config-route-map)# **set default interface** *intf_name*	Set the default egress

4. Apply the route map at the specified interface.

   To apply policy-based routing on the interface, execute the following commands in the interface configuration mode:

Command	**Function**
DGS-3610(config-if)# **ip policy route-map** [*name*]	Use the specified route-map for filtering on the interface
DGS-3610(config-if)# **no ip policy** *route-map* [*name*]	Cancel the route-map applied on the interface

For example:

Configure policy-based routing on the f 0/0 interface so that all incoming packets are forwarded to the device of 192.168.5.5.

```
DGS-3610(config)# access-list 1 permit any
DGS-3610(config)# route-map name
```

```
DGS-3610(config-route-map)# match ip address 1
DGS-3610(config-route-map)# set ip next-hop 192.168.5.5
DGS-3610(config-route-map)# int f 0/0
DGS-3610(config-if)# ip policy route-map name
```

To configure the policy-based routing for the packets reaching a router interface, execute the following commands in the interface configuration mode:

Command	Function
DGS-3610(config-if)# **ip policy route-map** *route-map*	Apply the policy-based routing at the interface

To configure load-balance or redundancy backup in the policy-based routing, execute the following command in the global configuration mode:

Command	Function
DGS-3610(config)# **ip policy** [**load-balance** | **redundance**]	Set the load-balance or redundancy for policy-based routing

The WCMP supports up to four next hops and the ECMP supports up to 32 next hops, when policy-based routing executes load-balance,

When the default policy-based route is configured, the WCMP supports up to four next hops and the ECMP supports up to 32 next hops.

For the route-map configuration command, see the *Protocol-independent Command Configuration Guide*.

Policy-based routing on the equipment:

Supported commands on the switch:

1. **[no] ip policy route-map**
2. **match ip address**
3. **set ip next-hop**
4. **set ip default next-hop**
5. **set tos**
6. **set dscp**

Supported commands on the router:

7. **[no] ip policy route-map**
8. **ip local policy route-map**
9. **match ip address**
10. **match length**

11. **set ip next-hop**

12. **set ip default next-hop**

13. **set interface**

14. **set default interface**

15. **set tos**

16. **set preference**

17. **set dscp**

Restrictions:

⚠ **Caution**

1. On our products with version 10.2, one interface can be configured with only one route map for the maximum. When multiple route maps are configured on an interface, they will overwrite each other and the policy-based routing only uses the first ACL configured in the route-map sequence. Therefore, when you use the policy-based routing, you are recommended to configure only one ACL for each route-map sequence.

2. If the configured route-map sequence has only the nexthop but without the ACL, this is equivalent to that all packets are matched. If the route-map sequence has only the ACL but has no nexthop, the matched packets are forwarded in the ordinary way. If the route-map sequence has neither the ACL nor the nexthop, it is equivalent to that all the matched packets are forwarded in the ordinary way.

3. Policy-based routing only supports ACL number configuration, but not ACL name configuration. If the ACL number is configured but the ACL does not exist, it is equivalent to that all the packets are matched. If the ACL is configured but there is no ACE in it, the route-map sequence is skipped and the matching starts from the ACL of the next route-map sequence.

4. If you would like that the IP packets to the local machine do not use policy-based routing, you should add the “deny device IP address” ACE at the beginning of the ACL in the PBR rule.

5. Configure PBR on the dial port does not be supported on the router now. It can not be take effect after configuring.

32 IPv6 Configuration

32.1 IPv6 Related Information

With the quick growth of Internet and the increasing consumption of the IPv4 address space, the limitation of the IPv4 is more obvious. The research and practice of the Internet Protocol Next Generation – Ipng becomes the hot spot at present. Furthermore, the Ipng workgroup of the IETF determines the protocol specification of Ipng and refers to as the “IP version 6” (IPv6). See the RFC2460 for detailed description of the specification for this protocol.

Key Features of Ipv6:

- More Address Space

The length of address will be extended to 128 bits from the 32 bits of Ipv4. Namely, there are 2^128-1 addresses for IPv6. The IPv6 adopts the level address mode and supports the address assignment method of several levels subnets from the Internet backbone network to the internal subnet of enterprises.

- Simplified Format of Packet Header

The design principle of new IPv6 packet header is to minimize the overhead. For this reason, some non-critical fields and optional fields are removed from the packet header and placed into the extended packet header. The length of the IPv6 address is 4 times of that for the IPv4; its packet header is only 2 times of that for the IPv4. The improved IPv6 packet header is more efficient for the router forwarding, for instance, there is no check sum in the IPv6 packet header and it is not necessary for the IPv6 router to process the fragment during forwarding (the segment is completed by the originator).

- High-efficient Level Addressing and Routing Structure

The IPv6 adopts the aggregation mechanism and defines flexible level addressing and routing structure, and several networks at the same level is presented as a unified network prefix at the higher level of routers, so it obviously reduces the route table item of the router to be maintained and greatly minimizes the routing selection and the storage overhead of the router.

- Simple Management: Plug and Play

Simplify the management and maintenance of the network node by the implement of a series of auto-discovery and auto-configuration functions. Such as the Neighbor Discovery, the MTU Discovery, the Router Advertisement, the Router Solicitation, the Router Solicitation and the Auto-configuration technologies provide related service for the plug and play. It should be mentioned that the IPv6 supports such address configuration methods as the stateful and the stateless. In the IPv4, the dynamical host configuration protocol (DHCP) implements the automatic setting of the host IP address and related configuration, while the IPv6 inherits this auto-configuration service of the IPv4 and refers to it as the Stateful Auto-configuration. Furthermore, the IPv6 also adopts an auto-configuration service, referred to as the Stateless Auto-configuration. During the stateless auto-configuration, the host obtains the local address of the link, the address prefix of local router and some other related configuration information automatically.

- Security

The IPSec is an optional extended protocol of the IPv4, while it is only a component of the IPv6 and used to provide the IPv6 with security. At present, the IPv6 implements the Authentication Header (AH) and Encapsulated Security Payload (ESP) mechanisms. Where, the former authenticates the integrity of the data and the source of the IP packet to ensure that the packet does come from the node marked by the source address, while the latter provides the data encryption function to implement the end-to-end encryption.

- More Excellent QoS Support

The new field in the IPv6 packet header defines how to identify and process the data flow. The Flow Label filed in the IPv6 packet header is used to identify the data flow ID, by which the IPv6 allows users to put forward the requirement for the QoS of communication. The router can identify all packets of some specified data flow by this field and provide special processing for these packet on demand.

- Neighbor Nodes Interaction-specific New Protocol

The Neighbor Discovery Protocol of the IPv6 uses a series of IPv6 control information message (ICMPv6) to carry out the interactive management of the neighbor nodes (the node of the same link). The Neighbor Discovery Protocol and high-efficient multicast and unicast Neighbor Discovery message replaces previous broadcast-based address resolution protocol (ARP) and the ICMPv4 router discovery message.

- Extensibility

The IPv6 provides powerful extensibility and the new features can be added to the extended packet header after the IPv6 packet header. Unlike the IPv4, the packet header can only support the option up to 40 bytes, while the size of the IPv6 extended packet header is only limited by the maximum bytes of the whole IPv6 packet.

The presently implemented IPv6 supports the following features:

- IPv6 Protocol
- IPv6 Address Format
- Type of IPv6 Address
- ICMPv6
- IPv6 Neighbor Discovery
- Path MTU Discovery

- ICMPv6 Redirection
- Address Conflict Detection
- IPv6 Stateless Auto-configuration
- IPv6 Address Configuration
- IPv6 Route Forwarding, Support Static Route Configuration
- Configuration of various parameters for the IPv6 protocol
- Diagnosis Tool **ping ipv6**

32.1.1 IPv6 Address Format

The basic format of an IPv6 address is X : X : X : X : X : X : X : X, where X is a 4 hex integers (16 bits). Each digit contains 4 bits of information, each integer contains 4 hex digits and each address contains 8 integers, so it is total for 128 bits. Some legal IPv6 addresses are as follows:

2001:ABCD:1234:5678:AAAA:BBBB:1200:2100

800 : 0 : 0 :0 : 0 : 0 : 0 : 1

1080 : 0 : 0 : 0 : 8 : 800 : 200C : 417A

These integers are hex integers, where A to F denotes the 10 to 15 respectively. Each integer in the address must be denoted and the starting 0 need not be denoted. Some IPv6 address may contain a series of 0 (such as the example 2 and 3). Once this condition occurs, the “: :” is allowed to denote this series of 0. Namely, the address 800:0:0:0:0:0:0:1 can be denoted as: 800 :: 1

These two colons denote that this address can be extended to the complete 128-bit address. In this way, the 16-bit group can be replaced with two colons only when they are all 0 and the two colons can only present for one time.

In the mixture environment of IPv4 and IPv6, there is a mixture denotation method.The lowest 32 bits in an IPv6 address can be used to denote an IPv4 address. The address can be expressed in a mixture mode, i.e., X: X : X : X : X : X : d . d . d . d. Where, the X denotes a 16-bit integer, while d denotes an 8-bit decimal integer. For instance, the address 0 : 0 : 0 : 0 : 0 : 0 : 192 .168 . 20 : 1 is a legal IPv6 address. After the abbreviated expression method is used, this address can be denoted as follows: : : 192 .168 . 20 . 1

For the IPv6 address is divided into two parts such as the subnet prefix and the interface identifier, it can be denoted as an address with additional numeric value by the method like the CIDR address. Where, this numeric value indicates how many bits represent the network part (the network prefix). Namely the IPv6 node address indicates the length of the prefix, and the length is differentiated from the IPv6 address by the slash. For instance: 12AB::CD30:0:0:0:0/60,The length of the prefix for the route in this address is 60 bits.

32.1.2 Type of IPv6 Address

In RFC2373, there are the following three defined types of IPv6 addresses:

- Unicast: Identifier of a single interface. The packet to be sent to a Unicast address will be transmitted to the interface of this address identification.
- Anycast: Identifiers of a group of interfaces. The packet to be sent to an Anycast address will be transmitted to one of the interfaces of this address identification (select the nearest one according to the route protocol).
- Multicast: Identifiers of a group of interfaces (In genera, they are of different nodes). The packet to be sent to a Multicast address will be transmitted to all interfaces which is added to this multicast address.

Caution

The broadcast address is not defined in the IPv6.

The following will introduce these types of addresses one-by-one:

32.1.2.1 Unicast Addresses

IPv6 unicast addresses include the following types:

- Aggregateable Global Addresses
- Link-level Local Addresses
- Site-level Local Addresses
- IPv4 Addresses-embedded IPv6 Addresses

1. Aggregateable Global Addresses

The format of the aggregateable global unicast addresses is shown as follows:

```
| 3 |   13 | 8   |    24      |    16      |              64 bits                  |
+--+-----+---+--------+--------+--------------------------------+
|FP| TLA |RES|   NLA     |  SLA     |            Interface ID               |
|    | ID   |      |  ID        |  ID        |                                       |
+--+-----+-----+------------+-------------+------------------------------------------   +
```

Above figure contains the following fields:

- FP field (Format Prefix):

The format prefix in an IPv6 address, 3 bits long, used to indicate which type of addresses the address belongs to when it is in the IPv6 address space. This field is ‘ 0 0 1’, which indicates that this is an aggregateable global unicast address.

- TLA ID field (Top-Level Aggregation Identifier):

Top-Level Aggregation Identifier, containing toppest address routing information. It refers to the maximum route information in the inter-working. It is 13 bits long and can provide up to 8192 different top level routes.

- RES field (Reserved for future use):

Reservation field, 8 bits. It will possibly be used to expand the top level or the next level aggregation identifier field.

- NLA ID field (Next-Level Aggregation Identifier):

Next-Level Aggregation Identifier, 24 bits. This identifier is used to control the top-level aggregation to arrange the address space by some institutions. In other word, these institutions (such as the large-sized ISP) can separate the 24-bit field according to the addressing level structure themselves. For instance, a large-sized ISP can separate it into 4 internal top-level routes by 2 bits, other 22 bits of the address space is assigned to other entities (such as the small-sized local ISP). If these entities obtain enough address space, the same measure can be taken to subdivide the space assigned to them.

- SLA ID field (Site-Level Aggregation Identifier):

Site-Level Aggregation Identifier, used to arrange internal network structures by some institutions. Each institution can use the same way as that in the IPv4 to create the level network structure themselves. If the 16 bits are taken as the plane address space, there are up to 65535 different subnets. If the former 8 bits are taken as the higher-level of routes within this organization, 255 large-scale subnets are allowed. Furthermore, each large-scale subnet can be subdivided into up to 255 small-scale subnets.

- Interface Identifier field (Interface Identifier):

It is 64 bits long and contains the 64 bit value of IEEE EUI-64 interface identifiers.

2. Link Local Addresses

The format of the link-level local addresses is shown as follows:

```
|    10     |
|   bits    |        54 bits          |              64 bits              |
+-----------+-------------------------+-----------------------------------+
|1111111010|            0            |           interface ID            |
+-----------+-------------------------+-----------------------------------+
```

The link-level local address is used to number the host on the single network link. The address of former 10-bit identification for the prefix is the link-level local address. The router will not forward the message of the source address of the destination address with the link-level local address forever. The intermediate 54-bit of this address is 0. The latter 64 indicates the interface identifier, this part allows the single network to connect to up to 2^{64}-1 hosts.

3. Site-level Local Addresses

The format of the site-level local addresses is shown as follows:

```
|    10      |
|  bits      |     38 bits    |   16 bits   |              64 bits              |
+-------------+----------------+--------------+--------------------------------------+
|1111111011|       0          | subnet ID |              interface ID          |
+-------------+---------------+-------------+---------------------------------------+
```

The site-level local address can be taken to transmit the data within the site, and the router will not forward the message of the source address of the destination address with the site-level local address to Internet. Namely, such packet route can only be forwarded within the site, but cannot be forwarded to out of the site. The former 10-bit prefix of the site-level local address is slightly different of that of the link-level local address, whose intermediate 38 bits are 0, the subnet identifier of the site-level local address is 16 bits, while the latter 64 bits also indicates the interface identifier, usually for the EUI-64 address of IEEE.

4. IPv4 Addresses-embedded IPv6 Addresses

The RFC2373 also defines 2 types of special IPv6 addresses embedded with IPv4 addresses:

- IPv4-compatible IPv6 address

```
|                        80 bits                        | 16 |         32 bits            |
+--------------------------------------------------+----+----------------------------+
|0000....................................................0000|0000|    IPv4 address   |
+---------------------------------------------------+----+--------------------------+
```

- IPv4-mapped IPv6 address

```
|                        80 bits                        | 16 |         32 bits            |
+--------------------------------------------------+----+---------------------------+
|0000........................................................0000|ffff|  IPv4 address     |
+--------------------------------------------------+----+--------------------------+
```

The IPv4-compatible IPv6 address is mainly used to the automatic tunneling, which supports both the IPv4 and IPv6. The IPv4-compatible IPv6 address will transmit the IPv6 message via the IPv4 router in the tunneling way. The IPv6 address of an IPv4 mapping is used to access the nodes that only support IPv4 by IP6 nodes. For example, when one IPv6 application of the IPv4/IPv6 host requests the resolution of a host name (the host only supports IPv4), the name server will internally generate the IPv6 addresses of the IPv4 mapping dynamically and return them to the IPv6 application.

32.1.2.2 Multicast Addresses

The format of the IPv6 multicast address is shown as follows:

```
|    8     |  4 |  4 |                 112 bits                  |
+----------+----+----+-------------------------------------------------------------------+
|11111111|flgs|scop|                  group ID                    |
+----------+----+----+-------------------------------------------------------------------+
```

The first byte of the address format is full 1, which denote a multicast address.

- Flag field:

It consists of 4 bits. At present, only the fourth bit is specified. The bit is used to indicate whether the address is a known multicast address specified by Internet Number Constitution or a temporary multicast address used in a specific condition. If this flag bit is 0, it indicates this address is a known multicast address. If this bit is 1, it indicates that this address is a temporary one. Other 3 flag bits are reserved for future use.

- Range field:

Composed of 4 bits and used to denote the range of multicast. Namely, whether the multicast group contains the local node, the local link and the local site or any position nodes in the IPv6 global address space.

- Group Identifier field:

112 bits long and used to identify a multicast group. Depending on whether a multicast address is temporary or known and the range of the address, a multicast identifier can denote different groups.

The multicast address of the IPv6 is this type of address taking FF00::/8 as the prefix One multicast address of an IPv6 usually identifies the interfaces of a serial of different nodes. When one message is sent to one multicast address, this message will be distributed to the interfaces of each node with this multicast address. One node (host or router) should add the following multicast:

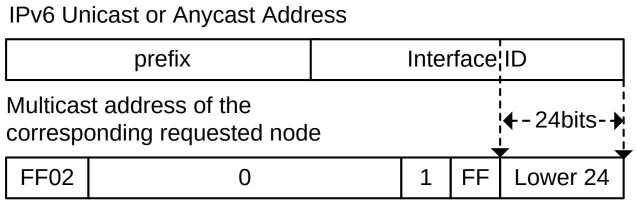
- The multicast address of all nodes for the local link is FF02::1
- The prefix of the multicast address for the solicited node is FF02:0:0:0:0:1:FF00:0000/104

If they are routers, it is necessary to add the multicast address FF02::2 of all routers for the local link.

The multicast address of the solicited node corresponds to the IPv6 unicast and anycast address, so it is necessary for the IPv6 node to add corresponding multicast address of the solicited node for each configured unicast address and anycast address. The prefix of the multicast address for the solicited node is FF02:0:0:0:0:1:FF00:0000/104, another 24 bits are comprised of the unicast address or the lower 24 bits of the anycast address, for instance, the multicast address of the solicited node corresponding to the FE80::2AA:FF:FE21:1234 is FF02::1:FF21:1234,

The multicast address of solicited node is usually used to the neighbor solicitation (NS) message. The format of the solicited node is shown as follows:

Figure 32-1


IPv6 Unicast or Anycast Address
prefix
Interface ID
Multicast address of the corresponding requested node
24bits
FF02
0
1
FF
Lower 24

32.1.2.3 Anycast Addresses

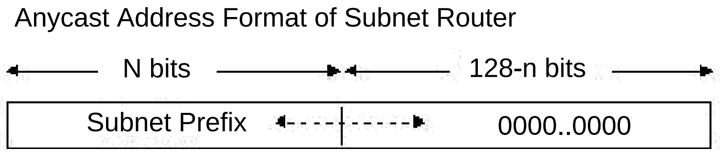
The anycast address is similar with the multicast address as more than one node shares an anycast address. The difference is that only one node expects to receive the data packet of the anycast address, while all nodes of the multicast address members expect to receive all packets sending to this address. The anycast address is assigned to normal IPv6 unicast address space, so the anycast address cannot be differentiated from the unicast address from the style. For this reason, each member of all anycast addresses has to be configured explicitly to identify the anycast address.

Caution The anycast address can only be assigned to the devie, but cannot be assigned to the host. Furthermore, the anycast address cannot be taken as the source address of the message.

The RFC2373 predefines an anycast address, referred to as the anycast address of the subnet router. The following diagram shows the anycast address format of the subnet router, which consists of the subnet prefix followed by a series of 0 (as the interface identifier).

Where, the subnet prefix identifies a specified link (subnet) and the message to be sent to the anycast address of the subnet router will be distributed to a router of this subnet. The anycast address of the subnet router is usually used to some node which needs to communicate with one router of the remote subnet.

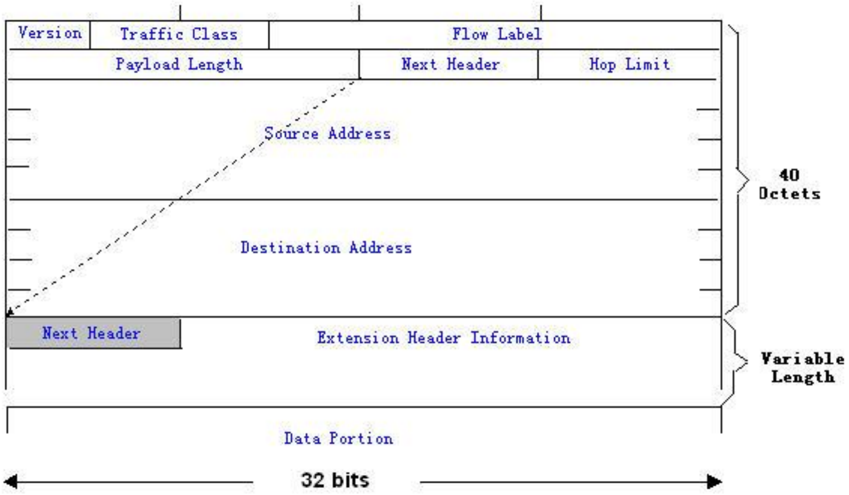
Figure 32-2



32.1.3 IPv6 Packet Header Structure

The format of the IPv6 packet header is shown as the figure below:

Figure 32-3



In the IPv4, all packet headers take 4 bytes as the unit. While in the IPv6, the packet header takes 8 bytes as the unit and the total length of the packet header is 40 bytes. IPv6 packet headers define the following fields:

- Version:

The length is 4 bits. For IPv6, the field must be 6.

- Traffic Class:

The length is 8 bits. It indicates a type of service provided to the packey and is equal to the “TOS” in the IPv4.

- Flow Label:

The length is 20 bits, used to identify the packet of the same service flow. One node can be taken as the sending source of several service flows, and the flow label and the source node identify one service flow unique.

- Payload Length:

The length is 16 bits, including the byte length of payloads and the length of various IPv6 extension options if any. In other words, it includes the lenth of the IPv6 packet besides the IPv6 header itself.

- Next Header:

This field indicates the protocol types in the header field following the IPv6 header. Similar to the IPv4 protocol field, the Next Header field can be used to indicate whether the high level is TCP or UDP. It also can be used to indicate whether an IPv6 extended header exists.

- Hop Limit:

The length is 8 bits. When one router forwards the packet for one time, this field will reduce 1. If this field is 0, this packet will be discarded. It is similar to the life span field in the IPv4 packet header.

- Source Address (Source Address):

The length is 128 bits. It indicates the sender address of an IPv6 packet.

- Destination Address (Destination Address):

The length is 128 bits. It indicates the receiver address of an IPv6 packet.

At present, the following extended header is defined for the IPv6:

- Hop-by-Hop Options:

This extended header must directly follow an IPv6 header. It contains the option data that must be checked by each node on the passed paths.

- Routing Header (Routing (Type 0)):

This extended header indicates the nodes that a packet will go through before reaching the destination. It contains the address list of various nodes that the packet goes through. The initial destination address of the IPv6 header is the first one of a series of addresses in the route header, other than the final destination address of the packet. After receiving this packet, the node of this address will process the IPv6 header and the routing header, and send the packet to the second address of the routing header list. In this way, continue it until the packet reaches the final destination.

- Fragment Header (Fragment):

This extended header is used to frag packets longer than source node and destination node path MTU by the source node.

- Destination Option Header (Destination Options):

This extended header replaces the IPv4 option field. At present, the only defined destination option is to fill the option with an integer multiple of 64 bits (8 bytes) when necessary. This extended header can be used to carry the information checked by the destination node.

- Upper-layer Extended Header (Upper-layer header):

It indicates the protocols for upper-layer transfer data, such as TCP(6) and UDP(17).

Furthermore, the extended header of the Authentication and the Encapsulating Security Payload will be described in the IPSec section. At present, the IPv6 implemented by use cannot support the IPSec.

32.1.4 IPv6 MTU Discovery

It is similar with the path MTU discovery of the IPv4, the path MTU discovery of the IPv6 allows one host to discover and adjust the size of the MTU in the data transmission path.

Furthermore, when the data packet to be sent is larger than the MTU in the data transmission path, the host will be fragment by itself. This host-fragmented behavior makes it not necessary for the router to process the fragment and save the resource of the IPv6 router, as well as improve the efficiency of the IPv6 network.

Caution The minimum link MTU is 68 bytes in the IPv4, which means the link of the path in each data transmission should support the link MTU with 68 bytes at least. The minimum link MTU is 1280 bytes in the IPv6. It is strongly recommended to use the 1500 link MTU for the link in the IPv6.

32.1.5 IPv6 Neighbor Discovery

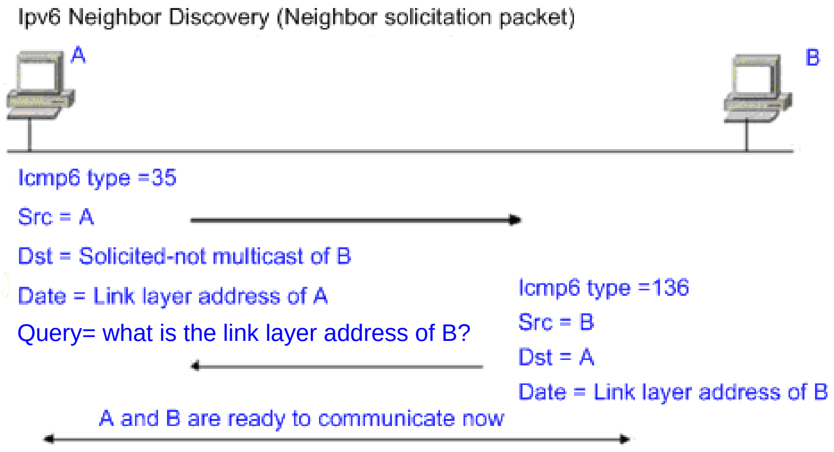
The IPv6 neighbor discovery processing makes use of the message of the ICMPv6 and the multicast addresses of the solicited neighbor to obtain the link layer address of the neighbor at the same link, and verify the reachability of the neighbor as well as maintain the status of the neighbor. These types of messages are briefly described respectively below.

32.1.5.1 Neighbor Solicitation Message

When a node is to communicate with another node, the first node must get the link layer address of the second node. At this time, it should send neighbor solicitation (NS) message to the second node and the destination address of the message is corresponding to the requested multicast address of the IPv6 address of the destination node. The sent NS message also contains the link layer address of itself. After receiving this NS message, corresponding node will retransmit a response message, referred to as the neighbor advertisement (NA), whose destination address is the source address of the NS and the content is the link layer address of the solicited node. After receiving the response message, the source node can communicate with the destination node.

The following is the neighbor solicitation procedure:

Figure 32-4


Ipv6 Neighbor Discovery (Neighbor solicitation packet)
A
B
Icmp6 type =35
Src = A
Dst = Solicited-not multicast of B
Date = Link layer address of A
Query= what is the link layer address of B?
Icmp6 type =136
Src = B
Dst = A
Date = Link layer address of B
A and B are ready to communicate now

The neighbor solicitation message can also be used to detect the reachability of the neighbor (for the existing neighbor). At this time, the destination address of the neighbor solicitation message is the unicast address of this neighbor.

When the link layer address of one node changes, the neighbor advertisement will be sent actively. At this time, the destination address of the neighbor advertisement message is the addresses of all nodes for this link.

When one neighbor is considered that the reachable time is expired, should enable the Neighbor Unreachability Detection (NUD), which will occur only when it is necessary to send the unicast message to this neighbor. The NUD will not be enabled for the multicast message transmission.

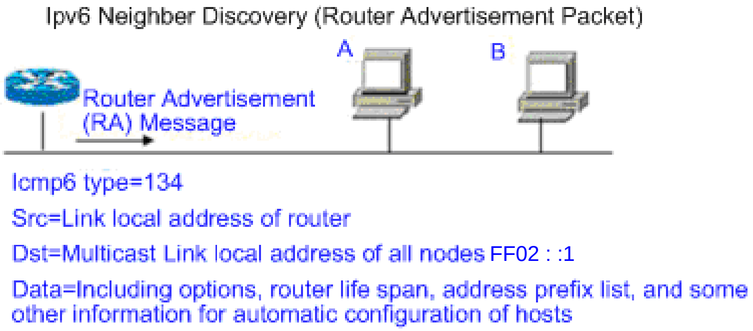
Furthermore, the neighbor solicitation message in the stateless address auto-configuration can also be used to detect the unique of the address, namely the address conflict detect. At this time, the source address of the message is unassigned address (: :).

32.1.5.2 Router Advertisement

The Router Advertisement (RA) is periodically sent to all nodes of the local links on the router.

The sending of the Router Advertisement (RA) is shown as the figure below:

Figure 32-5


Ipv6 Neighbor Discovery (Router Advertisement Packet)
A
B
Router Advertisement
(RA) Message
Icmp6 type=134
Src=Link local address of router
Dst=Multicast Link local address of all nodes FF02 : :1
Data=Including options, router life span, address prefix list, and some other information for automatic configuration of hosts

In general, the Router Advertisement (RA) contains the contents below:

- One or more IPv6 address prefixes are used to provide for the host to carry out the address auto-configuration.
- The effective data of the IPv6 address prefix.
- The usage of the host auto-configuration (Stateful or stateless).
- The information as the default router (namely, determine whether this router is taken as the default router. If yes, it will announce the time as the default router itself).
- Provide the host with some other information about the configuration such as the hop limit, the MTU and the neighbor solicitation retransmission interval.

The Router Advertisement (RA) is also used to respond to the Router Solicitation (RS) message sent by the host, and the Router Solicitation (RS) message allows the host to obtain the auto-configuration information immediately, but need not to wait the router to send the Router Advertisement (RA) once the host is activated. If there is no unicast address when the host is activated at just, the Router Solicitation (RS) message sent by the host will use the unassigned address (0:0:0:0:0:0:0:0) as the source address of the solicitation message. Otherwise, the existing unicast address is taken as the source address, while the Router Solicitation (RS) message uses the multicast address (FF02::2) of all routers for the local link as the destination address. As the response router solicitation (RS) message, the Router Advertisement (RA) message will use the source address of the solicitation message as the destination address (if the source address is the unassigned address, it will use the multicast address FF02::1) of all nodes for the local link.

The following parameters can be configured in the Router Advertisement (RA) message:

ra-interval, it is the sending interval of the Router Advertisement (RA).

ra-lifetime, it is the router lifetime, namely whether the router is acted as the default router of the local link and the time as this role.

prefix, it is the IPv6 address prefix of the local link, which can be used to carry out the auto-configuration by the host, including the configuration of other parameters for the prefix.

rs-initerval, it is the retransmitted time interval of the neighbor solicitation message.

reachabletime, it is the time maintained after the neighbor reachable time and the neighbor is considered to be reachable.

We configure the above parameters in the IPv6 interface property.

⚠ **Caution**

1. By default, no Router Advertisement (RA) message is positively sent on the interface. If you want to allow a Router Advertisement (RA) message to be sent, you can use the command **no ipv6 nd suppress-ra** in the interface configuration mode.
2. In order to make the stateless address auto-configuration of the node work normally, the length of the prefix for the router advertisement (RA) message should be 64 bits.

32.2 IPv6 Configuration

The following will introduce the configuration of various function modules of the IPv6 respectively:

32.2.1 Configuring IPv6 Address

The task of this section describes how to configure an IPv6 address on an interface. By default, no IPv6 address is configured.

Caution

Once the interface of IPv6 is created and the link of the interface is in the UP status, the system will automatically generate link-local addresses for the interface. At present, the IPv6 doesn't support the configuration of the anycast address.

The configuration procedure of the IPv6 address is shown as follows:

Command	Meaning
configure terminal	Enter the global configuration mode.
interface *interface-id*	Enter the interface configuration mode.
ipv6 enable	Enable the IPv6 protocol for an interface. If this command is not run, then the system automatically enables the IPv6 protocol when you configure an IPv6 address for an interface.
ipv6 address *ipv6-prefix/prefix-length* [**eui-64**]	Configure the unicast address of the IPv6 for this interface. The key word **Eui-64** indicates the generated ipv6 address consists of the configured address prefix and the 64 bits interface ID. Note: Whether the key word eui-64 is used, it is necessary to enter complete address format when the address is deleted (Prefix + interface ID/prefix length). When you configure an IPv6 address on an interface, then the IPv6 protocol of the interface is automatically enabled. Even if you use **no ipv6 enable**, you cannot disable the IPv6 protocol.
End	Return to the privileged EXEC mode.
show ipv6 interface vlan 1	View the information related to the ipv6 interface.
copy running-config startup-config	Save the configuration.

Use the **no ipv6 address** *ipv6-prefix***I***prefix-length* **[eui-64]**command to delete the configured address. The following is an example of the configuration of the IPv6 address:

```
DGS-3610(config)# interface vlan 1
DGS-3610(config-if)# ipv6 enable
DGS-3610(config-if)# ipv6 address fec0:0:0:1::1/64
DGS-3610(config-if)# end
DGS-3610(config-if)# show ipv6 interface vlan 1
Interface vlan 1 is Up, ifindex: 2001
address(es):
Mac Address: 00:00:00:00:00:01
INET6: fe80::200:ff:fe00:1 , subnet is fe80::/64
INET6: fec0:0:0:1::1 , subnet is fec0:0:0:1::/64
Joined group address(es):
ff01:1::1
```

```
ff02:1::1
ff02:1::2
ff02:1::1:ff00:1
MTU is 1500 bytes
ICMP error messages limited to one every 10 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds<240--160>
ND router advertisements live for 1800 seconds
```

32.2.2 Configuring Redirection Function for ICMPv6

This section will describe how to configure the redirection function of the ICMPv6 for the interface. By default, the redirection function of the IPv6 on the interface is opened. It is necessary to send the redirection message to the originator of the message when the router suffers from the following conditions at the same time during the packet forward:

- The destination address of the message is not the multicast address;
- The destination address of the message is not the router itself;
- The output interface of the next hop determined by the device for this message is the same as the interface this message received, namely, the next hop and the originator is of the same link;
- The node of the source address identification for the message is a neighbor of the local router. Namely, there is this neighbor in the neighbor table of the device.

Caution The device other than the host can generate the redirection message, and the router will not update its route table when it receives the redirection message.

The following is the configuration procedure of one interface to open the redirection function:

Command	Meaning
configure terminal	Enter the global configuration mode.
interface vlan *1*	Enter SVI configuration mode.
ipv6 redirects	Enable the IPv6 redirection function of the interface
End	Return to the privileged EXEC mode.
show ipv6 interface vlan *1*	Show the related configuration information of the interface
copy running-config startup-config	Save the configuration.

Use the **no ipv6 redirects** command to close the redirection function. The following is an example to configure the redirection function:

```
DGS-3610(config)# interface vlan 1
DGS-3610(config-if)# ipv6 redirects
DGS-3610(config-if)# end
DGS-3610# show ipv6 interface vlan 1
Interface vlan 1 is Up, ifindex: 2001
address(es):
Mac Address: 00:d0:f8:00:00:01
INET6: fe80::2d0:f8ff:fe00:1 , subnet is fe80::/64
INET6: fec0:0:0:1::1 , subnet is fec0:0:0:1::/64
Joined group address(es):
ff01:1::1
ff02:1::1
ff02:1::2
ff02:1::1:ff00:1
MTU is 1500 bytes
ICMP error messages limited to one every 10 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds<240--160>
ND router advertisements live for 1800 seconds
```

32.2.3 Configuring Static Neighbor

This section will describe how to configure a static neighbor. By default, the static neighbor is not configured. In general, the neighbor is to learn and maintain its status by the Neighbor Discovery Protocol (NDP) dynamically. At the same time, it is allowed to configure the static neighbor manually.

Table 32-1 The following is the procedure to configure a static neighbor:

Command	Meaning
configure terminal	Enter the global configuration mode.
ipv6 neighbor *ipv6-address interface-id hardware-address*	Use this command to configure a static neighbor on this interface.
End	Return to the privileged EXEC mode.
show ipv6 neighbors	View the neighbor list.
copy running-config startup-config	Save the configuration.

Use the **no ipv6 neighbor** command to allow delete specified neighbor. The following is an example to configure a static neighbor on SVI 1:

```
DGS-3610(config)# ipv6 neighbor fec0:0:0:1::100 vlan 1 00d0.f811.1234
DGS-3610(config)# end
DGS-3610# show ipv6 neighbors verbose fec0:0:0:1::100
IPv6 Address       Linklayer Addr   Interface
fec0:0:0:1::100    00d0.f811.1234   vlan 1
State: REACH/H Age: - asked: 0
```

32.2.4 Configuring Address Conflict Detection

This section describes how to configure address conflict detection times. Address conflict detection is what to be done before all unicast addresses are formally given to interfaces, namely to dectect the uniqueness of an address. The address conflict detection should be carried out whether it is the manual configuration address, the stateless auto-configuration address or the statefull auto-configuration address. However, it is not necessary to carry out the address conflict detection under the following two conditions:

- The management prohibits the address conflict detection, namely, the neighbor solicitation messages sent for the address conflict detection is set to 0.
- The explicit configured anycast address can not be applied to the address conflict detection.

Furthermore, if the address conflict detection function of the interface is not closed, the interface will enable the address conflict detection process for the configured address when it changes to the Up status from the Down status.

The following is the configuration procedure of the quantity of the neighbor solicitation message sent for the address conflict detection:

Command	Meaning
configure terminal	Enter the global configuration mode.
interface vlan *1*	Enter the configuration mode of the SVI 1.
ipv6 nd dad attempts *attempts*	The quantity of the neighbor solicitation message sent for the address conflict detection. When it is configured to 0, any neighbor solicitation message is disallowed. Enable the address conflict detection function on the interface.
End	Return to the privileged mode.
show ipv6 interface vlan *1*	View the IPv6 information of the SVI 1.
copy running-config startup-config	Save the configuration.

Use the **no ipv6 nd dad attempts** command to restore the default value. The following is an example to configure the times of the neighbor solicitation (NS) message sent for the address conflict detection on the SVI1:

```
DGS-3610(config)# interface vlan 1
DGS-3610(config-if)# ipv6 nd dad attempts 3
DGS-3610(config-if)# end
DGS-3610# show ipv6 interface vlan 1
Interface vlan 1 is Up, ifindex: 2001
address(es):
Mac Address: 00:d0:f8:00:00:01
INET6: fe80::2d0:f8ff:fe00:1 , subnet is fe80::/64
INET6: fec0:0:0:1::1 , subnet is fec0:0:0:1::/64
Joined group address(es):
ff01:1::1
ff02:1::1
ff02:1::2
ff02:1::1:ff00:1
MTU is 1500 bytes
ICMP error messages limited to one every 10 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 3
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds<240--160>
ND router advertisements live for 1800 seconds
```

32.2.5 Configuring Other Interface Parameters of Routers

The configuration parameters of the IPv6 in the interface of the devices is mainly comprised of 2 parts, one is used to control the behavior of the router itself, the other one is used to control the contents of the router advertisement (RA) sent by the router, to determine what action should be taken by the host when it receives this router advertisement (RA).

The following will introduce these commands one by one:

Command	Meaning
configure terminal	Enter the global configuration mode.
interface *interface-id*	Enter the interface configuration mode.
ipv6 enable	Enable the IPv6 function.
ipv6 nd ns-interval *milliseconds*	(Optional) Define the retransmission interval of the neighbor solicitation message.
ipv6 nd reachable-time *milliseconds*	(Optional) Define the time when the neighbor is considered to be reachable.
ipv6 nd prefix *ipv6-prefix/prefix-length* | **default** [[*valid-lifetime*	(Optional) Set the address prefix to be advertised in the router advertisement (RA) message.

Command	Meaning
preferred-lifetime] | [**at** *valid-date preferred-date*] | **infinite** | **no-advertise**]]	
ipv6 nd ra-lifetime *seconds*	(Optional) Set the TTL of the router in the router advertisement (RA) message, namely the time as the default router. When the setting is 0, it indicates that it will not act as the default router of the direct-connected network.
ipv6 nd ra-interval *seconds*	(Optional) Set the time interval for the router to send the router advertisement (RA) message periodically.
ipv6 nd managed-config-flag	(Optional) Set the “managed address configuration” flag bit of the router advertisement (RA) message, and determine whether the host will use the stateful auto-configuration to obtain the address when it receives this router advertisement (RA).
ipv6 nd other-config-flag	(Optional) Set the “other stateful configuration” flag bit of the router advertisement (RA) message, and determine whether the host will use the stateful auto-configuration to obtain other information other than the address when it receives this router advertisement (RA).
ipv6 nd suppress-ra	(Optional) Set whether suppress the router advertisement (RA) message in this interface.
End	Return to the privileged EXEC mode.
show ipv6 interface [*interface-id*] [**ra-info**]	Show the ipv6 interface of the interface or the information of RA sent by this interface.
copy running-config startup-config	(Optional) Save the configuration.

The **no** command of above commands can be used to restore the default value.

32.3 IPv6 Monitoring and Maintenance

It is mainly used to provide related command to show some internal information of the IPv6 protocol, such as display the ipv6 information, the neighbor table and the route table information of the interface.

Command	Meaning
show ipv6 interface [*interface-id*] [**ra-info**]	Show the IPv6 information in the interface.

Command	Meaning
show ipv6 neighbors [**verbose**] [*interface-id*] [*ipv6-address*]	Show the neighbor information.
show ipv6 route [**static**] [**local**] [**connected**]	Show the information of the IPv6 route table.

1. View the IPv6 information in an interface.

```
DGS-3610# show ipv6 interface
interface vlan 1 is Down, ifindex: 2001
address(es):
Mac Address: 00:d0:f8:00:00:01
INET6: fe80::2d0:f8ff:fe00:1 , subnet is fe80::/64
INET6: fec0:1:1:1::1 , subnet is fec0:1:1:1::/64
Joined group address(es):
ff01:1::1
ff02:1::1
ff02:1::2
ff02:1::1:ff00:1
MTU is 1500 bytes
ICMP error messages limited to one every 10 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds<240--160>
ND router advertisements live for 1800 seconds
```

2. View the information of the router advertisement (RA) message to be sent in an interface

```
DGS-3610# show ipv6 interface ra-info
vlan 1: DOWN
RA timer is stopped
waits: 0, initcount: 3
statistics: RA(out/in/inconsistent): 4/0/0, RS(input): 0
Link-layer address: 00:00:00:00:00:01
Physical MTU: 1500
ND router advertisements live for 1800 seconds
ND router advertisements are sent every 200 seconds<240--160>
Flags: !M!O, Adv MTU: 1500
ND advertised reachable time is 0 milliseconds
ND advertised retransmit time is 0 milliseconds
ND advertised CurHopLimit is 64
Prefixes: (total: 1)
fec0:1:1:1::/64(Def, Auto, vltime: 2592000, pltime: 604800, flags: LA)
```

3. View the neighbor table information of the IPv6.

```
DGS-3610# show ipv6 neighbors
```

```
IPv6 Address              Linklayer Addr  Interface
fe80::200:ff:fe00:1      0000.0000.0001 vlan 1
State: REACH/H Age: - asked: 0
fec0:1:1:1::1             0000.0000.0001 vlan 1
State: REACH/H Age: - asked: 0
```

33 IPV6 Tunnel Configuration

33.1 Overview

The IPv6 is designed to inherit and replace the IPv4. However, the evolution from the IPv4 to the IPv6 is a gradual process. Therefore, before the IPv6 completely replaces the IPv4, it is inevitable that these two protocols coexist for a period. At the beginning of this transition stage, IPv4 networks are still main networks. IPv6 networks are similar to isolated islands in IPv4 networks. The problems about transition can be divided into the following two types:

1. The problem about the communication between isolated IPv6 networks via IPv4 networks
2. The problem about the communication between IPv6 networks and IPv4 networks

This article discusses the tunnel technology that is used to solve problem 1. The solution to problem2 is NAT-PT (Network Address Translation-Protocol Translation), which is not covered in this article.

The IPv6 tunnel technology encapsulates IPv6 packets in IPv4 packets. In this way, IPv6 protocol packets can communicate with each other via IPv4 networks. Therefore, with the IPv6 tunnel technology, isolated IPv6 networks can communicate with each other via existing IPv4 networks, avoiding any modification and upgrade of existing IPv4 networks. An IPv6 tunnel can be configured between Area Border Routers or between an Area Border Router and the host. However, all the nodes at the two ends of the tunnel must support the IPv4 and IPv6 protocol stacks. At present, our company supports the following tunnel technologies:

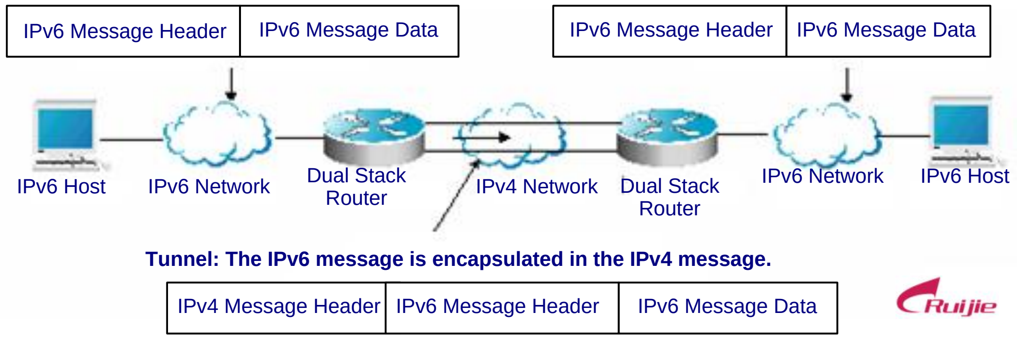
Tunnel Type	Reference
Manually Config Tunnel	RFC2893
automatic 6to4 Tunnel	RFC3056
Intra-Site Automatic Tunnel Addressing Protocol(ISATAP)	draft-ietf-ngtrans-isatap-22

Caution

The structure formed by connecting isolated IPv6 networks with the IPv6 tunnel technology is not the final network architecture of the IPv6. The technology is only for transition.

The model to use the tunnel technology is shown in the following figure:

Figure 33-1



The features of various tunnels are respectively introduced below.

33.1.2 IPv6 Manually Configured Tunnel

One manually configured tunnel is similar to one permanent link set up between two IPv6 domains via the backbone network of the IPv4.It is applicable to the relatively fixed connections that have a higher demand on security between two Area Border Routers or between an Area Border Router and a host.

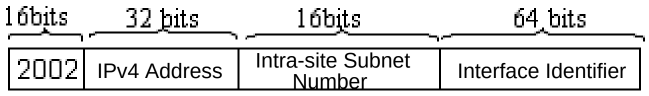
On a tunnel interface, you must manually configure the IPv6 address, source IPv4 address (tunnel source) and destination IPv4 address (tunnel destination) of the tunnel. The nodes at the two ends of the tunnel must support the IPv6 and IPv4 protocol stacks. In practical application, tunnels to be manually configured are always in pairs. Namely, configure a pair on two edge devices at the same time. We can think it as a point-to-point tunnel.

33.1.3 Automatic 6to4 Tunnel

The automatic 6to4 tunnel technology allows interconnection of isolated IPv6 networks via IPv4 networks. The differences between the automatic 6to4 tunnel and manually configured tunnel technologies are as follows: A manually configured tunnel is a point-to-point tunnel, while a 6to4 tunnel is a point -to-multipoint tunnel.

The 6to4 tunnel takes an IPv4 network as a Nonbroadcast multi-access (NBMA) link. Therefore, the devices of 6to4 need not be configured in pairs. The IPv4 addresses embedded in an IPv6 address will be used to search the other end of an automatic tunnel. The 6to4 tunnel can be taken as a point -to-multipoint tunnel. The automatic 6to4 tunnel can be configured on the Area Border Router of an isolated IPv6 network. For each packet, it automatically builds a tunnel connecting the Area Border Router in another IPv6 network. The destination address is the IPv4 address of the Area Border Router in the IPv6 network on the other end. The IPv4 address is extracted from the destination IPv6 address of the packet. The destination IPv6 address starts with the prefix 2002::/16 in the following form:

Figure 33-2



16bits	32 bits	16bits	64 bits
2002	IPv4 Address	Intra-site Subnet Number	Interface Identifier

IPv6 6to4 Address Format

The 6to4 address is an address for automatic 6to4 tunnel technology. The IPv4 address embedded in it is usually the global IPv4 address of the site area border router exit. When the automatic tunnel is built, the address is used as the IPv4 address for tunnel packet encapsulation. All the routers at the two ends of the 6ot4 tunnel must also support the IPv6 and IPv4 protocol stacks. A 6to4 tunnel is usually configured between Area Border Routers.

For example, the global IPv4 address of the 6to4 site area border router exit is 211.1.1.1 (Indicated as D301:0101 in hex), a subnet number in the site is 1 and the interface identifier is 2e0:ddff:fee0:e0e1, then the corresponding 6to4 address can be denoted as follows:

2002: D301:0101:1: 2e0:ddff:fee0:e0e1

⚠ Caution

The IPv4 address embedded in the 6to4 address cannot be a private IPv4 address (for example, the address of the network interface segment 10.0.0.0/8, 172.16.0.0/12 or 192.168.0.0/16) and must be the global IPv4 address.

Common application models of 6to4 tunnels:

- Simple application models

The simplest and most common application of 6to4 tunnels is used to interconnect multiple IPv6 sites. Each site must have one connection to one of their shared IPv4 networks at least. This IPv4 network can be the Internetor the internal backbone network of an organization. Each site must have a unique global IPv4 address. The 6to4 tunnel will use the address to form the IPv6 prefix of 6to4/48: 2002:IPV4 address/48.

- Mixture application models

Based on the application described above, by 6to4 relay devices provided at the edge of a pure IPv6 network, other 6to4 networks access the pure IPv6 network. The router used to implement the function is called 6to4 Relay Router.

33.1.4 ISATAP Tunnel

Intra-site Automatic Tunnel Addressing Protocol (ISATAP) is an IPv6 tunnel technology by which an intra-site IPv6 architecture takes an IPv4 network as one nonbroadcast multi-access (NBMA) link layer, namely taking an IPv4 network as the virtual link layer of the IPv6.

ISATAP is applicable when the pure IPv6 network inside a site is not ready for use and IPv6 packets need be transferred internally in the site. For example, a few of IPv6 hosts for test need communicate with each other inside the site. Through the ISATAP tunnel, the IPv4/IPv6 dual stack hosts on a same virtual link can communicate with each other inside the site.

On the ISATAP site, the ISATAP router provides standard router advertisement packet, allowing automatic configuration of the ISATAP host inside the site. At the same time, the ISATAP router performs the function that an intra-site ISATAP host and external IPv6 host forward packets.

The IPv6 address prefix used by ISATAP can be any legal 64-bit prefix for IPv6 unicast, including the global address prefix, link local prefix and site local prefix. The IPv4 address is placed as the ending 32 bits of the IPv6 address, allowing a tunnel to be automatically built.

It is very possible that ISATAP is used with other transition technologies. Especially when used with the 6to4 tunnel technology, it can make the dual stack host of an internal network access an IPv6 backbone network very easily.

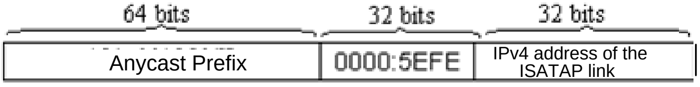
- ISATAP interface identifier

The unicast address used by ISATAP is in the form of a 64-bit IPv6 prefix plus a 64-bit interface identifier. The 64-bit interface identifier is generated in the revised EUI-64 address form. The value of the first 32 bits of the interface identifier is **0000:5EFE**, indidcating that it is an interface identifier of ISATAP.

- ISATAP address structure

An ISATAP address refers to the unicast address containing an ISATAP interface identifier in its interface identifier. TheISATAP address structure is shown in the following figure:

Figure 33-3



IPv6 ISATAP Address Format

The above figure shows that the interface identifier contains an IPv4 address. The address is the IPv4 address of a dual stack host and will be used when an automatic tunnel is automatically built.

For example, the IPv6 prefix is 2001::/64 and the embedded IPv4 address is 192.168.1.1. In the ISATAP address, the IPv4 address is denoted as the hexadecimal numeral of C0A8:0101. Therefore, its corresponding ISATAP address is as follows:

2001::0000:5EFE:C0A8:0101

33.2 IPv6 Tunnel Configuration

33.2.1 Configuring Manual IPv6 Tunnels

This section explains how to configure manual tunnels.

To configure a manual tunnel, configure an IPv6 address on the tunnel interface and manually configure the source interfaceand destination interfaceIPv4 addresses of the tunnel. Then, configure the hosts or routers at the two ends of the tunnel to ensure that they support the dual stacks (the IPv6 and IPv4 protocol stacks).

Caution

Be sure not to configure a manual tunnel with a same address as tunnel source and tunnel destination addresses on a switch.

Brief steps

```
config terminal
interface tunnel tunnel-num
tunnel mode ipv6ip
ipv6 enable
tunnel source {ip-address | type num}
tunnel destination ip-address
end
```

Detailed steps

Command	Meaning
configure terminal	Enter the global configuration mode.
interface tunnel *tunnel-num*	Specify a tunnel interface number to create a tunnel interface and enter the interface configuration mode.
tunnel mode ipv6ip	Specify that the type of a tunnel is the manually configured tunnel.
ipv6 enable	Enable the IPv6 function of the interface. You can also configure the IPv6 address to directly enable the IPv6 function of the interface.

Command	**Meaning**
tunnel source {*ip-address* | *type* *num*	Specify the IPv4 source address or referenced source interface number of a tunnel. Note: If you specify an interface, the IPv4 address must have been configured on the interface.
tunnel destination *ip address*	Specify the destination address of a tunnel.
end	Return to the privileged mode.
copy running-config startup-config	Save the configuration.

Refer to the section *Verifying IPv6 Tunnel Configuration and Mmonitoring* to check the working states of the tunnel.

33.2.2 Configuring 6to4 Tunnel

This section introduces how to configure a 6to4 tunnel.

The destination address of a 6to4 tunnel is determined by the IPv4 address which is extracted from the 6to4 IPv6 address. The routers on the two ends of the 6to4 tunnel must support the dual stacks, namely, the IPv4 and IPv6 protocol stacks.

⚠ Caution

On one switch, you can configure only one 6to4 tunnel. The encapsulation source address (IPv4 address) used by the 6to4 tunnel must be a global routable address. Otherwise, the 6to4 tunnel cannot work normally.

Brief steps

```
config terminal
interface tunnel tunnel-num
tunnel mode ipv6ip 6to4
ipv6 enable
tunnel source {ip-address | type num}
exit
ipv6 route 2002::/16 tunnel tunnel-number
end
```

Detailed steps

Command	**Meaning**
configure terminal	Enter the global configuration mode.

Command	Meaning
interface tunnel *tunnel-num*	Specify a tunnel interface number to create a tunnel interface and enter the interface configuration mode.
tunnel mode ipv6ip 6to4	Specify that the type of a tunnel is the 6to4 tunnel.
ipv6 enable	Enable the IPv6 function of the interface. You can also configure the IPv6 address to directly enable the IPv6 function of the interface.
tunnel source {*ip-address* | *type num*	Specify the encapsulation source address or referenced source interface number of a tunnel. Note: The IPv4 address must have been configured on the referenced interface. The used IPv4 address must be a global routable address.
Exit	Return to the global configuration mode.
ipv6 route *2002::/16* **tunnel** *tunnel-number*	Configure a static route for the IPv6 6to4 prefix 2002::/16 and associate the output interface to the tunnel interface, namely, the tunnel interface specified in the above Step 2.
End	Return to the privileged mode.
copy running-config startup-config	Save the configuration.

Refer to the section *Verifying IPv6 Tunnel Configuration and Monitoring* to check the working states of the tunnel.

33.2.3 Configuring ISATAP Tunnel

This section introduces how to configure an ISATAP device.

On an ISATAP tunnel interface, the configuration of an ISATAP IPv6 address and the advertisement configuration of a prefix is same to that of a normal IPv6 interface. However, the address configured for an ISATAP tunnel interface must be a revised EUI-64 address.

The reason is that the last 32 bits of the interface identifier in the IPv6 address are composed of theIPv4 address of the interface referenced by the tunnel source address. Refer to the above chapters and sections for more information about ISATAP address formats.

Caution	On a switch, it is allowed to configure multiple ISATAP tunnels at the same time. However, the tunnel source of each ISATAP tunnel must be different. Otherwise, there is no way to know which ISATAP tunnel a received ISATAP tunnel packet belongs to.

Brief steps

```
config terminal
interface tunnel tunnel-num
tunnel mode ipv6ip isatap
ipv6 address ipv6-prefix/prefix-length eui-64
tunnel source interface-type num
no ipv6 nd suppress-ra
end
```

Detailed steps

Command	**Meaning**
configure terminal	Enter the global configuration mode.
interface tunnel *tunnel-num*	Specify a tunnel interface number to create a tunnel interface and enter the interface configuration mode.
tunnel mode ipv6ip isatap	Specify that the type of a tunnel is the ISATAP tunnel.
ipv6 address *ipv6-prefix/prefix-length* **eui-64**	Configure the IPv6 ISATAP address. Be sure to specify to use the **eui-64** keyword. In this way, the ISATAP address will be automatically generated. The address configured on an ISATAP interface must be an ISATAP address.
tunnel source type *num*	Specify the source interface number referenced by a tunnel. On the referenced interface, the IPv4 address must have been configured.

Command	Meaning
no ipv6 nd suppress-ra	By default, it is disabled to send router advertisement packets on an interface. Enable the function with the command, allowing automatic configuration of the ISATAP host.
End	Return to the privileged EXEC mode.
copy running-config **startup-config**	Save the configuration.

Refer to the section *Verifying IPv6 Tunnel Configuration and Monitoring* to check the working states of the tunnel.

33.3 Verifying IPv6 Tunnel Configuration and Monitoring

This section introduces how to verify the configuration and actual running states of an IPv6 tunnel.

Brief steps

```
enable
show interface tunnel number
show ipv6 interface tunnel mumber
ping protocol destination
show ip route
show ipv6 route
```

Detailed steps

Command	Meaning
enable	Enter the privilege configuration mode.
show interface tunnel *tunnel-num*	View the information of a tunnel interface.
show ipv6 interface tunnel *tunnel-num*	View the IPv6 information of a tunnel interface.
ping *protocol destination*	Check the basic connectivity of a network.
show ip route	View the IPv4 router table.

Command	Meaning
show ipv6 route	View the IPv6 router table.

1. View the information of a tunnel interface.

```
DGS-3610# show interface tunnel 1
Tunnel 1 is up, line protocol is Up
Hardware is Tunnel, Encapsulation TUNNEL
Tunnel source 192.168.5.215  ,  destination 192.168.5.204
Tunnel protocol/transport IPv6/IP
Tunnel TTL is 9
Tunnel source do conformance check set
Tunnel source do ingress filter set
Tunnel destination do safety check not set
Tunnel disable receive packet not set
```

2. View the IPv6 information of a Tunnel interface.

```
DGS-3610# show ipv6 interface tunnel 1
interface Tunnel 1 is Up, ifindex: 6354
address(es):
Mac Address: N/A
INET6: fe80::3d9a:1601 , subnet is fe80::/64
Joined group address(es):
ff02::2
ff01::1
ff02::1
ff02::1:ff9a:1601
INET6: 3ffe:4:0:1::1 , subnet is 3ffe:4:0:1::/64
Joined group address(es):
ff02::2
ff01::1
ff02::1
ff02::1:ff00:1
MTU is 1480 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds<240--160>
ND router advertisements live for 1800 seconds
```

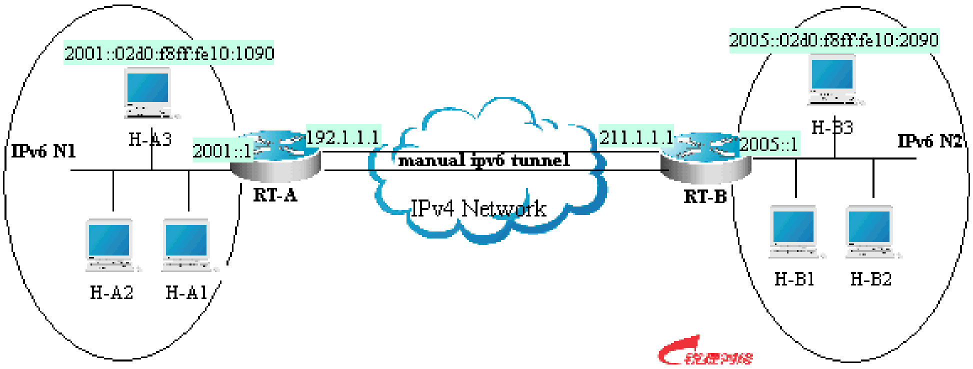
33.4 IPv6 Tunnel Configuration Instances

The following chapters/sections introduce IPv6 tunnel configuration instances.

- Manual IPv6 Tunnel Configuration Instance
- 6to4 Tunnel Configuration Instance
- ISATAP Tunnel Configuration Instance
- Configuration Instance for Composite Application of ISATAP and 6to4 Tunnels

33.4.1 Manual IPv6 Tunnel Configuration Instance

Figure 33-4



As shown in the above figure, IPv6 networks N1 and N2 are isolated by the IPv4 network. Two networks can beinterconnected through manual tunnel configuration, for example, the H-A3 host in N1 can access the H-B3 host in N2 through configuration.

In the figure, both RT-A and RT-B support the IPv4 and IPv6 protocol stacks. Tunnel configuration is performed on the Area Border Routers (RT-A and RT-B) in N1 and N2. Note that manual tunnel must be configured symmetrically, that is, manual tunnels must be configured on RT-A and RT-B.

The specific configurations related to the tunnel are respectively as follows:

Prerequisite: Suppose the routes of IPv4 are connected. No more route configuration about IPv4 is described.

RT-A configuration

#Connect the interfaces of the IPv4 network

```
interface FastEthernet 2/1
no switchport
ip address 192.1.1.1 255.255.255.0
```

#Connect the interfaces of the IPv6 network

```
interface FastEthernet 2/2
no switchport
ipv6 address 2001::1/64
no ipv6 nd suppress-ra  (optional)
```

#Configure manual tunnel interface

```
interface Tunnel 1
tunnel mode ipv6ip
ipv6 enable
tunnel source FastEthernet 2/1
tunnel destination 211.1.1.1
```

#Configure the router to the tunnel

```
ipv6 route 2005::/64 tunnel 1
```

RT-B configuration

#Connect the interfaces of the IPv4 network

```
interface FastEthernet 2/1
no switchport
ip address 211.1.1.1 255.255.255.0
```

# Connect the interfaces of the IPv6 network

```
interface FastEthernet 2/2
no switchport
ipv6 address 2005::1/64
no ipv6 nd suppress-ra  (optional)
```

#Configure the manual tunnel interface

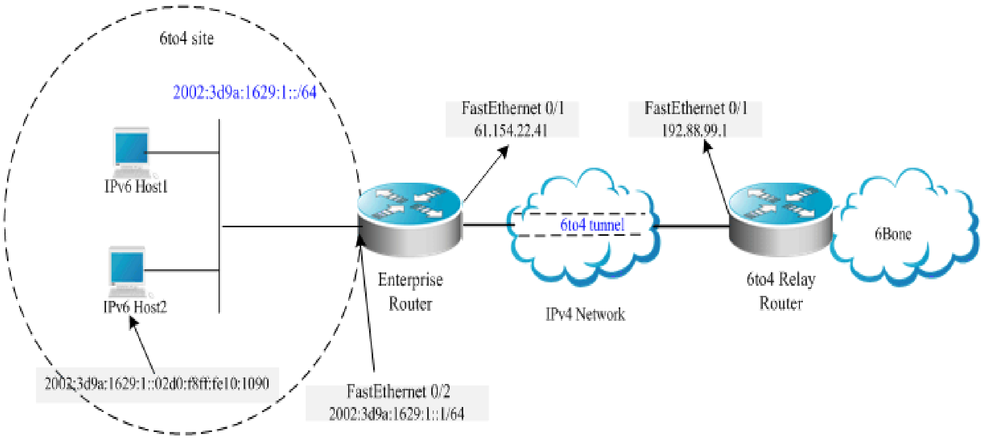
```
interface Tunnel 1
tunnel mode ipv6ip
ipv6 enable
tunnel source FastEthernet 2/1
tunnel destination 192.1.1.1
```

#Configure the route to the tunnel

```
ipv6 route 2001::/64 tunnel 1
```

33.4.2 6to4 Tunnel Configuration Instance

Figure 33-5



As shown in the above figure, using a 6to4 tunnel, an IPv6 network (6to4 site) accesses the IPv6 backbone network (6bone) via the 6to4 relay router.

With the 6to4 tunnel technology, isolated IPv6 networks can be interconnected and be accessed to the IPv6 backbone network via the 6to4 relay router very easily. The 6to4 tunnel is an automatic tunnel and the IPv4 address embeded in the IPv6 address is used to search the other end of the automatic tunnel. Therefore, you need not configure the destination end for the 6to4 tunnel. Additionally, unsimilar to a manual tunnel, the 6to4 tunnel need not be configured symmetrically.

61.154.22.41 in the hex format is 3d9a:1629

192.88.99.1 in the hex format is c058:6301

Caution

When configuring a 6to4 tunnel on an Area Border Router, be sure to use a routable global IPv4 address.

Otherwise, the 6to4 tunnel can not work normally.

The following shows the configuration of the two routers in the figure (Suppose IPv4 routes are connected. Ignore the configuration of IPv4 routes.):

Enterprise Router configuration

# Connect the interfaces of the IPv4 network

```
interface FastEthernet 0/1
no switchport
ip address 61.154.22.41 255.255.255.128
```

# Connect the interfaces of the IPv6 network

```
interface FastEthernet 0/2
no switchport
ipv6 address 2002:3d9a:1629:1::1/64
```

```
no ipv6 nd suppress-ra
```

# Configure the 6to4 tunnel interface

```
interface Tunnel 1
tunnel mode ipv6ip 6to4
ipv6 enable
tunnel source FastEthernet 0/1
```

# Configure the route to the tunnel

```
ipv6 route 2002::/16 Tunnel 1
```

# Configure the route to the 6to4 relay router to access 6bone

```
ipv6 route ::/0 2002:c058:6301::1
```

ISP 6to4 Relay Router configuration

# Connect the interfaces of the IPv4 network

```
interface FastEthernet 0/1
no switchport
ip address 192.88.99.1 255.255.255.0
```

# Configure the 6to4 tunnel interface

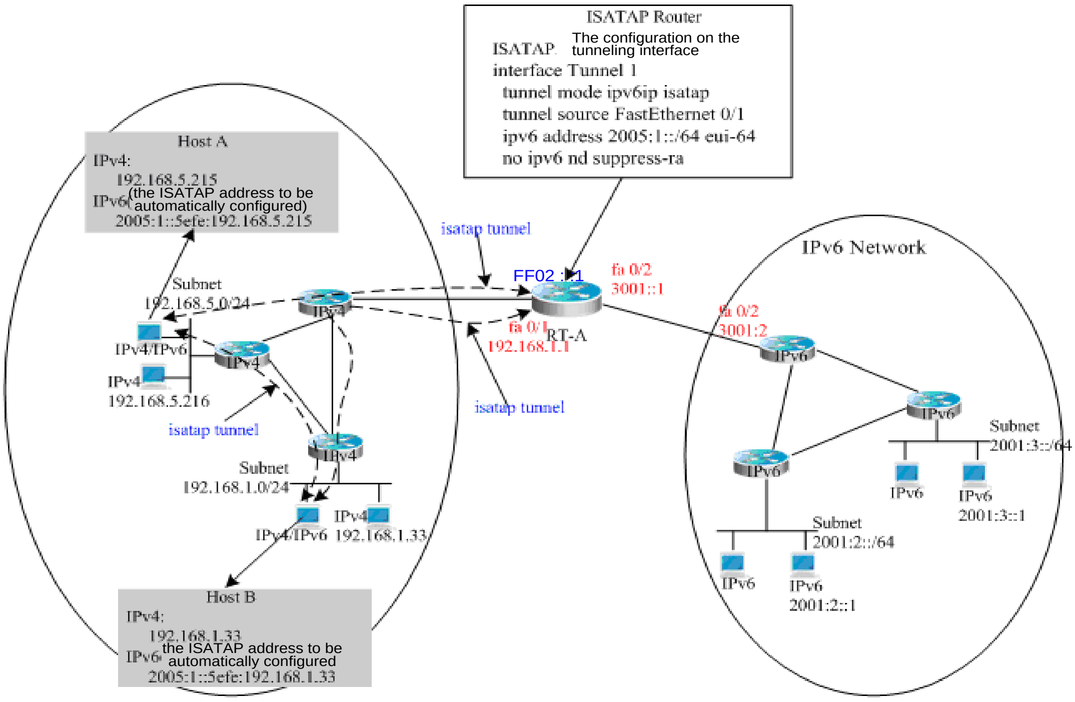
```
interface Tunnel 1
tunnel mode ipv6ip 6to4
ipv6 enable
tunnel source FastEthernet 0/1
```

# Configure the route to the tunnel

```
ipv6 route 2002::/16 Tunnel 1
```

33.4.3 ISATAP Tunnel Configuration Instance

Figure 33-6



```
interface Tunnel 1
  tunnel mode ipv6ip isatap
  tunnel source FastEthernet 0/1
  ipv6 address 2005:1::/64 eui-64
  no ipv6 nd suppress-ra
```

As shown in the above figure, it is one typical topology by use of an ISATAP tunnel. The ISATAP tunnel is used to communicate between isolated IPv4/IPv6 dual stack hosts inside the IPv4 site. The ISATAP router has the following two functions inside the ISATAP site:

- Receive a router request packet from the ISATAP host inside the site and then respond with a router advertisement packet for the ISATAP host inside the site to be automatically configured.
- Be responsible for packet forwarding of the ISATAP host inside the site and the IPv6 host outside the site.

In the above figure, when Host A and Host B send router requests to ISATAP Router, ISATAP Router will respond with a router advertisement packet. After receiving the packet, the hosts configure automatically and generate their own ISATAP addresses respectively. Then, the IPv6 communication between Host A and Host B will be done via the ISATAP tunnel. When Host A or Host B need communicate with the IPv6 host outside the site, Host A sends the packet to the ISATAP router RT-A via the ISATAP tunnel and then RT-A forwards the packet to the IPv6 network.

In the above figure, ISATAP Router (RT-A) is configured as follows:

# Connect the interfaces of the IPv4 network

```
interface FastEthernet 0/1
no switchport
```

```
ip address 192.168.1.1 255.255.255.0
```

# Configure the isatap tunnel interface

```
interface Tunnel 1
tunnel mode ipv6ip isatap
tunnel source FastEthernet 0/1
ipv6 address 2005:1::/64 eui-64
no ipv6 nd suppress-ra
```

# Connect the interfaces of the IPv6 network

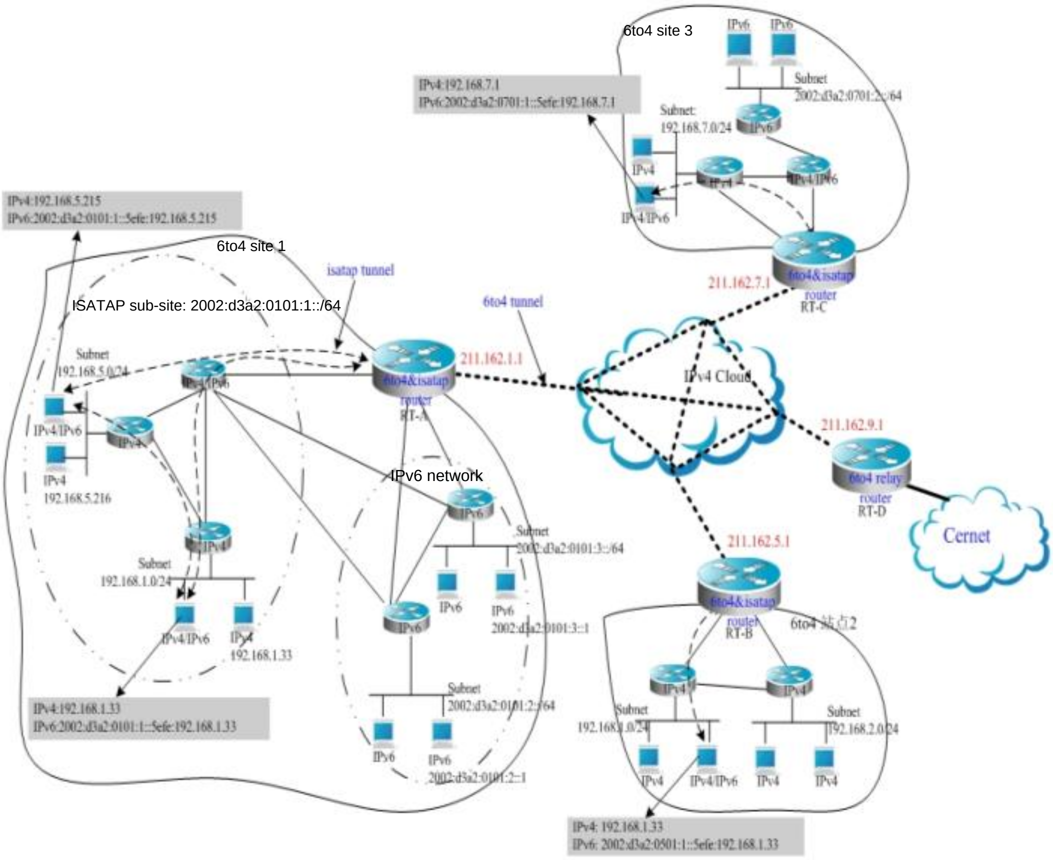
```
interface FastEthernet  0/2
no switchport
ipv6 address 3001::1/64
```

# Configure the route to the IPv6 network

```
ipv6 route 2001::/64 3001::2
```

33.4.4 Configuration Instance for Composite Application of ISATAP and 6to4 Tunnels

Figure 33-7



Note

In the above figure, it is an instance of composite application of 6to4 tunnel and ISATAP tunnels. With the 6to4 tunnel technology, various 6to4 sites are interconnected and the 6to4 site accesses the Cernet network via the **6to4 relay router**. At the same time, with the ISATAP tunnel technology inside the 6to4 site, the IPv6 hosts isolated by IPv4 inside the site perform IPv6 communication via the ISATAP tunnel.

Caution

In the above figure, the used global IP address containing the address of the 6to4 Relay router is only for convenience. When actually planning topologies, we should use a true global IP address and the address of the 6to4 Relay. At present, many organizations provide open and free 6to4 Relay routers address.

The configurations of Area Border Routers in the 6to4 site shown in the above figure are introduced respectively below. Please be noted that only main related configurations are listed here.

RT-A Configuration:

# Connect the interfaces of the Internet

```
interface GigabitEthernet 0/1
no switchport
ip address 211.162.1.1 255.255.255.0
```

# Connect the interfaces of the IPv4 network inside the site

```
interface FastEthernet  0/1

no switchport
ip address 192.168.0.1 255.255.255.0
```

# Configure the ISATAP tunnel interface

```
interface Tunnel 1
tunnel mode ipv6ip isatap
tunnel source FastEthernet 0/1
ipv6 address 2002:d3a2:0101:1::/64 eui-64
no ipv6 nd suppress-ra
```

# Connect interface 1 of the IPv6 network

```
interface FastEthernet 0/2
no switchport
2002:d3a2:0101:10::1/64
```

# Connect interface 2 of the IPv6 network

```
interface FastEthernet  0/2
no switchport
2002:d3a2:0101:20::1/64
```

# Configure the 6to4 tunnel interface

```
interface Tunnel 2
tunnel mode ipv6ip 6to4
ipv6 enable
tunnel source GigabitEthernet 0/1
```

# Configure the route to the 6to4 tunnel

```
ipv6 route 2002::/16 Tunnel 2
```

# Configure the routeto the 6to4 relay router RT-D to access the Cernet network

```
ipv6 route ::/0 2002:d3a2::0901::1
```

RT-B configuration:

# Connect the interfaces of the Internet

```
interface GigabitEthernet 0/1
no switchport
ip address 211.162.5.1 255.255.255.0
```

# Connect interface 1 of the IPv4 network inside the site

```
interface FastEthernet  0/1
no switchport
ip address 192.168.10.1 255.255.255.0
```

# Connect interface 2 of the IPv4 network inside the site

```
interface FastEthernet  0/2
no switchport
ip address 192.168.20.1 255.255.255.0
```

# Configure isatap interface Tunnel 1

```
tunnel mode ipv6ip isatap
tunnel source FastEthernet 0/1
ipv6 address 2002:d3a2:0501:1::/64 eui-64
no ipv6 nd suppress-ra
```

# Configure 6to4 tunnel interface

```
interface Tunnel 2
tunnel mode ipv6ip 6to4
ipv6 enable
tunnel source GigabitEthernet 0/1
```

# Configure the route to the 6to4 tunnel

```
ipv6 route 2002::/16 Tunnel 2
```

# Configure the routeto the 6to4 relay router RT-D to access the Cernet network

```
ipv6 route ::/0 2002:d3a2::0901::1
```

RT-C configuration:

# Connect the interfaces of the Internet

```
interface GigabitEthernet 0/1
no switchport
ip address 211.162.7.1 255.255.255.0
```

# Connect the interfaces of the IPv4 network inside the site

```
interface FastEthernet 0/1
no switchport
ip address 192.168.0.1 255.255.255.0
```

# Configuer the isatap tunnel interface

```
interface Tunnel 1
tunnel mode ipv6ip isatap
tunnel source FastEthernet 0/1
ipv6 address 2002:d3a2:0701:1::/64 eui-64
no ipv6 nd suppress-ra
```

# Connect the interfaces of the IPv6 network

```
interface FastEthernet 0/2
no switchport
2002:d3a2:0701:10::1/64
```

# Configure the 6to4 tunnel interface

```
interface Tunnel 2
tunnel mode ipv6ip 6to4
ipv6 enable
tunnel source GigabitEthernet 0/1
```

# Configure the route to the 6to4 tunnel

```
ipv6 route 2002::/16 Tunnel 2
```

#Configure the route to the 6to4 relay router RT-D to access the Cernet network

```
ipv6 route ::/0 2002:d3a2::0901::1
```

RT-D(6to4 Relay) configuration:

# Connect the interfaces of the Internet

```
interface GigabitEthernet 0/1
no switchport
ip address 211.162.9.1 255.255.255.0
```

# Connect the interfaces of the IPv6 network

```
interface FastEthernet 0/1
no switchport
2001::1/64
no ipv6 nd suppress-ra
```

# Configure the 6to4 tunnel interface

```
interface Tunnel 1
tunnel mode ipv6ip 6to4
ipv6 address 2002:d3a2::0901::1/64
```

```
tunnel source GigabitEthernet 0/1
```

#Configure the route to the 6to4 tunnel

```
ipv6 route 2002::/16 Tunnel 1
```

34 OSPFv3 Configuration

OSPF V2 (RFC2328, OSPFv2) runs under the IPv4. The RFC2740 describes OSPF V3 (OSPFv3) and its extended OSPFv2 protocol and provides support for IPv6 routes. This document briefly describes the OSPFv3 protocol and the configuration for running the OSPFv3.

Caution

Before learning this document, you must know the OSPFv2 protocol and related configuration.

The OSPFv3 protocol extends the OSPFv2 protocol and runs mechanisms and most configurations inside itself.

It still conforms to the OSPFv2.

34.1 OSPFv3 Protocol Overview

As an Interior Gateway Protocol (IGP), the OSPF runs among the three layers of devices in a same Autonomous System (AS).

Unlike a vector distance protocol, the OSPF is a link-state protocol. By exchanging various types of link-state advertisements (LSAs) used to record link state information between devices, it synchronizes link state information between devices and then calculates out OSPF route entries through the Dijkstra algorithm.

The OSPFv3 is described in the RFC2740 and supports the IPv6. This section describes the change on implementation in the OSPFv3 in contrast to the OSPFv2.

34.1.1 LSA Association Change

Just as described above, the OSPF is a link-state protocol and its implementation is based on LSAs. Through LSAs, we can know the topologies and address information of networks. In contrast to the IPv4, the IPv6 uses a 128-bit IP address structure and makes the design of LSAs modified accordingly. The types of LSAs are described as follows:

- Router-LSAs (Type 1)

Each device generates this type of LSAs by itself. They describe the states of its links in specified areas and the cost spent on reaching the links.In contrast to the OSPFv2, the Router-LSAs of the OSPFv3 only indicate the state information of links. They do not record the information about the network addresses connected to routers. The information will be acquired by newly added types of LSAs. Additionaly, in the OSPFv2, only one Router-LSA can be generated for each device in each area. While in the OSPFv3, multiple Router-LSAs can be generated. Thus, when performing the SPF calculation, we must consider all the Router-LSAs generated by the device. Router-LSAs and Network-LSAs describe the link topology of areas together.

⚠ **Caution**

Through the flag bits on Router-LSAs, we can know whether the routers are Area Border Routers (ABR), AS boundary routers (ASBR) or those at one end of a virtual link.

■ Network-LSAs (Type 2)

Network-LSAs only exist in broadcast networks or NBMA networks and are generated by DRs (Designated Routers) in a network. They describe the information about all the routers connected in specified areas on a network. Like Router-LSAs, Network-LSAs also only indicate link-state information and do not record network address information. Network-LSAs and Router-LSAs describe the link topology of areas together.

■ Inter-Area-Prefix-LSAs (Type 3)

Generated for an area by the ABRs in the area and used to describe the network information about reaching other areas. They replace type 3 summary-LSAs in OSPFv2. In contrast to the OSPFv2, destination network information is described with a prefix structure.

■ Inter-Area-Router-LSAs (Type 4)

Generated for an area by the ABRs in the area, used to describe the path information about reaching the ASBRs in other areas, and replacing type 4 summary-LSAs in the OSPFv2.

■ AS-external-LSAs (Type 5)

This type of LSAs are generated by ASBRs and used to describe the network information about reaching outside AS. Usually, the network information is generated through other route protocols. In contrast to the OSPFv2, destination network information is described with a prefix structure.

■ NSSA-LSA (Type 7)

Their function is the same to that of type 5 AS-external-LSAs. However, they are generated by ASBRs in the NSSA area.

■ Link-LSAs (Type 8)

In the OSPFv3, the newly added LSA type is generated by each device for each connected link and describes the local link address of the device in the current link and all set IPv6 address prefix information.

■ Intra-Area-Prefix-LSAs (Type 9)

In the OSPFv3, the newly added LSA type provides additional address information for Router-LSAs or Network-LSAs. Therefore, it has two effects:

1. Associate network-LSAs and record the prefix information of a transit network.

2. Associate router-LSAs and record the prefix information about routers in the current area, all Loopback interfaces, point-to-point links, point-to-multipoint links, virtual links and stub networks.

Other main changes of LSA association:

- LSA flooding scope change

In the OSPFv2, the LSA flooding includes flooding inside areas and flooding inside the AS.In the OSPFv3, local link flooding scopes occur. Type 8 Link-LSAs is the type that can flood only inside a local link flooding scope.

- Handling an unknown LSA type

This is an improvement made by the OSPFv3 based on the OSPFv2.

In the OSPFv2, when establishing an adjacency relation, you need to synchronize databases. If there is an irrecognizable LSA type in the database description packet, then you are unable to normally establish the adjacency relation. If there is an irrecognizable LSA type in a link-state updating packet, then the type of LSAs will be discarded.

In the OSPFv3, it is allowed to receive an unknown LSA type. By using the information recorded in the LSA header, we can determine how to handle received unrecognizable LSA type.

34.1.2 Interface Configuration

In the OSPFv3, the change based on interface configuration is as follows:

1. If an interface need participate in the running of OSPFv3, it must have been directly started under the interface configuration mode. In the OSPFv2, the interface is indirectly started via a **network** command under the OSPF route configuration mode.
2. If a configuration interface participates in the running of OSPFv3, then all addresses on the interface must participate in the running of the IPv6.In the OSPFv2, all addresses must be started via a **network** command.
3. In the environment where the OSPFv3 runs, when multiple OSPF entities can run on a same link, different devices connected by this link can select to participate in the running of an OSPF entity. The OSPFv2 does not support the function.

34.1.3 Router ID Configuration

Each device running the OSPFv3 process must be identified with a router ID in the IPv4 address format.

Unlike the OSPFv2, the OSPFv3 process will automatically acquire an IPv4 address as the router ID. After the device starts the OSPFv3 process, a user must use the router-id command to configure the router ID for the OSPFv3 process. Otherwise, the OSPFv3 process will not be able to start.

34.1.4 Authentication Mechanism Setting

The OSPFv2 itself supports two authentication modes: plain text authentication and key authentication based on MD5. The OSPFv3 itself does not provide any authentication. It will use the IPSec authentication mechanism. In the future, we will support the IPSec authentication mechanism.

34.2 OSPFv3 Basic Configuration

The OSPFv3 protocol of DGS-3610 series has the following features:

- Supports multi-instance OSPF;
- Supports network type setting;
- Supports virtual link;
- Supports passive interfaces;
- Supports an interface to select a participant OSPF entity;
- Supports sub intervals (Stub area);
- Supports route redistribution;
- Supports route information aggregation;
- Supports timer setting;

Subsequent support:

- Supports NSSA areas;
- Supports authentication. The OSPFv3 will use the IPSec authentication mechanism.

Default OSPFv3 configuration:

Router ID		**Undefined**
Interface Configuration	Interface type	Broadcast network
	Interface cost	Undefined
	hello packet sending interval	10 seconds
	Dead interval:	4 times of the hello packet interval.
	LSA sending delay	1 second
	LSA retransmit interval.	5 seconds
	Priority	1
	MTU check of database description packets	Enabled

Router ID		**Undefined**
Virtual Link	Virtual Link	Undefined
	hello packet sending interval	10 seconds
	Dead interval:	4 times of the hello packet interval.
	LSA sending delay	1 second
	LSA retransmit interval.	5 seconds
Area Configuration	Area	Undefined
	Default router cost of stub and NSSA areas	1
Route Information Convergence	Inter-area route Convergence	Off
	External route Convergence	Off
Management Distance	Intra-area route	110
	Inter-area route	110
	External route	110
Auto cost		Enable The default cost reference is 100 Mbps.
Changing LSAs Group Pacing		240 seconds
Timers of shortest path first (SPF)		The time between the receipt of the topology changes and SPF-holdtime :5 seconds The shortest interval between two calculating operations: 10 seconds
Filtering Routing information		Off
Route information filtering		Off
Passive interface		Off

To run the OSPFv3, follow these steps in the privileged mode:

Command	**Function**
configure terminal	Enter the global configuration mode.
ipv6 router ospf *process-id*	Start the OSPFv3 route process and enter the OSPFv3 configuration mode.
router-id *router-id*	Configure the Router ID used when this device runs the OSPFv3.
interface *interface-id*	Enter the interface configuration mode.
ipv6 ospf *process-tag* **area** *area-id* [**instance** *instance-id*]	Start the OSPFv3 on an interface. *instance-id:* Set an OSPFv3 entity number when an interface participates in the OSPFv3. The interfaces of different devices connected a same network, you can select to participate in different OSPFv3 entities.
copy running-config **startup-config**	Save the configuration.

Caution

In the interface configuration mode, first enable the interface to participate in OSPFv3 and then configure the ospfv3 process. After you configure the ospfv3 process, the interface will automatically participate in the corresponding process.

34.3 Configuring OSPFv3 Interface Parameters

In the interface configuration mode, you can modify parameter values of an interface to meet practical application needs.

To configure an OSPFv3 interface parameter, run the following commands in the interface configuration mode:

Command	**Function**
ipv6 ospf *process-id* **area** *area-id* [**instance-id** *instance-id*]	Configure the interface to participate in the OSPFv3 routing process.
ipv6 ospf network {**broadcast** | **non-broadcast** | **point-to-point** | **point-to-multipoint** [**non-broadcast**]} [**instance-id** *number*	Set the network type of an interface. The default is the broadcast network type.
ipv6 ospf cost *cost* [**instance-id** *number*	(Optional) Define the cost of an interface.
ipv6 ospf hello-interval *seconds* [**instance-id** *number*]	(Optional) Set the time interval to send the Hello packet on an interface. For all nodes in the whole network, the vale must be the same.
ipv6 ospf dead-interval *seconds* [**instance-id** *number*]	(Optional) Set the adjacency dead-interval on an interface. For all nodes in the whole network, the vale must be same.
ipv6 ospf transmit-delay *seconds* [**instance-id** *number*]	(Optional) Set link-state retransmit-interval.
ipv6 ospf retransmit-interval *seconds* [**instance-id** *number*]	(Optional) Set the LSA transmit delay on an interface.
ipv6 ospf priority *number* [**instance-id** *number*]	(Optional) Set the priority of an interface. The priority is used to select Designated Routers (DR) and Backup Designated Routers (BDR).

To disable the configuration, use the prefix command **no** before the command above.

⚠ **Caution**	You can modify the parameter setting of an interface based on actual needs. However, be sure that the settings of some parameters must be identical to those of neighbors. Otherwise, it is impossible to establish the adjacency relation. These parameters include the following: **instance, hello-interval and dead-interval.**

34.4 Configuring OSPFv3 Area Parameters

The OSPF protocol applies the concept of “hierarchical structure”, With the protocol, a network can be divided into a group of parts connected through a “backbone” in mutual independence. These parts are called Areas, and the backbone part is called Backbone Area indicated by the numerical value 0 (or 0.0.0.0).

By using this hierarchical structure, each device is allowed to keep the link state database in the area where it resides and the topology inside the area invisible to outside. In this way, the link state database of each device can be always in a reasonable size, route calculation time is not too much and the number of packets is not too big.

In the OSPF, the following types of special areas have been defined to meet actual needs:

- stub Area.

We call it a Stub Area.

If an area is at the end part of the whole network, we can design the area as a stub area.

If an area is designed as a stub area, it will not be able to learn about the AS external route information (type 5 LSAs). In practical application, external route information is very important in the linkstate database. Therefore, the devices inside a stub area will only learn little about route information, reducing the system resources required to run the OSPF protocol.

If a device inside a stub area need reach the outside AS, the task can be done in the following way: By use of the default route entries generated from the default route information published by Area Border Routers in the stub area.

- NSSA area (Not-So-Stubby Area)

We call it a Not-So-Stubby Area.

An NSSA is extended from a stub Area, and also blocks device flooding type 5 LSAs forward inside NSSA to reduce the consumption of device resources. However, unlike a stub area, it allows a certain amount of AS external route information to enter an NSSA in other ways, namely, to enter the NSSA by the way of type 7 LSAs.

At present, our company can not implement the NSSA area function of OSPFv3.

To configure OSPFv3 area parameters, perform the following command in the OSPFv3 configuration mode:

Command	**Function**
area *area-id* **stub** [**no-summary**]	Configure a stub area. no-summary: configure the area to a totally stub area, blocking inter-stub-area Area Border Routers to send type 3 information into the stub area.
area *area-id* **default-cost** *cost*	Configure the cost of the default route sent to a stub area or NSSA.

To disable the configuration, use the prefix command **no** before the command above.

Caution

After configured as the stub/nssa area, you can configure the default-cost parameter. If this area is changed as an ordinary area, the default-cost configuration will be deleted automatically.

34.4.1 Configuring OSPFv3 Virtual Connection

In the OSPF, all areas must be connected to the backbone area to ensure the communication with other areas.If some areas cannot be connected to the backbone area, they must connect the backbone area through virtual connections.

To establish a virtual connection, run the following command in the OSPFv3 configuration mode:

Command	**Function**
area *area-id* **virtual-link** *router-id* [**hello-interval** *seconds*] [**dead-interval** *seconds*] [**transmit-delay** *seconds*] [**retransmit-interval** *seconds*] [**instance** *instance-id*]	Configure a virtual link.

You can use the **no** mode of the command to invalidate configured contents.

Caution	1. It is not allowed to create a virtual connection in the stub area and NSSA. 2. A virtual connection can be taken as a special interface, so its configuration is the same to that of a normal interface. You must ensure that the configurations of **instance**, **hello-interval and dead-interval** are the same.

34.5 Configuring OSPFv3 Route Information Convergence

Each device in the network needs to maintain all the routing information of each network without route convergence. With convergence, some information can be integrated to alleviate the burden on the L3 device and network bandwidth. The larger the network scale is, the more important route convergence becomes.

DGS-3610 series support two route convergence configurations: inter-area convergence and external route convergence.

34.5.1 Configuring Inter-Area Convergence

The ABR of the OSPF needs to notify other areas of the route information in one area. If the route address of the area is continuous, the ABR can aggregate all the route information and notify other areas.

To configure inter-area convergence, run the following command in the OSPFv3 configuration mode:

Command	Function
area *area-id* **range** *ipv6-prefix/prefix-length* [**advertise** | **not-advertise**]	Configure inter-area convergence.

Use **no area** *area-id* **range** {*ipv6-prefix /prefix-length*} to delete configured inter-area convergence.

34.6 Configuring Bandwidth Reference Value of OSPFv3 Interface Measurement

The measurement of the OSPF protocol is a bandwidth value based on an interface. The cost value of the interface is calculated based on the bandwidth of the interface.

For example, if the bandwidth reference value of an interfaces is 100 Mbps and the bandwidth of network interfaces is 10Mbps, the automatically calculated interface cost value of the network interface is 100/10=10.

Currently, the default value of the network interface bandwidth is 100 Mbps.

To change the bandwidth reference value of the OSPFv3 interface, run the following command in the OSPFv3 configuration mode:

Command	Function
auto-cost [**reference-bandwidth** *ref-bw*]	Configure the bandwidth reference value for interface measurement.

⚠ Caution

You can run the **ipv6 ospf cost** *cost-value* command in the interface configuration mode to set the cost for a specified interface. A cost higher than that calculated based on measurement reference values takes precedence for selection.

34.7 Configuring OSPFv3 Timer

The OSPF protocol belongs to link-state protocols. When the link state changes, the OSPF process will trigger the SPF calculation. According to the designed conditions, you can execute the following command to configure the delay for SPF calculation and the time interval between two SPF calculations.

In the OSPFv3 configuration mode, run the following command:

Command	Function
timers spf *delay holdtime*	Configure the delay for SPF calculation and the time interval between two SPF calculations.

For the LSA information saved in the database, to synchronize the refresh, aging, check and calculation to use system resources more effectively, the OSPFv3 process refreshes the LSA information in the database periodically and the default interval is 4 seconds. In general, you need not adjust the parameter.

34.7.1 Configuring OSPFv3 Route Redistribution

Route information redistribution indicates redistributing the route information of one route protocol to another.

To configure the OSPFv3 route redistribution, run the following commands in the OSPFv3 configuration mode:

Command	**Function**
redistribute *protocol* [**metric** *metric-value*] [**metric-type** *type-value*] [**route-map** *map-tag*]	Redistribute routes from one routing protocol to another. You can reset the conditions for redistribution. Currently, the OSPFv3 supports static, connect, rip, bgp and isis route redistribution.
default-metric *number*	Configure the default measurement value of redistribution information.

You can use the **no redistribute** *protocol* mode to cancel route information redistribution.

Caution

At present, our company does not support the application of the tag parameter.

34.7.2 Configuring OSPFv3 Passive Interface

To prevent other Layer 3 devices in the network from learning about the route information of this device, you can set a network interface to a passive interface in the route protocol configuration mode

For the OSPFv3 protocol, if a network interface is configured to a passive network interface, this network interface will not receive/send any OSPF packet.

To configure an OSPFv3 passive interface, run the following command in the OSPFv3 configuration mode:

Command	**Function**
passive-interface {**default** | *interface-type* *interface-number* }	Configure a passive interface.

You can use the **no passive-interface** {*interface-id* **|** **default**} command to cancel the configuration of a passive interface.

34.8 OSPFv3 Debug and Monitoring

The OSPFv3 process supports plenty of debug commands and monitoring commands.

34.8.1 OSPFv3 Debug Command

In the privileged configuration mode, execute the following commands to start the debug commands of the OSPFv3 process:

Command	Function
debug ipv6 ospf event	Show the OSPFv3 event information.
debug ipv6 ospf ifsm	Show interface state machine events and changes.
debug ipv6 ospf lsa	Show the related OSPFv3 lsa information.
debug ipv6 ospf nfsm	Show neighbor state machine events and changes.
debug ipv6 ospf nsm	Show the ospf NSM module related information.
debug ipv6 ospf packet	Show the OSPFv3 packet information.
debug ipv6 ospf route	Show the OSPF routing calculation and addition information.

Use the above **undebug** commands to disable the above enabled **debug** commands.

⚠ **Caution**

The **debug** commands are provided for technicians.

Running a **debug** command can affect the performance of the system to a certain extent.

Therefore, after running the **debug** commands, be sure to use the **undebug** commands to disable the system performance.

34.8.2 OSPFv3 Monitoring Command

In the privileged configuration mode, execute the following commands to start the monitoring commands of the OSPFv3 process:

Command	Function
show ipv6 ospf	Show the information of the OSPFv3 process.
show ipv6 ospf interface [*interface-type interface-number*]	Show the interface information of the OSPFv3 process

Command	**Function**
show ipv6 ospf neighbor[*process-id*] [**detail**] [*neighbor-id* | *interface-type interface-number* [*neighbor-id*]]	Show the neighbor information of the OSPFv3 process.
show ipv6 ospf [*process-id*] **route**	Show the OSPFv3 route information.
show ipv6 ospf [*process-id*] **topology** [**area** *area-id*]	Show each area topology of the OSPFv3.
show ipv6 ospf [*process-id*] **virtual-links**	Show the virtual link information of the OSPFv3 process.

35 IP Multicast Routing Configuration

35.1 Overview

This chapter describes how to configure multicast routing protocols. For a complete description of the IP multicast routing commands, please refer to other chapters *IP Multicast Routing Commands*.

Traditional IP transmission only allows packet transmission from one host to a single host (unicast communication) or to all hosts (broadcast communication). IP multicast provides a third scheme, allowing packet transmission from one host to a subset of all hosts. These hosts are known as group members.

The destination address sent to the group member is a Class D IP address which can be in the range from 224.0.0.0 to 239.255.255.255. Transmission of multicast packets is similar to UDP, which is a best-effort service. It does not provide reliable transmission and error control like TCP.

The multicast application consists of senders and receivers. The sender, regardless of whether it is a member of a group, can send multicast packets. However, it’s required to join to certain group in advance for the receiver to receive the packets of this group.

Membership in a multicast group is dynamic; hosts can join and leave at any time. There is no restriction on the location or number of members in a multicast group. If necessary, a host can be a member of more than one multicast group at a time. Therefore, the active state of groups and number of group members can vary with the time.

Routers maintain routing tables to forward multicast packets through a multicast routing protocol (such as PIM-DM and PIM-SM) and learn the status of the members within a group on their directly attached subnets through the IGMP. A host can join in a certain IGMP group by sending IGMP Report packet.

IP multicast is ideal for “one-to-multiple” multimedia applications.

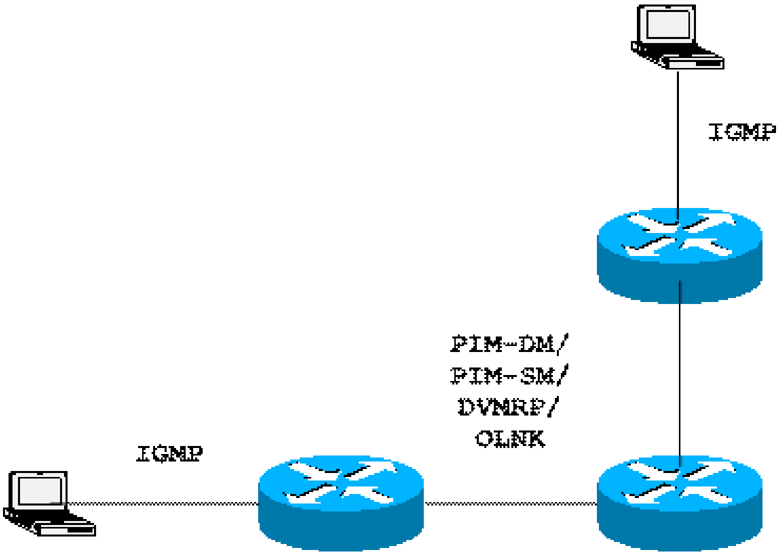
35.1.1 IP Multicast Routing Implementation

Multicast routing is composed of the following protocols in router software:

- IGMP is used between the hosts and routers in a LAN to track relations between group members..
- PIM-DM is a dynamic multicast routing protocol, which is used between routers for multicast forwarding based on multicast routing table.
- PIM-SMis a multicast routing protocol in the sparse mode.

The following figure shows multicast protocols applied in the IP multicast environment.

Figure 35-1 IP Multicast Routing Protocols within the IP Multicast Environment



35.1.2 IGMP Overview

To implement IP multicast, the multicast host, router, and multi-layer switch must support IGMP. This protocol is used by the host to notify routers or multi-layer switches of the multicast membership of the network they connect, to determine the forwarding of the multicast traffic.

Through the information obtained from the IGMP, the router or multi-layer switch can maintain one multicast member list, which is based on each interface. The multicast member list is activated only when at least one host of an interface is a member of the group. This switch supports IGMP v1-v3.

35.1.2.1 IGMPV1

There are only two packet types defined in IGMP Version 1: **Membership query** and **Membership report**.

A host sends a report packet to join a group, and the router sends the query packet periodically to ensure that a group has at least one host. When a group contains no host, the router will delete that group.

35.1.2.2 IGMPV2

In Version 2, there are only four packet types:

- **Membership query**
- **Version 1 membership report**
- **Version 2 membership report**
- **Leave group**

The process is basically the same as that of version 1, except that the leave mechanism of the host has been improved. For V2, the host can send a leave packet to notify the router, which then sends a query to verify the existence of the host, improving the efficiency of joining and leaving.

In addition, version 2 handles multiple routes of multiple access networks. In the multicast network that runs IGMP, there is a dedicated query multicast router or L3 multicast switch, which is responsible for sending IGMP query packets. This dedicated router or L3 switch is chosen through an election process. At the beginning, all the routers are queriers. When a router receives the query from a router with lower IP address for membership, it changes from the receiver to the non-querier. Therefore, ultimately only one router is in the query status. This router is the one with the lowest IP address in all multicast routers.

When the querier router fails, the IGMPv2 also handles the fault. The non-query router maintains the interval timers of other queriers. Each time when a router receives a membership query packet, it resets the timer. If the timer expires, the router starts to send query packets, and querier router election starts again.

The querier router must send membership query requests periodically to ensure that other routers on the network know that the querier router still works. For this purpose, the querier router maintains one query interval timer. When the membership query packet is sent, this timer will be reset. When the interval timer is zero or not necessary, the querier router sends another membership query.

When the device appears for the first time, that is, a new device is added, it sends a series of general query packets to check which multicast groups shall be forwarded on a specific interface. The number of common query packets sent by a router is based on the start query count configured of the router. The querying interval between the initial general query packets is defined through the startup query interval.

When a querier router receives a leave packet, it must send a particular group membership query to see whether the host is the last that leaves the group. Before the router stops forwarding packets to the group, it sends a series of such packets, the number of which is equal to the last member query number. The router sends multiple particular membership queries to ensure that there is no member in the group. Such a query is sent every other the seconds of the last-member query interval to separate the queries. When no response is received, the router stops forwarding multicast packets to the group at the particular interface.

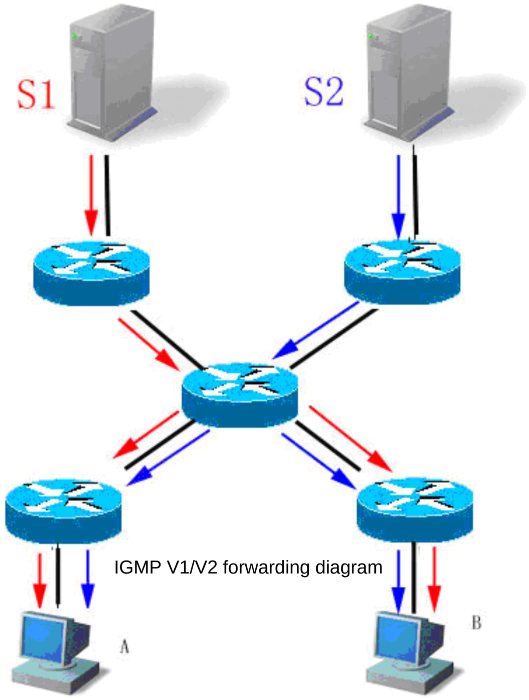
35.1.2.3 IGMPV3

In the applications of the IGMPV1 and V2, there are the following defects:

- Lack of effective measures to control multicast sources
- Difficult to establish the multicast path due to the unknown location of the multicast source
- Difficult to find a unique multicast address, possibly multicast groups are using the same multicast address.

On the basis of the IGMPV1/V2, the IGMPV3 provides an additional source filtering multicast function. In the IGMP V1/V2, the host determines to join a group and receive the multicast traffic to the group address from any source only based on the group address. On the other hand, the host running the IGMP V3 notifies this host the desired multicast group to join, and also the addresses of the multicast sources to receive. The host can indicate that it wants to receive multicast traffic from which sources through a list or an exclusion list. At the same time, another benefit of the IGMP v3 is that it saves bandwidth to avoid unnecessary, invalid multicast data traffics from occupying network bandwidth. It is particularly useful in the case where multiple multicast sources share one multicast address. The IGMPv1 and IGMPv2 can also implement “source address filters” in some sense, which, is performed on the reception end of the multicast traffic. As shown in the following diagram, there are two multicast sources (S1 and S2), which send the data traffic of the same multicast address (G). The multicast flow of S1 and S2 will be sent to all hosts that are receiving from G, If host A only wants to receive that of S1, filtering on the terminal by using the related client software has to be used to keep out the interference of S2 dataflow.

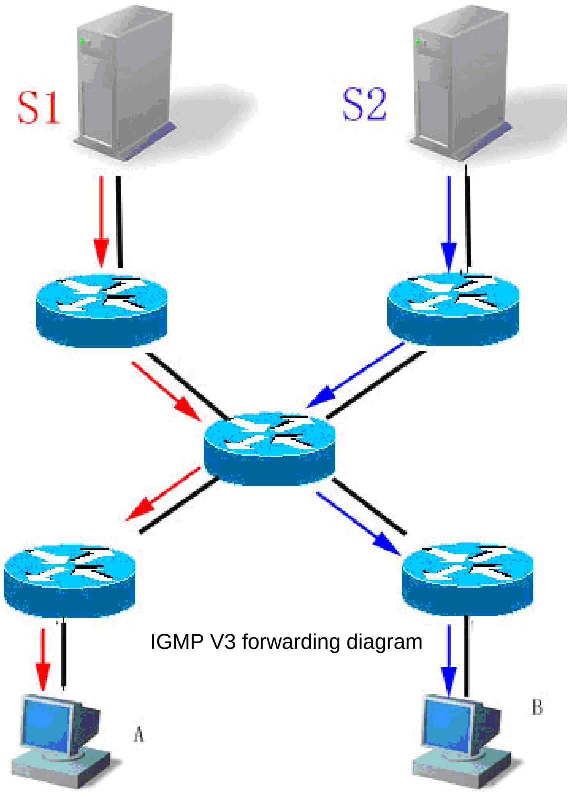
Figure 35-2



IGMP V1/V2 forwarding diagram

If the equipment in the network supports IGMP v3, host A wants to receive the traffic from S1 only, it can send the IGMPv3 packet of join G include S1. If host B wants to receive the traffic from S2 only, it can send the IGMPv3 packet of join G include S2. Therefore, the traffic is forwarded as shown in the following diagram, saving some bandwidth.

Figure 35-3



IGMP V3 forwarding diagram

In contrast to Version 2, Version 3 defines the following two packet types:

- **Membership Query**
- **Version 3 Membership Report**

There are three types of **Membership Query**:

- General Query Used to query all multicast members under an interface:
- Group-Specific Query Used to query the members of the specified group under an interface
- Group-and-Source-Specific Query Added in IGMPv3, used to check whether a member under an interface needs to receive multicast traffic of a group sent from a source in the specified source list

Different from the Membership Report in IGMP Version2, the Membership Report in the IGMP Version3 always has the destination address of 224.0.0.22. The Membership Report packets in IGMP Version3 include the information of multiple groups.

The IGMP Version3 also recognizes the Membership Report of both Versions 1 and 2 and the Leave Group packet of Version 2.

The process of IGMP Version3 is similar to that of the IGMP Version2. IGMP Version3 is downward compatible with IGMP Version1 and IGMP Version2.

35.1.3 PIM-DM Overview

The protocol independent multicast (PIM) is designed by the IDMR work group. As indicated by its name, the PIM does not rely on a certain unicast routing protocol. Instead, it can perform the RPF check by a unicast routing table containing various unicast routing protocols, rather than forward the multicast packets by maintaining a separate multicast routing table. Because the PIM need not to send or receive the multicast routing updates, its overhead is much lower than other multicast protocols. The PIM design is intended to support both the SPT and shared tree at the same time and to enable the flexible switching between them on the Internet. Therefore, the PIM takes the advantages of the SPT and shared tree and improves the multicast efficiency. The PIM has two modes: Dense-Mode and Sparse-Mode.

PIM-DM is the abbreviation of Protocol Independent Multicast Dense Mode. By default, when the multicast source starts sending multicast data, all the network nodes in the domain need to receive the data. Therefore, the PIM-DM maintains the multicast distribution tree through broadcast-prune to forward the multicast packets. PIM is independent of the specific unicast routing protocol, using the existing unicast routing table to implement RPF (Reverse Path Forwarding) check. RPF is the basis of multicast forwarding in the multicast routing protocol. It works in the following way: when the multicast information passes the source tree, the multicast router checks the multicast source address of the multicast packets to check whether the interfaces passed by the multicast packets are on the source branch. If yes, the RPF check is successful, and the multicast packets will be forwarded. Otherwise, the RPF check fails, and the multicast packets will be discarded.

When the multicast source starts to send data, the routers on the route forward the multicast packets to all PIM activated interfaces except the source RPF interface (that is, the interface to the multicast source on the shortest path). Thus all network nodes will receive these multicast packets in PIM-DM area. To implement multicast forwarding, the routers on the path need to create the appropriate multicast route entry (sending source, destination group) (S,G) for group G and source S to create the multicast distribution tree. (S,G) contains multicast source address, multicast group address, incoming interface, outgoing interface list, timer and identifier and so on. Once this tree is constructed, it will broadcast all the multicast traffic.

If there are no group members in a certain area, PIM-DM will send a pruning message to prune the forwarding interfaces which are connected to this area and create pruning state. Pruning state is corresponding to timeout timer. When timer expires, Pruning is transmitted into forwarding, which enables multicast data to flow down along these branches. Besides, pruning state contains multicast source and multicast group information of multicast. When multicast group members appear in pruning area, to reduce reaction period, PIM-DM will be active to send a prune message to upstream without waiting for timeout of upstream pruning state so as to enable pruning to forwarding state.

As long as Source S can still send messages to Group G, the first hop switch will periodically send (S,G) a state refresh message to initial broadcast tree to finish the refreshing. With PIM-DM state refresh mechanism, you can refresh the state of downstream so that pruning of broadcast tree branches will not time out.

Except for DR election in multi-path access network, PIM-DM also introduces the following mechanism: use assertion to select a single forwarder in case that multicast packets are forwarded repeatedly to the same segment; use join/prune suppression to reduce redundant join/prune messages; use pruning deny to deny these illegal pruning.

In PIM-DM domain, PIM-DM switches periodically send Hello message to find adjacent PIM switches and make judgment of leaf network and leaf routers and is also responsible for DR election in multi-path access network.

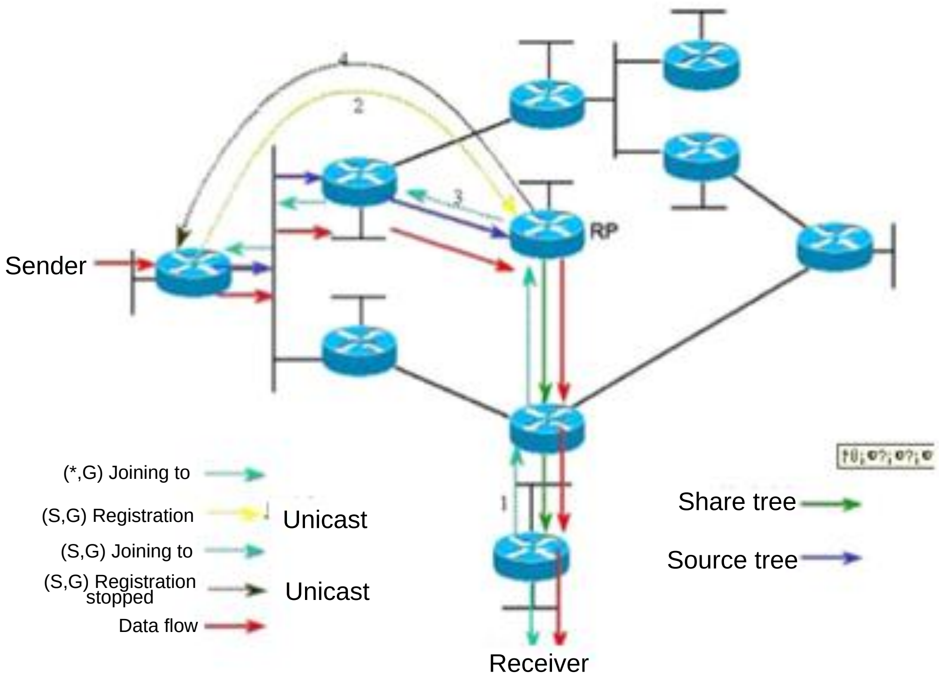
To be suitable for IGMP v1, PIM-DM is responsible for DR selection. Choose the highest Priority to be DR when all the PIM neighbors support DR Priority on the interface. If the priority is identical, choose the switch with the largest interface IP to be DR. If many switches do not announce their priorities in hello messages, switches with the highest interface IP value is selected to be DR.

PIM-DM v2 of our switches supports neighbor filtering list, CIDR, VLSM and IGMP v1, v2, v3.

35.2 PIM-SM Overview

The PIM-SM (Protocol Independent Multicast Sparse Mode) is a protocol independent multicast sparse mode. In the PIM-SM domain, the device which runs the PIM-SM protocol periodically sends the Hello messages, to detect the neighboring PIM-SM device, and be responsible for dispatching the selection of the device DR in the multiple access networks. Where, the DR is responsible for sending the join/prune message in the root node of the multicast distribution tree direction for the direct connection group member, or sending the data of the direct connection multicast source to the multicast distribution tree.

Figure 35-4 Join Mechanism of PIM-SM Explicitly



The PIM-SM will forward the multicast data packet by establishing the multicast distribution tree. The multicast distribution tree is divided into the Shared Tree, which takes the RP of the group G as the root, and the Shortest Path Tree, which takes the multicast source as the root. The PIM-SM will establish and maintain the multicast distribution tree by the join/prune mechanism explicitly. As shown in the figure above, when DR receives one Join from the receiving terminal, it will send one (*.G) join message to the RP direction of the group G in hop-by-hop multicast way, to join the share tree. When the source host sends the multicast data to the group, the source data is encapsulated into the registration message, and is sent to the RP in the unicast way by its DR, and then RP will forward the de-encapsulated data packet of the source to various group members. RP will send (S, G) the join information to the hop one equipment to the source direction, to add the shortest path tree of this source, the data packet of this source will be sent to the RP along its shortest path tree without the encapsulation. When the first multicast data reaches along this tree, RP will send the registration stop message to the DR of the source, to make DR stop registering the encapsulation process. Then, the multicast data of this source will not register the encapsulation, but be sent to the RP along the shortest path tree of the source, and then forwarded to various group members along the share tree by RP. If it doesn't require the multicast data, DR will multicast prune messages to the RP of the group G hop-by-hop, so as to prune the share tree.

The PIM-SM also concerns with the selection mechanism of the root node RP. One or more Candidate-BSRs are configured in the PIM-SM domain. It will apply a certain rule to select the BSR. The PIM-SM domain also configures the Candidate-RP, to send the information packet of the address and the service multicast group in the unicast way. The BSR will generate the BSR information which includes a system candidate RP and corresponding group address. The BSR message is sent hop-by-hop within the whole domain. The device receives and saves these BSR message. If the DR receives the member relationship report of some group from the direct connection host and there is no routing item of this group, the DR will use one Hash algorithm to map the group address to one candidate RP that can serve for this group. Then, DR sends the Join/Prune message to the RP direction hop-by-hop in the multicast way. If the DR receives the multicast data packet from the direct connection host and there is no the routing item of this group, the DR will use one Hash algorithm to map the group address to one candidate RP that can serve for this group. Then the DR encapsulates the multicast data into the registration message and sends it to the RP in the unicast way.

The PIM-SM and the broadcast/prune model-based PIM-DM differ in the aspects that the PIM-SM is based on the explicit join model, that is, the receiver sends the join message to the RP, but the router only forwards the packets of that multicast group on the output interface that has joined a multicast group. The PIM-SM uses the shared tree to forward multicast packets. Each group provides one Rendezvous Point (RP), and the multicast source sends the data to the RP along the shortest path, and then the RP sends the data to various terminals along the shortest path. This is similar to the CBT, but the PIM-SM does not use the concept of core. One major advantage of the PIM-SM is that it not only receives the multicast information through the shared tree, but also provides the mechanism for conversion from the shared tree to the SPT. Such conversion reduces the network delay and the possible congestion on the RP, but it consumes enormous router resources, so it is suitable for the case that there are only a few multicast data sources and network groups.

The PIM-SM uses the shared tree and SPT to distribute multicast frames. Suppose that other devices do not want to receive these multicasts unless otherwise stated definitely. When a host joins a group, the equipment connected to the host must notify the root by using the PIM join message, namely, the RP. This join message is transferred one after another through the router, creating a shared tree structure. Therefore, the RP records the transfer path and also the registration information from the first-hop router (DR) of the multicast source, and uses these two types of information to improve the shared tree. The branch/leaf information is updated through periodical query messages. In using the shared tree, the multicast source first sends multicast packets to the RP in order to ensure that all the receivers can receive them. *.G represents a tree, * represents all sources, and G represents a particular multicast address. The prune information is also used in the shared tree, that is, a branch/leaf does not want to receive the multicast frames.

The PIMv2 BSR is a method for distributing group-to-RP messages to all devices. The PIMv2 BSR eliminates the demand to set the RP for each device. The BSR uses the hop-by-hop to broadcast BSR messages and distribute the mapping information. At first, the BSR is selected from the device. The election method is similar to the election of the root-bridge on the L2 bridge, by using a priority value. Each BSR checks the BSR messages and only forwards those with the priority higher than or equal to its own (higher IP address). The selected BSR sends the BSR messages to the all-PIM-routers multicast group (224.0.0.13), where TTL is 1. After the neighbor PIMv2 router receives the messages, it multicasts them, and sets the TTL to 1. In this way, the GSR message is received by all devices hop-by-hop. Since the messages contain the IP address of the BSR, the candidate BSR can know which router is the current RP based on this message. The candidate RPs send candidate RP advertisement to announce the addresses in which they can become the RP, and the BSR stores them in its local candidate RP cache. The BSP notifies its local candidate RPs to all PIM routers periodically. These messages reach various devices hop-by-hop in the same way.

35.3 Basic Configuration of the Multicast Routing

Basic multicast configuration includes:

- Enabling multicast routing forwarding (required)
- Enabling multicast routing protocol (required)
- Enabling IGMP
- Configuring TTL threshold (optional)

35.4 Enabling Multicast Routing Forwarding

Enabling multicast routing to allow multicast packet forwarding conducted by the router software.

In global configuration mode, enter the following commands to enable the multicast packet forwarding:

Command	Function
ip multicast-routing	Enabling multicast routing forwarding

Caution

If this command is configured, the VLAN interface, L2AP member interface, and L3AP member interface will change. You need to execute **NO** of the command before restarting multicast routing forwarding.

35.5 Enabling IP Multicast Routing Protocol

So far our products support PIM-DM multicast routing protocol.

Enable PIM-DM at the interface to activate multicast with dense modeaccording to the following steps:

Command	Purpose
ip pim dense-mode	Enter the interface that needs to run PIM-DM and enable PIM-DM multicast routing process in the interface configuration mode.

It demonstrates how to configure PIM-DM on FastEthernet0/1 in the following example.

```
ip multicast-routing
interface FastEthernet 0/1
ip address 172.16.8.1 255.255.255.0
ip pim dense-mode
```

Note

When the multicast routing protocol is enabled on the interface, the IGMP function is activated at the same time.

35.5.1 Enabling IGMP

When multicast routing protocol is enabled, IGMP is enabled as well

Note

Hosts and routers of IGMP are activated simultaneously.

35.6 Advanced Multicast Routing Configuration

Advanced multicast routing configuration includes:

- Configuring multicast routing characteristics (optional)
- Configuring IGMP task list(optional)
- Configuring PIM-DM task list(optional)
- Configuring DVMRP interoperability task list(optional)

35.6.1 Configuring Multicast Routing Characteristics

35.6.1.1 Configuring TTL Threshold

Use **ip multicast ttl-threshold** to configure TTL threshold of multicast packet which is allowed to transmit through the interface, and use **no ip multicast ttl-threshold** to deploy the default value. The default value is 1.

Command	Purpose
ip multicast ttl-threshold *ttl-value*	Configure TTL threshold at the interface.

35.6.1.2 Configuring IP Multicast Boundary

Execute **ip multicast boundary** to configure multicast boundary of an interface and execute **no ip multicast boundary** to disable the configured boundary. The second configuration command will cover the first one.

Execute the following command in the interface configuration mode:

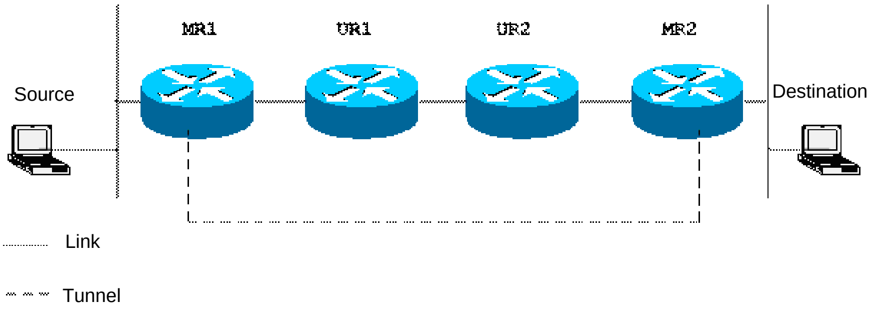
Command	Purpose
ip multicast boundary *access-list*	Configuring IP Multicast Boundary

35.6.1.3 Configuring IP Multicast Static Route

Multicast static route allows difference between multicast forwarding path and unicast path. RPF inspection will be processed in case of multicast packet forwarding. The actual receiving interface is the interface expected to receive packets (the interface is the next hop of unicast reaching the sender). The inspection is reasonable if the topologies of unicast and multicast are the same. But in some cases, unicast path is expected to differ from that of multicast.

The most common cases adopt tunnel technology. GRE tunnel is configured between two switches when multicast protocol is not supported by the switches on one path. Each unicast switch (UR) only supports the unicast packets while each multicast switch (MR) supports multicast packets in the figure below. Source sends multicast packets to destination by MR1 and MR2. MR2 forwards multicast packets only when they are received from tunnel. If so, unicast packets will also pass the tunnel when forwarded from destination to source. As we know, it is slower to forward packets through tunnel than direct sending.

Figure 35-5 Schematic Diagram of Configuring Multicast Static Routes



Through multicast static route configuration, a router can implement RPF inspection according to the configured information instead of unicast routing list. Therefore, multicast packets use tunnel while unicast packets do not. Multicast static routes only exist locally. They will not declare outgoing or implement routing forwarding.

In the global configuration mode, execute the following command to configure multicast static route.

Command	Purpose
ip mroute *source-address mask* {*interface-type interface-number*} [**distance**]	Configure multicast static route

The following example shows boundary configuration on FastEthernet 5/2.

```
interface FastEthernet 5/2
ip multicast boundary acl
ip access-list standard acl
permit 192.168.20.97 255.255.255.0
```

35.6.1.4 Monitoring and Maintenance of Multicast Routing

You can remove the content of a particular cache or a routing table if they are suspected to be invalid. Execute the following commands in the privileged configuration mode:

Command	Purpose
clear ip mroute [* | group-address | source-address]	Delete entries from multicast routing table.

You can determine the resource utilization and solve network problems by displaying IP multicast route table, associated cache and database. Execute the following command in the administration mode:

Command	Purpose
show ip rpf {source-address}	Show RPF information.

35.6.2 Configuring IGMP

35.6.2.1 Configuring IGMP Version

Execute the following command in the interface configuration mode to configure the IGMP version.

Command	Purpose
ip igmp version{*1* | *2* | *3*}	Configure the running IGMP version.

Use **no ip igmp version** to set the current IGMP version as the default value Version2.

35.6.2.2 Adding Membership Information on Routers Statically

Sometimes the subnet connected to an interface has no host that can send IGMP member reports, but you still want the switch to forward the multicast packets of one group to the subnet. In this case, you can configure the interface as a static connection multicast group, to forward the multicast frames to the interface.

In the interface mode, execute the following commands for the configuration:

Command	Function
DGS-3610# **config termina**l	Enter the global configuration mode.
DGS-3610(config)# **interface** *interface-id*	Enter the interface configuration mode.
DGS-3610(config-if)# **ip igmp static-group** *group-address*	Add the static group on the configuration interface.
DGS-3610(config-if) # **exit**	Enter the privileged mode.

You can execute the **no ip igmp static-group** *group-address* command to cancel the configured static connection group.

35.6.2.3 Configuringjoin-group

This command configures the switch related interface as with the host behavior and needs to join corresponding multicast group. In this way, the sub switch can learn corresponding group packet actively. If required, it will use this configuration when one group member is added to the interface. Use the no form of this command to cancel the join of the switch in this group.

Command	Function
DGS-3610# **config terminal**	Enter the global configuration mode.
DGS-3610(config)# **interface** *interface-id*	Enter the interface configuration mode.
DGS-3610(config-if)# **ip igmp join-group** *group-address*	Configure to join the host group on the interface.
DGS-3610(config-if) # **exit**	Enter the privilege mode.

Execute the **no ip igmp join-group** group-address command to leave corresponding multicast group.

The following command shows how to add the gigabitethernet0/1 interface to the multicast group 224.1.1.1:

```
interface gigabitethernet 0/1
ip igmp join-group 224.1.1.1
```

35.6.3 Configuring Query Count of the Last Member

When the packet of leaving group is received, the querier sends the specific membership query to verify whether there is any member in the group. By default the period is 2.

Run the following commands for configuration in the interface mode:

Command	Function
ip igmp last-member-query-count *lmqc*	Configure query count of the last member The default range is 1 - 7.

Execute the command **no ip igmp last-member-query-count** to restore the default configuration.

35.6.4 Configuring Query Interval of the Last Member

When the packet of leaving group is received, the querier device sends the specific membership query to verify whether there is any member in the group. If no report is received during the last-member query interval, the device will regard the host that is leaving the group is the last member of that group, and then delete the information of the group. By default the period is 1 ms.

Run the following commands for configuration in the interface mode:

Command	Function
ip igmp last-member-query-interval *lmqi*	Configure the query interval of the last member Interval range: <1-255>. Unit:is 0.1s

Execute the command **no ip igmp last-member-query-interval** to restore the default configuration.

35.6.5 Configuring Query Interval of the General Member

Whenever a group membership query interval passes, the **querier** sends the membership query packet on regular basis to verify the current membership. The destination address to send the group membership query packet is the all-hosts multicast address 224.0.0.1, and TTL is 1. By default that period is 125 s.

Run the following commands in the interface mode:

Command	Function
ip igmp last-member-query-count *seconds*	Configure the query times within the range: 1-18000. Unit: s

Execute the command **no ip igmp query-interval** to restore the default configuration.

35.6.6 Configuring the Maximum Response Interval

The membership query packet sent by the **querier** requires the maximum response interval. Interval decreasing can make the device know the change of the members quickly, which will result in increase of the member reports diffusing in the network. The network administrator can consider a tradeoff between the two factors and then decide a proper value for the period, 10 seconds by default. Another consideration in configuring the interval is that it shall be shorter than the query interval.

Run the following commands for configuration in the privileged mode:

Command	Function
ip igmp query-max-response-time *seconds*	Configure the response interval. The range is 10-250, in 0.1 s.

Execute the command **no ip igmp query-max-response-time** to restore the default configuration.

35.6.7 Configuring the Timeout Interval of the Other Queriers

Configuring the timeout interval of the other querier in the interface layer , it can control the time interval of the non-querier. Note that the non-querier status can be updated by the packet of other queriers.

Run the following commands in the interface mode:

Command	Function
ip igmp query-timeout *seconds*	Configure the query time within the range of 60 – 300, The unit is s.

Execute the command **no ip igmp query-timeout** to restore the default configuration.

35.6.8 Configuring the IGMP Group Member Quantity Limit

This command in the global configuration mode is used to limit the IGMP group record quantity of the IGMP. The packets of the members will not be IGMP-buffered or forwarded when exceeding that limit.

This command can be used to configure every interface, while can be configured independently for specific interfaces or globally. The packets of the member will be ignored when exceeding the limit configured for the interface or globally. Run the following commands in the interface mode:

Command	Function
DGS-3610(config) # **ip igmp limt** *number*	Configure the IGMP Status quantity limit globally. Range: 1-65536
DGS-3610(config-if) # **ip igmp limit** *number*	Configure the IGMP status quantity limit on the interface. The range is 1-65536, 1024 by default.

35.6.8.1 Configuring the Member Information of Filtering Group

Namely, configure the access control of the multicast group. By default, the interface on one interface can join any multicast group. When the administrator wants to control the range of the multicast groups that a host can join, he can enable this feature. By configuring a standard IP access list, you can set the range of the allowed/prohibited range of multicast group addresses, and apply them to a particular interface.
In the interface mode, execute the following commands for the configuration:

Command	Function
DGS-3610# **config terminal**	Enter the global configuration mode.
DGS-3610(config) # **access-list** *access-list-name* **permi**t *A.B.C.D 0.0.0.0*	Define an access control list.
DGS-3610(config)# **interface** *interface-id*	Enter the interface configuration mode.
DGS-3610(config-if) # **ip igmp access-group** *access-list-name*	Configure the access control list of the group address as the multicast group within the address range for access-list-name can enter into this interface.
DGS-3610(config-if) # **no ip igmp access-group**	Delete the access control list, and allow all groups to enter.

You can execute the **no ip igmp access-group** command to restore the access control to its default, that is, not restricting any group.

The following command shows how to restrict the hosts at the Gigabitethernet 0/1 interface so that they can only join the group of 225.2.2.2:

```
access-list 1 permit 225.2.2.2 0.0.0.0
interface ethernet 0
ip igmp access-group 1
```

Note

When ACL is located from 1 to 99, IGMP v1/v2/v3 will only match group (g).

When ACL is 100-199, IGMP v1 / v2 will match (source IP of 0.0.0.0, group IP).

When ACL is located in 100-199, IGMP v3 will match (source ip, group ip), For source ip, indicates the source ip of IGMP v3 report packet. If the corresponding source IP does not exist, such as exclude{ }/is_ exclude{ }/to_ exclude{ }/include{ }/is_include{}/to_include{ }, the source ip is 0.0.0.0.

35.6.9 Configuring Immediate Group Leaving

In the IGMP version2, this command can be used to reduce the delay in leaving group. When the host issues this packet, it shall leave immediately without the need for the **querier** to send the specific group query.This command is suitable only when the interface has one receiving host.

Command	**Function**
DGS-3610# **config terminal**	Enter the global configuration mode.
DGS-3610(config)# **interface** *interface-id*	Enter the interface configuration mode.
DGS-3610(config-if)# **ip igmp immediate-leave group-list** *access-list-name*	Configure the immediate-leave from the group with list *access-list-name*.
DGS-3610(config-if) # **exit**	Enter the privileged mode.
DGS-3610(config)# **access-list** *access-list-name* **permit** A.B.C.D 0.0.0.0	Configure the address range of the member group list.

The command **no ip igmp access-group** restores the access control to default without limit for any group.

35.6.10 Configuring IGMP PROXY - SERVER

This command is used to enable the service function of all downlink mroute-proxy interfaces. If this command is configured on the interface, this interface will become the uplink interface of corresponding mroute-proxy, associate with the related downlink interface, and maintain the group information notified b y the downlink interface.

At present, the maximum configurable quantity of this command is limited. It can configure up to 32. Up to 255 downlink interfaces can be associated with each proxy-server. After the interface receives the query packet, the proxy-server interface will carry out corresponding response according to the member information maintained by itself. The proxy-server interface will judge the member information maintained itself is connected from the interface with mroute-proxy. Hence, the configuration of proxy-server is equal that this interface only executes the host behavior, but not executes the router behavior. Execute the following commands in the interface mode:

Command	**Function**
DGS-3610(config-if) # **ip igmp proxy-service**	Configure it as the proxy-server status on the interface.

35.6.11 Configuring IGMP MROUTE - PROXY

After this command is configured, the interface can forward packets to corresponding uplink interface.

After corresponding uplink interface is configured as the proxy-server interface, this interface can forward various igmp protocol packets sent by its members. Execute the following commands in the interface mode:

Command	**Function**
DGS-3610(config-if)# i**p igmp mroute-proxy**	Configure it as the mroute-proxy status on the interface.

35.6.12 Enabling IGMP SSM-MAP

When this command is configured, the dynamic learned group information will be added into the related source record message forcibly. This command is usually used together with the **ip igmp ssm-map static** command.

Execute the following command in the interface mode:

Command	**Function**
DGS-3610(config)# **ip igmp ssm-map enable**	Enable the ssm-map function globally.

35.6.13 Configuring IGMP SSM-MAP STATIC

This command is used together with the **ip igmp ssm-map enable** command. After this command is configured, the received message under v3 will be mapped into the corresponding source record.

Execute the following command in the interface mode:

Command	Function
DGS-3610(config)# **ip igmp ssm-map static** *11 192.168.2.2*	All groups that comply with acl 11 will be mapped into the source address 192.168.2.2.

35.6.14 ClearingUp Dynamic Group Membership in IGMP Cache from Response Message

To clear up dynamic group member information acquired from response message which is stored in IGMP cache, execute the following command in the privilege mode:

Command	Function
DGS-3610# **clear ip igmp group**	Clear up the dynamic group membership in the IGMP cache from responding message. No parameter indicates clearing up all information of the igmp group.

35.6.15 Clearing Up All Information on Specified Interface in IGMP Cache

To clear up all information of specified interface in the IGMP cache, execute the following command in the privilege mode:

Command	Function
DGS-3610# **clear ip igmp interface** *interface-type*	Clear up the message on the interface in the IGMP cache.

35.6.16 Displaying the Status of IGMP Group Member in Directly-connected Subnet

Execute the following command in privileged mode to display the status of IGMP group member in directly-connected subnet:

Command	Function
DGS-3610# **show ip igmp groups**	Show the status of IGMP group member in directly-connected subnet.
DGS-3610# **show ip igmp groups detail**	Show the details of all members in the directly-connected subnets.
DGS-3610# **show ip igmp groups** *A.B.C.D*	Display the status of specified group member in directly-connected subnet.

Command	Function
DGS-3610# **show ip igmp groups** *A.B.C.D* **Detail**	Show the details of the specified member in the directly-connected subnets.
DGS-3610# **show ip igmp interface** *interface-type*	Show the information of the specified interface in the directly-connected subnets.
DGS-3610# **show ip igmp groups** *interface-type* **detail**	Show the details of the specified interface in the directly-connected subnets.
DGS-3610# **show ip igmp groups** *interface-type A.B.C.D*	Show the information of the specific group of the specified interface in the directly-connected subnets.
DGS-3610# **show ip igmp groups** *interface-type A.B.C.D* **detail**	Show the details of the specific group of the specified interface in the directly-connected subnets.

Switch# show ip igmp groups

```
Group Address    Interface            Uptime    Expires   Last Reporter
239.255.255.250  Vlan1                00:00:40  00:02:19  192.168.65.43
224.0.1.40       FastEthernet0/1      00:01:24  00:02:17  202.113.2.2
230.0.0.2        FastEthernet0/1      04:02:10  00:02:25  202.113.2.2
230.0.0.3        FastEthernet0/1      04:02:10  00:02:17  202.113.2.2
230.0.0.0        Vlan2               04:02:09  00:02:21  202.113.1.1
```

35.6.17 Showing the configuration information of the IGMP interface

To show the configurations of the IGMP interface, run the following command in the user mode:

Command	Function
DGS-3610# **show ip igmp interface** [*interface-type interface-number*]	Show the configuration information of the IGMP interface.
DGS-3610# **show ip igmp interface**	Show the configuration information of all the IGMP interfaces.

```
Switch# show ip igmp interface
FastEthernet 0/0
mtu is 1500
IP interface state is: DOWN
Internet address is 192.11.11.11 mask is 255.255.255.0
igmp config general query interval is 18000
igmp config robustness is 2
igmp current general query interval is 18000
igmp group member interval is 36010
igmp host robustness is 2
igmp join group unsolicited report counter is 2
igmp join group unsolicited report interval is 1
igmp last member query counter is 7
igmp last member query interval is 255  1/10seconds
igmp has 5 different config in this interface
igmp nif learnt mem num is 0
igmp nif limit num is 1024
igmp other querier interval is 255
igmp querier ip is 192.11.11.11
igmp query response interval is 100 1/10seconds
igmp router robustness is 2
igmp special query num is 0
igmp version is 3
IGMP is enabled on interface
```

35.6.18 Show the Configuration Information of IGMP SSM-MAP

To show the configuration information of IGMP SSM-MAP, execute the following command in the user mode:

Command	Function
DGS-3610# **show ip igmp ssm- mapping**	Show the Configuration Information of IGMP SSM-MAP.
DGS-3610# **show ip igmp ssm- mapping** *233.3.3.3*	Shown the mapping information from IGMP SSM-MAP to group 233.3.3.3.

35.6.19 Show Enabled Condition of IGMP Debugging Switch

To show the enabled condition of the IGMP debugging switch, execute the following command in the privilege mode:

Command	Function
DGS-3610# **show debugging**	Show the enabled condition of the IGMP debugging switch.

35.6.20 IGMP debug switch

To turn on IGMP debug switch and check the IGMP behavior, execute the following command in the privileged mode:

Command	Function
DGS-3610# **debug ip igmp all**	Turn on all IGMP debug switches
DGS-3610# **debug ip igmp decode**	Turn on IGMP debug decode switch
DGS-3610# **debug ip igmp encode**	Turn on IGMP debug encode switch
DGS-3610# **debug ip igmp events**	Turn on IGMP debug event switch

Command	**Function**
DGS-3610# **debug ip igmp fsm**	Turn on IGMP debug final-state-machine switch
DGS-3610# **debug igmp tib**	Turn on IGMP debug tree switch.
DGS-3610# **debug ip igmp warnning**	Turn on IGMP debug warning switch.

You can use **no debug ip igmp** to disable the degugging information swith of IGMP.

35.6.21 Configuring PIM-DM

35.6.21.1 Enabling PIM-DM

PIM-DM should be enabled on each interface. After the device enables PIM-DM on the interface, it can only exchange the PIM-DM control message with other devices, maintain and update the multicast route table and forward the multicast message.

To configure PIM-DM on the interface, execute the following command in the interface mode:

Command	**Function**
DGS-3610(config-if)# **ip pim dense-mode**	Enable the PIM-DM protocol on the interface.
DGS-3610(config-if)# **no ip pim dense-mode**	Disable the PIM-DM protocol on the interface.

In general, the PIM-DM protocol should be enabled on all interfaces of the devices.

Caution

The enabling of PIM-DM on the interface will take effect only when the multicast routing is enabled in the global configuration mode.

When this command is configured, if the “Failed to enable PIM-DM on <interface name>, resource temporarily unavailable, please try again” occurs, retry to configure this command.

When this command is configured, if the “PIM-DM Configure failed! VIF limit exceeded in NSM!!!” occurs, it indicates current allowed interface configuration exceeds the upper limit of the multicast interfaces. Please remove some unnecessary PIM-SM or DVMRP interface.

35.6.21.2 Set the Hello message sending interval

After the interface enables the PIM-DM, it will send the Hello message to neighbor device interface periodically. You can set the interval of sending Hello messages according to the network condition.

To configure the sending interval of Hello message, please execute the following commands in the interface mode:

Command	Function
DGS-3610(config-if)# **ip pim query-interval** *seconds*	Set the sending interval of the Hello message on the interface as seconds (unit: sec).
DGS-3610(config-if)# **no ip pim query-interval**	Restore the sending interval of Hello message in the interface to default value.

The sending interval of Hello message in the interface is 30 seconds by default.

Note

When the sending interval of the Hello message is updated, the Hello hold time will be updated as 3.5 times of the Hello sending interval automatically.

35.6.21.3 Configuring PIM-DM State Refresh

In the administration mode, it is permitted to forward PIM-DM state refresh control message by default. For the first-hop router directly connected to the source, the interface configuration state refresh interval is the interval at which the state refersh packets are sent. In this case, it is only effective for the upstream interfaces. For subsequent routers, it is the interval at which the interfaces are allowed to receive and process the state refresh packets.

Command	Function
No ip pim state-refresh isable	Allow to process and forward state-refresh messages.
ip pim state-refresh origination-interval [*interval*]	configure the interval of sending state refresh message periodically on the first hop directly connected to source, which is valid only to upstream interfaces. For subsequent routers, it is the interval of sending state refresh message which is permitted to receive and process on the interface.

The following example shows how to configure the interval of state refresh message on the FastEthernet0/1 interface.

```
ip multicast-routing
!
interface FastEthernet 0/1
ip address 172.16.8.1 255.255.255.0
ip pim state-refresh origination-interval 60
ip pim dense-mode
```

35.6.21.4 Configuring PIM Neighbor Filtering

The function of neighbor filtering can be enabled on the interface to enhance the network security. When the neighbor filtering is configured, if a neighbor is refused by the neighbor filtering access list, the PIM-DM either refuses to establish the connection with the neighbor or terminates the established connection with the neighbor. To disable or enable some groups to go through this region, you need to configure boundary group filtering list.

Please execute the following commands for configuring the neighbor filtering function of PIM.

Command	Function
ip pim neighbor-filter *access-list*	Enable the function of PIM neighbor filtering in current interface.
no ip pim neighbor-filter *access-list*	Disable the function of PIM neighbor filtering in current interface.
ip multicast boundary *access-list-name*	Configure multicast boundary of an interface.

By default, the neighbor filtering function is disabled in the interface.

Note

ip pim neighbor-filter command description:

When the associated ACL rule is set to **permit**, only the neighbor address in the ACL list can be regarded as the PIM neighbor of the current interface. When the associated ACL rule is set to **deny**, any neighbor address in the ACL list cannot be regarded as the PIM neighbor of the current interface.

35.6.21.5 Configuring the Status Update Function of PIM

When the PIM-DM is enabled, if the RPF interface in the multicast entries is directly connected to the multicast source, that is, some PIM interfaces are in the same network segment of the multicast source, the device sends status update messages periodically to the downlink devices to update the status of the whole network. You can disable the processing and forwarding of the PIM-DM status update messages in the global mode.

Execute the following command in the global configuration mode to configure the status renew function of PIM-DM:

Command	Function
ip pim state-refresh disable	Disable the processing and forwarding of the PIM-DM status update messages

Command	Function
no ip pim state-refresh disable	Enable the processing and forwarding of the PIM-DM status update messages

The status renew function is enabled by default.

Caution	Disabling the status update messages may cause the re-convergence of the converged PIM-DM multicast forward tree, resulting in unnecessary bandwidth waste and routing table vibration. Therefore, do not disable the status update function.

35.6.21.6 Configuring the Interval of Sending PIM Status Update Messages

When the PIM-DM is enabled, if the RPF interface in the multicast entries is directly connected to the multicast source, the device sends status update messages periodically to the downlink devices to update the status of the whole network. You can modify the sending interval of the PIM status update message according to the actual condition of the network.

To set the sending interval on an interface, execute the following commands in the interface mode.

Command	Function
ip pim state-refresh origination-interval *seconds*	Set the interval of sending PIM status update message of the current interface to seconds, which is an integer between 1 and 100 in the unit of seconds.
no ip pim state-refresh origination-interval	Cancel the sending delay of PIM status update message specified for the current interface

For the status update messages, the sending interval of PIM is 60 seconds by default.

Note	Only the devices that are directly connected to multicast sources send the PIM status update messages periodically to downlink interfaces. If a device is not directly connected with multicast sources, the sending interval of PIM status update message configured on its downlink ports is invalid.

35.6.21.7 Monitoring and Maintaining PIM-DM

PIM-DM provides the **show** command to monitor and maintain PIM-DM. Through the **show** command, you can view the interface, multicast group and multicast routing tables of PIM-DM.

Show the status of PIM-DM

Command	Function
show ip pim dense-mode interface [*interface-type interface-number*] [*detail*]	Show the PIM-DM interface information.
show ip pim dense-mode neighbor [*interface-type interface-number*]	Show the PIM-DM neighbor information.

For detailed using guide of above-mentioned commands, please refer to the *Command Reference of PIM-DM*.

Following examples show how to use these commands:

1. **show ip pim dense-mode interface detail command:**

```
DGS-3610# show ip pim interface detail
wm0 (vif-id: 0):
Address 193.168.1.53/24
Hello period 30 seconds, Next Hello in 30 seconds
Neighbors:
192.168.1.152/32
192.168.1.149/32
wm1(vif-id: 2):
Address 193.168.10.53/24
Hello period 30 seconds, Next Hello in 8 seconds
Neighbors: none
```

In the above example, the IP address of wm0 is set to 193.168.1.53, subnet mask is set to 255.255.255.0, the sending interval of Hello message is set to 30 seconds, and the IP addresses of the two neighbors are set to 192.168.1.152 and 192.168.1.149. The interface configuration of wm1 is the same except that wm1 has no neighbors.

2. **show ip pim dense-mode neighbor** command:

```
DGS-3610# show ip pim dense-mode neighbor detail
Neighbor 192.168.1.152 (wm0)
Up since 17:16:20, Expires in 00:01:20
Neighbor 192.168.1.149 (wm0)
Up since 17:16:12, Expires in 00:01:26
```

The device in the above example has two neighbors. The neighbor 192.168.1.152 is connected with wm0 and has lived for 17 hours, 16 minutes and 20 seconds, and will expire after 1 minute and 20 seconds. The lifetime and remaining time of the neighbor 192.168.1.149 are similar to that of 192.168.1.152.

35.6.22 Configuring PIM-SM

The PIM-SM configuration items include the following. However, only the first and second items are mandatory, and others are optional according to the network condition.

- Enabling multicast routing (required)

- Enabling PIM-SM (required)
- Configuring the Hello message sending interval (optional)
- Configuring PIM-SM neighbor filtering (optional)
- Configuring the priority of specified device DR (optional)
- Configuring the candidate BSR status (optional)
- Configuring static RP (optional)
- Configuring candidate RP (optional)
- Configuring particular source multicast (optional)
- Configuring flood/prune time for the timer (optional)
- Configuring the speed limit on the sending of registered packets (optional)
- Configuring reachability detection for registered packets (optional)
- Configuring the source address of registration packets (optional)
- Configuring the RP suppression time (optional)
- Configuring the time of the KAT timer (optional)
- Switching the last-hop device from shared tree to the shortest path tree (optional)
- Switching the last-hop device from shared tree to the shortest path tree in multiple multicast groups (optional)
- Show the status of the PIM-SM (optional)

35.6.22.1 Enabling Multicast Routing

The multicast routing must be enabled before the multicast packets can be transmitted, and so that enabling the PIM-SM is meaningful.

35.6.22.2 Enabling PIM-SM

The PIM-SM must be enabled on each interface. The device can interact with other devices for PIM-SM control messages, maintain and update multicast routing tables and forward multicast packets only after PIM-SM is enabled on the interface.

To configure the PIM-SM on the interface, execute the following command in the interface mode:

Command	Function
DGS-3610(config-if)# **ip pim sparse-mode**	Enable the PIM-SM protocol on the interface
DGS-3610(config-if)# **no ip pim sparse-mode**	Disable the PIM-SM protocol on the interface

Caution	Enabling the PIM-SM is effective only when the multicast routing is enabled in the global configuration mode. During the execution of this command, if the prompt "Failed to enable PIM-SM on <Interface Name>, resource temporarily unavailable, please try again" appears, re-execute this command. When this command is configured, if the “PIM-DM Configure failed! VIF limit exceeded in NSM!!!” occurs, It indicates current allowed interface configuration exceeds the upper limit of the multicast interfaces. Please remove some unnecessary PIM-SM or DVMRP interface.

35.6.22.3 Set the Hello message sending interval

When the PIM-SM is enabled on the interface, the device periodically sends Hello messages to the interfaces of neighbor devices. You can set the interval of sending Hello messages according to the network condition.

To configure the sending interval of Hello message, please execute the following commands in the interface mode:

Command	Function
DGS-3610(config-if)# **ip pim query-interval** *seconds*	Set the sending interval of the Hello message on the interface as seconds (unit: sec).
DGS-3610(config-if)# **no ip pim query-interval**	Restore the sending interval of Hello message in the interface to default value.

The sending interval of Hello message in the interface is 30 seconds by default.

Note	When the interval of sending the Hello message is updated, the message holding time is updated according to the following rules: If the message holding time is not configured or shorter than the sending interval, it is updated to that 3.5 times of the sending interval. Otherwise, the holding time is the same as the configured value.

35.6.22.4 Configuring PIM Neighbor Filtering

The function of neighbor filtering can be set on the interface to enhance the network security. When the neighbor filtering is configured, if a neighbor is refused by the neighbor filtering access list, the PIM-DM either refuses to establish the connection with the neighbor or terminates the established connection with the neighbor.

Please perform following commands for configuring the neighbor filtering function of PIM

Command	Function
ip pim neighbor-filter *access-list*	Enabling the function of PIM neighbor filtering in current interface.

Command	**Function**
no ip pim neighbor-filter *access-list*	Disabling the function of PIM neighbor filtering in current interface.

By default, the neighbor filtering function is disabled in the interface.

Note

ip pim neighbor-filter command description:

When the associated ACL rule is set to **permit**, only the neighbor address in the ACL list can be regarded as the PIM neighbor of the current interface. When the associated ACL rule is set to **deny**, any neighbor address in the ACL list cannot be regarded as the PIM neighbor of the current interface.

35.6.22.5 Configuring the Priority of Specified Device DR

Execute the command to set the priority of specified device. The higher the weight value, the higher the priority.

Please execute the following command in the interface mode:

Command	**Function**
ip pim dr-priority *priority*	Configuring the priority, the range is from 1 to 4294967294.
no ip pim dr-priority *priority*	Restore to the default value, the value is 1.

35.6.22.6 Configuring the Candidate BSR Status of the Device

Configure the device in an interface and make it as the candidate BSR status. Configuring the candidate RP generates the globally unique BSR in the PIM-SM domain. The BSR collects and distributes the RP in the domain to ensure the uniqueness of RP mapping in the domain.

Please execute the following command in the interface mode:

Command	**Function**
ip **pim bsr-candidate** *IFNAME (HASH) (PRIORITY)*	Configure the candidate BSR for the device. Learn and compete for global BSR through BSM messages.
no ip pim bsr-candidate *IFNAME (HASH) (PRIORITY)*	Cancel configuration of current candidate BSR

35.6.22.7 Configure the Static RP

In a small-scale network, you can use the static RP to use the PIM-SM, which requires that the static RP configuration of all devices in the PIM-SM domain must be consistent to ensure the uniqueness of PIM-SM multicast routes.

If a device in the PIM-SM domain runs BSR, search RP accoording to the order:
If **override** is configured, the static RP is prior to the RP in the RP mapping table distributed by BSR;
If **override** is not configured, the RP mapping table distributed by BSR is prior to the static RP.

Please execute the following commands in the global configuration mode:

Command	**Function**
ip pim rp-address A.B.C.D *((SIMPLERANGE | EXPRANGE | ACCESSLIST)*	Use the static RP to configure this device
no ip pim rp-address A.B.C.D *((SIMPLERANGE | EXPRANGE | ACCESSLIST)*	Cancel the static RP configuration.

Caution

Please pay attention to following points when using this command:

- If both the BSR and static RP configurations are effective, the dynamic configuration takes priority.
- The static RP address can be configured for multiple multicast groups (by ACL) or all multicast groups (not by ACL). However, a static RP address can be configured for several times.
- If several addresses can be configured for RP, the high address is firstly used.
- Only the permitted filtered addresses defined in the ACL are invalid multicast groups. The default filtering 0.0.0.0/0 is to filter all multicast groups 224/4.
- After the configuration, the static RP source address is inserted to the tree of group-based static RP group. Each static multicast group maintains the link table structure of a static RP group. The link tables are ordered decreasingly by the IP addresses. When an RP is selected in a group, the first element, namely, the RP with the highest IP address is firstly selected.
- To delete a static RP address, the address from all groups is deleted, and one address is selected from the existing tree structure as the RP address.

35.6.22.8 Configuring Candidate RP

The configured candidate RP can be sent to the BSR by certain interval and then flooded to all the PIM-SM devices in the domain, thus ensuring the uniqueness of RP mapping.

Please execute the following commands in the global configuration mode:

Command	Function
ip pim rp-candidate *IFNAME (PRIORITY) (INTERVAL) (GROUPLIST)*	Use the candidate RP to configure this device
no ip pim rp-candidate	Cancel the candidate RP configuration.

You can use the ACL to specify an interface as the candidate RP of a particular group. It should be noted that the group calculation is based on the permit ACE only, but not the deny ACE.

35.6.22.9 Configuring Particular Source Multicast

Configuring the particular source multicast enables the device to receive the multicast data packets directly from the multicast source, without following the RP tree. To configure the particular source multicast, execute the following command.

Command	Function
ip pim ssm {default |range access-list]}	Configure particular source multicast
nop pim ssm	Cancel particular source multicast.

35.6.22.10 Configuring Duration for the Flood/Prune Timer

The time from a PIM device receiving the prune packet to pruning the interface and notifying the downlink devices is controlled by a prune timer. By default, the timer is set to 3 seconds. If the timer is too long, the time of the packet pruning process is too long, while the downlink interface still receives the multicast packets, thus wasting the bandwidth. On the other hand, if the timer is too short, this increases the load of the switch. Therefore, you should set this timer appropriately to meet the actual environmental needs. When all neighbors support this option, the device will use the maximum override interval among all the neighbors as the value of the prune wait timer.

Please execute the following commands in the global configuration mode:

Command	Function
ip pim rp-candidate *IFNAME (PRIORITY)* *(INTERVAL) (GROUPLIST)*	Use the candidate RP to configure this device
no ip pim rp-candidate	Cancel the candidate RP configuration

35.6.22.11 Configuring the Speed Limit on the Sending of RP

This command configures the speed for the DR to send the RP. The **no** form of this command means no speed limitation. The configuration is for each (S, G) status, but not the system bandwidth.

Please execute the following commands in the global configuration mode:

Command	Function
ip pim register-rate-limit *<1-65535>*	Set the maximum RP packets <1-65535> sent in a second
no ip pim rp-candidate	Cancel the speed limit configuration (no speed limitation)

35.6.22.12 Configuring Reachability Detection for RP

This command detects whether the RP sent from DR can reach the destination device.

Please execute the following commands in the global configuration mode:

Command	Function
ip pim register-rp-reachability	Detect whether the RP can reach the destination device
no ip pim register-rp-reachability	The reachability is not detected.

35.6.22.13 Configuring the Source Address of RP

This command sets the source address of RP sent from DR. This **no** form of this command sets the RPF interface address as the default source address for the response to the PR sent from DR to the source host. The configured address must be reachable for the response to the correct Register-Stop information in the RP. The address is generally a loop address of the interface. It also can be other physical address. Such address must be advertised by unicast route on the DR interface.

Please execute the following commands in the global configuration mode:

Command	Function
ip pim register-source *[SOURCEADDRESS* | *IFNAME]*	Configure the source address used in RP
no ip pim register-source	Set the RPF interface address as the source address of RP

35.6.22.14 Configure the RP Suppression Time

This command configures the RP suppression time. This value configured on the DR modifies the RP suppression time defined on the DR. If the **ip pim rp-register-kat** is not configured, the value defined for the RP modifies the RPkeepalive period.

Please execute the following commands in the global configuration mode:

Command	Function
ip pim register-suppression *<1-65535>*	Configure the RP suppression time
no ip pim register-suppression	Set the suppression time to 60 seconds

35.6.22.15 Configuring the Time of the KAT Timer

The KAT timer is for the monitoring of PIM RP.

Please execute the following commands in the global configuration mode:

Command	Function
ip pim rp-register-kat *<1-65535>*	Configure the time of the KAT timer
no ip pim rp-register-kat	Use the default KAT value

35.6.22.16 Switching Last-Hop Device from Shared Tree to Shortest Path Tree

The last-hop device is allowed to switch from the shared tree to the shortest path tree.

If the sending speed of a source is faster than or equal to the transmission speed, the join information of a PIM is triggered and a source tree is constructured. If the ultimate keyword is defined, all the sources of the specified group use the shared tree. If the transmission speed is slower than the threshold transmission speed, the tree device is switched to the shared tree and sends a prune packet to the source.

Please execute the following commands in the global configuration mode:

Command	Function
ip pim spt-threshold	Allow the last-hop device to switch from the shared tree to the shortest path tree
no ip pim spt-threshold	Disable this function

35.6.22.17 Switching the last-hop device from shared tree to the shortest path tree in multiple multicast groups

The last-hop device is allowed to switch from the shared tree to the shortest path tree in multiple multicast groups.

Please execute the following commands in the global configuration mode:

Command	Function
ip pim spt-threshold group-list *(SIMPLERANGE* | *EXPRANGE* | *ACCESSLIST)*	Allow the last-hop device to switch from the shared tree to the shortest path tree
no ip pim spt-threshold group-list *(SIMPLERANGE* | *EXPRANGE* | *ACCESSLIST)*	Disable this function

35.6.22.18 Monitoring and maintaining PIM-SM

PIM-DM provides **show** command to monitor and maintain PIM-SM. Through the command, you can view the interface, multicast group and multicast routing tables of PIM-SM.

Show the status of the PIM-DM

With the following commands provided in our product 10.1, you can view the PIM-SM status information on the local host.

Command	Function
show debugging pim sparse-mode	Show the status of the debugging switch
show ip pim interface [interface-type interface-number] [**detail**]	Show the PIM-SM information of the interface.
show ip pim neighbor [interface-type interface-number]	Show the PIM neighbor information.
Show ip sparse-mode mroute	Show the multicast routing table information of PIM-SM
show ip pim sparse-mode bsr-router	Execute this command to show the detailed information of BSR.

Command	Function
show ip pim sparse-mode rp-hash *A.B.C.D*	Execute this command to show the RP information selected.
show ip pim sparse-mode rp mapping	Show the group-RP mapping information and RP settings
show ip sparse-mode nexthop	Show the next hop of PIM-SM from NSM.
show memory pim sparse-mode	Show the memory statistics information of PIM-SM background program

For the detailed using guide of above-mentioned commands, please refer to the *Command Reference of PIM-SM*.

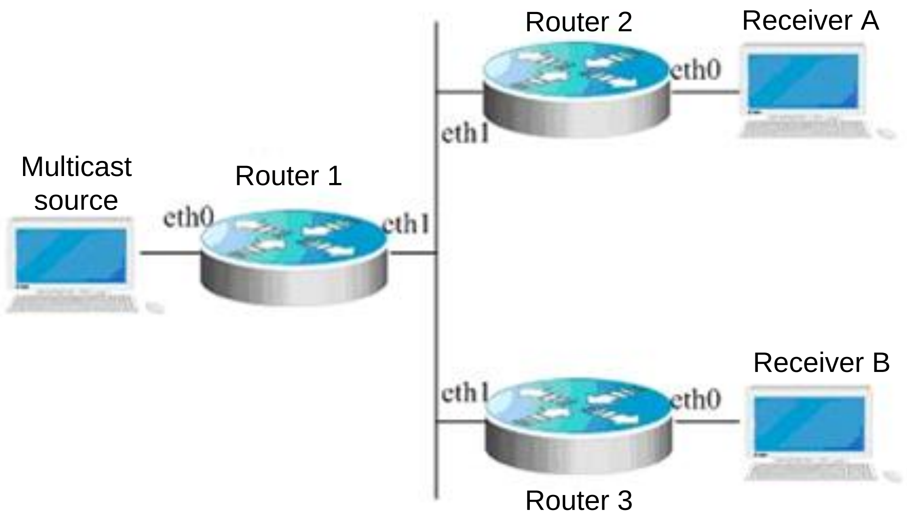
35.7 Multicast Routing Configuration Examples

35.7.1 PIM-DM Configuration Example

35.7.1.1 Configuration Requirements

The network topology structure is shown in the following figure. Device 1 and the multicast source locate in a same network, device 2 and receiver A locate in a same network, and device 3 and receiver B locate in a same network. Suppose the devices are connected with the host correctly and the IP addresses are configured.

Figure 35-6 Example of PIM-DM networking diagram



35.7.1.2 Device Configuration

Take the device 1 as an example to show how to configure PIM-DM. The steps of device 2 and 3 are similar to device 1.

Step 1: Enable multicast router

```
DGS-3610# configure terminal
DGS-3610(config)# ip multicast-routing
```

Step 2: Enable PIM-DM in the interface eth0

```
DGS-3610(config)# interface eth 0
DGS-3610(config-if)# ip pim dense-mode
DGS-3610(config-if)# exit
```

Step 3: Enable PIM-DM in the interface eth1 and return to the privileged user mode.

```
DGS-3610(config)# interface eth 1
DGS-3610(config-if)# ip pim dense-mode
DGS-3610(config-if)# end
```

The configuration of device 2 and 3 is similar to device 1. Firstly enable the multicast router, then enable the PIM-DM on each interface.

Note

When the PIM-SM is enabled, the IGMP is automatically enabled on the interfaces.

35.7.2 PIM-SM Configuration Example

35.7.2.1 Device Configuration

Following is the configuration of two devices:

ROUTE_A:

```
!
ip multicast-routing
!
interface Loopback0
ip address 192.168.100.142 255.255.255.0
ip pim-sm
!
interface Ethernet1/1
ip address 192.168.1.142 255.255.255.0
ip pim-sm
ip pim-sm dr-priority 100
!
interface serial2/0
ip address 192.168.21.142 255.255.255.0
physical-layer speed 128000
ip pim-sm
```

```
!
route rip
network 192.168.21.0
network 192.166.1.0
network 192.166.100.0
version 2
!
ip pim-sm bsr-candidate Loopback0 30 201
ip pim-sm rp-candidate Loopback0
!
```

ROUTER_B:

```
!
ip multicast-routing
!
interface Ethernet0/1
ip address 192.168.200.144 255.255.255.0
ip pim-sm
ip pim-sm dr-priority 200
!
interface Serial0/0
ip address 192.168.21.144 255.255.255.0
ip pim-sm
!
```

Note

When PIM-SM is enabled, IGMP is automatically enabled in each interface respectively, without the need manual configuration.

35.7.3 BSR Configuration Examples

Following example to show the BSR configuration of two devices:

ROUTER_A:

```
!
ip multicast-routing
!
interface Loopback0
ip address 192.166.100.42 255.255.255.0
ip pim-sm
!
interface Ethernet1/1
ip address 192.166.1.142 255.255.255.0
ip pim-sm
!
interface serial2/0
ip address 192.168.21.142 255.255.255.0
physical-layer speed 12800
ip pim-sm
```

```
!
router rip
network 192.168.21.0
network 192.168.100.0
!
ip pim-sm bsr-candidate Loopback0 30 201
!
```

ROUTER_B:

```
!
ip multicast-routing
!
interface Loopback0
ip address 192.168.100.144 255.255.255.0
ip pim-sm
!
interface Ethernet0/1
ip address 192.168.200.144 255.255.255.0
ip pim-sm
!
ip pim-sm bsr-candidate Loopback0 30
!
```

36 Port-Based Flow Control Configuration

36.1 Storm Control

36.1.1 Overview

Excessive broadcast, multicast or unicast packets with unknown names in LAN will result in slow network speed and considerably increased possibility of packet transmission timeout. This is called LAN storm. Protocol stack implementation errors or wrong network configuration may also lead to such storms.

Storm control can be conducted to broadcast, multicast and unknown unicast data flows respectively.When the rate of the broadcast, multicast or unicast packets with unknown names received by the interface exceeds the specified threshold, the device only allows the packets within the bandwidth threshold. The packets that exceed the threshold will be discarded until the data flow becomes normal again. This prevents excessive flood packets from entering the LAN to for a storm.

36.1.2 Configuring Storm Control

By default, the storm control function for broadcast, multicast and unknown unicast packets is disabled.

When the user sets a bandwidth for an interface by percentage, this percentage applies to all the ports and any other settings will not take effect.

In the interface configuration mode, execute the following command to configure storm control:

Command	Function
DGS-3610(config-if)**# storm-control** {**broadcast** | **multicast** | **unicast**} [{ **level** *percent* | **pps** *packets* | *rate-bps*]	**broadcast**: Enable the broadcast storm control function. **multicast**: Enable the unknown multicast storm control function. **unicast**: Enable the unknown unicast storm control function. ***percent**:* Set according to the bandwidth percentage, for example, 20 means 20% ***packets*:** Set according to the pps, which means packets per second ***Rate-bps***: rate allowed

In the interface configuration mode, you can disable the storm control of the appropriate interface by executing the **no storm-control broadcast, no storm-control multicast, or no storm-control unicast** commands.

The following example enables the multicast storm control on GigabitEthernet 0/1 and set the allowed rate to 4M.

```
DGS-3610# configure terminal
DGS-3610(config)# interface GigabitEthernet 0/1
DGS-3610(config-if)# storm-control multicast 4096
DGS-3610(config-if)# end
```

Caution

The reference bandwidth for the level-based storm control is the maximum bandwidth supported by the physical interface, but not converted from the bandwidth of the physical interface in service.

36.1.3 Viewing the Enable Status of Storm Control

To view the storm control status of the interface, execute the following command:

Command	Function
DGS-3610# **show storm-control** [*interface-id*]	Show storm control information.

The instance below shows the enabled status of the storm control function of interface Gi1/3:

```
DGS-3610# show storm-control gigabitEthernet 0/3
Interface  Broadcast Control  Multicast Control  Unicast Control action
GigabitEthernet 0/3 Disabled  Disabled   Disabled    none
```

You can also view the enabling status of the storm control function of all interfaces at a time:

```
DGS-3610# show storm-control
Interface  Broadcast Control  Multicast Control  Unicast Control Action
--------- ------------------ ------------------ ------- ------- ------
GigabitEthernet 0/1   Disabled   Disabled   Disabled   none
GigabitEthernet 0/2   Disabled  Disabled  Disabled  none
GigabitEthernet 0/3   Disabled  Disabled  Disabled  none
GigabitEthernet 0/4   Disabled  Disabled  Disabled  none
GigabitEthernet 0/5   Disabled  Disabled  Disabled  none
GigabitEthernet 0/6   Disabled  Disabled  Disabled  none
GigabitEthernet 0/7   Disabled  Disabled  Disabled  none
GigabitEthernet 0/8   Disabled  Disabled  Disabled  none
GigabitEthernet 0/9   Disabled  Disabled  Disabled  none
GigabitEthernet 0/10  Disabled  Disabled  Disabled  none
GigabitEthernet 0/11  Disabled  Disabled  Disabled  none
GigabitEthernet 0/12  Disabled  Disabled  Disabled  none
GigabitEthernet 0/13  Disabled  Disabled  Disabled  none
GigabitEthernet 0/14  Disabled  Disabled  Disabled  none
GigabitEthernet 0/15  Disabled  Disabled  Disabled  none
GigabitEthernet 0/16  Disabled  Disabled  Disabled  none
GigabitEthernet 0/17  Disabled  Disabled  Disabled  none
GigabitEthernet 0/18  Disabled  Disabled  Disabled  none
GigabitEthernet 0/19  Disabled  Disabled  Disabled  none
GigabitEthernet 0/20  Disabled  Disabled  Disabled  none
GigabitEthernet 0/21  Disabled  Disabled  Disabled  none
GigabitEthernet 0/22  Disabled  Disabled  Disabled  none
GigabitEthernet 0/23  Disabled  Disabled  Disabled  none
GigabitEthernet 0/24  Disabled  Disabled  Disabled  none
```

36.2 Protected Port

36.2.1 Overview

Under certain application contexts, it is required that some ports on the same device should not communicate mutually. In such cases, communication, including unicast frames, broadcast frames and multicast frames, among these ports is not forwarded between the protected ports. To achieve this purpose, you can set some ports as protected ports.

After these ports are set as the protected ports, they cannot communicate with each other; but protected ports can still communicate with unprotected ports.

Protected ports provide two modes: denying layer 2 forwarding between protected ports but allowing layer 3 routing between protected ports; denying layer 2 forwarding and layer 3 routing between protected ports. If both modes are supported, the first one is defaulted.When you set two protected ports as a SPAN port pair, the frames transmitted or received by the source port of SPAN are sent to the destination port of SPAN according to the SPAN setting. Therefore, it is not recommended to set the destination port of SPAN as the protected port (and you can also save system resources).

The device supports the Aggregated Port as the protection port. When you set an Aggregated Port as the protection port, all the member ports of the Aggregated Port will be set as the protection port.

36.2.2 Configuring Protected Ports

Set one port as the protection port:

Command	Function
DGS-3610(config-if)# **switchport protected**	Set this interface as a protected port

You can reset a port as unprotected port with interface configuration command **no switchport protected**.

The following example describes how to set the Gigabitethernet 0/3 as the protection port.

```
DGS-3610# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DGS-3610(config)# interface gigabitethernet 0/3
DGS-3610(config-if)# switchport protected
DGS-3610(config-if)# end
```

36.2.3 Configuring L3 Protected-Ports Route Deny

Command	Function
DGS-3610(config)# **protected-ports route-deny**	Disable layer 3 routing between protected ports

With the command **no protected-ports route-deny**, you can enable layer 3 routing between protected ports.

The following example shows how to disable layer 3 routing between protected ports.

```
DGS-3610# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

DGS-3610(config)# protected-ports route-deny

DGS-3610(config)# end
```

Enter the **show running-config** command to view the configuration.

36.2.4 Showing Protected Port Configuration

Command	Function
DGS-3610(config-if)# **show interfaces switchport**	Show the configuration of the switching port

You can use the command of **show interfaces switchport** to view the configuration of protected port.

```
DGS-3610# show interfaces gigabitethernet 0/3 switchport
Interface   Switchport  Mode   Access Native Protected   VLAN lists
---------   ----------  ----   ------  -----  --------   ----
GigabitEthernet 0/3  enabled   Trunk  1   1    Enabled    ALL
```

36.3 Port Security

36.3.1 Overview

Based on the feature of port security, you can exercise strict control over the input of a specific port by restricting access to the MAC address and IP (optional) of the port on the device. After you configure some security addresses for the secure port (whose port security function is enabled), this port does not forward any packets other than those whose source addresses are the secure ones. In addition, you can also restrict the maximum number of security addresses on a port. If you set the maximum value to 1 and configure one security address for this port, the workstation (whose address is the configured secure M address) connected to this port will occupy all the bandwidth of this port exclusively.

To enhance security, you can bind the MAC address with the IP address as the security address. Of course you can also designate the MAC address without binding the IP address.

You can add the security addresses on the port in the following ways:

You can manually configure all the security addresses of the port by using the commands in the interface configuration mode.

You can also let this port automatically learn these addresses, which will become the security address on this port till the total number reaches the maximum value. Note that, however, the automatically-learned security addresses will not be bound with the IP address. On the same port, if you have configured a security address bound up with the IP address, the port cannot be added with any security address by automatic learning.

Manually configure some security addresses, and let the device learn the rest.

When a port is configured as a secure port and the maximum number of its security addresses is reached, a security violation occurs if the port receives a packet whose source address is not one of the security addresses on the port. When security violations occur, you can handle them through the following methods:

protect: When the maximum number of security addresses is reached, the secure port discards the packet of unknown addresses (none of which are among the security addresses of the port).This is the default method for handling exceptions.

restrict: When violation occurs, the system sends a Trap notice.

shutdown: When violation occurs, the system disables the port and sends a Trap notice.

36.3.2 Configuring Port Security

36.3.2.1 Default Configuration of Port Security

The table below shows the default configuration of port security:

Item	Default Configuration
Port security switch	The port security function is disabled for all the ports.
Maximum number of security addresses	128
Security address	None
Violation handling mode	Protect

36.3.2.2 Port Security Configuration Guide

The following restrictions are applied to port security configuration:

- A secure port is not an aggregate port.
- A secure port is not the destination port of SPAN.
- A secure port is and can only be an access port.

The 802.1X authentication and port security are mutually exclusive in enabling. The 802.1X authentication and port security can ensure the validity of the network users. You can enable either of them to control port access.

At the same time, the security addresses of the stated IP addresses and MAC addresses share with the ACLs the hardware resources of the system. Therefore, when you apply the ACLs on one secure port, the stated IP addresses on the port can be configured with less security addresses.

The security addresses for the same secure port must have the same format, namely either all or none of them are bound with IP addresses. If a security port includes these two types of security addresses at the same time, the security address not bound with the IP address will fail (the security address bound with the IP address has a higher priority).

36.3.2.3 Configuration of Secure Ports and Violation Handling Modes

In the interface configuration mode, configure secure ports and violation handling modes with the following commands:

Command	Function
DGS-3610(config-if)# **switchport port-security**	Enable the port security function of this interface.

Command	**Function**
DGS-3610(config-if)# **switchport port-security maximum** *value*	Set the maximum number of security addresses on the interface. The range is between 1 and 1000 and the default value is 128.
DGS-3610(config-if)# **switchport port-security violation**{**protect** | **restrict** | **shutdown**}	Set the violation handling mode: **protect**: Protected port. When the number of security addresses if full, the security port will discard the packets from unknown address (that is, not any among the security addresses of the port). **restrict**: When violation occurs, the system sends a Trap notice. **shutdown**: When violation occurs, the system disables the port and sends a Trap notice. When a port is closed because of violation, you can recover it from the error status through the **errdisable recovery** command in the global configuration mode.

In the interface configuration mode, you can disable the port security function of an interface with the command **no switchport port-security**. Execute the command **no switchport port-security maximum** to recover to the default maximum value. Execute the command **no switchport port-security violation** to set violation handling to the default mode.

The instance below describes how to enable the port security function on interface gigabitethernet 0/3. The maximum number of addresses is set to 8 and the violation handling mode is set to **protect**.

```
DGS-3610# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DGS-3610(config)# interface gigabitethernet 0/3
DGS-3610(config-if)# switchport mode access
DGS-3610(config-if)# switchport port-security
DGS-3610(config-if)# switchport port-security maximum 8
DGS-3610(config-if)# switchport port-security violation protect
DGS-3610(config-if)# end
```

Note

If the security address MAC+IP has been configured on the secure port, the exception handling rule for the port will not take effect.

36.3.2.4 Configuration of Security addresses on the Security Port

In the interface configuration mode, add security addresses for secure ports with the following commands:

Command	**Function**
DGS-3610(config-if)# **switchport port-security mac-address** *mac-address* [**ip-address** *ip-address*]	Manually configure the security address on the interface. **ip-address** (optional): IP address bound up with the security address.

In the interface configuration mode, you can execute the command **no switchport port-security mac-address** *mac-address* to delete the security address of this interface.

The example below describes how to configure a security address for interface gigabitethernet 0/3: 00d0.f800.073c and bind it with an IP address: 192.168.12.202.

```
DGS-3610# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DGS-3610(config)# interface gigabitethernet 0/3
DGS-3610(config-if)# switchport mode access
DGS-3610(config-if)# switchport port-security
DGS-3610(config-if)# switchport port-security mac-address 00d0.f800.073c  ip-address
192.168.12.202
DGS-3610(config-if)# end
```

36.3.2.5 Configuration of Aging Time for Security addresses

You can configure the aging time for all the security addresses on an interface. To enable this function, you need to set the maximum number of security addresses. In this way, you can make the device automatically add or delete the security addresses on the interface.

In the interface configuration mode, configure the aging time for security addresses with the following command:

Command	**Function**
DGS-3610(config-if)#**switchport port-security aging**{**static** | **time** *time* }	**Static**: When this keyword is added, the aging time will be applied to both the manually configured address pool and automatically learnt addresses. Otherwise, it is applied only to the automatically learnt addresses. **Time**: indicates the aging time for the security address on this port. Its range is 0-1440 and unit is Minute. If you set it to 0, the aging function actually is disabled. The aging time is the absolute time, which means that an address will be deleted automatically after the *Time* specified expires after the address becomes the security address of the port. The default value of *Time* is 0.

In the interface configuration mode, execute **no switchport port-security aging time** to disable the port security aging. Execute the **no switchport port-security aging static** to apply the aging time only to dynamically learned security address.

The example below describes how to configure the port security aging time on interface Gigabitethernet 0/3. The aging time is set to 8 minutes and it is applicable to statically-configured security addresses:

```
DGS-3610# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DGS-3610(config)# interface gigabitthernet 0/3
DGS-3610(config-if)# switchport port-security aging time 8
DGS-3610(config-if)# switchport port-security aging static
DGS-3610(config-if)# end
```

36.3.2.6 Configuring ARP Check of Security Addresses

ARP check can avoid bogus ARP on secure ports and prevent illegal information from pretending to be the IP address of key network device, causing network communication disorder.

ARP check restriction:

1. With ARP check enabled, the maximum number of security addresses binding IP on all ports is halved.

2. The ARP check does not take effect for existing security addresses. To validate a configured security address, you can disable it and then enable it. In ARP check, the strategy management module is used, sharing hardware resources with other strategy management modules. In case of hardware resource shortage, the ARP check of some security addresses may not take effect.

3. When many security address entries of MAC+IP exist, the ARP Check Cpu function has a great impact on the CPU performance and can reduce the CPU efficiency.

By default, a security address only checks IP packets. The administrator needs to check the validity of ARP packets. Execute the following command to enable ARP check in the interface configuration mode.

Command	Function
DGS-3610(config-if)# **switchport port-security arp-check**	Enable the ARP check function of security addresses

You can disable the ARP check function executing the command **no switchport port-security arp-check** in the global configuration mode.

36.3.3 Viewing Port Security Information

In the privileged mode, you can view the security information of a port with the following commands.

Command	Function
DGS-3610#**show port-security interface** [*interface-id*]	View the port security configuration information of an interface.
DGS-3610#**show port-security address**	View the security address information.
DGS-3610# **show port-security address** [*interface-id*]	Show the security address information on an interface.
DGS-3610# **show port-security**	Show the statistics of all the security ports, including the maximum number of security addresses, the number of current addresses, and violation handling mode.

The example below shows the port security configuration on interface **gigabitethernet 0/3**:

```
DGS-3610# show port-security interface gigabitethernet 0/3
Interface Gi0/3
Port Security: Enabled
Port status : down
Violation mode:Shutdown
Maximum MAC Addresses:8
Total MAC Addresses:0
Configured MAC Addresses:0
Aging time : 8 mins
SecureStatic address aging : Enabled
```

The instance below shows all the security addresses in the system.

```
DGS-3610# show port-security address
Vlan Mac Address IP Address Type Port Remaining Age(mins)
----------------------------------------- -------------------
1  00d0.f800.073c   192.168.12.202    Configured   Gi0/3    8
1  00d0.f800.3cc9   192.168.12.5     Configured   Gi0/1    7
```

You can also only show the security address on one interface. The instance below shows the security address on interface gigabitstethernet 0/3.

```
DGS-3610# show port-security address interface gigabitethernet 0/3
Vlan Mac Address IP Address Type Port Remaining Age(mins)
---- --------------- ---------- ------ ------------------
1    00d0.f800.073c  192.168.12.202 Configured Gi0/3    8
```

The example below shows the statistic information of the secure port.

```
DGS-3610# show port-security
Secure Port MaxSecureAddr(count) CurrentAddr(count) Security Action
-------- -----------------  -----------------  ------------
```

```
Gi0/1       128                 1               Restrict
Gi0/2       128                 0               Restrict
Gi0/3       8                    1              Protect
```

37 Configuration of 802.1X

This chapter describes the contents related to the AAA service configurations. The 802.1X is used to control the authentication over network access of users, and provide authorization and accounting functions for users.

This chapter includes:

- Overview
- Configuring 802.1X
- Viewing the Configuration and Current Statistics of the 802.1X
- Other Precautions for Configuring 802.1X

Note

For details about usage and descriptions of the CLI commands used in this section, please refer to *Configuring 802.1X command*.

37.1 Overview

In an IEEE 802 LAN, users can access the network device without needing authentication and authorization as long as they are connected to the network device. Therefore, an unauthorized user can access the network without obstruction by connecting the LAN. With wide application of the LAN technology and particularly the appearance of the operation network, it is necessary to address the safety authentication needs of the network. It has become the focus in the industry that how to provide users with the authentication on the legality of network or device access on the basis of simple and cheap Ethernet technologies. The IEEE 802.1x protocol is developed under such a context.

As a Port-Based Network Access Control standard, the IEEE802.1x provides LAN with point-to-point security access. Specially designed by the IEEE Standardization Commission to tackle the security defects of Ethernet, this standard can provide a means for authenticating the devices and users connected to the LAN by utilizing the advantages of IEEE 802 LAN.

The IEEE 802.1x defines a mode based on Client-Server to restrict unauthorized users from accessing the network. Before a client can access the network, it must first pass the server authentication.

Before the client passes the authentication, only the EAPOL (Extensible Authentication Protocol over LAN) packets can be transmitted over the network. After successful authentication, normal data flows can be transmitted over the network.

By using 802.1x, our devices provide Authentication, Authorization, and Accounting (AAA).

- Authentication: It is used to check whether a user has the access right, thus restricting illegal users.
- Authorization: It authorizes the services available to users, controlling the rights of valid users.
- Accounting: It records users' use of network resources, providing the supporting data for charging.

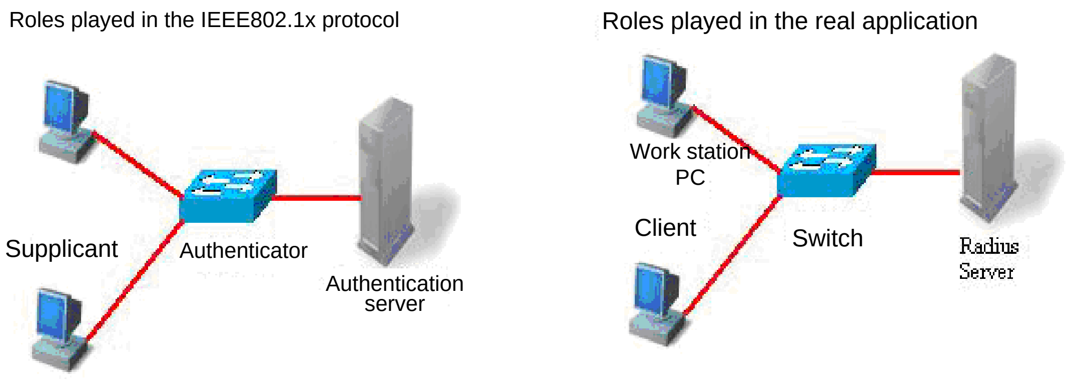
The 802.1x is described in the following aspects as below:

- Device Roles
- Authentication Initiation and Packet Interaction During Authentication
- States of Authorized Users and Unauthorized Users
- Topologies of Typical Applications

37.1.1 Device Roles

In the IEEE802.1x standard, there are three roles: **supplicant, authenticator, and authentication server.** In practice, they are the Client, network access server (NAS) and Radius-Server.

Figure 37-1



- Supplicant:

The **supplicant** is a role played by end users, usually a PC. It requests for the access to network services and responds to the request packets from the authenticator. The supplicant must run the IEEE 802.1x client. Currently, the most popular the IEEE802.1X client carried by Windows XP. In addition, we have also launched the STAR Supplicant software compliant of this standard.

- Authenticator:

The **authenticator** is usually an access device like the switch. The responsibility of the device is to control the status of the connection of a client to the network according to the current authentication status of that client. Between the client and server, this device plays the role of a mediator, which requests the client for username, verifies the authentication information from the server, and forwards it to the client. Therefore, the switch acts as both the IEEE802.1X authenticator and the RADIUS Client, so it is referred to as the network access server (NAS). It encapsulates the acknowledgement received from the client into the RADIUS format packets and forwards them to the RADIUS Server, while resolving the information received from the RADIUS Server and forwards the information to the client.

The device acting as the authenticator has two types of ports: controlled Port and uncontrolled Port. The users connected to a controlled port can only access network resources before they first pass the authentication, while those connected to an uncontrolled port can directly access network resources without authentication. We can control users by simply connecting them to a controlled port. On the other hand, the uncontrolled port is used to connect the authentication server, for ensuring normal communication between the server and device.

- Authentication server:

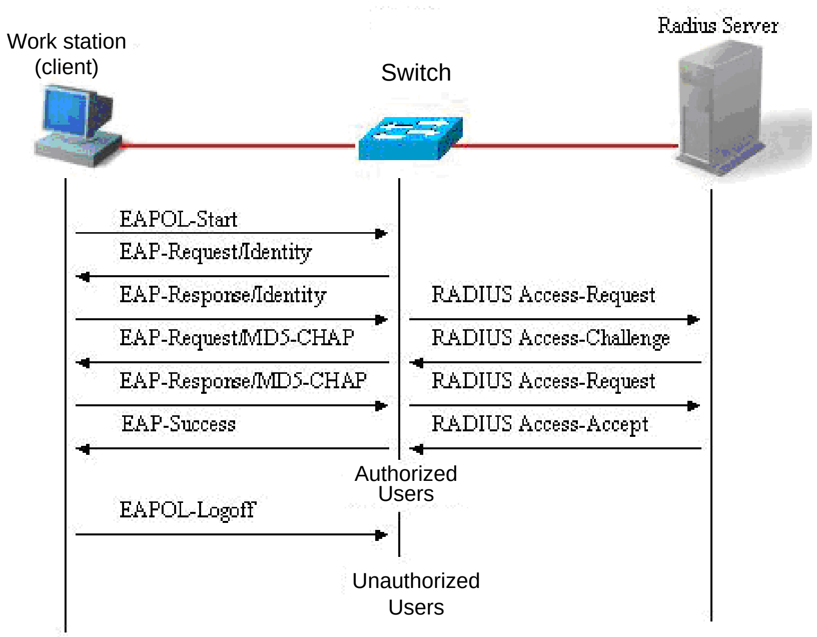
The **authentication server** is usually an **RADIUS** server, which works with the authenticator to provide users with authentication services. The authentication server saves the user name and password and related authentication information. One server can provide authentication services for multiple authenticators, thus allowing centralized management of users. The authentication server also manages the accounting data from the authenticator. Our 802.1X device is fully compatible with the standard Radius Server, for example, the Radius Server carried on Win2000 Server and the Free Radius Server on Linux.

37.1.2 Authentication Initiation and Packet Interaction During Authentication

The supplicant and the authenticator exchange information with each other by using the EAPOL protocol, while the authenticator and authentication server exchange information by using the RADIUS protocol, completing the authentication process with such a conversion. The EAPOL protocol is encapsulated on the MAC layer, with the type number of 0x888E. In addition, the standard has required for an MAC address (01-80-C2-00-00-03) for the protocol for packet exchange during the initial authentication process.

The following diagram shows a typical authentication process, during which the three role devices exchange packets with one another.

Figure 37-2



This is a typical authentication process initiated by users (in some special cases, the switch can actively initiate authentication request, whose process is the same as that shown in the diagram, except that it does not contain the step where the user actively initiates the request).

37.1.3 States of Authorized Users and Unauthorized Users

The 802.1X check whether the users on the port are allowed to access the network according to the authentication status of the port. Since we expand the 802.1X based on users, we check whether a user is allowed to access network resources according to the authentication status of that user under a port. All users under an uncontrolled port can use network resources, while those under a controlled port can access network resources only if they are authorized. When a user just initiates an authentication request, its status is unauthorized, in which case it cannot access the network. When the authentication is passed, its status is changed to authorized, in which case it can use the network resources.

If the workstation does not support 802.1X while the machine is connected with the controlled port, the workstation will not respond to the request due to no support when the equipment requests the username of the user. This means that the user is still unauthorized and cannot access the network resources.

On the contrary, if the client supports 802.1X and the connected switch does not: The EAPOL-START frames from the user are not responded, and the user deems its connected port as an uncontrolled port and directly uses network resources, when the user fails to receive any response after it sends the specified number of EAPOL-START frames.

On an 802.1X-enabled device, all ports are uncontrolled ports by default. We can set a port as a controlled port, to impose authentication over all the users under that port.

When a user has passed authentication (the switch has received success packets from the RADIUS Server), the user is authorized and therefore can freely use network resources.If the user fails in the authentication and remains in the unauthenticated status, it is possible to initiate authentication once again. If the communication between the switch and the RADIUS server is faulty, the user is still unauthorized and therefore still cannot use the network.

When the user sends the EAPOL-LOGOFF packets, its status is changed from authorized to unauthorized.

When a port of the switch is changed to the LINK-DOWN status, all the users on the port change to the unauthorized status.

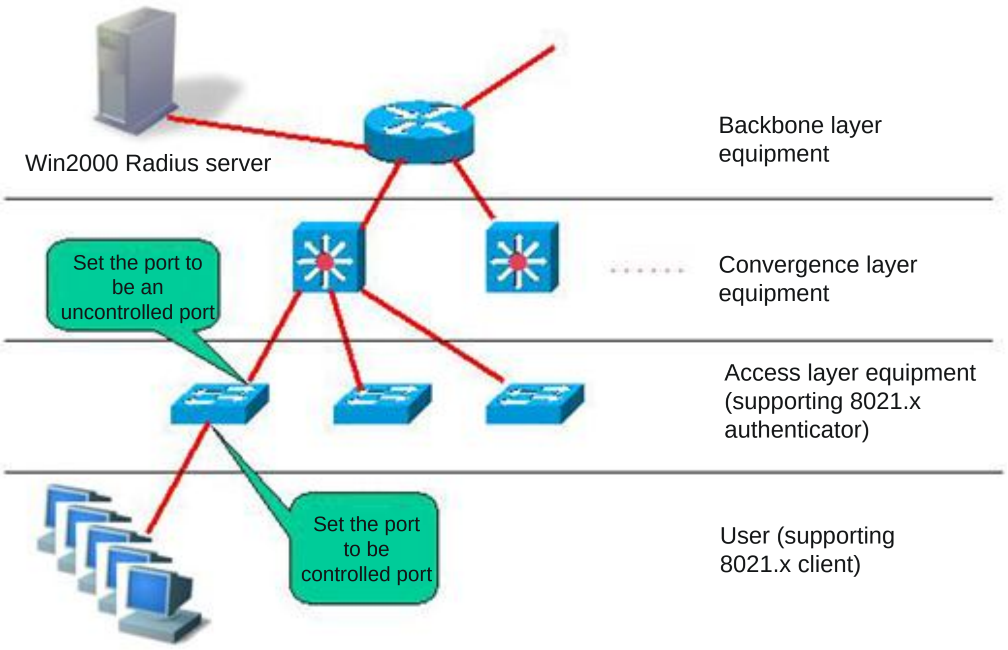
When the device restarts, all users on the device turn into the unauthorized status.

To force a user to pass the authentication, you can add a static MAC address.

37.1.4 Topologies of Typical Applications

A. The 802.1X-enabled device is used as the access layer device

Figure 37-3

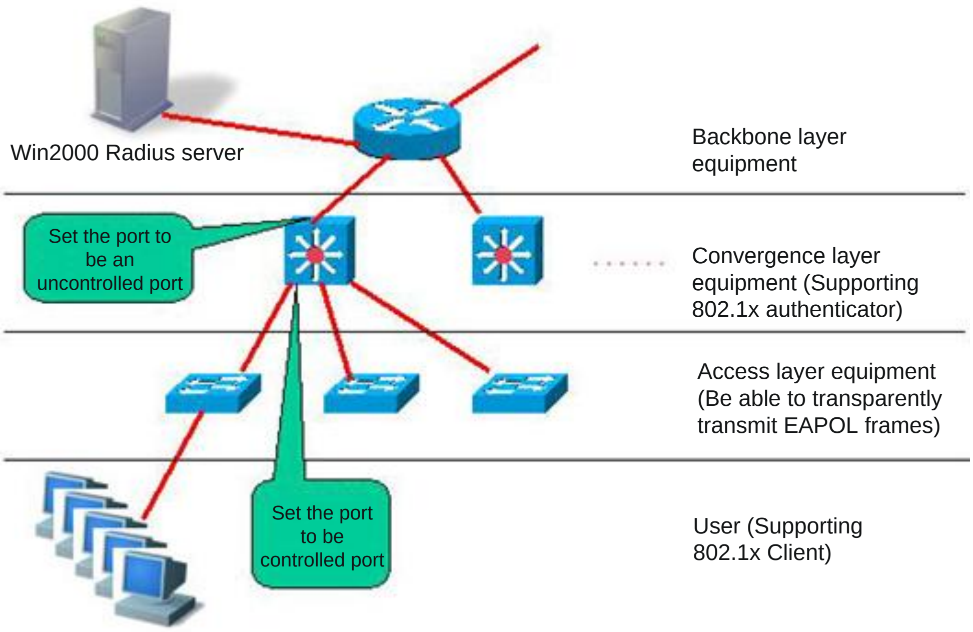

Win2000 Radius server
Backbone layer equipment
Set the port to be an uncontrolled port
Convergence layer equipment
Access layer equipment (supporting 8021.x authenticator)
Set the port to be controlled port
User (supporting 8021.x client)

This solution is described as below:

- Requirements of this solution:
  1. The user supports 802.1X. That is, it is installed with the 802.1X client (Windows XP carried, Star-supplicant or other IEEE802.1X-compliant client software).
  2. The access layer device supports IEEE 802.1X.
  3. One or multiple RADIUS-compliant servers are available as the authentication server.
- Key points for configuration of this solution:
  1. The ports connected to the Radius Server and the uplink ports are configured as **uncontrolled ports**, so that the device can normally communicate with the server and the authorized users can access network resources through the uplink interface.
  2. The ports connected to the user must be set to **controlled ports**, to control the accessed users, and the users cannot access network resources unless they first pass the authentication.
- Characteristics of this solution:
  1. Each 802.1X-enabled device is responsible for a small number of clients, thus offering higher speed.The devices are mutually independent, and the restart operation of the device does not affect the users connected with other devices.
  2. User management is performed on the Radius Server in a centralized manner. The administrator does not have to know which device a user is connected to, making management much easier.
  3. The administrator can manage the device on the access layer through the network.

B. The 802.1X-enabled device is used as the convergence layer device

Figure 37-4


Win2000 Radius server
Backbone layer equipment
Set the port to be an uncontrolled port
Convergence layer equipment (Supporting 802.1x authenticator)
Access layer equipment (Be able to transparently transmit EAPOL frames)
Set the port to be controlled port
User (Supporting 802.1x Client)

This solution is described as below:

- Requirements of this solution:
  1. The user supports 802.1X. That is, it is installed with the 802.1X client (Windows XP carried, Star-supplicant or other IEEE802.1X-compliant client software).
  2. The access layer device should be able to transparently transmit IEEE 802.1X. frames (EAPOL)
  3. The convergence layer device supports 802.1X (playing the role of the authenticator)
  4. One or multiple RADIUS-compliant servers are available as the authentication server.

- Key points for configuration of this solution:
  1. The ports connected to the Radius Server and the uplink ports are configured as **uncontrolled ports**, so that the device can normally communicate with the server and the authorized users can access network resources through the uplink interface.
  2. The ports connected to the access layer devices must be set to the **controlled ports**, to control the accessed users, and the users cannot access network resources unless they first pass the authentication.

- Characteristics of this solution:

1. The convergence layer device must be of high quality since the network is large and numerous users are connected, since any of its fault may cause the failures of accessing the network.
2. User management is performed on the Radius Server in a centralized manner. The administrator does not have to know which device a user is connected to, facilitating administrator management.
3. The access layer device can be the less expensive non-NM devices (as long as they support transparent transmission of EAPOL frames).
4. The administrator cannot manage the device on the access layer through the network.

37.2 Configuring 802.1X

The following sections describe how to configure 802.1X.

- Default Configuration of 802.1X
- Precautions for Configuring 802.1X
- Configuring the communication between the device and Radius server
- Setting the 802.1X Authentication Switch
- Enabling/Disabling the Authentication of a Port
- Enabling Timed Re-authentication
- Changing the QUIET Time
- Setting the Packet Retransmission Interval
- Setting the Maximum Number of Requests
- Setting the Maximum Number of Re-authentications
- Setting the Server-timeout
- Configuring the device to initiate the 802.1X authentication actively
- Configuring 802.1X Accounting
- Configuring the IP authorization mode
- Releasing Advertisement
- List of Authenticable Hosts under a Port
- Authorization
- Configuring the Authentication Mode
- Configure the backup authentication server.
- Configuring and Managing Online Users
- Implementing User-IP Binding
- Port-based Traffic Charging
- Implementing Automatic Switching and Control of VLAN
- Shielding Proxy Server and Dial-up

- Configuring On-line Client Probe
- Configuring the Option Flag for EAPOL Frames to Carry TAG

37.2.1 Default Configuration of 802.1X

The following table lists some defaults of the 802.1X

Item	**Default**
Authentication	DISABLE
Accounting	DISABLE
Radius Server *ServerIp *Authentication UDP port *Key	*No default *1812 *No default
Accounting Server *ServerIp *Accounting UDP port	*No default *1813
All port types	Uncontrolled port (all ports can perform communication directly without authentication)
Timed re-authentication	Off
Timed reauth_period	3,600 seconds
Interval between two authentication requests	10 seconds
Retransmission interval	3 seconds
Maximum retransmissions	3
Client timeout period	3 seconds, if within which no response is received from the client, the communication is deemed as a failure
Server timeout period	5 seconds, if within which no response is received from the server, the communication is deemed as a failure
Lists of authenticable hosts under a port	No default

37.2.2 Precautions for Configuring 802.1X

- You can perform the following configuration only to the products that support 802.1X.
- The 802.1X can run on both L2 device and L3 device.
- It is required to configure the IP address of the authentication server before the Radius-server authentication mode can operate normally.
- You cannot enable 1X authentication for ports with safety feature enabled.

- You cannot enable 1X authentication for Aggregate Port.
- If the 1x function is enabled on only one port of a switch, all the ports will send the 1x protocol packets to the CPU.

37.2.3 Configuring the Communication Between the Device and Radius Server

The Radius Server maintains the information of all users: user name, password, authorization information and accounting information. All users are managed on the Radius Server in a centralized manner, without being distributed over various devices, making easier management for the administrator.

In order for the switch to normally communicate with the RADIUS SERVER, you must set the following parameters:

Radius Server end: You must register a Radius Client. During registration, you must provide the Radius Server device's IP address, authentication UDP port (add the accounting UDP port, if needed), and the agreed key for communication between the device and Radius Server, and select EAP support for the Client. The procedure for registering one Radius Client on the Radius Server varies from software. Please refer to the relevant document.

Device end: The following settings are necessary at the device end to ensure the communication between the device and the server: Configure the IP address of the Radius Server, authentication (accounting) UDP port and the agreed password for the communication with the server.

In the privileged mode, you can set the communication between the device and the Radius Server via the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
radius-server host *ip-address* [**auth-port** *port*] [**acct-port** *port*]	Configure the RADIUS server
Radius-server key *string*	Configure RADIUS Key.
end	Return to the privileged mode.
write	Save the configuration.
show radius server	Show the RADIUS server.

You can execute the **no radius-server host** *ip-address* **auth-port** command to restore the authentication UDP port of the Radius Server to its default. You can execute the **no radius-server key** command to delete the authentication key of the Radius Server. The following example sets the Server IP to 192.168.4.12, authentication UDP port to 600, and the key to agreed password:

```
DGS-3610# configure terminal
DGS-3610(config)# radius-server host 192.168.4.12
DGS-3610(config)# radius-server host 192.168.4.12 auth-port 600
DGS-3610(config)# radius-server key MsdadShaAdasdj878dajL6g6ga
DGS-3610(config)# end
```

- The officially agreed authentication UDP port is 1812.
- The officially agreed accounting UDP port is 1813.
- No less than 16 characters are recommended for the agreed password between the device and the Radius Server.
- The port of the device to connect the Radius Server shall be configured as uncontrolled port.

37.2.4 Setting the 802.1X Authentication Switch

When the 802.1X authentication is enabled, the switch will impose authentication over the host connected to the controlled port, and the hosts that fail the authentication are not allowed to access the network.

In the privileged mode, you can enable the 1x authentication through the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
radius-server host *ip-address* [**auth-port** *port*] [**acct-port** *port*]	Configure the RADIUS server
Radius-server key string	Configure RADIUS Key.
aaa authentication dot1x *auth* **group radius**	Configure the dot1x authentication method list
dot1x authentication *auth*	dot1x applies authentication method list
end	Return to the privileged mode.
write	Save the configuration.
show running-config	Show the configuration.

The following example enables 802.1X authentication:

```
DGS-3610# configure terminal
DGS-3610(config)# aaa new-model
DGS-3610(config)# radius-server host 192.168.217.64
DGS-3610(config)# radius-server key starnet
```

```
DGS-3610(config)# aaa authentication dot1x authen group radius
DGS-3610(config)# dot1x authentication authen
DGS-3610(config)# end
DGS-3610# show running-config
!
aaa new-model
!
aaa authentication dot1x authen group radius
!
username DGS-3610 password 0 starnet
!
radius-server host 192.168.217.64
radius-server key 7 072d172e071c2211
!
!
!
dot1x authentication authen
!
interface VLAN 1
 ip address 192.168.217.222 255.255.255.0
 no shutdown
!
!
line con 0
line vty 0 4
!
end
```

To apply the RADIUS authentication method in the 802.1X, configure the IP address of the Radius Server and make sure normal communication between the device and the Radius Server. Without the coordination of the Radius Server, the device cannot perform authentication. For detailed settings of the communication between the Radius Server and the device, please see the previous section.

37.2.5 Enabling/Disabling the Authentication of a Port

If you enable authentication for a port when the 802.1X is enabled, the port becomes a controlled port, and the users under the port must first pass authentication before they can access the network. However, the users under the uncontrolled port can directly access the network.

In the privileged mode, you can set authentication for a port through the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
interface *interface*	Enter the interface configuration mode and specify the Interface to configure.

Command	Function
dot1x port-control auto	Set the port to be a controlled port (enable interface authentication). You can use the no option of the command to disable the authentication of the interface.
end	Return to the privileged mode.
write	Save the configuration.
show dot1x port-control	View the authentication configuration of the 802.1X interface.

You can use the **no dot1x port-control** command to disable the authentication of the interface. The following example sets Ethernet interface 1/1 to be a controlled interface:

```
DGS-3610# configure terminal
DGS-3610(config)# interface f 1/1
DGS-3610(config-if)# dot1x port-control auto
DGS-3610(config)# end
```

When a port is set as a controlled port, only the EAP packets are allowed to pass; the packets to the CPU are also under control.

37.2.6 Enabling Timing Re-authentication

The 802.1X can ask users for re-authentication periodically, to prevent pretending of authorized users. This can also detect disconnection, making more accurate charging. In addition to the re-authentication switch, you can also define the re-authentication interval, which is 3600 seconds by default. In the case of charging based on duration, you should determine the re-authentication interval according to the specific network size, which should be sufficient and accurate.

In the privileged mode, you can enable/disable re-authentication and set the re-authentication interval through the following steps.

Command	Function
configure terminal	Enter the global configuration mode.
dot1x re-authentication	Enable timing re-authentication.
dot1x timeout re-authperiod *seconds*	Set the re-authentication interval.
End	Return to the privileged mode.
Write	Save the configuration.
show dot1x	Show the dot1x configurations.

You can use the **no dot1x re-authentication** command to disable timing re-authentication, and use the **no dot1x timeout re-authperiod** command to restore the re-authentication interval to the default.

The following example enables re-authentication and sets the re-authentication interval to 1000 seconds.

```
DGS-3610# configure terminal
DGS-3610(config)# dot1x re-authentication
DGS-3610(config)# dot1x timeout re-authperiod 1000
DGS-3610(config)# end
DGS-3610# show dot1x
802.1X Status:          Disabled
Authentication Mode:    EAP-MD5
Authed User Number:     0
Re-authen Enabled:      Enabled
Re-authen Period:       1000 sec
Quiet Timer Period:     10 sec
Tx Timer Period:        3 sec
Supplicant Timeout:     3 sec
Server Timeout:         5 sec
Re-authen Max:          3 times
Maximum Request:        3 times
Client Oline Probe:     Disabled
Eapol Tag Enable:       Disabled
Authorization Mode:     Disabled
```

If re-authentication is enabled, please pay attention to the reasonableness of the re-authentication interval, which must be set according to the specific network size.

37.2.7 Changing the QUIET Time

When user authentication fails, the device does not allow that user to re-authenticate until a specified period passes, which is referred to as Quiet Period. This value functions to protect the device from malicious attacks. The default value of Quiet Period is set to 5 seconds.

A shorter Quiet Period may speed up re-authentication for users.

In the privileged mode, you can set the Quiet Period through the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
dot1x timeout quiet-period *seconds*	Set the Quiet Period.
end	Return to the privileged mode.
write	Save the configuration.
show dot1x	Show the dot1x configurations.

You can use the **no dot1x timeout quiet-period command to** restore the Quiet Period to its default.In the example below the QuietPeriod value is set to 500 seconds:

```
DGS-3610# configure terminal
DGS-3610(config)# dot1x timeout quiet-period 500
DGS-3610(config)# end
```

37.2.8 Setting the Packet Retransmission Interval

After the device sends the EAP-request/identity, it resends that message if no response is received from the user within a certain period. By default, this value is 3 seconds. You should modify this value to suit the specific network size.

In the privileged mode, you can set the packet retransmission interval through the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
dot1x timeout tx-period *seconds*	Setting the Packet Retransmission Interval
end	Return to the privileged mode.
write	Save the configuration.
show dot1x	Show the dot1x configurations.

You can use the **no dot1x timeout tx-period** to restore the packet re-transmission interval to its default. The following example sets the packet retransmission interval to 100 seconds:

```
DGS-3610# configure terminal
DGS-3610(config)# dot1x timeout tx-period 100
DGS-3610(config)# end
```

37.2.9 Setting the Maximum Number of Requests

If the device does not receive response within the ServerTimeout after it sends an authentication request to the Radius Server, it will retransmit the packets.The maximum number of requests indicates the maximum retransmission requests of the device.The authentication fails if this number is exceeded. By default, this value is 3. You should modify this value to suit the specific network size.

In the privileged mode, you can set the maximum number of retransmissions through the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
dot1x max-req *count*	Set the maximum number of packet re-transmissions.
end	Return to the privileged mode.
write	Save the configuration.
show dot1x	Show the dot1x configurations.

```
DGS-3610#show dot1x
```

You can use the **no dot1x max-req** command to restore the maximum number of packet re-transmissions to its default. The following example sets the maximum number of packet retransmissions to 5:

```
DGS-3610# configure terminal
DGS-3610(config)# dot1x max-req 5
DGS-3610(config)# end
```

37.2.10 Setting the Maximum Number of Re-authentications

When the user authentication fails, the device attempts to perform authentication for the user once again. When the number of attempts exceeds the maximum number of authentications, the device believes that this user is already disconnected, and ends the authentication process accordingly. By default, the number is 3. However, you can modify this value.

In the privileged mode, you can set the maximum number of re-authentications through the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
dot1x reauth-max *count*	Setting the Maximum Number of Re-authentications
end	Return to the privileged mode.
write	Save the configuration.
show dot1x	Show the dot1x configurations.

You can use the **no dot1x reauth-max** command to restore the maximum number of re-authentications to its default. The following example sets the maximum number of re-authentications to 3:

```
DGS-3610# configure terminal
DGS-3610(config)# dot1x reauth-max 3
DGS-3610(config)# end
DGS-3610#
```

37.2.11 Setting the Server-timeout

This value indicates the maximum response time of the Radius Server. If the switch does not receive the response from the Radius Server within this period, it deems the authentication as a failure.

In the privileged mode, you can set the Server-timeout and restore it to its default through the following steps:

Command	Function
configure terminal	Enter the global configuration mode.

Command	Function
dot1x timeout server-timeout *seconds*	Set the maximum response time of the Radius Server. You can use the no option of the command to restore it to its default.
end	Return to the privileged mode.
write	Save the configuration.
show dot1x	Show the dot1x configurations.

37.2.12 Configuring Acti ve Initiation of 802.1X Authentication

The 802.1X is security access authentication based on port. Users must first undergo authentication before they can access the network. In most cases, authentication is initiated on the user end through EAPOL-START packets. For the information about packet interaction during the authentication process, please see **Authentication Initiation and Packet Interaction During Authentication**.

However, authentication needs to be initiated by the device in some cases. Fro example, when the device is reset and the status of the authentication port changes from linkdown to linkup, the device needs to automatically initiate authentication to ensure that the authenticated users can continue to use the network. In addition, if you use an 802.1X client that does not actively initiate authentication requests (for example, the Windows XP 802.1X client), the device should be able to actively initiate authentication. The device forcedly asks all the users under the authentication port to authenticate by sending the EAP-request/identity multicast packets.

The following section describes how to configure active initiation of 802.1X authentication from the deviceand how you should configure appropriately in different application environments.

Turn on/off the switch for the active authentication initiation of the device

When this function is disabled, the device can only initiate an authentication request at resetting or when the status of the authentication port is changed. This ensures that the on-line users can continue to use the network. The device will not actively initiate an authentication request in any other cases. When this function is enabled, you can configure the times of automatic authentication initiation, authentication request interval, and whether to stop sending requests when the users pass the authentication.

In the privileged mode, you can enable automatic authentication through the following steps:

Command	Function
configure terminal	Enter the global configuration mode.

Command	**Function**
dot1x auto-req	Enable automatic authentication. It is disabled by default.
end	Return to the privileged mode.
write	Save the configuration.
show dot1x	Show the dot1x configurations.

The **no** option of the command turns off the function. The following settings take effect only when the function is enabled,. The user can set the number of active authentication requests initiated by the device, which can be determined according to the actual network environment.

In the privileged mode, you can set the number of automatic authentication requests through the following steps:

Command	**Function**
configure terminal	Enter the global configuration mode.
dot1x auto-req packet-num *num*	The device actively initiates num 802.1X authentication request packets. If num is equal to 0, the device will continually send that packet. The default is 0 (infinite).
end	Return to the privileged mode.
write	Save the configuration.
show dot1x auto-req	Show the configuration.

The **no** option of the command restores default. The following contents introduce how to configure the packet sent interval.

In the privileged mode, you can set the packet sending interval through the following steps:

Command	**Function**
configure terminal	Enter the global configuration mode.
dot1x auto-req req-interval *interval*	Setting the Packet Sending Interval
end	Return to the privileged mode.
write	Save the configuration.
show dot1x auto-req	Show the configuration.

The **no** option of the command restores default. Since sending the authentication request multicast packet will cause re-authentication for all users under the authentication interface, the sent interval shall not be too small lest the authentication efficiency is affected.

It is possible to set to the function of stopping sending the request packets when the user authentication passes. In some applications (only one user under a port, for example), we can stop sending authentication requests to the related port when the device finds the user authentication passes. If the user gets offline, the request is sent continually.

In the privileged mode, you can set this function through the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
dot1x auto-req user-detect	Stop sending the packets when there is some authentication user under the port. This function is enabled by default.
end	Return to the privileged mode.
write	Save the configuration.
show dot1x auto-req	Show the configuration.

The **no** option of the command disables the function. Before setting this function, take careful considerations on the current network application environment.

The above three commands provide you with flexible application strategies. You can select the appropriate configuration command according to the specific network application environment. To help you easily configure, the following configuration table is provided for your reference:

	Solution 1	Solution 2	Solution 3
User environment	One port for any user	One port for one user	One port for multiple users
Configuration command recommended	Not necessary to enable the dot1x auto-req function	**dot1x auto-req** **dot1x auto-req packet-num** *num* **dot1x auto-req req-interval** *interval* **dot1x auto-req user-detect**	**dot1x auto-req** **dot1x auto-req packet-num** *0* **dot1x auto-req req-interval** *interval* **no dot1x auto-req user-detect**

37.2.13 Configuring 802.1X Accounting

Our 802.1X has implemented the accounting function. Accounting is based on duration. In other words, the 802.1X records the length of the period between the first successful authentication of the user and the user's logoff or when the device detects user disconnection.

After the first successful authentication of the user, the device sends an accounting start request to the server. When the user gets off-line or the device finds that the user has got off line or when the physical connection of the user is broken, the device sends an accounting end request to the server. The server group records this information in the database of the server group. Based on such information, the NMS can provide the basis for accounting.

Our 802.1X stresses reliable accounting, and it specially supports the backup accounting server to avoid failures of the accounting server. When a server can no longer provide the accounting service due to various reasons, the device will automatically forward the accounting information to another backup server. This greatly improves the reliability of accounting.

When a user exits by itself, the accounting duration is accurate. When the connection of the user is broken by accident, the accounting accuracy depends on the re-authentication interval (the device detects the disconnection of a user by using the re-authentication mechanism).

To enable the accounting function of the device, the following settings are necessary on the device:

1. On the Radius Server, register the device as a Radius Client, like the authentication operation.
2. Set the IP address of the accounting server.
3. Set the accounting UDP port.
4. Enable the accounting service on the precondition that the 802.1X has been enabled.

In the privileged mode, you can set the accounting service through the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Enable the AAA function
aaa group server radius *gs*	Configure the accounting server group.
server *192.168.4.12* **acct-port** *11*	Add a server to the server group.
exit	Return to the global configuration mode.
aaa accounting network *acct* **start-stop group** *gs*	Configure the accounting method list.
dot1x accounting *acct*	Apply the accounting method list for the 802.1X.
end	Return to the privileged mode.
write	Save the configuration.
show running-config	Show the configuration.

The **no aaa accounting network** command deletes the accounting method list. The **no dot1x accounting** command restores the default dot1x accounting method. The following example sets the IP address of the accounting server to 192.1.1.1, that of the backup accounting server to 192.1.1.2, and the UDP port of the accounting server to 1200, and enables 802.1X accounting:

```
DGS-3610# configure terminal
DGS-3610(config)# aaa new-model
DGS-3610(config)# aaa group server radius acct-use
DGS-3610(config-gs-radius)# server 192.168.4.12 acct-port 1200
DGS-3610(config-gs-radius)# server 192.168.4.13 acct-port 1200
DGS-3610(config-gs-radius)# exit
DGS-3610(config)# aaa accounting network acct-list start-stop group acct-use
DGS-3610(config)# dot1x accounting acct-list
DGS-3610(config)# end
DGS-3610# write memory
DGS-3610# show running-config
```

Caution

1. The accounting key must be agreed with the Radius Server, the same as that of authentication.
2. The accounting function cannot be enabled unless the AAA is enabled.
3. The accounting is impossible unless the 802.1X authentication passes.
4. By default, the accounting function of the 802.1X is disabled.
5. For the database format of accounting, see the related Radius Server documentation.

Also, the account update is supported. After the account update interval is set on the NAS device, the NAS device will send account update packets to the Radius Server periodically. On the Radius Server, you can define the number of periods before which the account update packet of a user is not received from the NAS device, the NAS or user will be regarded as off-line. Then, the Radius Server can stop the accounting of the user, and delete the user from the on-line user table.

In the privileged mode, you can set the account update function through the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Enable the AAA function
aaa accounting update	Set the account update function.
end	Return to the privileged mode.
write	Save the configuration.
show running-config	Show the configuration.

You can disable the account update service by executing the **no aaa accounting update** command.

```
DGS-3610# configure terminal
DGS-3610(config)# aaa accounting update
DGS-3610(config)# end
DGS-3610# write memory
DGS-3610# show running-config
```

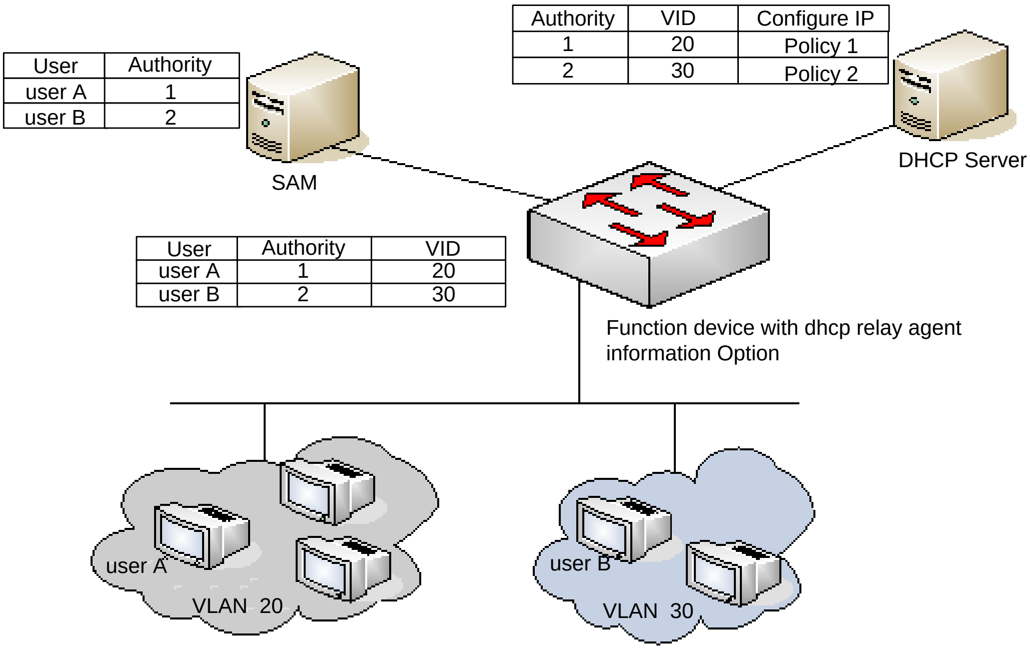
37.2.14 Configuring IP Authorization Modes

The 802.1X implemented on DGS-3610 series can force the authenticated users to use fixed IP. By configuring the IP authorization mode, the administrator can limit the way the user gets IP address. There are four IP authorization modes: DISABLE, DHCP SERVER, RADIUS SERVER and SUPPLICANT. There are detailed below respectively:

DISABLE mode (default): The device has no limitation for the user IP, and the user only needs to pass the authentication to be able to access the network.

DHCP SERVER mode: The user IP is obtained via specified DHCP SERVER, and only the IP allocated by the specified DHCP SERVER is considered legal. For the DHCP mode, it is possible to use DHCP relay option82 to implement a more flexible IP allocation policy with the 802.1X. Here is a typical diagram for the plan:

Figure 37-5



User	Authority
user A	1
user B	2

Authority	VID	Configure IP
1	20	Policy 1
2	30	Policy 2

User	Authority	VID
user A	1	20
user B	2	30

The user initiates IP requests via the DHCP Client. The network device with dhcp relay option82 converges the user authority on the SAM server to construct the option82 field and encapsulate it in the DHCP request packet. That option82 field consists of “vid + permission”. The DHCP Server chooses different allocation policies by using the option82 field.

In this mode, it is required to configure the DHCP Relay and the related option82. If the DHCP relay function is enabled and the option82 policy is selected, see the *DHCP Relay Configuration Guide and Command References* for the configurations.

RADIUS SERVER mode: The user IP is specified by the RADIUS SERVER. The user can only use the IP specified by the RADIUS SERVER to be able to access the network.

SUPPLICANT mode: The IP bound to the user is the IP of the PC during the SUPPLICANT's authentication. After the authentication, the user can only use that IP to be able to access the network.

The application models in the four modes are as follows:

- DISABLE mode: Suitable for the environment with no limits for the users. The user can access the network once he/she passes the authentication.
- DHCP SERVER mode: The user PC gets the IP address via DHCP. The administrator configures the DHCP RELAY of the device to limit the DHCP SERVER that the users can access. In this way, only the IPs allocated by the specified DHCP SERVER are legal.
- RADIUS SERVER mode: The user PC uses fixed IP. The RADIUS SERVER is configured with <user-IP> mapping relations that are notified to the device via the Framed-IP-Address attributes of the device. The user has to use that IP to be able to access the network.
- SUPPLICANT mode: The user PC uses fixed IP. The SUPPLICANT notifies the device of the information. The user has to use the IP during authentication to be able to access the network.

Caution

When a user switches modes, it will cause offline of all authenticated users. So, it is recommended to configure the authentication mode before use.

In the privileged mode, configure the IP authorization mode as follows:

Command	**Function**
configure terminal	Enter the global configuration mode.
aaa new-model	Enable the AAA function
aaa authorization ip-auth-mode {disabled | dhcp-server | radius-server | supplicant }	Configure the IP authorization mode
end	Return to the privileged mode.
write	Save the configuration.
show running-config	Show the configuration.

The example below configures the IP authorization mode as the RADIUS-SERVER mode:

```
DGS-3610# configure terminal
DGS-3610(config)# aaa authorization ip-auth-mode radius-server
```

```
DGS-3610(config)# end
DGS-3610# show running-config
!
aaa new-model
!
aaa authorization ip-auth-mode radius-server
!
DGS-3610# write memory
```

37.2.15 Releasing Advertisement

Our 802.1X allows you to configure the Reply-Packet field on the Radius Server. When authorization succeeds, the information of the field is shown on our 802.1X client of Star-Supplicant, by which the operators can release some information.

Such information is shown during the first authorization of the user, but not during re-authentication. This avoids frequently disturbing the user.

The window for showing the advertisement information supports html, which converts the http://XXX.XXX.XX in the packet into links capable of direct switching, for easier browsing.

Releasing of the advertising information:

1. The operator configures the Reply Packet attribute on the Radius Server end.
2. Only our Star-supplicant client supports such information (free for the users of our switch), while other clients cannot see the information, which however does not affect their normal use.
3. No setting is required at the device end.

37.2.16 List of Authenticable Hosts under a Port

To enhance the security of the 802.1X, we have made expansion without affecting the IEEE 802.1X, allowing the NM to restrict the list of hosts authenticated of a port. If the list of hosts authenticated of a port is empty, any user can be authenticated. If the list is not empty, only the hosts in the list can be authenticated. The hosts that can be authenticated are identified by using the MAC addresses.

The following example adds/deletes the hosts that can be authenticated under a port.

Command	Function
configure terminal	Enter the global configuration mode.
dot1x auth-address-table address *mac-addr* **interface** *interface*	Set the list of the hosts that can be authenticated.
end	Return to the privileged mode.
write	Save the configuration.

Command	Function
show running-config	Show the configuration.

Caution

If the list of the host is empty, the port allows any host authentication.

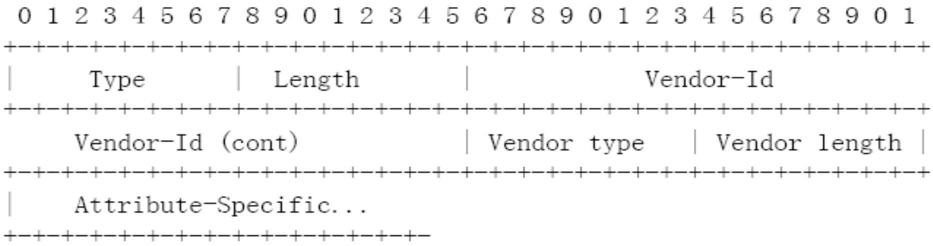
37.2.17 Authorization

To make it easier for operators, our products can provide services of different qualities for different types of services, for example, offering different maximum bandwidths. Such information is all stored on the Radius Server, and the administrator does not need to configure every device.

Since the Radius has no standard attribute to represent the maximum data rate, we can only transfer the authorization information through the manufacturer customized attributes.

The general format of the definition is as follows:

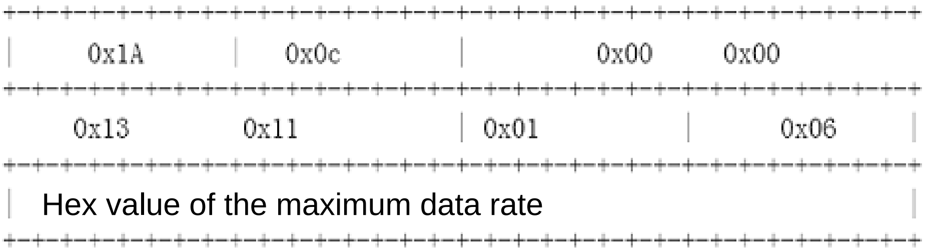
Figure 37-6



```
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |  Length       |            Vendor-Id
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     Vendor-Id (cont)           | Vendor type   | Vendor length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Attribute-Specific...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

For the maximum data rate, you need to fill in the following values:

Figure 37-7

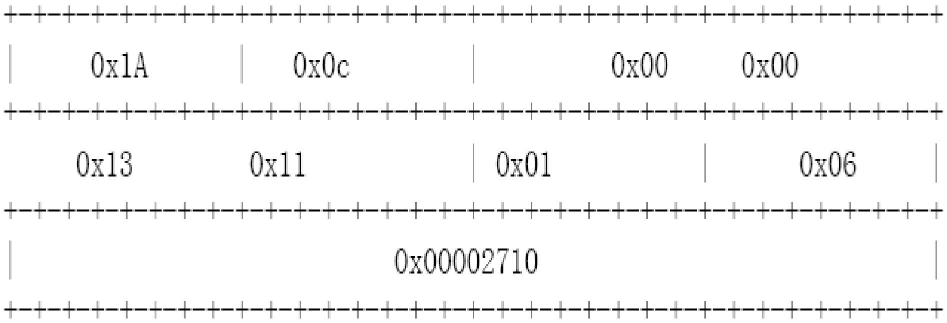


```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     0x1A      |  0x0c         |          0x00      0x00
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     0x13         0x11          | 0x01          |     0x06      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Hex value of the maximum data rate                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The unit of the maximum data rate is kbps.

For users with the maximum data rate of 10M, you need to fill in the following values:

Figure 37-8



```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     0x1A      |    0x0c       |         0x00     0x00
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     0x13          0x11         | 0x01          |      0x06      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           0x00002710                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

For the customized header, follow those provided above. The maximum data rate is 10M, that is, 10000kbsp, and makes 0x00002710 in the Hex system. You only need to fill in the corresponding field.

This function calls for no settings on the device end, and works as long as the device end supports authorization.

37.2.18 Configuring Authentication Modes

In the standard, the 802.1X implements authentication through the EAP-MD5. The 802.1X designed on DGS-3610 series can perform authentication through both the EAP-MD5 (default) mode and the CHAP and PAP mode. The advantage of the CHAP is that it reduces the communication between the device and the RADIUS SERVER, thus alleviating the pressure on the RADIUS SERVER. Same as the CHAP mode, the communication between the PAP and RADIUS SERVER occurs only once. Although the PAP mode is not recommended for its poor security, it can meet the special needs of the user in some cases. For example, when the security server only supports the PAP authentication mode, this mode can be selected to fully exploit the existing resources, protecting the existing investment.

In the privileged mode, you can set the authentication mode of the 802.1X through the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
dot1x auth-mode mode	Configure the authentication mode
end	Return to the privileged mode.
write	Save the configuration.
show dot1x	Show the configuration.

The following example configures the authentication mode to the CHAP mode:

```
DGS-3610# configure terminal
DGS-3610(config)# dot1x auth-mode CHAP
```

```
DGS-3610(config)# end
DGS-3610# show dot1x
802.1X Status:        Disabled
Authentication Mode:  CHAP
Authed User Number:   0
Re-authen Enabled:    Disabled
Re-authen Period:     3600 sec
Quiet Timer Period:   10 sec
Tx Timer Period:      3 sec
Supplicant Timeout:   3 sec
Server Timeout:       5 sec
Re-authen Max:        3 times
Maximum Request:      3 times
Client Oline Probe:   Disabled
Eapol Tag Enable:     Disabled
Authorization Mode:   Group Server
```

37.2.19 Configuring the Backup Authentication Server.

Our 802.1X-based authentication system can support the backup server. When the master server is down due to various reasons, the device automatically issues a server submission authentication request to the method list server group.

In the privileged mode, you can set the backup authentication server through the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
aaa group server radius *gs-name*	Configure the server group.
server sever	Configure the server.
server server-backup	Configure the backup server.
end	Return to the privileged mode.
write	Save the configuration.
show dot1x	Show the configuration.

The following example configures 192.168.4.12 to be the backup server:

```
DGS-3610# configure terminal
DGS-3610# aaa new-model
DGS-3610(config)# aaa group server radius auth-ll
DGS-3610(config-gs-radius)# server 192.168.4.1
DGS-3610(config-gs-radius)# server 192.168.4.12
DGS-3610(config-gs-radius)# end
DGS-3610#
```

37.2.20 Configuring and Managing Online Users

DGS-3610 series provides management for authenticated users via SNMP. The administrator can view the information of the authorized users via SNMP, and forcedly log off a user. The user forcedly logged off must pass the authentication again before it can use network resources.

This function calls for no configuration on the device.

37.2.21 Implementing User-IP Binding

With our clients and the correctly configured Radius Server, you can implement unique user-IP binding. A user must undergo authentication by using the IP address allocated by the administrator. Otherwise, authentication will fail.

For this function, you do not need to configure the device. The user needs to use our client and the administrator needs to configure the Radius Server.

37.2.22 Port-based Traffic Charging

In addition to the duration-based billing, DGS-3610 series provide the traffic-based billing function when each port of the equipment has only one user access.

This function calls for no configuration on the device but need the support of the Radius server.

37.2.23 Implementing Automatic Jumping and Control of VLAN

If “down VLAN” of a user is set on the Radius server, the Radius server will notify the device via the manufacturer-defined attribute. DGS-3610 series automatically jumps the VLAN of the port connected with the user into the VID configured on the Radius server, and the administrator need not any manual configuration on the device. You can view the real VLAN of the user with the **show dot1x summary** command.

Follow these steps to configure a port to allow dynamic VLAN jump:

Command	Function
configure terminal	Enter the global configuration mode.
interface *interface*	Enter the interface configuration mode.
[no] dot1x dynamic-vlan enable	Configure whether to allow dynamic vlan jumping, which is disabled by default.
end	Return to the privileged mode.
write	Save the configuration.

Command	Function
show dot1x	Show the configuration.

37.2.24 Shielding Proxy Server and Dial-up

The two major potential threats to network security are: The user sets its own proxy server and the user makes dial-up to access the network after authentication. DGS-3610 series provide the function of shielding proxy servers and dial-up connections.

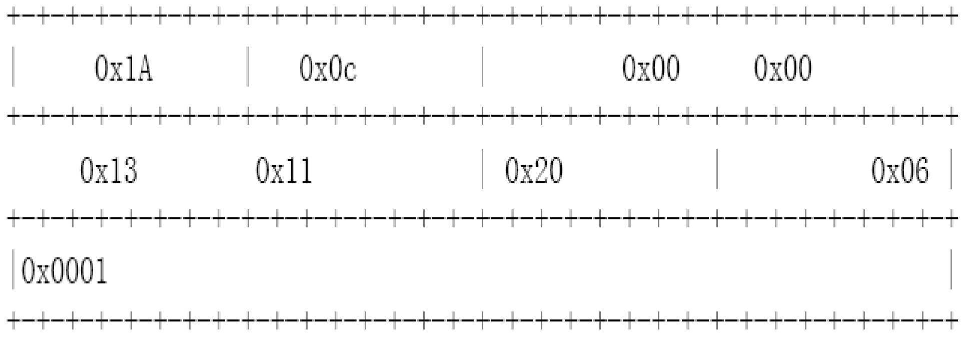
To implement this function, no setting is needed on the device endand it only needs the corresponding attributes configured on the Radius server end. Since the Radius has no standard attributes to indicate the maximum data rate, we can transfer the authorization information only through the manufacturer-defined attributes. For the general format defined, see the Authorization section.

The proxy server shielding function defines the Vendor type of 0x20, and the dial-up shielding function defines the Vendor type of 0x21.

The Attribute-Specific field is a 4-byte manufacturer defined attribute, which defines the actions taken against proxy server access and dial-up access. 0x0000 means normal connection, without shielding detection. 0x0001 means shielding detection.

To shield the access via the proxy server, you should fill in the following information:

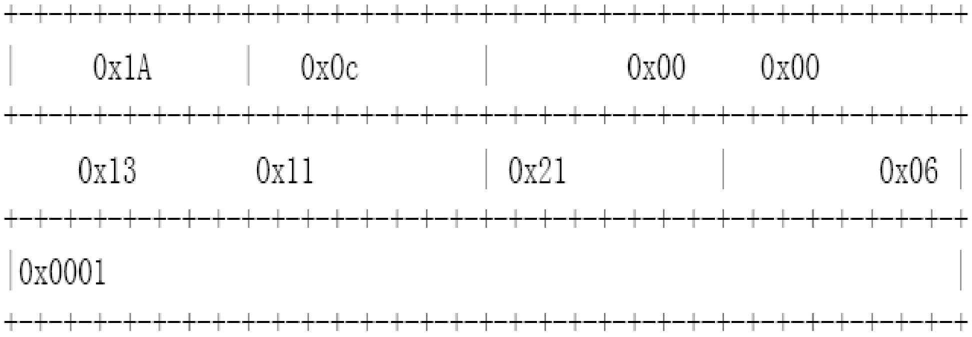
Figure 37-9



```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     0x1A      |  0x0c         |         0x00      0x00
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     0x13          0x11         | 0x20          |           0x06 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0x0001                                                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

To shield the access via the dial-up connection, you should fill in the following information:

Figure 37-10



```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     0x1A      |   0x0c        |          0x00      0x00
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     0x13          0x11         | 0x21           |          0x06 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0x0001                                                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

37.2.25 Configuring On-line Client Probe

To ensure accurate charging, an on-line probe mechanism is needed to detect whether a user is on-line within a short period. The re-authentication mechanism specified in the standard can meet such needs, but it needs the participation of the RADIUS server. Accurate user probe will occupy enormous resources of the device and RADIUS server. To meet the need to implement accurate charging with fewer resources occupied, we use a new client on-line probe mechanism. Such mechanism only needs interaction between the device and client and occupies little network traffic, and it implements minute-level charging accuracy (you can set the charging accuracy).

⚠ **Caution**

To implement on-site monitoring of the client, the client software must support this function.

The following two timers affect the performance and accuracy of on-line probe:

- Hello Interval: It is the interval at which the client sends an advertisement.
- Alive Interval: Client online interval. If the device has not received the client advertisement during this interval, it actively disconnects the client and notifies the billing server. The interval must be greater than the Hello Interval.

In the privileged mode, you can configure the on-line probe function of the client through the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
dot1x client-probe enable	Enable the on-line probe function of the client
dot1x probe-timer interval *interval*	Configure the Hello Interval
dot1x probe-timer alive interval	Configure the Alive Interval of the device.
end	Return to the privileged mode.
write	Save the configuration.

Command	Function
show dot1x	Show the configuration.

37.2.26 Configuring the Option Flag for EAPOL Frames to Carry TAG

In accordance with IEEE 802.1X, the EAPOL packets cannot be added with VLAN TAG. However, based on the possible application requirements, the selection flag is provided. When the flag is turned on, tags can be output according to the related output rule of the trunk ports.

The typical application environment is to enable 802.1X authentication on the convergence layer. For more information, see **Topologies of Typical Applications**.

In the privileged mode, you can configure the flag for EAPOL frames to carry TAG through the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
dot1x eapol-tag	Enable the flag for EAPOL frames to carry TAG. By default, the function is disabled.
end	Return to the privileged mode.
write	Save the configuration.
show dot1x	Show the configuration.

You can disable this function by executing the **no dot1x eapol-tag** command.

37.2.27 Configuring the Port-Based User Authentication

The 802.1X user access control is based on the MAC by default. Only the authenticated user can use the network. Other users connecting to the same port cannot access the network. In the port-based authentication, however, after a user connecting to a port is authenticated, this port is an authenticated port and all users connecting to the port can access the network.

To configure the control mode of a port to the port-based control mode, perform following configuration step by step from the privileged mode.

Command	Function
interface *<interface-id***>**	Enter the interface mode
configure terminal	Enter the global configuration mode.
dot1x port-control auto	Enable the function being controlled

Command	Function
dot1x port-control-mode *{mac-based|port-based***}**	Select the controlled mode
End	Return to the privileged mode.
Write	Save the configuration
show dot1x port-control	Show the configuration of port 802.1X

You can run **no dot1x port-control-mode** to restore to the default control mode.

The following example shows how to configure the authentication mode of a port

```
DGS-3610(config)#
DGS-3610#configure terminal
DGS-3610(config)#dot1x port-control-mode port-base
```

Caution

In the port-based authentication mode, a port can be connected with only one authenticated user.

In the port-based authentication mode, you can enable or disable the dynamic users to migrate among the authenticated ports. By default, the migration is allowed. To prohibit the migration, runt the following commands one by one in the privileged mode.

Command	Function
configure terminal	Enter the global configuration mode.
dot1x stationarity enable	Disable the migration among ports.
end	Exit to the privileged mode.
Write	Save the configuration.

37.3 Viewing the Configuration and Current Statistics of the 802.1X

Our 802.1X provides a full range of state machine information, which is very useful for network management and can be used by the administrator to monitor user status in real time and make easy troubleshooting.

- Viewing the Radius Authentication and Accounting Configuration
- Viewing the Number of Current Users
- Viewing the List of the Addresses Authenticable
- Viewing the User Authentication Status Information
- Showing the 1x Client Probe Time Configuration

37.3.1 Viewing the Radius Authentication and Accounting Configuration

Run the **show radius server** command to check the related configuration of the Radius Sever, and run the **show aaa user** command to view the user-related information.

```
DGS-3610# sh radius server
Server IP:       192.168.5.11
Accounting Port: 1813
Authen  Port:    1812
Server State:    Ready
```

37.3.2 Viewing the Number of Current Users

Our 802.1X allows you to view the numbers of two types of users: one is the number of current users, and the other is that of the authorized users. The number of current users refers to the total number of users authenticated (whether successfully or unsuccessfully), while the number of authorized users means the total number of users authorized.

In the privileged mode, run the **show dot1x** command to check the current number of users and authenticated users, 1x configuration, including the current number of users and authenticated users.

The following example shows the 802.1X configuration:

```
DGS-3610# show dot1x
802.1X Status:         Disabled
Authentication Mode:   EAP-MD5
Authed User Number:    0
Re-authen Enabled:     Disabled
Re-authen Period:      3600 sec
Quiet Timer Period:    10 sec
Tx Timer Period:       3 sec
Supplicant Timeout:    3 sec
Server Timeout:        5 sec
Re-authen Max:         3 times
Maximum Request:       3 times
Client Oline Probe:    Disabled
Eapol Tag Enable:      Disabled
Authorization Mode:    Disabled
```

37.3.3 Viewing the List of the Authenticable Addresses

Our 802.1X has expanded functions that allow you to set the hosts that can be authenticated on a particular port. This function allows the administrator to view the currently available settings.

In the privileged mode, you can view the list of hosts authenticable through the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
dot1x auth-address-table address *mac-addr* **interface** *interface*	Set the list of the hosts that can be authenticated.
end	Return to the privileged mode.
write	Save the configuration.
show dot1x auth-address-table	Show the list of the hosts that can be authenticated.

Use the **no dot1x auth-address-table address** command to delete the specified authenticable host list. The following example shows the list of the hosts that can be authenticated.

```
DGS-3610# show dot1x auth-address-table
interface:g3/1
-----------------------------------
mac addr: 00D0.F800.0001
```

37.3.4 Viewing the User Authentication Status Information

The administrator can view the authentication status of the current users of the switch for easier troubleshooting.

In the privileged mode, you can view the user authentication status information through the following steps:

Command	Function
show dot1x summary	Viewing the user authentication status information

The following example shows the user authentication status information.

```
DGS-3610# show dot1x summary
 ID   MAC       Interface  VLAN  Auth-State  Backend-State Port-Status
---- ----------- --------- ----  ----------  ------------   -----------
1   00d0f8000001 Gi3/1     1   Authenticated  IDLE       Authed
```

37.3.5 Showing the 1x Client Probe Timer Configuration

In the privileged mode, you can view the 1x timer setting through the following steps:

Command	Function
show dot1x probe-timer	Show the 1X timer setting

The following example shows the 1.1x timer setting:

```
DGS-3610# show dot1x probe-timer
```

```
Hello Interval: 20 Seconds
Hello Alive: 250 Seconds
DGS-3610#
```

37.3.6 Other Precautions for Configuring 802.1X

1. When there is no IP authorization mode, each device supports 10,000 authenticated users.

2. Concurrent use of 1X and ACL

   In the non-IP authorization mode, if you enable the 802.1X authentication function of a port and at the same time associate one ACL with an interface, the ACL takes effect on the basis of the MAC address. In other words, only the packets from the source MAC addresses of the users that have passed the authentication can pass ACL filtering, and the packets from other source MAC addresses will be discarded. The ACL can only work on the basis of the MAC address.

   For example, if the MAC address that has passed the authentication is 00d0.f800.0001, then all the packets from the source MAC address of 00d0.f800.0001 can be switched. If the port is associated with an ACL, the ACL will further filter these packets that can be switched, for example, rejecting the ICMP packets from the source MAC address.

   In the IP authorization mode, you are recommended not to set the ACL on the controlled interface, since the ACL has a higher priority than the authentication user, and so the IP+MAC binding that has passed the authentication will not take effect. On a port, the following users are authenticated:

   User 1: mac: 00d0.f800.0001 ip: 192.168.65.100

   User 2: mac: 00d0.f800.0002 ip: 192.168.65.101

   Then, set one ACL on the interface as follows:

   ip access-list extended ip_acl:

   deny icmp any any

   The original purpose is to allow the communication of authenticated users and forbid sending ICMP packets. However, the ACL has a higher priority than the IP + MAC that has passed the authentication and the last default ACE of the ACL is **deny any any**, so the authenticated users cannot communicate.

   If the **ip_acl** is added with **permit any any** behind it, any authenticated users can still communicate after changing its IP address, so the IP + MAC one-to-one binding is not achieved. Therefore, IP authentication + ACL is not recommended.

3. The hardware entries for user authentication and the other applications (for example, ACL, port IP security address) share the filtering entries and filtering domain templates in the IP authentication mode. If other applications exhaust the hardware resources, the user authentication may fail in the IP authorization mode, or though successful, the

users cannot communicate. For the filtering domain templates in particular, at least one must be available for user authentication in the IP authentication mode.

AAA Configuration

The access control is used to control specific users who can access the network server and specific services that the users can access on the network. The authentication, authorization and accounting (AAA) is a key security mechanism for access control.

37.4 Basic AAA Principles

Authentication, Authorization and Accounting (short for AAA) provide a consistence framework for configuring the authentication, authorization and accounting functions, which are supported by DGS-3610 series.

The AAA provides the following services in a modular manner:

- Authentication:It verifies whether a user can access the network, where the Radius protocol or Local can be used. The authentication is the method to identify a user before his/her access to the network and network services. The AAA is configured by the definition of a naming list for authentication method and its application on every interface.The method list defines the authentication type and execution order. Before a defined authentication is executed, the method list must be applied on a specific interface. The default method list is exceptional. If no other method list is defined, the default method list will automatically apply on all interfaces. The defined method list overwrites the default method list. All authentication methods other than the local, line password and allowing authentication must be defined with AAA.
- Authorization: This means authorizing the user with services. The AAA authorization is implemented through the definition of attribute pairs that describe the operations on the user by the authorization. These attributes can be stored on the network device or the RADIUS security server remotely. All authorization methods must be defined with AAA. When the AAA authorization is enabled, it is automatically applied on all interfaces of the network device.
- Accounting: This means recording the user's usage of network resources. When the AAA accounting is enabled, the network access server starts to send the user's network resource usages to the Radius security server through statistics records. Every accounting record is composed of attribute pairs and stored in the security server. These records can be read for analysis by special software to implement the accounting, statistics and tracing for the user's network resource usage. All accounting methods must be defined with AAA. When the AAA accounting is enabled, it is automatically applied on all interfaces of the network device.

Note

The AAA of some products only provides the authentication function. For all problems with product specifications, contact the market or technical support personnel of D-Link Cooporation.

Although the AAA is the primary access control method, our product also provides simple control accesses out of the range of AAA, such as the local username authentication, line password authentication and more. The difference lies in the degree of their network protection, and the AAA provides the security protection of a higher level.

The AAA has the following advantages:

- Powerful flexibility and controllability
- Expandability
- Standardized authentication
- Multiple backup systems

37.4.1 Basic AAA Principles

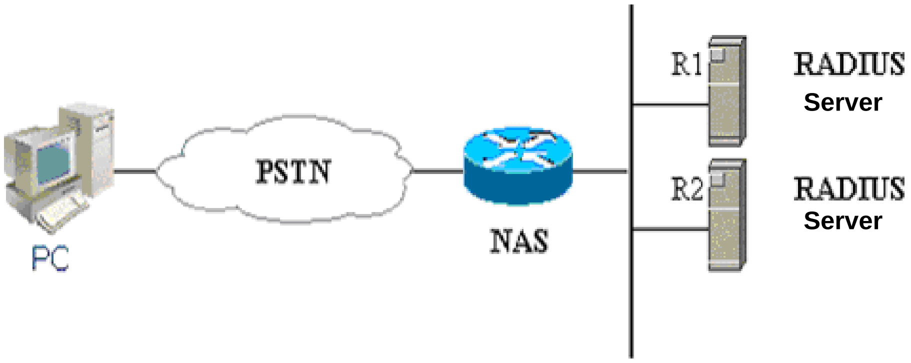
The AAA can configure dynamically authentication, authorization and accounting for a single user (line) or server. It defines the authentication, authorization and accounting by means of creating method lists and then applies them on specific services or interfaces.

37.4.2 Method List

Since the authentication for users can be implemented in a variety of ways, you need to use the method list to define the sequence of using different methods to perform authentication for the users. The method list can define one or more security protocols for authentication, so that there are backup systems available for the authentication in case of the failure of the first method. Our product works with the first method in the method list for user authentication, and then selects the next method in the method list in case of no reply from that method. This process goes on till an authentication method listed successfully allows communication or all methods listed are used up. If all methods listed are used up but the communication is not allowed, it declares failure of authentication.

Caution Our product will try the next method only when there is no reply from a method. During the authentication, if the user access is refused by a method, the authentication process ends and no other methods will be attempted.

Figure 37-11 A typical AAA network configuration



The figure above illustrates a typical AAA network configuration, including two security servers: R1 and R2 are both RADIUS servers.

Suppose the system administrator has defined a method list, R1 is used first to capture the identity information, then R2, and finally the local username database on the NAS. If a remote PC user attempts to access the network via dial-up, the NAS first queries the authentication information from R1. If the user passes the authentication on R1, R1 sends a SUCCESS reply to the NAS, and thus the user's access to the network is allowed. If R1 returns FAIL reply, the user's access is refused and the disconnected. If R1 has no reply, the NAS regards it as ERROR and queries authentication information from R2. This process continues for the remaining methods till the user passes the authentication or is refused or the session is terminated. If ERROR is returned for all methods, the authentication fails and the user is disconnected.

⚠ **Caution**	The REJECT response is not the same as the TIMEOUT response. REJECT means the user fails to comply with the standard in the available authentication database and does not pass the authentication, thus the access request will be refused. TIMEOUT means there is no reply from the security server to the authentication. When a TIMEOUT is detected, the AAA selects the next authentication method in the method list to continue the authentication process.

37.5 Basic AAA Configuration Steps

First you must choose a security solution, evaluate the potential security risks in the specific network and select the proper measures to prevent unauthorized accesses. For the security risk evaluation and the possible security solutions, see Chapter 2, **Security Overview**. We recommend the use of AAA as much as possible to guarantee network security.

37.5.1 Overview of AAA Configuration Steps

The AAA configuration may become simple when the basic operation process of AAA is understood.On DGS-3610 series, the AAA is configured through the following steps:

1. Enable AAA with the global configuration command **aaa new-model**.
2. Configure the security protocol parameters if you decide to use the security server, such as RADIUS.
3. Define the authentication method list by using the **aaa authentication** command.
4. Apply the method list on specific interface or line, if necessary.

⚠ **Caution**	When the specific method list is applied, the default authentication method list is applied if no named method list is clearly specified. As a result, if you do not want to use the default authentication method list, you shall specify a specific method list.

For complete descriptions of the commands mentioned in this chapter, see the related chapters in the *Security Configuration Command Reference*.

37.5.2 Enabling AAA

It is required to enable AAA first to use the AAA security features.

To enable AAA, execute the following command in the global configuration mode:

Command	Function
DGS-3610(config)# **aaa new-model**	Enable AAA

37.5.3 Disabling AAA

To disable AAA, execute the following command in the global configuration mode:

Command	Function
DGS-3610(config)# **no aaa new-model**	Disable AAA

37.5.4 Subsequent Configuration Steps

After the AAA is enabled, you can configure the other parts related with the selected security solutions. The following table lists the possible configuration tasks and their description chapters.

Methods of AAA access control security solution

Configuration task	Step	Chapter
Configuring Local Login Authentication	3	Configuring authentication
Defining AAA Authentication Method List	3	Configuring authentication
Applying Method List on Specific Interface or Line	4	Configuring authentication
Configuring Radius Security Protocol Parameters	2	Configuring Radius
Enabling Radius Authorization	5	Configuring authorization

If you are using AAA for authentication, see **Configuring Authentication**.

37.6 Configuring Authentication

ID authentication means a user is authenticated before the use of network resources. In most cases, the authentication is implemented with the AAA security features. We recommend the use of AAA.

37.6.1 Defining AAA Authentication Method List

To configure the AAA authentication, the first step is to define a named list of the authentication method, and then the applications use the defined list for authentication. The method list defines the authentication type and execution order. The defined authentication methods must be applied on specific interfaces before they can be executed. The default method list is exceptional.When not configured, all applications will use the default method list.

The method list is just a list to define the authentication method to be queried in turn to verify the user identity. The method list can define one or more security protocols for authentication, so that there are backup systems available for the authentication in case of failure of the first method. Our product works with the first method in the method list for user authentication, and then selects the next method in the method list in case of no reply from that method. This process goes on till an authentication method successfully allows communication or all methods are used up. If all listed methods are used up but the communication is not allowed, it declares failure of authentication.

Caution

Our product will try the next method only when there is no reply from a method. During the authentication, if the user access is refused by a method, the authentication process ends and no other methods will be attempted.

37.6.2 Example of Method List

In a typical AAA network configuration, there are two servers: R1 and R2 are both RADIUS servers. Suppose the network administrator has chosen a security solution, and the NAS authentication uses an authentication method to authenticate the Telnet connection: First, R1 is used for user authentication. In case of no reply, R2 will be used. If there is no reply from both R1 and R2, the local database of the access server will perform the authentication. To configure the above authentication list, run the following commands:

Command	Function
configure terminal	Enter the global configuration mode.
aaa authentication login default group radius local	Configure a default authentication method list, where "default" is the name of the method list. The protocols included in this method list are listed behind the name in the order by which they will be queried. The default method list is applied on all applications.

If the system administrator hopes to apply this method list on a specific *Login connection*, he/she must create a named method list and then apply it on the specific connection. The example below shows how to apply the authentication method list on line 2 only.

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
aaa authentication login test group radius local	Define a method list named "test" in the global configuration mode.
DGS-3610(config)# **line vty** *2*	Enter the configuration layer of line 2
DGS-3610(config-line)# **login authentication** *test*	In the line configuration mode, apply the method list named “test” on the line.

If a remote PC user attempts to access the network (NAS) through Telnet, the NAS first queries the authentication information from R1. If the user passes the authentication on R1, R1 sends an ACCEPT reply to the NAS, and then the access is allowed. If R1 returns the REJECT reply, the access is refused and then disconnected. If R1 does not respond, NAS considers TIMEOUT and queries the authentication information from R2. This process continues for the remaining methods till the user passes the authentication or is refused or the session is terminated.If all servers (R1 and R2) return TIMEOUT, the authentication will be performed by the NAS local database.

Caution

The REJECT response differs from the TIMEOUT response. REJECT means the user fails to comply with the standard in the available authentication database and does not pass the authentication, thus the access request is refused. TIMEOUT means there is no reply from the security server to the authentication. When an TIMEOUT reply is detected, the AAA selects the next authentication method in the method list to continue the authentication process.

37.6.3 General Steps in Configuring AAA Authentication

The following tasks are common for the configuration of AAA authentication.

- Enable AAA by using the global configuration command **aaa new-model**.
- Configure the security protocol parameters if you decide to use the security server, such as RADIUS. See **Configuring Radius** for details.
- Define the authentication method list by using the **aaa authentication** command.
- Applying method list on a specific interface or line, if possible.

37.6.4 Configuring the AAA Line Authentication

This section describes how to configure the AAA authentication methods supported by our product:

Caution The AAA security features are available for your configuration only after the AAA is enabled through the command **aaa new-model** in the global configuration mode. For details, see **AAA Overview**.

In many cases, the user needs to access the network access server (NAS) through Telnet. Once such a connection is set up, it is possible to configure NAS remotely. To prevent unauthorized accesses to the network, it is required to perform authentication on the user identity.

The AAA security services make it easy for the network devices to perform line-based authentication. No matter which line authentication method you decide to use, you just need to execute the **aaa authentication login** command to define one or more authentication method lists and apply it on the specific line that need the line authentication.

To configure the AAA PPP authentication, execute the following command in the global configuration mode:

Command	Function
configure	terminal
aaa new-model	Enable AAA.
aaa authentication login {**default** |*list-name} method1 [method2...]*	Define an accounting method list, or repeat this command to define more.
line vty *line-num*	Enter the line that needs to apply the AAA authentication.
login authentication {**default**|*list-name*}	Apply the method list on the line.

The keyword "list-name" is used to name the created authentication method list, which can be any string of characters. The keyword "method" means the actual algorithm for authentication. The next authentication method is attempted only when the current method returns ERROR (no reply). If the current method returns FAIL, no authentication method will be used any more. To make the authentication return successfully, even if no specified method has reply, it is possible to specify **none** as the last authentication method.

In the example below, it is possible to pass the identity authentication even if the Radius server returns TIMEOUT. **aaa authentication login default group radius none**

⚠ **Caution**	Since the keyword **none** enables any dial-up user to pass the authentication even if the security server has no reply, it is only used as the backup authentication method. We suggest not using the "none" identity authentication in general cases. In special case when all possible dial-up users are trustful, and no delay due to system fault is allowed for the user's work, it is possible to use **none** as the last identity authentication method in case the security server has no reply. And we recommend adding the local authentication method before the **none** authentication method.

Keyword	**Description**
local	Use the local username database for authentication
none	Do not perform authentication
group radius	Use Radius for authentication

The table above lists the AAA line authentication methods supported by our product.

37.6.4.1 Line Authentication Through Local Database

To configure the line authentication with local database, you need to configure the local database first. Our product supports authentication based on the local database. To establish the user name authentication, run the following commands in the global configuration mode:

Command	**Function**
configure terminal	Enter the global configuration mode.
username *name* [**password** *password*] or **username** *name* [**access-class** *number*]	Establish the user authentication by using password or access list.
username *name* [**privilege** *level*]	Set the privilege level for the user (optional).
username *name* [**autocommand** *command*]	Set the automatic command execution after user login (optional)
end	Return to the privileged mode.
show running-config	Confirm the configuration.

To define the local authentication method list and apply it, run the following commands:

Command	**Function**
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.

Command	Function
aaa authentication login {**default** | *list-name*} **local**	Define the local method list.
end	Return to the privileged mode.
show aaa *method-list*	Confirm the configured method list.
configure terminal	Enter the global configuration mode.
line vty *line-num*	Enter the line configuration mode
login authentication {**default** | *list-name*}	Apply the method list.
end	Return to the privileged mode.
show running-config	Confirm the configuration.

37.6.4.2 Use Radius for Line Authentication

To configure the use of RADIUS authentication server for line authentication, it is required to first configure the RADIUS server. Our product supports the authentication based on the RADIUS server. To configure the RADIUS server, run the following commands in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
radius-server host *ip-address* [**auth-port** *port*] [**acct-port** *port*]	Configure the RADIUS server
end	Return to the privileged mode.
show radius server	Show the RADIUS server.

After the RADIUS server is configured, make sure of successful communication with the RADIUS server before configuring the RADIUS for authentication. For details of the RADIUS server configurations, see **Configuring RADIUS**.

Now it is possible to configure the RADIUS server based method list. Run the following commands:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
aaa authentication login {**default** | *list-name*} **group radius**	Define the local method list.

Command	Function
end	Return to the privileged mode.
show aaa *method-list*	Confirm the configured method list.
configure terminal	Enter the global configuration mode.
line vty *line-num*	Enter the line configuration mode
login authentication {**default** | *list-name*}	Apply the method list.
end	Return to the privileged mode.
show running-config	Confirm the configuration.

37.6.5 Example of Authentication Configuration

The example below illustrates how to configure the network device and use “Radius + local” for authentication.

```
DGS-3610(config)# aaa new-model
DGS-3610(config)# username DGS-3610 password starnet
DGS-3610(config)# radius-server host 192.168.217.64
DGS-3610(config)# aaa authentication login test group radius local
DGS-3610(config)# line vty 0
DGS-3610(config-line)# login authentication test
DGS-3610(config-line)# end
DGS-3610# show running-config
!
aaa new-model
!
!
aaa authentication login test group radius local
username DGS-3610 password 0 starnet
!
radius-server host 192.168.217.64
!
line con 0
line vty 0
login authentication test
line vty 1 4
!
!
```

In the example above, the access server uses the Radius server (IP 192.168.217.64) to perform authentication for the login users. If the Radius server has no reply, the local database will be used for identity authentication.

37.7 Configuring Authorization

The AAA authorization enables the administrator to control services available to users. After the AAA authorization service is enabled, the network device configures user sessions through user configuration files stored locally or in the server. After the authorization, the user can only use the services allowed in the profile.

Our product supports the network authorization for such networks as PPP and SLIP network connections. It supports the following two authorization methods:

- Radius authorization method – The network access server requests the authorization information from the Radius security server. The Radius security server stores the user-specific right attribute pair.
- Local authorization method – The network access server accesses the local database (defined through the **username**) and then grants the user with specific rights. In the local database, only limited functions can be defined for the users, which are applicable for simple authorization for the users.

⚠ **Caution**

At present, the configuration does support the 802.1X AAA authorization, while the 802.1X is implemented through other commands.

37.7.1 Preparations for Authorization

The following tasks must be completed before the AAA authorization is configured:

- Enable the AAA server. For details, see **AAA Overview**.
- Configure the AAA authentication. The authorization is generally done after the user passes the authentication and depends on the normal operation of the authentication. For details of the AAA authentication, see **Configuring Authentication**.
- (Optional) configure security protocol parameters. If the security protocol is required for authorization, it is required to configure the security protocol parameters. Our product supports RADIUS. For details of the RADIUS, see **Configuring RADIUS**.
- (Optional) if the local authorization is required, you need to use the **username** command to define user rights.

37.7.2 Configuring Authorization List

To enable AAA authorization, execute the following command in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.

Command	Function
aaa authorization network{**default** | *list-name} method1 [method2*|*…*]	Enable the AAA authorization and define the authorization method.

37.7.3 RADIUS Authorization

To use the Radius security server for authorization, you can execute the **aaa authorization** command with the keyword **Radius**. The following shows how to configure the Radius.

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
radius-server host *ip-address* [**auth-port** *port*] [**acct-port** *port*]	Configure the RADIUS server
end	Return to the privileged mode.
show radius server	Show the RADIUS server.
configure terminal	Enter the global configuration mode.
aaa authorization network {**default** | *list-name*} **group radius**	Define the Radius authorization method.

37.7.4 Local Authorization

To use the local authorization, you need to execute the **aaa authorization** command with keyword **local**. If the local authorization is selected, the network access server queries the local user database to determine the functions allowed for the users. The global configuration command **username** is used to define the functions related with local authorization.

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
username *name* **privilege** *level*	Set the privilege level for the user
end	Return to the privileged mode.
show running-config	Confirm the configuration.
configure terminal	Enter the global configuration mode.
aaa authorization network {**default** | *list-name*} **local**	Define the local authorization method.

37.7.5 None Authorization

To enable no authorization for the user, you need to execute the **aaa authorization** command with keyword **none**.

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
aaa authorization network {**default** | *list-name*} none	Define the none authorization.

37.7.6 Example of Configuring Network Authorization

The example below illustrates how to perform network authorization.

```
DGS-3610# configure terminal
DGS-3610(config)# aaa new-model
DGS-3610(config)# radius-server host 192.168.217.64
DGS-3610(config)# username DGS-3610 privilege 6
DGS-3610(config)# aaa authorization network test group radius local none
DGS-3610(config)# end
DGS-3610# show running-config
aaa new-model
!
aaa authorization network test group radius local  none
!
username DGS-3610 password 0 starnet
username DGS-3610 privilege 6
!
radius-server host 192.168.217.64
```

37.8 Configuring Accounting

The AAA accounting function enables you to trace the services and network resources used by the user. After the accounting function is enabled, the network access server or router sends the user's network accesses to the Radius security server by means of attribute pair. You may use some analysis software to analyze these data to implement the billing, audition and tracing function for the user's activities.

37.8.1 Accounting Types

Our product currently supports the following accounting types:

- Network Accounting

37.8.2 Network Accounting

The network accounting provides the accounting information about user session, including the packet number, bytes, IP address and username.

Note

The format of Radius accounting information varies with the Radius security server. The contents of the account records may also vary with our product version.

37.8.3 Preparations for Accounting

The following tasks must be completed before the AAA accounting is configured:

- Enable the AAA security server. For details, see **AAA Overview**.
- Define the security protocol parameters. Our product supports the Radius security protocol. For details of the RADIUS, see **Configuring RADIUS**.

37.8.4 Configuring Accounting

To configure the AAA accounting function, execute the following command in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
radius-server host *ip-address* [**auth-port** *port*] [**acct-port** *port*]	Configure the RADIUS server
end	Return to the privileged mode.
show radius server	Show the RADIUS server.
configure terminal	Enter the global configuration mode.
aaa accounting network acct start-stop group radius	Configure the AAA network accounting function.

Note

The keyword **start-stop** is used for the network access server to send the accounting information at the start and end of the network service to the security server.

37.8.5 Monitoring AAA users

To view the information of the current login users, run the following commands in the privileged user mode:

Command	**Function**
show aaa user { **id** | **all** }	View the information of the current AAA user.

37.8.6 Example of Configuring Accounting

Below is an example to use the Radius for accounting:

```
DGS-3610# config
DGS-3610(config)# aaa new-model
DGS-3610(config)# radius-server host 192.168.217.64
DGS-3610(config)# aaa accounting network acct start-stop group radius
DGS-3610(config)# end
DGS-3610# show running-config
!
aaa new-model
!
aaa accounting network acct start-stop group radius
!
username DGS-3610 password 0 starnet
username DGS-3610 privilege 6
!
radius-server host 192.168.217.64
```

Note

For the information about how to configure the accounting method list command, see the related command reference manual.

38 Radius Configuration

38.1 Radius Overview

The Remote Authentication Dial-In User Service (Radius) is a distributed client/server system that works with the AAA to perform authentication for the users who are attempting to make connection and prevent unauthorized access. In the implementation of our product, the RADIUS client runs on the router or the network access server (NAS) to send the authentication requests to the central RADIUS server. The central center includes all information of user authentication and network services.

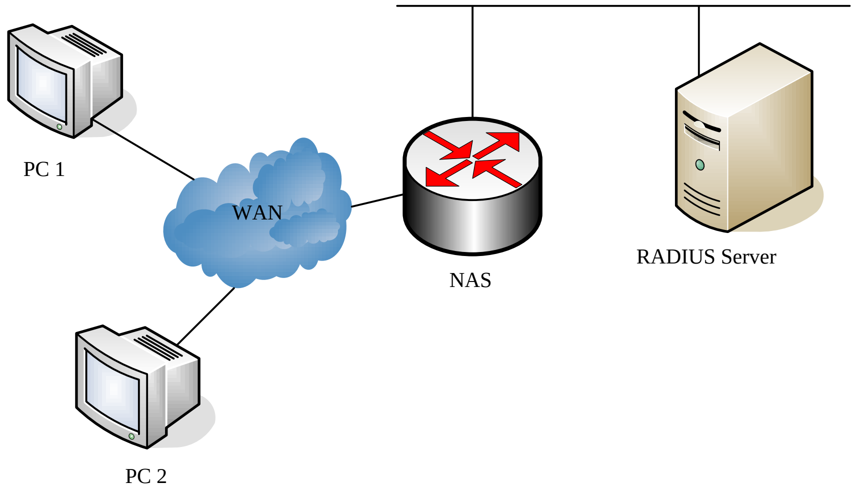
Since the RADIUS is a completely-open protocol, it has become a component and been installed in such systems as UNIX and WINDOWS 2000, so it is the security server most widely used for the time being.

The running process of the RADIUS is as follows:

- Prompt the user to enter username and password.
- The username and the encrypted password are sent to the RADIUS server via the network.
- The RADIUS returns one of the following responses:
- The user authentication passes.
- The user authentication fails and it prompts to reenter the username and password.
- The RADIUS server sends the challenge request to gather more authentication information from the user.
- The user authorization information is included in the ACCEPT response.

Here is a typical RADIUS topology:

Figure 38-1 Typical RADIUS network configuration



38.2 RADIUS Configuration Tasks

To configure Radius on the network device, perform the following tasks first:

- Enable AAA. For the details, see **AAA Overview**.
- Define the RADIUS authentication method list through the **aaa authentication** command. For details about how to use **aaa authentication** to define the authentication method list, see **Configuring Authentication**.
- Apply the defined authentication list on the specific line; otherwise the default authentication list will be used for authentication. For more details, see **Configuring Authentication**.

After the configuration is completed, you may start to configure the RADIUS. The configuration of the RADIUS consists of the following parts:

- Configuring Radius Protocol Parameters
- Specify the RADIUS authentication.

38.2.1 Configuring Radius Protocol Parameters

Before configuring the Radius on the network device, the network communication shall operate perfectly on the Radius server. To configure RADIUS protocol parameters, run the following commands:

Command	Function
configure terminal	Enter the global configuration mode.

Command	**Function**
radius-server host *ip-address* [**auth-port** *port*] [**acct-port** *port*]	Configure the IP address or hostname of the remote Radius security server and specify the authentication port and accounting port.
radius-server key *string*	Configure the sharing password for the communication between the device and Radius server
radius-server retransmit *retries*	Specify the times of sending requests before the router confirms Radius invalid (3 by default)
radius-server timeout *seconds*	Specify the waiting time before the router resend request (2 seconds by default)
radius-server deadtime *minutes*	Specify the waiting time before the server is considered dead in case of no response to the request sent by the device (5 minutes by default).

⚠ **Caution**

To configure the RADIUS, it is necessary to configure RADIUS Key. The shared password on the network device and the shared password on the Radius server must be the same.

38.2.2 Specifying the Radius Authentication

This means defining the authentication method list for the Radius after the Radius server is specified and the Radius authentication sharing password is defined. Since the RADIUS authentication is done via AAA, it is required to execute the **aaa authentication** command to define the authentication method list and specify the authentication method as RADIUS. For more details, see **AAA Configurations**.

38.2.3 Specify Radius Private Attribute Type

The contents in this section enable free configuration of private attributes. The default configurations are as follows:

Default configuration of private attributes of our products:

ID	**Function**	**TYPE**
1	max down-rate	1
2	qos	2
3	user ip	3
4	vlan id	4
5	version to client	5

ID	Function	TYPE
6	net ip	6
7	user name	7
8	password	8
9	file-directory	9
10	file-count	10
11	file-name-0	11
12	file-name-1	12
13	file-name-2	13
14	file-name-3	14
15	file-name-4	15
16	max up-rate	16
17	version to server	17
18	flux-max-high32	18
19	flux-max-low32	19
20	proxy-avoid	20
21	dailup-avoid	21
22	ip privilege	22
23	login privilege	42
24	limit to user number	50

Default configuration of extended manufacturer ID:

ID	Function	TYPE
1	max down-rate	76
2	qos	77
3	user ip	3
4	vlan id	4
5	version to client	5
6	net ip	6
7	user name	7
8	password	8
9	file-directory	9
10	file-count	10
11	file-name-0	11
12	file-name-1	12
13	file-name-2	13
14	file-name-3	14

ID	Function	TYPE
15	file-name-4	15
16	max up-rate	75
17	version to server	17
18	flux-max-high32	18
19	flux-max-low32	19
20	proxy-avoid	20
21	dailup-avoid	21
22	ip privilege	22
23	login privilege	42
24	limit to user number	50

Note

Two functions cannot be configured with the same type number.

Here is an example about how to configure the private type for network device:

```
RedGiant# show radius vendor-specific
id   vendor-specific      type-value
---- -------------------- ----------
1    max down-rate        76
2    qos                  77
3    user ip              3
4    vlan id              4
5    version to client    5
6    net ip               6
7    user name            7
8    password             8
9    file-diractory       9
10   file-count           10
11   file-name-0          11
12   file-name-1          12
13   file-name-2          13
14   file-name-3          14
15   file-name-4          15
16   max up-rate          75
17   version to server    17
18   flux-max-high32      18
19   flux-max-low32       19
20   proxy-avoid          20
21   dailup-avoid         21
22   ip privilige         22
23   login privilege      42
24   limit to user number 50
```

```
RedGiant# configure
RedGiant(config)# radius attribute 24 vendor-type 67
RedGiant(config)# show radius vendor-specific
id   vendor-specific      type-value
---- -------------------- ----------
1    max down-rate        76
2    qos                  77
3    user ip              3
4    vlan id              4
5    version to client    5
6    net ip               6
7    user name            7
8    password             8
9    file-diractory       9
10   file-count           10
11   file-name-0          11
12   file-name-1          12
13   file-name-2          13
14   file-name-3          14
15   file-name-4          15
16   max up-rate          75
17   version to server    17
18   flux-max-high32      18
19   flux-max-low32       19
20   proxy-avoid          20
21   dailup-avoid         21
22   ip privilige         22
23   login privilege      42
24   limit to user number 50
RedGiant(config)#
RedGiant(config)#
```

38.3 Monitoring RADIUS

To monitor the RADIUS, execute the following commands in the privileged user mode:

Command	Function
debug radius event	Turn on the Radius debug switch to view the Radius debug information

38.4 Radius Configuration Example

In a typical Radius network configuration diagram, the RADIUS server performs authentication for visiting users, enables the accounting function for them and records their network usage.

Note

The RADIUS server can be a component that comes with the Windows 2000/2003 server (IAS) or the UNIX system, or the special server software of some manufacturers.

Here is an example about how to configure the Radius for network devices:

```
DGS-3610# configure terminal
DGS-3610(config)# aaa new-model
DGS-3610(config)# radius-server host 192.168.12.219
auth-port 1645 acct-port 1646
DGS-3610(config)# radius-server key aaa
DGS-3610(config)# aaa authentication login test group radius
DGS-3610(config)# end
DGS-3610# show radius server
Server IP:       192.168.12.219
Accounting Port: 1646
Authen  Port:    1645
Server State:    Ready
DGS-3610#configure terminal
DGS-3610(config)#line vty 0
DGS-3610(config-line)#login authentication test
DGS-3610(config-line)#end
DGS-3610#show running-config
!
aaa new-model
!
!
aaa authentication login test group radius
!
username DGS-3610 password 0 starnet
!
radius-server host 192.168.12.219 auth-port 1645 acct-port 1646
!
line con 0
line vty 0
login authentication test
line vty 1 4
!
```

39 SSH Terminal Service

39.1 About SSH

SSH is short for Secure Shell. The SSH connection functions like a Telnet connection, except that all transmissions based on the connection are encrypted. When the user logs on to the device via a network environment where security cannot be guaranteed, the SSH feature provides safe information and powerful authentication function to protect the devices from IP address fraud, plain password interception and other kinds of attacks.

39.2 SSH Support Algorithms

Support algorithm	SSH1	SSH2
Signature authentication algorithm	RSA	RSA, DSA
Key exchanging algorithm	RSA public key encryption based key exchanging algorithm	KEX_DH_GEX_SHA1 KEX_DH_GRP1_SHA1 KEX_DH_GRP14_SHA1
Encryption algorithm	DES, 3DES, Blowfish	DES, 3DES, AES-128, AES-192, AES-256
User authentication algorithm	User password based authentication method	User password based authentication method
Packet authentication algorithm	Not supported	MD5, SHA1, SHA1-96, MD5-96
Compression algorithm	NONE (uncompressed)	NONE (uncompressed)

39.3 SSH Support

Caution

DGS-3610 series support only the SSH server (compatible with the SSHv1 and SSHv2) but do not support the SSH client.

39.4 SSH Configuration

39.4.1 Default SSH Configurations

Item	Default value
SSH service end status	Off
SSH version	Compatible mode (supporting versions 1 and 2)
SSH user authentication timeout period	120s
SSH user re-authentication times	3

39.4.2 User Authentication Configuration

1. Considering the SSH connection security, the login without authentication is forbidden. Therefore, During login authentication, the login authentication mode must have password configured (no-authentication login allowed for Telnet).
2. The username and password entered every time must have lengths greater than zero. If the current authentication mode does not need the username, you can enter any value with the length greater than zero.

39.4.3 Enabling SSH SERVER

The SSH SERVER is disabled by default. To enable the SSH, just enter the global configuration mode, generate the public key and make the SSH SERVER status turn into ENABLE.

Command	Description
configure terminal	Enter the configuration mode
enable service ssh-server	Enable SSH server.
crypto key generate {rsa|dsa}	Generate the key

⚠ **Caution**

Delete the key through **crypto key zeroize** instead of **[no] crypto key generate**.

39.4.4 Disabling SSH SERVER

To disable the SSH Server, execute the **no enable service ssh-server** command in the global configuration mode.

Command	Description
configure terminal	Enter the configuration mode
no enable service ssh-server	Disable the SSH Server.

39.4.5 Configuring SSH Server Support Version

By default, the SSH Server V1 and V2 are compatible. You can configure the SSH version through the following commands.

Command	Description
configure terminal	Enter the configuration mode.
ip ssh version {**1 | 2**}	Configure the SSH support version.
no ip ssh version	Reset SSH to the default configuration, supporting SSHv1 and SSHv2.

39.4.6 Configuring SSH User Authentication Timeout Duration

By default, the user authentication timeout duration of the SSH SERVER is 120 seconds. Run the following commands to configure the SSH user authentication timeout duration.

Command	Description
configure terminal	Enter the configuration mode
ip ssh time-out *time*	Configure the SSH timeout duration (1-120sec)
no ip ssh time-out	Reset the SSH user authentication timeout duration to the default value, 120 seconds.

39.4.7 Configuring SSH Re-authentication Times

This command is used to set the authentication attempts for SSH user requesting connections to prevent illegal actions such as malicious guesswork. The authentication attempts are set to 3 times for the SSH Server by default. A user can enter the username and password for three times to attempt the authentication. Run the following commands to configure the SSH re-authentication times:

Command	Description
configure terminal	Enter the configuration mode

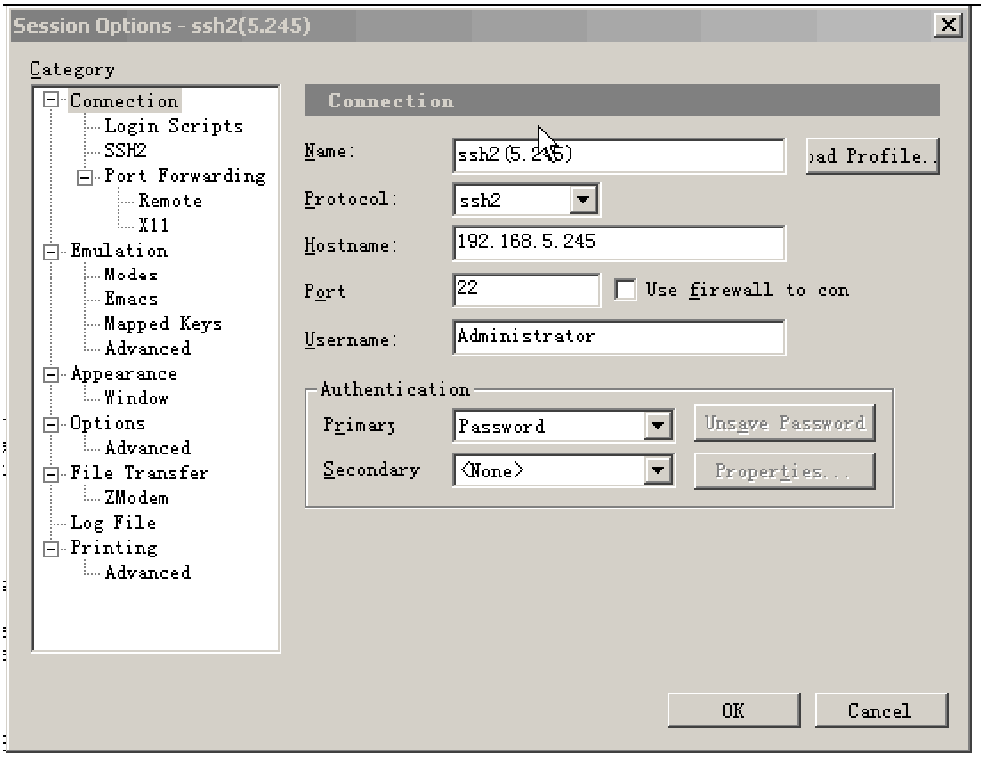
Command	Description
ip ssh authentication-retries *retry times*	Configure SSH re-authentication times (range 0-5)
no ip ssh authentication-retries	Reset the SSH re-authentication times to the default value 3.

Note: For details of the above commands, see **SSH Command Reference Manual**.

39.5 Device Management Through SSH

You may enable the SSH function for device management. It is disabled by default. Since the Telnet that comes with the Windows operating system does not support SSH, third-party client software must be used. Currently, the clients with sound forward compatibility include Putty, Linux and SecureCRT. With the client software SecureCRT as an example, the SSH client configuration is described as follows (see the UI below):

Figure 39-1



Session Options - ssh2(5.245)

Connection

Name: ssh2 (5.245)

Protocol: ssh2

Hostname: 192.168.5.245

Port: 22 □ Use firewall to con

Username: Administrator

Authentication

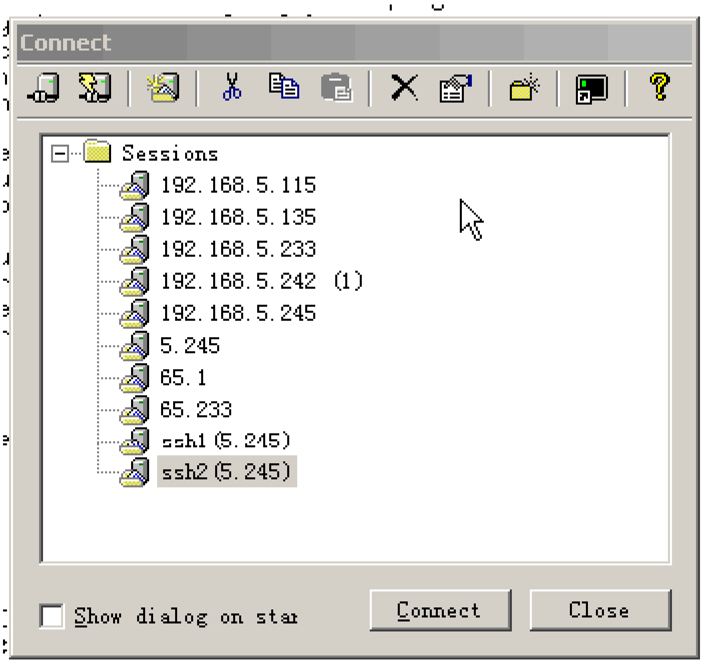
Primary: Password

Secondary: <None>

As shown in the above figure, protocol 2 is used for login, so SSH2 is chosen in **Protocol**. **Hostname** indicates the IP address of the host for login, 192.168.5.245. Port 22 is the default number of the port for SSH listening. **Username** indicates the username, and does not take effect when the device only requires password. **Authentication** indicates the authentication mode, and the username/password authentication is supported here. The used password is the same as the Telnet password.

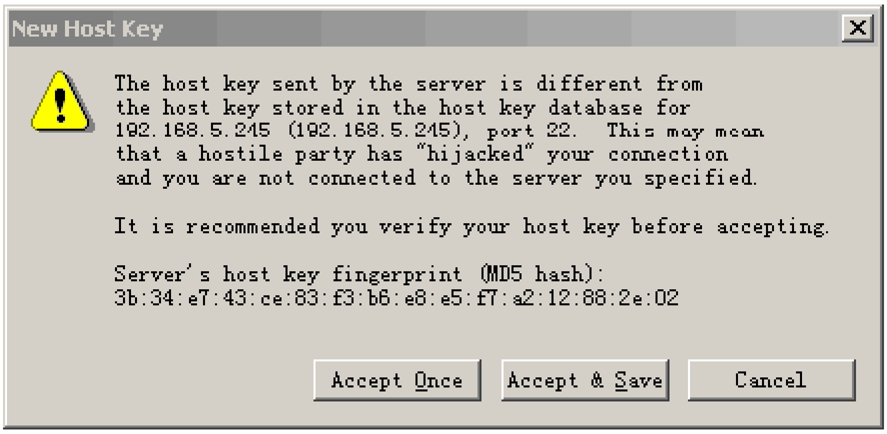
Click **OK**, and the following dialog box appears:

Figure 39-2



Click **Connect** to log into the host just configured, as shown below:

Figure 39-3



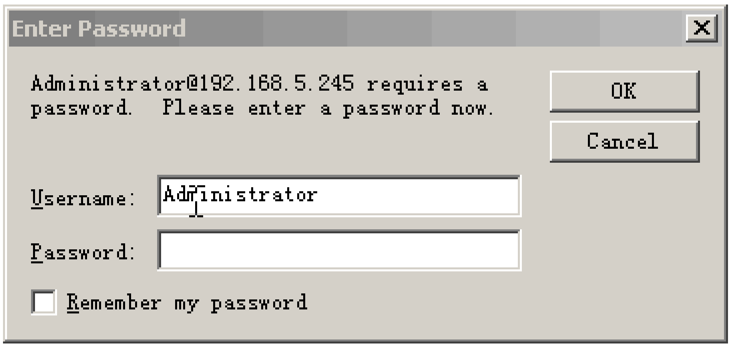
The host key sent by the server is different from the host key stored in the host key database for 192.168.5.245 (192.168.5.245), port 22. This may mean that a hostile party has "hijacked" your connection and you are not connected to the server you specified.

It is recommended you verify your host key before accepting.

Server's host key fingerprint (MD5 hash):
3b:34:e7:43:ce:83:f3:b6:e8:e5:f7:a2:12:88:2e:02

Ask the machine that is logging into the host 192.168.5.245 to see whether the key from the server end is received or not. Select **Accept & Save** or **Accept Once** to enter the password confirmation dialog box, as shown below:

Figure 39-4



Enter Password

Administrator@192.168.5.245 requires a password. Please enter a password now.

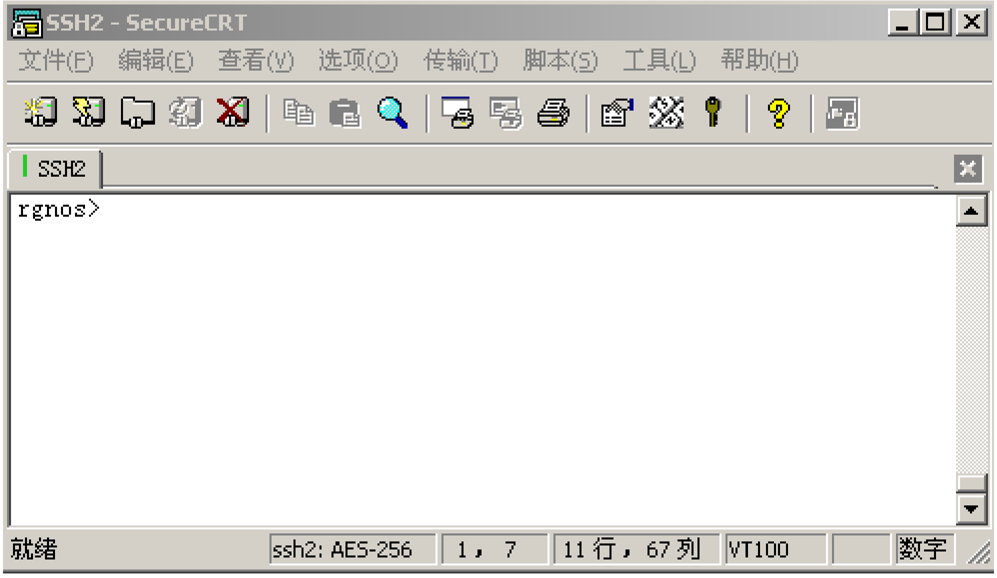
Username: Administrator

Password:

□ Remember my password

Enter the Telnet login password to enter the UI that is the same as the Telnet. See the interface below:

Figure 39-5



```
rgnos>
```

SSH2 - SecureCRT
文件(F) 编辑(E) 查看(V) 选项(O) 传输(T) 脚本(S) 工具(L) 帮助(H)
SSH2
就绪
ssh2: AES-256
1， 7
11 行， 67 列
VT100
数字

40 CPU Protection Configuration

40.1 Overview

40.1.1 Function of CPU Protect

Malicious attacks often occur in the network environment, and such attacks will create too much load for our switches. Sometimes when the packets in the network overload the switches, this may cause too high CPU utilization on the switch and its abnormal operation.

Our L3 switches provide the CPP feature to reduce the CPU load and protect the normal processing capability of the switch. When a switching card is attacked, the CLI management interface for the card can still work normally, without too high CPU utilization. The management packets from other switching cards can be processed in time by the switch.

Our switches allow you to configure the CPP on the switching card or management card to adjust the corresponding thresholds for the most detailed management.

Caution

The CPP (CPU Protect Policy) is a means used to enhance the switch security. With the CPP, the processor and channel bandwidth resource of the switch are protected to ensure the normal packet forwardingand normal running of protocols.

40.1.2 Principles of CPU Protect

The packets to be sent to the CPU of the management board are classified according to their L2, L3 and L4 information into: ARP, BPDU, DHCP, IGMP, RIP, OSPF, PIM, GVRP, VRRP, TTL-1 IPv4 packets, IPv6 multicast packets, unknown ipv4 broadcast packets.

The CPU ports have eight priority queues. You can configure the queue for each type of packet and the hardware can automatically send the packets of the type to the specified queue according to your configuration.

The CPU port sorts the packet queues through the strict priority algorithm. With this algorithm, each queue has a different priority, where queue 7 has the highest priority, queue 6 a lower one, and queue 0 the lowest. The packets of the high priority queue are always transmitted earlier than those in the lower priority queue. This way, you can map each type of packets to a different priority queue according to its importance to ensure prior transmission of the most important packets.

The switch provides a protection method to control the bandwidth and priority for each type of packets sent to the CPU. You can configure the maximum rate and priority for each type of packet sent to the CPU port in packets per second (PPS).

40.2 Configuring CPU Protect

The following sections describe how to configure CPU Protect.

- CPU Protect Default value
- Configuring the Bandwidth for Each Type of Packets
- Configuring the Priority for Each Type of Packets

40.2.1 Default Value of CPU Protect

The default bandwidth of each type of packets is set to 1000pps, with the priority of 0.

The following lists the recommended factory settings of the maximum bandwidth and priority of each type of packets.

Type	Default maximum bandwidth (pps)	Default priority
TP-Guard	128	0
ARP	500	0
BPDU	128	6
DHCPS	128	0
DOT1X	128	0
GVRP	128	0
IPV6-MC	128	0
DVMRP	128	3
IGMP	128	3
OSPF	128	3
PIM	128	3
RERP	128	6
RIP	128	0
RLDP	128	6
VRRP	128	6
Unknow-IPMC	128	0
Err-TTL	128	0
DHCP_RELAY_CLIENT	128	0
DHCP_RELAY_SERVER	128	0

Type	Default maximum bandwidth (pps)	Default priority
DHCP_OPTION82	128	0
UDP_HELPER	128	0

Through the command **no cpu-protected type**, the maximum bandwidth and priority setting of the packet can be reset to the default value. The default maximum bandwidth is 1000pps, priority is 0.

40.2.2 Configuring the Bandwidth for Each Type of Packets

In the configuration mode, configure the queue of each type of packets through the following steps:

Command	Function
DGS-3610(config)# **cpu-protect type {arp | bpdu | dhcp | ipv6mc | igmp | rip | ospf | vrrp | pim | err-ttl | unknown-ipmc | dvmrp} pps** *pps_vaule*	Set the queue for the packets in PPS, which is an integer.
DGS-3610# **end**	Return to the privileged mode.

This example shows the profile configuration process:

```
DGS-3610(config)#cpu-protect type bpdu pps 200
Set packet type bpdu pps 100.
```

40.2.3 Configuring the Priority for Each Type of Packets

In the configuration mode, configure the queue of each type of packets through the following steps:

Command	Function
DGS-3610(config)# **cpu-protec type** {**arp | bpdu | dhcp | ipv6mc | igmp | rip | ospf | vrrp | pim | err-ttl | unknown-ipmc**} **pri** *pri_vaule*	Set the queue for the packets in PPS, which is an integer.
DGS-3610# **end**	Return to the privileged mode.

This example shows the profile configuration process:

```
DGS-3610(config)# cpu-protect type bpdu pri 7
Set packet type bpdu priority 7.
```

40.3 Viewing CPU Protect Information

On the switch, you can view the following information about the CPU Protect:

- Viewing the statistics of packets received by the CPU of the management board
- Viewing the Statistics of packets received by the CPU of the Line Card
- Viewing the Statistics of received packets of a specific type

40.3.1 Viewing the statistics of Packets Received by the CPU of the Management Board

In the privileged mode, show the CPP information of the management board with the following commands:

Command	**Function**
DGS-3610# **show cpu-protect mboard**	Show the statistics of the packets received by the CPU of the management board

The following example shows how to show the CPP information of the management board:

```
DGS-3610#show cpu-protect mboard
 Type            Pps          Total        Drop
 ------------    ---------    ---------    ---------
 arp             500          19           0
 bpdu            200          24           0
 dhcp            0            0            0
 gvrp            0            0            0
 ipv6-mc         0            0            0
 dvmrp           0            0            0
 igmp            0            0            0
 ospf            0            0            0
 pim             0            0            0
 rip             0            0            0
 vrrp            0            0            0
 unknow-ipmc     0            0            0
 err-ttl         0            0            0
```

40.3.2 Viewing the Statistics of Packets Received by the CPU of the Line Card

In the privileged mode, show the statistics of the packets received by the CPU of a specific line card with the following commands:

Command	**Function**
DGS-3610# **show cpu-protect slot** *slot_id*	Show the packets received by the CPU of a specific line card. slot_id: slot ID

The following example shows the CPU protection information of the line card in slot 2.

```
DGS-3610(config)# show cpu-protect slot 2
```

```
Type            Pps        Total      Drop
------------    ---------  ---------  ---------
arp             200        200        15
bpdu            200        8          0
dhcp            200        0          0
gvrp            200        0          0
ipv6-mc         200        0          0
dvmrp           200        0          0
igmp            200        0          0
ospf            200        0          0
pim             200        0          0
rip             200        0          0
vrrp            200        0          0
unknow-ipmc     200        0          0
err-ttl         20         3          0
```

40.3.3 Viewing the Statistics of Received Packets of a Specific Type

In the privileged mode, show the priority and bandwidth of each type of packet with the following commands:

Command	Function
DGS-3610# **show cpu-protect type arp | bpdu | dhcp | ipv6mc | igmp | rip | ospf | vrrp | pim | ttl1 | unknown-ipmc | dvmrp**	Show the statistics of the packets received of a each type

The following example shows the statistics of the arp packets through the **show cpu-protec type arp** command:

```
DGS-3610(config)# show cpu-protect type arp
 Slot       Type         Pps       Total      Drop
 ---------  ------------ --------- ---------  ---------
 MainBoard  arp          200       15         0
 Slot-2     arp          200       15         0
```

Caution

1. Packet speed restriction is measured by the software, so a slight deviation of the number of packets is normal.
2. The actual information printed may be different from the example.

41 Anti-attack System Guard Configuration

41.1 Overview

It is known that many attacks of hackers and invasion of network virus start with scanning the active hosts in the network. The great amount of scanning packet consumes network bandwidth significantly and causes abnormal operation of the network communication.

DGS-3610 series provide the anti-scanning function to prevent hacker scanning and the Worm.Blaster-like attacks, and reduce the CPU load of the layer 3 devices.

At present, two types of scanning attacks are detected:

1. The scanning of the change for the destination IP address is called the **Scan Dest Ip Attack**. This scanning is the most serious threat to the network for it consumes the network bandwidth and adds the load of the devices, so it becomes the primary means of most hacker attacks.
2. The destination IP address does not exist, while a large number of packets are sent continuously, which is referred to as the **Same Dest Ip Attack**.This attack is mainly designed to reduce the load of the CPU for the devices. For the layer 3 switches, if the destination IP address exists, the packet will be forwarded directly by the switching chip and does not occupy the resource of the CPU for the switches. If the destination IP address does not exist, the CPU of the devices will attempt to connect periodically. Furthermore, if there are a large number of such attacks, they will consume the CPU resource. Of course, the hazard of this attack is much weaker than the first one.

For the above two kinds of attacks, it is possible to adjust the attack threshold, attack host isolation duration and more parameters on the interfaces of DGS-3610 series, to relieve the burden of the network or devices. The administrator can tune the administration configuration of the device according to the network conditions. If the configuration of each interface is identical, the administrator can set a batch of ports through the **interface range** function.

41.2 Anti-attack System Guard Configuration

The anti-attack system guard is completed in the global configuration mode. It is required to enter the global configuration mode first for anti-attack system guard configuration.

41.2.1 IP Anti-Scanning Configuration Task List

- Enable the anti-attack system guard function of the interface
- Set the isolation period for illegal attacking IP
- Set the threshold to judge illegal attacking IP
- Set the maximum monitored IPs
- Set exceptional IPs free from monitoring
- Clear the isolation status of isolated IPs
- View Related Information of System Guard

41.2.2 Enabling the Anti-Attack System Guard Function of the Interface

You can enable the system guard in the interface mode. The system guard only supports physical ports.

Command	Meaning
configure terminal	Enter the global configuration mode.
interface *interface-id*	Enter the configuration mode of this **interface**. Legal interfaces include physical **interfaces**.
system-guard enable	Enable the system guard function.
end	Return to the privileged mode.
show system-guard	Check the configuration entities.
copy running-config startup-config	Save the configuration.

If you want to disable the system guard on this interface, execute **no system-guard** to set in the interface mode.

41.2.3 Setting the Isolation Period for Illegal Attacking IP

The islation time of illegal attack IP is port-based. You may configure the isolation time of the illegal attack user in the interface mode. Communication in the IP recovers automatically after it is isolated for a period of time.

Command	Meaning
configure terminal	Enter the global configuration mode.
interface *interface-id*	Enter the configuration mode of this interface. Legal interfaces include physical interfaces.
system-guard isolate-time *seconds*	Configure the isolation time of unauthorized users. Its value range is 30s – 3600s, 120s by default.
end	Return to the privileged mode.
show system-guard	Check the configuration entities.
copy running-config startup-config	Save the configuration.

If you want to restore the default value of the isolation time, execute the **no system-guard isolation-time** command to set in the interface mode.

In addition, when an illegal user is isolated, the device sends a LOG record to the log system for the query of the administrator. Furthermore, it sends another LOG notice when the illegal isolation is removed.

41.2.4 Setting the Threshold to Judge Illegal Attacking IP

There are two attack methods that may affect the device performance.

1. Scan a batch of IP network segments.
2. Attack an inexistent IP by sending IP packets continuously.

The above limits are configured on our devices. Once one of a batch of packets sent by a user exceeds the packet limit controlled by the administrator, the user will be considered to be an unauthorized attacker and be isolated. The judging threshold of illegal attacking IP is also port-based. You may configure it in the interface mode.

Command	Meaning
configure terminal	Enter the global configuration mode.
interface *interface-id*	Enter the configuration mode of this interface. Legal interfaces include physical interfaces.
system-guard same-dest-ip-attack-packets *number*	Configure the maximum threshold for continuously sending IP packets to an inexistent IP for attack. The value range is 1 – 2000 packets per second, 20 by default. Setting to 0 indicates this attack is not monitored.
system-guard scan-dest-ip-attack-packets *number*	Configure the maximum threshold for scanning and attacking a batch of IP network segments. The value range is 1 – 1000 packets per second, 10 by default. Setting to 0 indicates this attack is not monitored.
end	Return to the privileged mode.

Command	Meaning
show system-guard	Check the configuration entities.
copy running-config startup-config	Save the configuration.

⚠ **Caution**

The smaller the threshold is set, the weaker the accuracy of the judging for the attacked host is. It is easy to isolate the normal host online incorrectly. It is recommended that administrators configure corresponding threshold according to the security of the actual network environment.

If you want to restore the default value of corresponding parameters, execute the **no system-guard same-dest-ip-attack-packets** and **no system-guard scan-dest-ip-attack-packets** commands for setting in the interface mode.

41.2.5 Setting the Maximum Number of Monitored IPs

You can set the maximum quantity of the attacked hosts monitored by the devices, 20% of the quantity of the actually-operated hosts. However, if you detect that the isolated hosts reach or approach to the maximum quantity of the monitored hosts, the quantity of the monitored hosts can be enlarged to meet the requirements for better system guard.

You can set the maximum quantity of the attacked host through the following steps:

Command	Meaning
configure terminal	Enter the global configuration mode.
system-guard detect-maxnum *number*	Set the maximum number of monitored hosts. This value is based on line card, ranging from 1 to 500, 100 by default.
end	Return to the privileged mode.
show system-guard	Check the configuration entities.
copy running-config startup-config	Save the configuration.

⚠ **Caution**

If you change the quantity of the monitored hosts to be less than the original quantity, it can cause data clearing of current monitored host. In case of a large number of isolated IP addresses, it may display **chip resource full**, because the device has isolated many users, causing full occupation of the hardware chip resource (This quantity is about 100-120 IP addresses for each port according to the actual switch operation and the ACL setting). However these users are not isolated actually, so it is necessary for administrators to take other measures to handle these attackers.

If you want to restore the default value of the maximum quantity for monitored hosts, execute the **no system-guard detect-maxnum** command in the global configuration mode.

41.2.6 Setting Exceptional IPs Free From Monitoring

You may set exceptional IPs free from monitoring. Packets that meet the exceptional IPs are allowed to be sent to the CPU.

Command	Meaning
configure terminal	Enter the global configuration mode.
system-guard exception-ip *ip mask*	Add the exceptional IP mask for anti-attack function. Up to 255 exceptional IP entries are supported.
end	Return to the privileged mode.
show system-guard exception-ip	Show all exceptional IP entries.
copy running-config startup-config	Save the configuration.

In the global configuration mode, you can delete an exceptional IP entry through the **no** option of this command. All exceptional IP entries can be deleted through the **no** and **all-eip** options of this command .

For example, to delete all exceptional IPs:

```
DGS-3610(config)# no system-guard exception-ip all-eip
```

To delete a single exceptional IP:

```
DGS-3610(config)# no system-guard exception-ip 192.168.5.145/32
```

⚠ **Caution**

An isolated IP is still in the isolated status before being aged even if it is among exceptional IPs. To send the IP packets to the CPU, you may execute the **clear system-guard** command to cancel the isolation of the IP.

41.2.7 Clearing the Isolation Status of Isolated IPs

An isolated user will automatically recover after a period of isolation. To clear the isolation manually, execute the following command in the privileged mode:

Command	**Meaning**
clear system-guard **[interface** *interface-id* **[ip-address** *ip-address***]]**	Clear Isolated Users. Where, **clear system-guard** indicates clearing all isolated users; **clear system-guard interface** *interface-id* indicates clearing all users under that port; **clear system-guard interface** *interface-id* **ip-address** *ip-address* indicates clearing the specified IP user under the interface.

41.2.8 Viewing Related Information of System Guard

41.2.8.1 View Related Information of System Guard

Execute the **show system-guard** command to view the configuration parameters of the system guard:

Command	**Meaning**
show system-guard [interface *interface-id***]**	View the configuration parameters of the system guard.

Here is an example:

```
DGS-3610# show system-guard
detect-maxnum number   : 100  ------ The maximum quantity of the hosts monitored by the
device
isolated host number   : 11   ----- The quantity of the hosts isolated by the device
inteface  state   isolate time  same-attack-pkts   scan-attack-pkts
---------------------------- ----------------   ------------------
Fa 0/1   ENABLE   120           20                 10
Fa 0/2   DISABLE  110           21                 11
……

DGS-3610# show system-guard interface Fa 0/1

detect-maxnum number   : 100  ------ The maximum quantity of the hosts monitored by the
device
isolated host number   : 11   ------------ The quantity of the hosts isolated by the device

intefacestate solate time ame-attack-pkts   scan-attack-pkts
---------------------------- ----------------
Fa 0/1    ENABLE     120        20                 10
```

41.2.8.2 Viewing the Information of Isolated IPs for System Guard

Command	Meaning
show system-guard isolate-ip [interface *interface-id***]**	Check the information of isolated IPs of the ports for anti-scanning

```
DGS-3610# show system-guard isolated-ip
interface ip-address    isolate reason   remain-time(second)
----------   ------------------  --------------------
Fa 0/1    192.168.5.119   scan ip attack     110
Fa 0/1    192.168.5.109   same ip attack     61
```

The fieds above indicate respectively the port on which the isolated IP address appears, the isolated IP address, the isolated reason and the remaining isolated time.

41.2.8.3 Viewing Monitored Users

Command	Meaning
show system-guard detect-ip [interface *interface-id***]**	View the IP that is being monitored.

```
DGS-3610# show system-guard detect-ip
interface ip-address ame ip attack packets  scan ip attack packets
-------------  ------------- ---------- --------  --------
Fa 0/1       192.168.5.118         0             8
Fa 0/1        192.168.5.108       12             2
```

41.2.8.4 Show Exceptional IPs Free From Monitoring

To show the exceptional IPs that allow device access in the anti-attack function:

Command	Meaning
show system-guard exception-ip	Check all exceptional IPs.

```
DGS-3610# show system-guard exception-ip
Exception IP Address    Exception Mask
 --------------------   ---------------
192.168.5.145           255.255.255.0
192.168.4.11            255.255.255.0
```

42 GSN Configuration

42.1 Overview of GSN Security Solution

The GSN security solution consists of the following four elements:

42.2 Security policy Management Platform

42.3 Security Agent

42.4 Restore System

42.5 Security Switch

42.6 Security Policy Management Platform (SMP)

Through policy configuration, the SMP checks whether to allow or forbid transmission of data packets through security devices. Installing policies is the process to configure policies on the devices. Removing policies is the process to remove policies from the devices.

42.6.1 Security Agent

The Security Agent is the software running on a network-accessed host in the enterprise network. It is responsible for collecting the client information, recognizing the network behavior of users, monitoring the network communication and security status of the client, and sending the collected information to the security policy management platform so that the administrator can make appropriate security policies. At the same time, the security agent automatically downloads the new security policies from the security policy management platform and executes the specified security policies locally.

42.6.2 Restore System

The restore system performs the following for abnormal behaviors:

For the users not complying with the enterprise security policies, the administrator can preset an appropriate policy on the security management platform to shield most network access rights of these “invalid users”, leaving only a green security channel. This security channel only leads to the enterprise security policy upgrade servers, including the Windows patch upgrade server, anti-virus software library server, or other upgrade servers of the enterprise.

When the security agent detects that its own security policy does not comply with the security level set by the management platform, the security agent will immediately upload its own security log to the security policy management platform. According to the alarm log from the security agent, the policy management platform selects one from the preset policies and delivers it to all the security switches. After receiving the latest policy configuration, the security switches immediately apply them so that the user of the alarm can only access the specified upgrade server according to the restore action specified by the policy server, and automatically install these patches.

When the user has completed all the restore actions specified by the policy server, the security agent will perform security detection to the client operation platform. If the agent meets all the security policy sets, the security agent will notify the security policy management platform to remove the access list restriction over the agent, setting the client as a normal user.

42.6.3 Security Switch

As part of the security solution, the Security Switch is responsible for receiving policies from the security policy management platform, installing them, and controlling the users according to the installed policies.

42.7 Configuring the GSN Security Switch

42.7.1 Configuring the Switch GSN Security

By default, the GSN security solution is disabled.

Command	Description
configure terminal	Enter the configuration mode
[**no**] **security gsn enable**	Enable GSN global configuration

The following example enables the GSN function of the equipment:

```
DGS-3610# configure terminal
DGS-3610(config)# security gsn enable
```

42.7.2 Configuring the Communication Between SMP Servers

In order to communicate with the SMP Server, you must configure the IP address of the SMP Server and security authentication name for the equipment.

Command	Description
Configure terminal	Enter the configuration mode

Command	**Description**
[**no**] **security** { [**v1** | **v2**] **community** *community* | **v3 user** *username* }	Configure the security name for communication with the SMP server. This command supports SNMP v1, v2 and v3. By default, no community is configured. By default, security v1 community and security community are the same for configuring v1. If you select v3, you need to configure the corresponding v3 user through the **snmp-server** command. For the related configuration command, see the *SNMP Configuration* chapter.
[**no**] **smp-server host** *ip-address*	Configure the SMP server address

Note

When you configure the security v3 user, you need to configure the corresponding v3 user on the SNMP part.

42.7.3 Configuring the Minimum Interval for Tranmission of Security Events

To prevent illegal users from attacking the SMP by frequently sending security events through forgery, you can set the minimum interval for the transmission of security events.

According to the actual conditions, you can set this interval with the following commands:

Command	**Description**
Configure terminal	Enter the configuration mode
[**no**] **security event interval** *interval*	Configure the minimum interval of the security event, within the range of 1-65535s; By default, the interval is 5 seconds.

42.7.4 Configuring the Address Binding Switch Supported by the Port

This command allows you to control whether to generate the address binding policy on the port. When an authentication port is connected to multiple users, the administrator must enable the address binding of that port:

Command	**Description**
Configure terminal	Enter the configuration mode
interface *interface*	Enter the interface configuration mode.

Command	Description
[**no**] **security address-bind enable**	Enable the address binding policy

Note

This function takes effect only when the global GSN support is enabled and the configured port is an authentication port. In addition, when you use this function, you should disable the 802.1X IP authorization. Otherwise, the actual running effect of the security policy will be affected.

42.8 GSN Configuration Display

42.8.1 Showing smp server

You can show the information of the SMP server through the following step:

Command	Description
show smp-server	Show the smp server

For example,:

```
DGS-3610# show smp-server
SMP-Server IP:192.168.217.220
```

42.8.2 Showing security event interval

You can show the information of the policy-map through the following step:

Command	Description
show security event interval	Show the minimum interval of the security event

For example:

```
DGS-3610# show security event interval
Event sending interval(Seconds):5
```

42.9 Precuations for GSN Configuration

42.9.1 Number of GSN-Supporting Entries

Since the policy installation of the GSN is implemented through hardware filtering, the number of policies supported by the GSN varies with the chips of the products. In addition, the hardware entries used by the GSN may be occupied by other modules. Therefore, when you enable the appropriate function (for example, the ARP anti-spoofing function), the number of available entries becomes smaller, and the number of entries supported by the GSN decreases accordingly. To support more dynamic policies and enhance the control over

GSN, you should not enable any other functions that may consume hardware entries as far as possible when you enable GSN.

42.9.2 Functions in Conflict with the GSN

Due to the features of GSN application, the GSN is in conflict with the following functions. Avoid enabling the functions at the same time that may cause function exception.

1. The GSN should not be used together with the IP authorization of 1x.
2. The GSN should not be used together with port security.
3. The GSN does not support the installation of policies on the AP port, while a port installed with policies cannot join the AP port. If you add a port installed with the GSN policies to an AP port, the functions of the port may become faulty. If a port installed with policies needs to join an AP port, you should first delete the installed policies on the port.

42.9.3 Other Precuations for Using the GSN

Since the GSN is ultimately implemented through hardware filtering, the following configuration may affect the use of the GSN:

Global IP+MAC binding: The isolation may fail if a global IP+MAC binding is configured, one MAC user is allowed to pass, but the GSN is set to isolate the MAC user.

ACL: When the entries set by the ACL are in conflict with the policies delivered by the GSN, the GSN function may fail. When the GSN is enabled, you are recommended not to enable the ACL.

43 Dynamic ARP Inspection Configuration

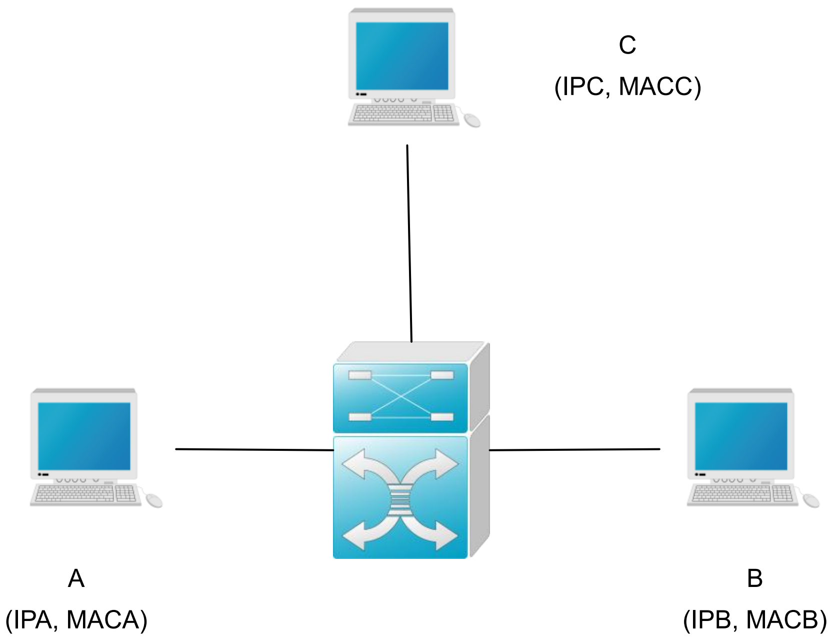
43.1 Understanding DAI

DAI, an acronym of Dynamic ARP Inspection, refers to validity inspection of received ARP packets. Illegal ARP packets will be discarded.

43.1.1 Understanding ARP Spoofing Attack

ARP itself does not check the validity of incoming ARP packets. Due to the drawback of ARP, attackers can launch ARP spoofing attacks easily. The most typical one is the intermediary attack, which is described as follows:

Figure 43-1



As shown in the diagram, devices A, B and C are connected to DGS-3610 series and located in the same subnet. Their IP and MAC addresses are respectively represented with (IPA, MACA), (IPB, MACB) and (IPC, MACC). When device A needs to communicate with device B in the network layer, device A broadcasts an ARP request in the subnet to query the MAC value of device B. Upon receiving this ARP request packet, device B updates its ARP buffer using IPA and MACA, and sends an ARP response. Upon receiving this response, device A updates its ARP buffer using IPB and MACB.

With this model, device C can mistake the corresponding relationship of ARP entries in device A and device B. It broadcasts the ARP response to the network continuously. The IP address in the response is IPA/IPB, and the MAC address is MACC. Then, ARP entries (IPB and MACC) exist in device A, and ARP entries (IPA and MACC) exist in device B. Communication between device A and device B is changed to communication with device C, which is unknown to devices A and B. Device C acts as an intermediary and it just modifies the received packets appropriately and forwards to another device. This is the well-known intermediary attack.

43.1.2 Understanding DAI and ARP Spoofing Attacks

DAI ensures that only legal ARP packets are forwarded by the device. It mainly performs the following operations:

- Intercept all the ARP request and response packets at the untrusted port that corresponds to VLAN with the DAI inspection function enabled.
- Check the validity of the intercepted ARP packets according to the setting of DHCP database before further processing.
- Release the packets that do not pass the inspection.
- Appropriately process the packets that pass the inspection and send them to the destinations.

Validity of ARP packets is checked according to the DHCP snooping binding database. For details, refer to the configuration guide *DHCP Snooping Configuration*.

43.1.3 Understanding DAI Global Switches

Typically, packets are forwarded by hardware, while the DAI function must be implemented by software. Therefore, for ARP packets:

- When the DAI global switch is turned on, all the ARP packets are processed by software, and cannot be forwarded by the hardware.
- When the DAI global switch is turned off, the hardware, instead of the software, forwards ARP packets within VLAN, and DAI inspection is not performed on the ARP packets sent to the local system.

Note that the global switch only determines whether to check the incoming and outgoing ARP packets.

For specific configuration commands, refer to *ip arp inspection*.

43.1.4 Interface Trust Status and Network Security

ARP packets are checked according to the trust status of each port on the device. DAI check is ignored for the packets that are received through trusted ports and are considered as legal ARP packets. DAI check will be performed strictly for the ARP packets that are received through untrusted ports.

In a typical network configuration, the layer 2 port connected to the network device need be set as a trusted port, and the layer 2 port connected to the host device need be set as an untrusted port.

Note: Incorrectly configuring a layer 2 port as an untrusted port may affect normal communication of the network.

For specific configuration commands, refer to *ip arp inspection trust, show ip arp inspection interface.*

43.1.5 Restricting Rate of ARP Packets

Because DAI validity check consumes certain CPU resources, the rate of ARP packets is restricted, that is, the number of ARP packets received per second is restricted. This effectively prevents the denial of service attack against the DAI function. By default, the maximum number of ARP packets received through an untrusted port is 15. This restriction does not apply to the trusted port. To configure this rate restriction, use the **ip arp inspection limit-rate** command in the layer 2 interface configuration mode.

For specific configuration commands, refer to *ip arp inspection limit-rate show ip arp inspection interface*

43.2 Configuring DAI

DAI is an **ARP**-based security filtering technology. A series o f filtering policies are configured, so that validity of ARP packets that pass the device is checked more effectively.

To use the functions of DAI, selectively perform the following tasks:

- Enabling the global DAI function (required)
- Enabling the DAI packet check function for specified VLAN (required)
- Setting the trust status of ports (optional)
- Setting the maximum receiving rate of ARP packets for a port (optional)
- Related configuration of DHCP snooping database (optional)

43.2.1 Enabling Global DAI Function

This feature is disabled by default.

DAI-related security check will be performed for ARP packets only when the global DAI function is enabled.

If this global switch is enabled, the words **ip arp inspection** can be seen through the **show running-config** command.

Command	**Function**
DGS-3610(config)# **ip arp inspection**	Enable the global DAI function
DGS-3610(config)# **no ip arp inspection**	Disable the global DAI function

43.2.2 Enabling the DAI Packet Check Function for Specified VLAN

By default, the DAI packet check function is disabled for all VLANs.

If no DAI packet check function of VLAN vid is enabled, DAI-related security check will be skipped for the ARP packets with vlan-id = vid (ARP packet rate restriction is not skipped).

You can execute the **show ip arp inspection vlan** command to check whether the DAI packet check function is enabled for all VLANs.

To configure the DAI packet check function for VLAN, execute the following commands in the interface configuration mode:

Command	**Function**
DGS-3610(config)# **ip arp inspection vlan** *vlan-id*	Turn on the DAI packet check function switch for VLAN *vlan-id*
DGS-3610(config)# **no ip arp inspection vlan** [*vlan-id*]	Turn off the DAI packet check function switch for VLAN *vlan-id* Disable the DAI packet check function for all VLANs if *vlan-id* is ignored

43.2.3 Setting the Trust Status of Ports

This command is used in the layer 2 interface configuration mode, and this layer 2 interface is a member port of SVI.

All the layer 2 ports are untrustable by default.

If the port is trustable, ARP packets will not be checked further. Otherwise, the validity of the current ARP packet will be checked according to the information in the DHCP snooping database.

To set the trust status of a port, execute the following commands in the interface configuration mode:

Command	**Function**
DGS-3610(config-if)# **ip arp inspection trust**	Set the port as a trusted port
DGS-3610(config-if)# **no ip arp inspection trust**	Set the port as an untrusted port

43.2.4 Set Maximum Receiving Rate of ARP Packets for a Port

This command is used in the layer 2 interface configuration mode, and this layer 2 interface is a member port of SVI.

By default, the DAI globacl check switch is turned on, and the DAI rate restriction of all ports is 15PPS.

By default, the default ARP packet receiving rate of each untrusted switching port is 15 ARP packets per second. By default, this does not apply to trusted switching ports.

If the number of ARP packets received through this port within one second exceeds this threshold, the subsequent packets will be discarded.

The rate restriction of each layer 2 interface can be viewed through the **show ip arp inspection interface** command.

To set the maximum ARP packet receiving rate for a port, execute the following commands in the interface configuration mode:

Command	**Function**
DGS-3610(config-if)# **ip arp inspection limit-rate** { *<1-2048>* **| none**}	Set the maximum ARP packet receiving rate for a port, in packets/second **none**: There is no restriction
DGS-3610(config-if)# **no ip arp inspection limit-rate**	Restore the default setting

43.2.5 Related Configuration of DHCP Snooping Database

Refer to *DHCP Snooping Configuration*.

If DHCP Snooping database is not configured, all the ARP packets pass the inspection.

43.3 Showing DAI Configuration

43.3.1 Showing DAI Enabling Status of VLAN

To show the enabling status of VLAN, execute the following command in the global configuration mode:

Command	**Function**
DGS-3610(config)# **show ip arp inspection vlan**	Show the enabling status of each VLAN

43.3.2 Showing DAI Configuration Status of Each Layer 2 Interface

To show the DAI configuration status of each layer 2 interface, execute the following command in the global configuration mode:

Command	**Function**
DGS-3610(config)# **show ip arp inspection interface**	Show the DAI configuration of each layer 2 interface (including trust status and rate restriction)

44 Access Control List Configuration

44.1 Overview

As part of the GSN security solution, DGS-3610 series uses access control lists to provide a powerful data flow filtering function. At present, DGS-3610 series support the following access lists:

- Standard IP access control list
- Extended IP access control list
- MAC access control list
- MAC extended access control list
- Expert extended access control list
- IPV6 extended access control list

Depending on the conditions of networks, you can choose different access control lists to control data flows.

44.1.1 Access Control List Introduction

ACLs is the short for Access Control Lists, or Access Lists. It is also popularly called firewall, or packet filtering in some documentation. ACLs controls the data packets on the network device interface by defining some rules:Allow or deny. According to usage ranges, they can be divided into ACLs and QoS ACLs.

By filtering the data flows, you can restrict the communication data types in the network and restrict the users of the network and the device they can use. When data flows pass the device, ACLs classify and filter them, that is, check the data flows inputted from the specified interface and check whether to permit or deny them according to the matching conditions.

Generally, the security ACLs is used to control specific data flows allowed to pass through the network device. The QoS policy performs priority classification and processing for the dataflow.

ACLs consist of a series of entries, known as Access Control Entry (ACE). Each entry specifies its matching condition and behavior.

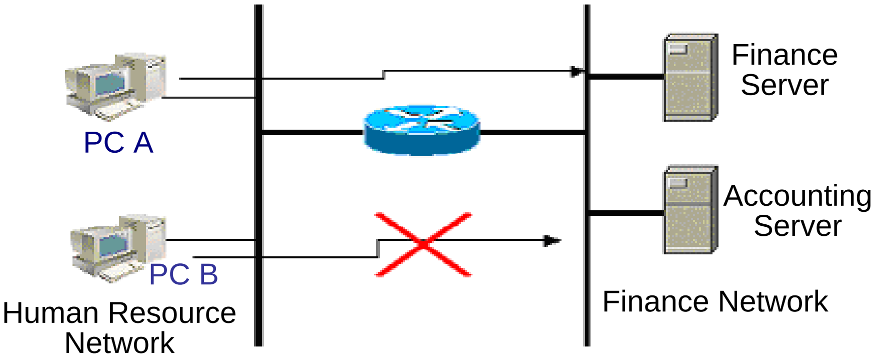
Access list rules can be about the source addresses, destination addresses, upper layer protocols, time-ranges or other information of data flows.

44.1.2 Why to Configure Access Lists

There are many reasons why we need configure access lists, shown as follows:

- Restrict route updating: Control the places of sending and receiving the route updating information.
- Restrict network access: To ensure network security, make users unable to access some services by defining rules. (When a user only needs to access the WWW and E-mail services, other services like TELNET are disabled). Or, allow users to access services only in a given period or only allow some hosts to access networks. Figure 45-1 is a case. In the case, only host A can access the Finance Network, while Host B cannot.

Figure 44-1 Using Access List to Control Network Access



44.1.3 When to Configure Access Lists

Depending on your requirements, you can select the basic access list or dynamic access list. In general, the basic access list can meet the security requirements. However, experienced hackers can provide spoof source addresses through some software so as to deceive the devices and successfully access the network. Before the user can access the network, the dynamic access list requires the pass of authentication so that the hackers are difficult to invade the network. So, in some sensitive areas the dynamic access list can be used to ensure the network security.

Note

The behavior of providing spoof source addresses to deceive devices is called spoofing and it is an inherent problem of all access lists. Even you use the dynamic list, a spoofing problem may occur. During the valid access period of an authenticated user, a hacker may use a counterfeit user address and accesses the network. There are two methods to solve the problem. One method is to set free time for a user to access the network as little as possible, making a hacker difficult to attack the network. The other method is to use the IPSEC encryption protocol to encrypt network data, ensuring that all the data entering devices are encrypted.

Access lists are usually configured in the following locations of network devices:

- Devices between the internal network and external network (such as the Internet)
- Devices at the borders of two parts in a network
- Devices on the access control port

The execution of the ACL statements must follow the statement order in the table strictly. Starting from the first statement, once the header of a packet matches a conditional judge statement in the table, the sequential statements are ignored.

44.1.4 Input/Output ACL, Filtering Domain Template and Rules

When a device interface receives a packet, the input ACL checks whether the packet matches an ACE of the input ACL on the interface. When a device interface is ready to output a packet, the output ACL checks whether the packet matches an ACE of the output ACL on the interface.

When detailed filtering rules are formulated, all or some of the above eight items may be used. As long as the packet matches one ACE, the ACL processes the pakcet as the ACE defined (permit or deny). The ACE of an ACL identifies Ethernet packets according to some fields of Ethernet packet. The fields include the following:

Layer-2 fields:

- 48-bit source MAC address (all the 48 bits must be declared)
- 48-bit destination MAC address (all the 48 bits must be declared)
- 16-bit layer-2 type field

Layer 3 fields:

- Source IP address field (you can specify all the address values of the IP address, or specify a type of streams of the defined subnet)
- Destination IP address field (you can specify all the address values of the IP address, or specify a type of streams of the defined subnet)
- Protocol type fields

Layer 4 fields:

- You can specify one TCP source port, destination port, or both
- You can specify one UDP source port, destination port, or both

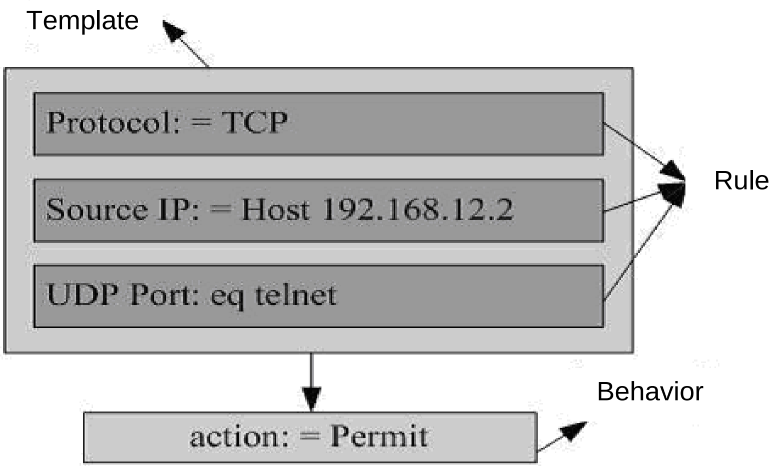
The filtering domain consists of the fields in the packets based on which the packets are identified and classified when you create an ACE. A filtering domain template is the definition formed by these field. For example, when one ACE is generated, you want to identify and classify packets according to the destination IP field of a packet. When another ACE is generated, you want to identify and classify packets according to the source IP address field of a packet and the source port field of UDP. In this way, these two ACEs use different filtering domain templates.

Rules refer to the values of the ACE filtering domain template. For example, one ACE is:

- **permit tcp host** *192.168.12.2* **any eq telnet**

In this ACE, the filtering domain template is a collection of the following fields: Source IP Address Fields, IP Protocol Fields and Destination TCP Port Fields. Corresponding values (rules) are respectively as follows: Source IP Address=host 192.168.12.2; IP Protocol=tcp; TCP Destination Port=Telnet.

Figure 44-2 Analysis of the ACE: **permit tcp host 192.168.12.2 any eq telnet**



Note

A filtering domain template can be the collection of L3 fields (Layer 3 Field) and L4 fields (Layer 4 Field) or the collection of multiple L2 fields (Layer 2 Field). However, the filtering domain templates of a standard and extended ACL cannot be the collection of L2 and L3, L2 and 4, L2 and L3, or L4 fields. To use the combination of L2, L3 and L4 fields, you can apply the Expert ACLs.

Precaustions for ACL associating with SVI in the DGS-3610 series out direction:

1. Priority higher than that of ACL in the in direction;
2. No default **deny any any**;
3. Supporting application of IP standard, IP extended, MAC extended and expert ACLs;
4. There are some restrictions during the matching of destination IP addresses and destination MAC addresses in ACL. If the destination MAC address is matched in MAC extended and expert ACLs, table entries are set but do not take effect when the ACL is applied in the SVI out direction. If the destination IP address is matched in IP standard, IP extended and expert ACLs, the configured ACL does not take effect when the destination IP

address is not in the IP range of the SVI-associated subnet. Suppose the IP address of vlan 1 is **192.168.64.1 255.255.255.0**, ACE is set to **deny udp any 192.168.65.1 0.0.0.255 eq 255**, and an IP extended ACL is created. The ACL does not take effect when it is applied to the output of vlan 1 because the destination IP is not in the IP range of the vlan 1 subnet. If ACE is set to deny udp any 192.168.64.1 0.0.0.255 eq 255, the ACL takes effect because the destination IP conforms to the rules.

5. If a member port of SVI is used for routing instead of directly connecting PC, the ACL in the SVI out direction does not take effect for packet flows that output at the member port.

6. Not supporting ACL in the out direction associated to routing port or L3 AP

44.2 Configuring IP Access Lists

To configure access lists on a device, you must specify unique names or numbers for the access lists of a protocol to uniquely identifying each access list inside the protocol. The following table lists the protocols that can use numbers to specify access lists and the number ranges of access lists that can be used by each protocol.

Protocol	Number Range
Standard IP	1-99, 1300 - 1999
Extended IP	100-199, 2000 - 2699

44.2.1 Guide to Configure IP Access Lists

When you create an access list, defined rules are applied to all packets on a device. The device decides to forward or block a packet by judging whether the packet matches a rule.

Basic Access Lists include standard access lists and extended access lists. The typical rules defined in access lists are as follows:

- Source address
- Destination address
- Upper layer protocol
- Time range

Standard IP access lists (1 – 99, 1300 – 1999) forward or block packets according to source IP addresses. Extended IP access lists (100 – 199, 2000 – 2699) use the above four combinations to forward or block packets. Other types of access lists forward or block packets according to related codes.

A single access list can use multiple separate access list statements to define multiple rules. Where, all statements use a same number or name to bind them to a same access list. However, the more the used statements, the more difficult to read and understand an access list.

44.2.1.1 Implicating "Deny Any Data Flow" Rule Statement

The ending part of each access list implicates a "Deny any data flow" rule statement. Therefore, if a packet matches no rule, it is denied.

as shown in the following example:

```
access-list 1 permit host 192.168.4.12
```

This list allows only the packets of host 192.168.4.12 and denies any other host. This is because the list contains the following rule statement at the end: **access-list 1 deny any**

Here is another example:

```
Access-list 1 deny host 192.168.4.12
```

If the list contains the only statement above, the packets from any host will be denied on the port.

Caution

It is required to consider the routing update packet when defining the access list. Since the end of the access list "denies all dataflow", this may cause all routing update packets blocked.

44.2.1.2 Order of Entering Rule Statements

Each added rule is appended to the access list. If a statement is created, then you cannot delete it separately and can only delete the whole access list. Therefore, the order of access list statements is very important. When deciding to forward or block packets, a device compares packets and statements in the order of statement creation. After finding a matching statement, it will not check other rule statements.

If you have created a statement and it allows all data flows to pass, the following statements will not be checked.

as shown in the following example:

```
access-list 101 deny ip any any
access-list 101 permit tcp 192.168.12.0 0.0.0.255  eq  telnet any
```

Because the first rule statement denies all IP packets, the host Telnet packet of the 192.168.12.0/24 network will be denied. When the device discovers that the packets match the first rule statement, it will not check other rule statements.

44.2.2 Configuring IP Access List

The configuration of the basic access list includes the following steps:

Define a basic access list

Apply the access list to a specific interface.

There are two methods to configure a basic access list.

Method 1: Run the following command in the global configuration mode:

Command	**Function**
DGS-3610(config)# **access-list** *id* {**deny** | **permit**} {src *src-wildcard* | **host** *src* | **any** } [**time-range** *tm-rng-name*]	Define an access list
DGS-3610(config)# **interface** *interface*	Select the interface to which the access list is applied.
DGS-3610(config-if)# **ip access-group** *id* { **in** | **out** }	Apply the access list to the specific interface

Method 2: Run the following command in the ACL configuration mode:

Command	**Function**
DGS-3610(config)# **ip access-list** { **standard** | **extended** } { *id* | *name* }	Enter the access list configuration mode
DGS-3610(config-xxx-nacl)# [*sn*] { **permit** | **deny** } {src *src-wildcard* | **host** *src* | **any** } [**time-range** *tm-rng-name*]	Add table entries for ACL. For details, please see command reference.
DGS-3610(config-xxx-nacl)# **exit** DGS-3610(config)# **interface** *interface*	Exit from the access control list mode and select the interface to which the access list is applied.
DGS-3610(config-if)# **ip access-group** *id* { **in** | **out** }	Apply the access list to the specific interface

Note

Method 1 only configures the numerical value ACL. Method 2 can configure names and numerical value ACL and specify the priorities of table entries (in the devices that support ACE priority levels).

44.2.3 Configuration of Showing IP Access Lists

To monitor access lists, please run the following command the in privileged user mode:

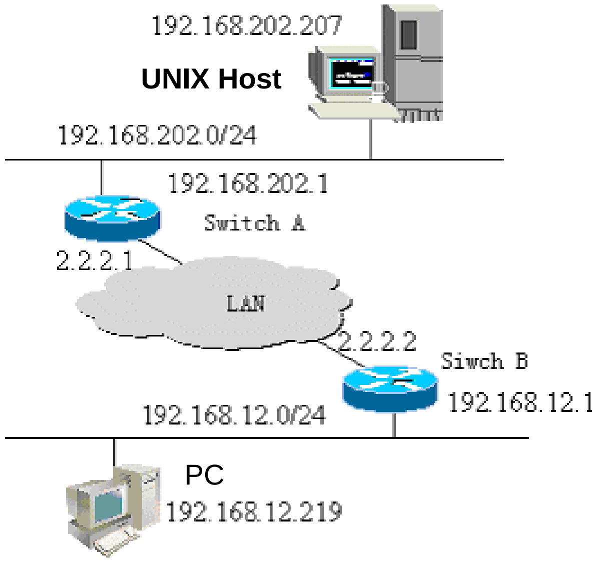
```
DGS-3610# show access-lists [ id | name ]
```

This command can be used to view the basic access list.

44.2.4 IP Access List Example

Configuration requirements: There are two devices Switch A and Switch B, as shown in Figure 45-3:

Figure 44-3 Basic Access List Example



To implement the following security functions by configuring access lists on Switch B:

Hosts in the 192.168.12.0/24 network segment can only access the remote TELNET services of UNIX hosts in the normal working period and deny the PING service.

On the Switch B console, access to any of the services of hosts in the 192.168.202.0/24 network segment is denied.

Note

The above case simplifies the application in the bank system. It only allows the hosts on the Local Area Network of branches or savings agencies to access the central host and forbids accessing the central host on the device.

- Device configuration

Switch B configuration:

```
DGS-3610(config)# interface GigabitEthernet 0/1
DGS-3610(config-if)# ip address 192.168.12.1 255.255.255.0
DGS-3610(config-if)# exit
DGS-3610(config)# interface GigabitEthernet 0/2
DGS-3610(config-if)# ip address 2.2.2.2 255.255.255.0
DGS-3610(config-if)# ip access-group 101 in
DGS-3610(config-if)# ip access-group 101 out
```

According to requirements, configure an extended access list numbered 101

```
DGS-3610(config)# access-list 101 permit tcp 192.168.12.0 0.0.0.255 any eq telnet
time-range check
DGS-3610(config)# access-list 101 deny icmp 192.168.12.0 0.0.0.255 any
DGS-3610(config)# access-list 101 deny ip 2.2.2.0 0.0.0.255 any
DGS-3610(config)# access-list 101 deny ip any any
```

Configure the time range

```
DGS-3610(config)# time-range check
DGS-3610(config-time-range)# periodic weekdays 8:30 to 17:30
```

Note

For access list 101. the last rule statement **access-list 101 deny ip any any** is not needed, for the ending part of the access list implicates a **deny any** rule statement.

Switch A configuration:

```
DGS-3610(config)# hostname DGS-3610
DGS-3610(config)# interface GigabitEthernet 0/1
DGS-3610(config-if)# ip address 192.168.202.1 255.255.255.0
DGS-3610(config)# interface GigabitEthernet 0/2
DGS-3610(config-if)# ip address 2.2.2.1 255.255.255.0
```

44.3 Configuring MAC Extended Access List

To configure MAC access lists on a device, you must specify unique names or numbers for the access lists of a protocol to uniquely identifying each access list inside the protocol. The following table lists the range of the numbers that can be used to specify MAC access lists.

Protocol	Number Range
MAC Extended Access List	700-799

44.3.1 Configuration of MAC Extended Access List

When you create an MAC access list, defined rules will be applied to all packets on a device. The device decides to forward or block a packet by judging whether the packet matches the rules.

The typical rules defined in MAC access lists are as follows:

- Source MAC address
- Destination MAC address
- Ethernet protocol type
- Time-range

The MAC extended access list (number 700 – 799) forwards or blocks the packets based on the source and destination MAC addresses, and can also match the Ethernet protocol type.

A single MAC access list can use multiple separate access list statements to define multiple rules. Where, all statements use a same number or name to bind these statements to a same access list.

44.3.2 Configuring MAC Extended Access List

The configuration of an MAC access list includes the following steps:

1. Define an MAC access list
2. Apply the access list to a specific interface

There are two methods to configure an MAC access list.

Method 1: Run the following command in the global configuration mode:

Command	Function
DGS-3610(config)# **access-list** *id* {**deny** | **permit**}{**any** | **host** *src-mac-addr*} {**any** | **host** *dst-mac-addr}* [*ethernet-type*] [**cos** *cos*]	Define an access list. For details about commands, please see command reference.
DGS-3610(config)# **interface** *interface*	Select the interface to which the access list is to be applied.
DGS-3610(config-if)# **mac access-group** *id* { **in** | **out** }	Apply the access list to the specific interface

Method 2: Run the following command in the ACL configuration mode:

Command	Function
DGS-3610(config)# **mac access-list extended** {*id* | *name*}	Enter the access list configuration mode
DGS-3610(config-mac-nacl)# [sn] { **permit** | **deny** }{**any** | **host** *src-mac-addr*} {**any** | **host** *dst-mac-addr*} [*ethernet-type*] [**cos** *cos*]	Add table entries for ACL. For details about commands, please see command reference.
DGS-3610(config-mac-nacl)# **exit** DGS-3610(config)# **interface** *interface*	Exit from the access control list mode and select the interface to which the access list is to be applied.
DGS-3610(config-if)# **mac access-group** {*id* | name} { **in** | **out**}	Apply the access list to the specific interface

Note

Method 1 only configures the numerical value ACL. Method 2 can configure names and numerical value ACL and specify the priorities of table entries (supporting priority ACE products).

44.3.3 Configuration of Showing MAC Extended Access Lists

To monitor access lists, please run the following command the in privileged mode:

```
DGS-3610# show access-lists [ id | name]
```

You can view basic access lists

44.3.4 MAC Extended Access List Example

You can implement the following security functions by configuring MAC access lists:

The 0013.2049.8272 host using the IPX protocol cannot access the giga 0/1 port of a device.

It can access other ports.

Configure an Ethernet port, apply the access list 101 on the Ethernet port and check all the packets passing in and out on the port.

```
DGS-3610> enable
DGS-3610# configure terminal
DGS-3610(config)# mac access-list extended mac-list
DGS-3610(config-mac-nacl)# deny host 0013.2049.8272 any ipx
DGS-3610(config-mac-nacl)# permit any any
DGS-3610(config-mac-nacl)# exit
DGS-3610(config)# interface gigabitEthernet 0/1
DGS-3610(config-if)# mac access-group mac-list in
DGS-3610(config-if)# end
DGS-3610# show access-lists
mac access-list extended mac-list
deny host 0013.2049.8272 any ipx
permit any any
DGS-3610#
```

Note

For access lists, **permit any any** cannot be discarded, for the ending part of an access list implicates a **deny any** rule statement.

44.4 Configuring Expert Extended Access List

To configure expert extended access lists on a device, you must specify unique names or numbers for the access lists of a protocol to uniquely identifying each access list inside the protocol.The table below lists the number range of the Expert access list.

Protocol	Number Range
Expert extended access list	2700-2899

44.4.1 Expert Extended Access List Configuration Guide

When you create an expert access list, defined rules will be applied to all packets on a device. The device decides to forward or block a packet by judging whether the packet matches the rules.

The typical rules defined in expert access lists are as follows:

All information in basic access lists and MAC extended access lists

VLAN ID

Expert extended access lists (2700 – 2899) are the syntheses of basic access lists and MAC extended access lists and can filter VLAN IDs.

A single expert access list can use multiple separate access list statements to define multiple rules. Where, all statements use a same number or name to bind these statements to a same access list.

44.4.2 Configuring Expert Extended Access Lists

The configuration of an expert access list includes the following steps:

1. Define an expert access list
2. Apply the access list to a specific interface (particular application case)

There are two methods to configure an expert access list.

Method 1: Run the following command in the global configuration mode:

Command	Function
DGS-3610(config)# **access-list** *id* {**deny** | **permit**} [*prot* | {[*ethernet-type*] [**cos** *cos*]}] [**VID** *vid*] {src *src-wildcard* | **host** *src* } {**host** *src-mac-addr* | **any**} {dst *dst-wildcard* | **host** *dst* | **any**}{**host** *dst-mac-addr* | **any**}] [**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*] [**time-range** *tm-rng-name*]	Define an access list. For details about commands, please see command reference.
DGS-3610(config)# **interface** *interface*	Select the interface to which the access list is applied.
DGS-3610(config-if)# **expert access-group** *id* {**in** | **out** }	Apply the access list to the specific interface

Method 2: Run the following command in the ACL configuration mode:

Command	Function
DGS-3610(config)# **expert access-list extended** *{id|name}*	Enter the access list configuration mode
DGS-3610(config-exp-nacl)# [*sn*]{ **permit** | **deny** }[*prot* | {[*ethernet-type*] [**cos** *cos*]}] [**VID** *vid*] {src *src-wildcard* | **host** *src* | **interface** *idx*}{**host** *src-mac-addr* | **any**} {dst *dst-wildcard* | **host** *dst* | **any**}{**host** *dst-mac-addr* | **any**}][**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*] [[**time-range** *tm-rng-name*]	Add table entries for ACL. For details about commands, please see command reference.
DGS-3610(config-exp-nacl)# **exit** DGS-3610(config)# **interface** *interface*	Exit from the access control list mode and select the interface to which the access list is applied.
DGS-3610(config-if)# **expert access-group** {*id*|*name*} {**in**|**out**}	Apply the access list to the specific interface

Note

Method 1 only configures the numerical value ACL. Method 2 can configure names and the numerical value ACL. In a version supporting priority table entries, method 2 can also specify the priorities of table entries (the [*sn*] option in a command).

44.4.3 Configuration of Showing Expert Extended Access Lists

To monitor access lists, please run the following command the in privileged user mode:

```
DGS-3610# show access-lists [id | name]
```

You can view expert access lists

44.4.4 Expert Extended Access List Example

You can implement the following security functions by configuring expert access lists:

The 0013.2049.8272 host using vlan 20 cannot access the giga 0/1 port of a device.

It cannot access other ports.

```
DGS-3610> enable
DGS-3610# config terminal
DGS-3610(config)# expert access-list extended expert-list
DGS-3610(config-exp-nacl)# permit ip vid 20 any host 0013.2049.8272 any any
DGS-3610(config-exp-nacl)# deny any any any any
DGS-3610(config-exp-nacl)# exit
DGS-3610(config)# interface gigabitEthernet 0/1
DGS-3610(config-if)# expert access-group expert-list in
DGS-3610(config-if)# end
DGS-3610# show access-lists
expert access-list extended expert-list
permit ip vid 20 any host 0013.2049.8272 any any
deny any any
```

44.5 Configuring IPv6 Extended Access List

44.5.1 Configuring IPv6 Extended Access List

The configuration of an IPv6 access list includes the following steps:

1. Define an IPv6 access list
2. Apply the access list to a specific interface (application particular case)

There is the following method to configure a basic access list. Run the following command in the ACL configuration mode:

Command	Function
DGS-3610(config)# **ipv6 access-list** *name*	Enter the access list configuration mode

Command	**Function**
DGS-3610(config-ipv6-nacl)# [*sn*] {**permit** | **deny** }*prot* {*src-ipv6-prefix/prefix-len* | **host** *src-ipv6-addr* | **any**} {*dst-ipv6-pfix/pfix-len* | **any** | **host** *dst-ipv6-addr*} [**dscp** *dscp*] [**flow-label** *flow-label*] [**time-range** *tm-rng-name*]	Add table entries for ACL. For details about commands, please see command reference.
DGS-3610(config-exp-nacl)# **exit** DGS-3610(config)# **interface** *interface*	Exit from the access control list mode and select the interface to which the access list is to be applied.
DGS-3610(config-if)# **ipv6 traffic-filter** *name* {**in** | **out**}	Apply the access list to the specific interface

44.5.2 Configuration of Showing IPv6Extended Access Lists

To monitor access lists, please run the following command the in privileged user mode:

```
DGS-3610# show access-lists [name]
```

This command can be used to view the basic access list.

44.5.3 IPv6 Extended Access List Example

You can implement the following security functions by configuring access lists:

The 192.168.4.12 host can access the gi 0/1 port of a device.

It cannot access other ports.

```
DGS-3610> enable
DGS-3610# config terminal
DGS-3610(config)# ipv6 access-list v6-list
DGS-3610(config-ipv6-nacl)# permit ipv6 ::192:68:4:12/24 any
DGS-3610(config-ipv6-nacl)# deny ipv6 any any
DGS-3610(config-ipv6-nacl)# exit
DGS-3610(config)# interface gigabitEthernet 0/1
DGS-3610(config-if)# ipv6 traffic-filter v6-list in
DGS-3610(config-if)# end
DGS-3610# show access-lists
ipv6 access-list extended v6-list
petmit ipv6 ::192.168.4.12 any
deny any any
DGS-3610#
```

44.6 Configuring Access List ACL80

The ACL80 is also called the user-defined access list, which means matching the first 80 bytes of a packet for filtering. A packet consists of a series of byte flows. The ACL80 enables a user to match and filter the specified 16 bytes by bits in the first 80 bytes.

Note

The specified 16 bytes do not include the following fields:

Packet SMAC, DMAC,SIP, DIP,ETYPE,PROTOCOL,L4_SPORT, L4_DPORT,VID.

Besides matching the above fields, you can match 16 bytes

For any 16-byte field, it is possible to compare the configured value by bits. In other words, it allows setting any bit of those 16 bytes to 0 or 1. There are two factors in filtering any byte: filtering rule and filter domain template. The bits of the both correspond to each uniquley. The filtering rule specifies the value of the field to be filtered. The filter domain template specifies whether to filter the related fields in the filtering rule (1 indicates matching the bit in the corresponding filtering rule, 0 for not). Therefore, when it is time to match a bit, it is required to set 1 for the corresponding bit in the filter domain template. If the filter domain template bit is set to 0, no match will be done no matter what the corresponding bit is in the filtering rule.

For example,

```
DGS-3610(config)# expert access-list advanced name
DGS-3610(config-exp-dacl)# permit 00d0f8123456 ffffffffffff 0
DGS-3610(config-exp-dacl)# deny 00d0f8654321 ffffffffffff 6
```

The user-defined access control list matches any byte of the first 80 bytes in the layer-2 data frames according to the user definitions, and then performs corresponding processing for the packets. To use the user-defined access control list correctly, it is necessary to have in-depth knowledge about the structure of layer-2 data frame. The following illustrates the first 64 bytes in a layer-2 data frame (each letter indicates a hexadecimal number, and each two letters indicate a byte).

AA AA AA AA AA AA BB BB BB BB BB BB CC CC DD DD

DD DD EE FF GG HH HH HH II II JJ KK LL LL MM MM

NN NN OO PP QQ QQ RR RR RR RR SS SS SS SS TT TT

UU UU VV VV VV VV WW WW WW WW XY ZZ aa aa bb bb

In the figure above, the meaning of each letter and the value of offset are shown below:

Letter	Meaning	Offset	Letter	Meaning	Offset
A	Destination MAC	0	O	TTL field	34
B	Source MAC	6	P	Protocol ID	35
C	Data frame length field	12	Q	IP checksum	36

Letter	Meaning	Offset	Letter	Meaning	Offset
D	VLAN tag field	14	R	Source IP address	38
E	DSAP (destination service access point) field	18	S	Destination IP address	42
F	SSAP (source service access point) field	19	T	TCP source port	46
G	Ctrl field	20	U	TCP destination port	48
H	Org Code field	21	V	Sequential number	50
I	Encapsulated data type	24	W	Confirmation field	54
J	IP version No.	26	XY	IP header length and reservation bits	58
K	TOS field	27	Z	Reservation bit and flags bit	59
L	IP packet length	28	a	Windows size field	60
M	ID	30	b	Others	62
N	Flags field	32			

In the table above, the offset of each field is the same as that in the SNAP+tag 802.3 data frame. In the user-defined access control list, the user can use two parameters, the rule mask and offset, to abstract any byte from the first 64 bytes of the data frame, and then compare it with the user defined rule to filter the matched data frame for corresponding processing. The user defined rule can be some fixed attributes of the data. For example, the user wants to filter all the TCP packets by defining the rule as 06, rule mask as FF and offset as 35. Here, the rule mask and offset work together to abstract the contents of the TCP protocol ID field in the received data frame, and compare it with the rule to filter all TCP packets.

Note

DGS-3610-26P does not support ACL80. ACL80 does not support the function of matching packets of Ethernet, 803.3snap and 802.3llc. If the value of matching DSAP to the cntl field is set to AAAA03, it indicates the 803.3snap packet is to be matched. If the value is set to E0E003, it indicates that the 803.3llc packet is to be matched. The field cannot be matched for Ethernet packets.

Precautions for configuration:

Only 16 bytes can be matched at will for ACL80. If the resource is occupied, you cannot match any other byte. For example,

```
DGS-3610(config)# expert access-list advanced name
DGS-3610(config-exp-dacl)#permit 11223344556677889900aabbccd
deeff ffffffffffffffffffffffffffffffff 50
```

Add another ACE:

```
DGS-3610(config-exp-dacl)#permit 11223344556677889900aabbccd
```

```
deeff ffffffffffffffffffffffffffffff 54
```

Configuration of the second ACE fails because the 16 bytes are occupied by the first ACE. To configure for the second ACE, you must delete the first one.

44.7 Configuring TCP Flag Filtering Control

The TCP flag filtering feature provides a flexible mechanism. At present, TCP flag filtering control supports the match-all option. When the TCP flags in a received packet exactly match those defined in the ACL table entry, the packet will be checked by the ACL rule. A user can define any combination of TCP flags to filter some packets with specific TCP flags.

For example,

```
permit tcp any any match-all rst
```

Allow the packets with a TCP flag RST set and 0 in other positions to pass

Note

When the protocol number of the naming ACL and numerical value configuration is TCP, you can select to configure this filtering feature. MAC extended and IP standard ones do not have this function.

Please configure a TCP Flag by following these steps:

Command	Function
DGS-3610(config)# **ip access-list extended** { id | *name* }	Enter the access list configuration mode
DGS-3610(config-ext-nacl)# [*sn*] [**permit** | **deny**] **tcp** *source source-wildcard* [**operator port** [*port*]] *destination destination-wildcard* [**operator port** [*port*]] [**match-all** *flag-name*][**precedence** *precedence*]	Add table entries for ACL. For details about commands, please see command reference.
DGS-3610(config-exp-nacl)# **exit** DGS-3610(config)# **interface** *interface*	Exit from the access control list mode and select the interface to which the access list is to be applied.
DGS-3610(config-if)# **ip access-group** {*id* | *name*} {**in** | **out**}	Apply the access list to the specific interface

The following example explains how to configure a TCP Flag

1. Enable rights and password

```
DGS-3610> enable
DGS-3610#
```

2. Enter the global configuration mode.

```
DGS-3610# configure terminal
DGS-3610(config)#
```

3. Enter the ACL configuration mode.

```
DGS-3610(config)# ip access-list extended test-tcp-flag
DGS-3610(config-ext-nacl)#
```

4. Add an ACL entry

```
DGS-3610(config-ext-nacl)# permit tcp any any match-all rst
```

5. Add a deny entry

```
DGS-3610(config-ext-nacl)# deny tcp any any match-all fin
```

6. Adding/delete entries repeatedly.

7. end

```
DGS-3610(config-ext-nacl)# end
```

8. Show

```
DGS-3610# show  access-list test-tcp-flag
ip access-lists extended test-tcp-flag
10 permit tcp any any match-all rst
20 deny tcp any any match-all fin
```

44.8 Configuring ACL Entries by Priority

To embody the ACE priority, there are standards for each ACL to normalize the ACE arranging method under the ACL by using the numbered start point – increment mode, as detailed below:

- ACE is sorted in the ascend order in the chain table by the sequential numbers
- Starting from the start point number, if no number is specified, it increases by step on the basis of the previous ACE number.
- To specify number, the ACE is inserted in sorting mode, and the increment ensures new ACE can be inserted between two adjacent ACEs.
- The ACL specifies the start point number and the number increment.

The **ip access-list resequence** {*acl-id*| *acl-name*} *sn-start sn-inc* command is available, with details in the related command reference.

Whenever the above command is run, the ACEs will be re-sorted under the ACL list. For example, the ACE numbers under the ACL named tst_acl is as follows:

In the beginning

```
ace1: 10
ace2: 20
ace3: 30
```

The ACE numbers are as follows after **ip access-list resequence** *tst_acl 100 3* is run:

```
DGS-3610(config)# ip access-list resequence tst_acl 100 3
ace1: 100
ace2: 103
ace3: 106
```

When adding ace4 without entering sn-num, the numbers are as follows:

```
DGS-3610(config-std-nacl)# permit …
ace1: 100
ace2: 103
ace3: 106
ace4: 109
```

When adding ace5 by entering seq-num = 105, the numbers are as follows:

```
DGS-3610(config-std-nacl)# 105 permit …
ace1: 100
ace2: 103
ace5: 105
ace3: 106
ace4: 109
```

The reference of the numbers is to implement the priority adding ace mode in step 4.

Delete ACE

```
DGS-3610(config-std-nacl)# no 106
ace1: 100
ace2: 103
ace5: 105
ace4: 109
```

The above numbers can also facilitate deleting ACE.

44.9 Configuring ACL Based on Time-range

You can run the ACLs based on time, for example, make the ACL take effect during certain periods in a week. For this purpose, you must first set a time-range.

time-range implementation depends on the system clock. If you want to use this function, you must assure that the system has a reliable clock.

In the privileged configuration mode, you can create a time-range through the following steps:

Command	Function
DGS-3610# **configure terminal**	Enter the global configuration mode.
DGS-3610(config)# **time-range** *time-range-name*	Identify a time-range by using a meaningful display character string as its name

Command	**Function**
DGS-3610(config-time-range)# **absolute** [**start time** date] **end time** *date*	Set the absolute time range (optional). For details, see the configuration guide of time-range.
DGS-3610(config-time-range)# **periodic** *day-of-the-week time* **to** [*day-of-the-week*] *time*	Set the periodic time range (optional). For details, see the configuration guide of time-range.
DGS-3610# **show time-range**	Verify the configurations.
DGS-3610# **copy running-config startup-config**	Save the configuration.
DGS-3610(config)# **ip access-list extended** *101*	Enter the ACL configuration mode.
DGS-3610(config-ext-nacl)# **permit ip any any time-range** *time-range-name*	Configure the ACE of a time-range.

Note

The length of the name should be 1-32 characters, not including space.

You can set one absolute time range at most. The application based on time-ranges will be valid only in this time range.

You can set one or more periodic intervals. If you have already set a running time range for the **time-range**, the application takes effect at periodic intervals in that time range.

The following example shows how to deny HTTP data flows during the working hours in a week by using the ACLs as example:

```
DGS-3610(config)# time-range no-http
DGS-3610(config-time-range)# periodic weekdays 8:00 to 18:00
DGS-3610(config)# end
DGS-3610(config)# ip access-list extended limit-udp
DGS-3610(config-ext-nacl)# deny tcp any any eq www time-range no-http
DGS-3610(config-ext-nacl)# exit
DGS-3610(config)# interface gigabitEthernet 0/1
DGS-3610(config-if)# ip access-group no-http in
DGS-3610(config)# end
```

Example of displaying time range:

```
DGS-3610# show time-range
time-range entry: no-http(inactive)
periodic Weekdays 8:00 to 18:00
time-range entry: no-udp
periodic Tuesday 15:30 to 16:30
```

44.10 Configuration Examples

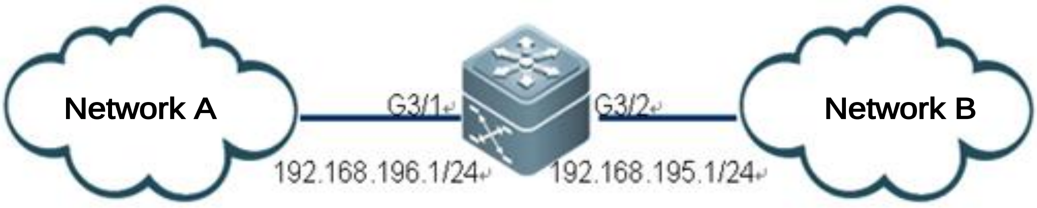
44.10.1 Configuring TCP One-Way Connection

The one-way ACL function can be enabled through the configuration of TCP flag filtering

44.10.1.1 Configuration Requirements

To ensure the security of network A, the host of network A can initiate a TCP communication request to the host of network B. But on the contrary, the host of network B cannot initiate any TCP communication request to the host of netowrk A.

44.10.1.2 Topology



As shown in the figure above, two networks are connected through a L3 switch. Network A is connected to the G3/1 interface and network B is connected to the G3/2 interface.

44.10.1.3 Analysis

To forbid the host of network B from initiating any TCP communication request to network A, you can perform configuration to filter TCP connection request packets initiated from network B and forwarded at the G3/2 interface. According to the TCP connection process, the SYN flag of the initial TCP flag field in the initial TCP request packet can be set and the ACK flag bit is set to 0. You can select the **Match-all** option in the extended access control list to filter the packets with the initial SYN flag bit set to 1 and ACK flag bit set to 0 in the G3/2 input direction, thus implementing one-way access from network A to network B.

44.10.1.4 Configuration Steps

1) Defining an access control list

```
# Enter the switch configuration mode.
DGS-3610# configure terminal
# Create an extended ACL ACL101 in the configuration mode.
DGS-3610(config)# ip access-list extended 101
# Deny the packets with the SYN of TCP Flag set to 1 and other flag bits (including the
ACK flag bit) set to 0.
DGS-3610(config-ext-nacl)# deny tcp any any match-all SYN
```

```
# Permit other IP packets
DGS-3610(config-ext-nacl)# permit ip any any
```

2) Applying the ACL to the interface

```
# Exit the ACL mode.
DGS-3610(config-ext-nacl)# exit
# Enter the application of the interface G3/2
DGS-3610(config)# interface gigabitEthernet 3/2
# Apply ACL 101 in packet filtration in the G3/2 input direction
DGS-3610(config-if)# ip access-group 101 in
```

3) Showing ACL configuration

```
# In the privileged mode, execute the show command to display ACL configuration.
DGS-3610# show access-lists 101
ip access-list extended 101
 10 deny tcp any any match-all syn
 20 permit ip any any
```

45 QOS Configuration

45.1 QOS Overview

The fast development of the Internet results in more and more demands for multimedia streams. Generally, people have different service quality requirements for different multimedia, which requires the network to be able to allocate and dispatch resources according to the user demands. As a result, the traditional "best effort" forwarding mechanism cannot meet the user demands. So the QOS emerges.

The QOS (Quality of Service) is used to evaluate the ability for the service provider to meet the customer demands. In the Internet, the QOS mechanism is introduced to improve the network service quality, where the QOS is used to evaluate the ability of the network to deliver packets. The commonly-mentioned QOS is an evaluation on the service ability for the delay, jitter, packet loss and more core demands.

45.1.1 Basic Framework of QoS

The devices that have no QoS function cannot provide the capability of transmission quality service, and will not ensure special forwarding priority for certain dataflow. When abundant bandwidth, all the traffic can be well processed. But when congestion occurs, all traffic also has an equal chance of being dropped.This kind of forwarding policy is otherwise called the service of best effect, since the device now is exerting its performance of data forwarding and the use of its switching bandwidth is maximized.

The device of this module features the QoS function to provide transmission quality service. This makes it possible to select specific network traffic, prioritize it according to its relative importance, and use congestion-management and congestion-avoidance techniques to provide preferential treatment. The network environment with QoS configured is added with predictability of network performance and allocates network bandwidth more effectively to maximize the use of network resources.

The QoS of this device is based on the DiffServ (Differentiated Serve Mode) of the IETF Internet Engineering Task Force. According to the definitions in the DiffServ architecture, every transmission packet is classified into a category in the network, and the classification information is included in the IP packet header. The first 6 bits in the TOS (Type Of Service) field for IPv4 packet header or the Traffic Class field for Ipv6 packet header carry the classification information of the packet. The classification information can also be carried in the Link layer packet header. Below shows the special bits in the packet:

- Carried by the first 3 bits in the Tag Control Information of 802.1Q frame header, which contains the priority information of one of the 8 categories. These three bits are generally called User Priority bits.
- Carried by the first 3 bits of the TOS field for IPv4 packet header or Traffic Class field for IPv6 packet header, called IPprecedence value; or carried by the first 6 bits of the TOS field for IPv4 packet header or Traffic Class field for IPv6 packet header, called Differentiated Services Code Point (DSCP) value.

In a DiffServ-compliant network, every device has the same transmission service policy for the packets with the same classification information, and vice versa. The class information in the packet can be assigned by all the systems along the way, such as hosts, devices, or other network devices. It's based on a policy set by a manager, or contents in the packet, or both. The assignment of class information in order to identify packets usually consumes enormous resources of the network device. To reduce the processing overhead on the backbone network, such assignment is often used on the network edge. Based on the class information, the devices can provide different priorities for different traffic, or limit the amount of resources allocated per traffic class, or appropriately discard the packets of less important, or perform other operations. This behavior of these independent devices is called per-hop behavior in the DiffServ architecture.

If all devices in the network are providing consistent per-hop behavior, this network forms the end-to-end QoSsolution for the DiffServ architecture.

45.1.2 QOS Processing Flow

45.1.2.1 Classifying

The process of classifying involves putting the packets to the dataflow indicated with CoS value according to the trust policy or the analysis of the packet contents. As a result, the core task of classifying is to determine the CoS value of a packet. It happens when the port is receiving the inbound packets. When a port is associated with a policy-map that represents a QoS policy, the classification will take effect and be applied on all the packets input through that port.

For general non-IP packets, the switch classifies the packets according to the following criteria:

- If the packet itself does not contain any QoS information, which means the layer-2 packet header has no User Priority bits, it gets the QoS information of the packet by using the default CoS value of the packet input port. Like the User Priority bits of the packet, the default CoS value of the port ranges 0~7.
- If the packet itself contains QoS information, which means the layer-2 packet header has User Priority bits, it gets the CoS information directly from the packet.

Note

The above criteria take effect only when the QoS trust mode of the port is enabled. Enabling the QoS trust mode of a port does not mean getting the QoS information directly from the packet or the input port of the packet without analyzing the packet contents.

- If the policy-map associated with the port is using the ACL classifying based on the mac access-list extended, the associated ACLs will be matched by getting the source MAC address, destination MAC address and Ethertype domain of the packet on that port, to determine the DSCP value of the packet. Note that, if a port is associated with a policy-map but has no DSCP value set for it, the device will assign the priority for the packets of this classification through the default behavior: following the priority information contained in the layer-2 packet header of the packet or the default priority of the port.

Note

The above three criteria may apply simultaneously on the same port. In this case, they will take effect according to the sequence 3, then 2 and then 1. In other words, the ACLs work first for the classifying operation. When it fails, the criteria 2 will be used, and so on. Here, if the QoS trust mode of the port is enabled, criteria 2 and 1 will be used to get the QoS information directly from the packet or the port; otherwise, default DSCP value 0 will be assigned for the packets failing the classifying operation.

For IP packets, the device classifies the packets according to the following criteria:

- If the port trust mode is Trust ip-precedence, it extracts from the ip precedence field (3 bits) of the IP packet and fills the CoS field (3 bits) of the output packet.
- If the port trust mode is Trust cos, it extracts directly the CoS field (3 bits) of the packet and overwrite the ip precedence field (3 bits) of the packet. There are the following two cases. Case 1 is that the layer-2 packet header does not contain User Priority bits, and now the CoS value is got from the default CoS value of the packet input port. Case 2 is that the layer-2 packet header contains User Priority bits, and now the CoS is got directly from the packet header.
- If the Policy-map associated with the port is using the ACLs classifying based on the ip access-list (extended), the associated ACLs will be matched by getting the source IP address, destination IP address, Protocol field and layer-4 TCP/UDP port field of the packet, to determine the DSCP value of the packet, and the CoS value is determined according to the mapping from DSCP to CoS. Note that, if a port is associated with a policy-map but has no DSCP value set for it, the switch will use the above criteria 1 and 2 to determine the priority.

Just like the criteria for non-IP packet classifying, the above classifying criteria can apply on the same port at the same time. In this case, they will take effect according to the sequence 3, then 2 and then 1.

For details of the CoS-to-DSCP map and IP-precedence-to-DSCP map, see the descriptions below.

45.1.2.2 Policing

The Policing action happens after the data classifying is completed. It is used to constrain the transmission bandwidth occupied by the classified dataflow. The Policing action will check every packet in the classified dataflow. If the packet is occupying more bandwidth as allowed by the police that applies on that dataflow, the packet will be treated specially, either to be discarded or assigned with another DSCP value.

In the QoS processing flow, the Policing action is optional. If no Policing action is enabled, the DSCP value of packets in the classified data flow will remain unchanged, and no packet will be discarded before the packet is sent for the Marking action.

45.1.2.3 Marking

After the Classifying and Policing actions, the Marking action will write the QoS information for the packet to ensure that the DSCP value of the classified packet can be transferred to the next hop device in the network. Here, the QoS ACLs can be used to change the QoS information of the packet, or the QoS information is reserved in the Trust mode. For example, the Trust DSCP can be selected to reserve the DSCP information in the IP packet header.

45.1.2.4 Queuing

The Queuing action is responsible for transferring the packets in the dataflow to an output queue of the port. The packets in different output queues will have transmission service policies of different levels and qualities.

Each port has 8 output queues. The two mapping tables DSCP-to-CoS Map and Cos-to-Queue Map configured on the device convert the DSCP value of the packet into output queue number so as to determine the specific output queue to transfer the packets into.

45.1.2.5 Scheduling

The Scheduling action is the last cycle in the QoS process. After the packets are transferred into different output queues of the port, the device works with WRR or another algorithm to transmit the packets in those 8 queues.

It is possible to set the weight in the WRR algorithm to configure the number of packets to be transmitted in every cycle of packet output, thus affecting the transmission bandwidth. Alternatively, it is possible to set the weight in the DRR algorithm to configure the number of packet bytes to be transmitted in every cycle of packet output, thus affecting the transmission bandwidth.

45.2 Configuring QOS

45.2.1 Default QOS Configuration

Make clear the following points of QoS before configuration:

- One interface can be associated with at most one policy-map.
- One policy-map can have multiple class-maps.
- One class-map can be associated at most one ACL, and all ACEs in that ACL must have the same filter domain template.
- The number of ACEs associated with one interface meets the constraint described in the section **Configuring secure ACL**.

By default, the QoS function is disabled. That is, the device treats all packets equally. When you associate a Policy Map with a port and set the trust mode of the port, the QoS function of that port is enabled. To disable the QoS function of a port, you may remove the Policy Map setting and set the trust mode of the port to Off. Below is the default QoS configuration:

Default CoS value	0
Number of Queues	8
Queue Scheduling	WRR
QueueWeight	1:1:1:1:1:1:1:1
WRR Weight Range	1:15
DRR Weight Range	1:15
Trust mode	No Trust

Default mapping table from CoS value to queue

CoS Value	0	1	2	3	4	5	6	7
Queue	1	2	3	4	5	6	7	8

Default mapping table from CoS to DSCP

CoS Value	0	1	2	3	4	5	6	7
DSCP value	0	8	16	24	32	40	48	56

Default mapping table from IP-Precedence to DSC

IP-Precedence	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

Default mapping table from DSCP to CoS

DSCP	0	8	16	24	32	40	48	56
CoS	0	1	2	3	4	5	6	7

45.2.2 Configuring the QOS Trust Mode of the Interface

By default, the QoS trust mode of an interface is disabled.

Command	Description
configure terminal	Enter the configuration mode
interface *interface*	Enter the interface configuration mode.
mls qos trust {cos | ip-precedence | dscp}	Configure the Qos trust mode of the interface Cos, dscp or ip-precedence
no mls qos trust	Restore the Qos trust mode of the interface to default

The command below set the trust mode of interface gigabitEthernet 0/4 to DSCP:

```
DGS-3610(config)# interface gigabitEthernet 0/4
DGS-3610(config-if)# mls qos trust dscp
DGS-3610(config-if)# end
DGS-3610# show mls qos interface g0/4
Interface GigabitEthernet 0/4
Attached input  policy-map:
Default COS: trust dscp
Default COS: 0
DGS-3610#
```

45.2.3 Configuring the Default CoS Value of an Interface

You may configure the default CoS value for every interface through the following steps.

By default, the CoS value of an interface is 0.

Command	Description
configure terminal	Enter the configuration mode
interface *interface*	Enter the interface configuration mode.
mls qos cos *default-cos*	Configure the default CoS value of the interface, where default-cos is the desired default CoS value, ranging 0~7.
no mls qos cos	Default CoS value

The example below sets the default CoS value of interface g0/4 to 6:

```
DGS-3610# configure terminal
DGS-3610(config)# interface g 0/4
DGS-3610(config-if)# mls qos cos 6
DGS-3610(config-if)# end
DGS-3610# show mls qos interface g 0/4
Interface GigabitEthernet 0/4
Attached input  policy-map:
```

```
Default COS: trust dscp
Default COS: 6
DGS-3610#
```

45.2.4 Configuring Class Maps

You may create and configure Class Maps through the following steps:

Command	Description
configure terminal	Enter the configuration mode
ip access-list extended {*id* | *name*} **…** **ip access-list standard** {*id* | *name*} **…** **mac access-list extended** {*id* | *name*} **…** **expert access-list extended** {*id* | *name*} **…** **ipv6 access-list extended** *name* **…** **access-list** *id* [**…**]	Create ACL Please refer to the chapter of ACL
[no] class-map *class-map-name*	Create and enter into the class map configuration mode, where class-map-name is the name of the class map to be created. The no option will delete an existing class map
[no] match access-group {*acl-num* | *acl-name* }	Set the matching ACL, where a*cl-name* is the name of the created ACL, acl-num is the ID of the created ACL; the no option delete that match.

For example, the following steps creates a class-map named class1, which is associated with an ACL:acl_1. This class-map will classify all TCP packets with port 80.

```
DGS-3610(config)# ip access-list extended acl_1
DGS-3610(config-ext-nacl)# permit tcp any any eq 80
DGS-3610(config-ext-nacl)# exit
DGS-3610(config)# class-map class1
DGS-3610(config-cmap)# match access-group acl_1
DGS-3610(config-cmap)# end
```

45.2.5 Configuring Policy Maps

You may create and configure Policy Maps through the following steps:

Command	Description
configure terminal	Enter the configuration mode
[no] policy-map *policy-map-name*	Create and enter into the policymap configuration mode, where policy-map-name is the name of the policymap to be created. The no option will delete an existing policy map.
[no] class *class-map-name*	Create and enter into the data classifying configuration mode, where class-map-name is the name of the class map to be created. The **no** option deletes that data classification.
[no]set ip dscp *new-dscp*	Set new ip dscp value for the IP packets in the dataflow; it does not take effect for non-IP packets. *new-dscp* is the new DSCP value to be set, whose range varies with the specific product.
police *rate-bps burst-byte* **[exceed-action** {**drop** | **ds*cp*** *dscp-value*}] **no police**	Limit the bandwidth of the dataflow and specify the action for the excessive bandwidth part, where *rate-bps* is the limited bandwidth per second (kbps). *burst-byte* is the limited burst bandwidth (Kbyte). **drop** means dropping the packet of the excessive bandwidth part, **dscp** *dscp-value means changing the* DSCP value of the packet in excessive bandwidth part, and *dscp-valu*e value range varies with specific products.

For example, the following steps create a policy-map named policy1 and associate it with interface gigabitethernet 1/1.

```
DGS-3610(config)# policy-map policy1
DGS-3610(config-pmap)# class class1
DGS-3610(config-pmap-c)# set ip dscp 48
DGS-3610(config-pmap-c)# exit
Router(config-pmap)# exit
DGS-3610(config)# interface gigabitethernet 1/1
DGS-3610(config-if)# switchport mode trunk
DGS-3610(config-if)# mls qos trust cos
DGS-3610(config-if)# service-policy input policy1
```

45.2.6 Configuring the Interface to Apply Policy Maps

You may apply the Policy Maps to a port through the following steps:

Command	Description
configure terminal	Enter the configuration mode
interface *interface*	Enter the interface configuration mode.

Command	Description
[**no**] **service-policy** {**input** | **output**} *policy-map-name*	Apply the created policy map to the interface, where the *policy-map-name* is the name of the created policy map, input is the input rate limit and output is the output rate limit.

45.2.7 Configuring the Output Queue Scheduling Algorithm

You may schedule the algorithms for the output queue of a port: WRR, SP, RR and DRR. By default, the output queue algorithm is WRR (Weighted Round-Robin).

You may set the port priority queue scheduling method through the following steps. For details of the algorithm, see the **Overview of QoS**.

Command	Description
configure terminal	Enter the configuration mode
mls qos scheduler {**sp** | **rr** | **wrr** | **drr**}	Set the port priority queue scheduling algorithm, where **sp** is absolute priority scheduling, **rr** is round-robin, **wrr** is weighted round-robin with frame quantity, and **drr** weighted round-robin with frame length
no mls qos scheduler	Restore the default **wrr** scheduling

Note

The DGS-3610 products do not support the WFQ scheduling algorithm.

In the stack mode, if the QOS mapping table is set to a non-default value, the incoming packets from the stack port are still scheduled according to the default queue mapping relationship.

If the WRR algorithm is configured and the weight of each ouput queque is changed, output packets may not be distributed according to the weight if the output rate limit of the output port is set to a value less than 128Kbps.

For example, the following steps set the port output algorithm to SP:

```
DGS-3610# configure terminal
DGS-3610(config)# mls qos scheduler sp
DGS-3610(config)# end
DGS-3610# show mls qos scheduler
Global Multi-Layer Switching scheduling
Strict Priority
DGS-3610#
```

45.2.8 Configuring Output Round-Robin Weight

You may set the output round-robin weight through the following steps:

Command	Description
configure terminal	Enter the configuration mode
{**wrr-queue** | **drr-queue**} **bandwidth** *weight1...weightn*	**weight1...weightn** are the weight values specified for the output queues. For the count and value range, see the default QoS settings
no {**wrr-queue** | **drr-queue**} **bandwidth**	The no option restores the default weight value.

The example below sets the wrr scheduling weight to 1:2:3:4:5:6:7:8

```
DGS-3610# configure terminal
DGS-3610(config)# wrr-queue bandwidth 1 2 3 4 5 6 7 8
DGS-3610(config)# end
DGS-3610# show mls qos queuing
Cos-queue map:
cos qid
--- ---
0   1
1   2
2   3
3   4
4   5
5   6
6   7
7   8
wrr bandwidth weights:
qid weights
--- -------
0   1
1   2
2   3
3   4
4   5
5   6
6   7
7   8
DGS-3610(config)#
```

45.2.9 Configuring Cos-Map

You may set cos-map to select the queue the output packets enter. The default value of cos-map is provided in the default QoS configuration section.

Command	Description
configure terminal	Enter the configuration mode
priority-queue Cos-Map *qid cos0 [cos1 [cos2 [cos3 [cos4 [cos5 [cos6 [cos7]]]]]]]*	*qid* is the queue id; *cos0..cos7* are the CoS values associated with that queue.
no priority-queue cos-map	Restore default of cos-map

Below is the example of configuring CoS Map

```
DGS-3610# configure terminal
DGS-3610(config)# priority-queue Cos-Map 1 2 4 6 7 5
DGS-3610(config)# end
DGS-3610# show mls qos queuing
Cos-queue map:
cos qid
--- ---
0   1
1   2
2   1
3   4
4   1
5   1
6   1
7   1

wrr bandwidth weights:
qid weights
--- -------
0   1
1   2
2   3
3   4
4   5
5   6
6   7
7   8
```

45.2.10 Configuring CoS-to-DSCP Map

CoS-to-DSCP Map is used to map the CoS value of a packet to internal DSCP value. You may follow these steps to set CoS-to-DSCP Map. The default value of CoS-to-DSCP is provided in the default QoS configuration section.

Command	Description
configure terminal	Enter the configuration mode
mls qos map cos-dscp *dscp1...dscp8* **no mls qos map cos-dscp**	Change the CoS-to-DSCP Map settings, where dscp1...dscp8 are the DSCP values corresponding to CoS values 0 ~ 7. The DSCP value range varies with specific products.

For Example:

```
DGS-3610# configure terminal
DGS-3610(config)# mls qos map cos-dscp 56 48 46 40 34 32 26 24
DGS-3610(config)# end
DGS-3610# show mls qos maps cos-dscp
cos dscp
--- ----
0   56
1   48
2   46
3   40
4   34
5   32
6   26
7   24
```

45.2.11 Configuring DSCP-to-CoS Map

DSCP-to-CoS is used to map the internal DSCP value of a packet to CoS value so that it is possible to select output queue for packets.

The default value of DSCP-to-CoS Map is provided in the default QoS configuration section. You may follow these steps to set DSCP-to-CoS Map:

Command	Description
configure terminal	Enter the configuration mode
mls qos map dscp-cos *dscp-list* **to** *cos*	Set CoS to DSCP Map, where dscp-list is the list of DSCP values to be set, DSCP values separated by spaces, value range varying with specific products, cos means the CoS values corresponding to the DSCP values, ranging 0~7
no mls qos map dscp-cos	Restore the default value

For example, the following steps set the DSCP values 0, 32 and 56 to map 6:

```
DGS-3610# configure terminal
DGS-3610(config)# mls qos map dscp-cos 0 32 56 to 6
DGS-3610(config)# show mls qos maps dscp-cos
dscp cos    dscp cos   dscp cos   dscp cos
---- ---    ---- ---   ---- ---   ---- ---
 0   6       1   0      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
20   2      21   2     22   2     23   2
24   3      25   3     26   3     27   3
28   3      29   3     30   3     31   3
32   6      33   4     34   4     35   4
36   4      37   4     38   4     39   4
40   5      41   5     42   5     43   5
44   5      45   5     46   5     47   5
48   6      49   6     50   6     51   6
52   6      53   6     54   6     55   6
56   6      57   7     58   7     59   7
60   7      61   7     62   7     63   7
```

45.2.12 Configuring Port Rate Limit

You may follow these steps to limit the port rate:

Command	Description
configure terminal	Enter the configuration mode
interface *interface*	Enter the interface configuration mode.
rate-limit output *bps burst-size*	Port rate limit, where input is the input rate limit, output is the output rate limit, bps is the bandwidth limit per second (kbps), and burst-size is the burst bandwidth limit (Kbyte)
no rate-limit	Cancel port rate limiting

```
DGS-3610# configure terminal
DGS-3610(config)# interface gigabitEthernet 0/4
DGS-3610(config-if)# rate-limit input 100 100
DGS-3610(config-if)# end
DGS-3610#
```

45.2.13 Configuring IPpre to DSCP Map

IPpre-to-Dscp is used to map the IPpre values of a packet to internal DSCP values. The default settings of IPpre-to-DSCP Map are provided in the default QoS configuration section. you may follow these steps to configure IPpre-to-Dscp Map:

Command	Description
configure terminal	Enter the configuration mode
mls qos map ip-prec-dscp *dscp1...dscp8*	Modify the setting of IP-Precedence-to-Dscp Map, where dscp1...dscp8 are the DSCP values corresponding to IP-Precedence values 0~7
no mls qos map ip-prec-dscp	

For Example:

```
DGS-3610# configure terminal
DGS-3610(config)# mls qos map ip-precedence-dscp 56 48 46 40 34 32 26 24
DGS-3610(config)# end
DGS-3610# show mls qos maps ip-prec-dscp
ip-precedence dscp
------------- ----
0     56
1     48
2     46
3     40
4     34
5     32
6     26
7     24
```

45.3 QOS Display

45.3.1 Showing class-map

You may show the contents of class-map through the following steps:

Command	Description
show class-map [*class-name*]	Show the contents of the class map entity

For example,

```
DGS-3610# show class-map
Class Map cc
Match access-group 1
DGS-3610#
```

45.3.2 Showing policy-map

You may show the contents of policy-map through the following steps:

Command	Description
show policy-map [*policy-name* [**class** *class-name*]]	Show QoS policy map, *policy-nam*e is the selected name of policy map, specified as **class** Show the class map bound with the policy map in case of *class-name*

For example,

```
DGS-3610# show policy-map
Policy Map pp
Class cc
DGS-3610#
```

45.3.3 Showing mls qos interface

You may show the QoS information of all ports through the following steps:

Command	Description
show mls qos interface [*interface*| *policers*]	Show the QoS information of the interface, The **Policers** option shows the policy map applied on the interface.

For example,

```
DGS-3610# show mls qos interface gigabitEthernet 0/4
Interface GigabitEthernet 0/4
Attached input  policy-map: pp
Default COS: trust dscp
Default COS: 6
DGS-3610#show mls qos interface policers
Interface: GigabitEthernet 0/4
Attached input  policy-map: pp
DGS-3610#
```

45.3.4 Showing mls qos queueing

You may show the QoS queue information through the following steps:

Command	Description
show mls qos queuing	Show the QoS queue information, CoS-to-queue map, wrr weight and drr weight;

For example:

```
DGS-3610# show mls qos queuing
```

```
Cos-queue map:
cos qid
--- ---
0   1
1   2
2   1
3   4
4   1
5   1
6   1
7   1
wrr bandwidth weights:
qid weights
--- -------
0   1
1   2
2   3
3   4
4   5
5   6
6   7
7   8
```

45.3.5 Showing mls qos scheduler

You may show the QoS scheduling method through the following steps:

Command	Description
show mls qos scheduler	Show the port priority queue scheduling method.

For example:

```
DGS-3610# show mls qos scheduler
Global Multi-Layer Switching scheduling
Strict Priority
DGS-3610#
```

45.3.6 Showing mls qos maps

You may show the mls qos maps table through the following steps:

Command	Description
show mls qos maps [**cos-dscp** | **dscp-cos** | **ip-prec-dscp**]	Show dscp-cos maps dscp-cos maps ip-prec-dscp maps

For example:

```
DGS-3610# show mls qos maps cos-dscp
cos dscp
```

```
--- ----
0   0
1   8
2   16
3   24
4   32
5   40
6   48
7   56
DGS-3610# show mls qos maps dscp-cos
dscp cos   dscp cos   dscp cos   dscp cos
---- ---   ---- ---   ---- ---   ---- ---
 0   6       1   0       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
20   2      21   2      22   2      23   2
24   3      25   3      26   3      27   3
28   3      29   3      30   3      31   3
32   6      33   4      34   4      35   4
36   4      37   4      38   4      39   4
40   5      41   5      42   5      43   5
44   5      45   5      46   5      47   5
48   6      49   6      50   6      51   6
52   6      53   6      54   6      55   6
56   6      57   7      58   7      59   7
60   7      61   7      62   7      63   7
DGS-3610# show mls qos maps ip-prec-dscp
ip-precedence dscp
------------- ----
0     56
1     48
2     46
3     40
4     34
5     32
6     26
7     24
```

45.3.7 Showing mls qos rate-limit

You may show the port rate limiting information through the following steps:

Command	Description
show mls qos rate-limit [interface *interface*]	Show the rate limit of [port]

```
DGS-3610# show mls qos rate-limit
Interface GigabitEthernet 0/4
rate limit input bps = 100 burst = 100
```

45.3.8 Showing policy-map interface

You can show the configuratiom of port policymap through following steps

Command	Function
show policy-map interface *interface]*	Showing the configuration of (port) policymap

```
DGS-3610# show policy-map interface f0/1
```

```
FastEthernet 0/1  input (tc policy): pp
    Class cc
    set ip dscp 22
    mark count 0
```

Note

The switch device currently does not support the statistic of mark count.

46 VRRP Configuration

46.1 Overview

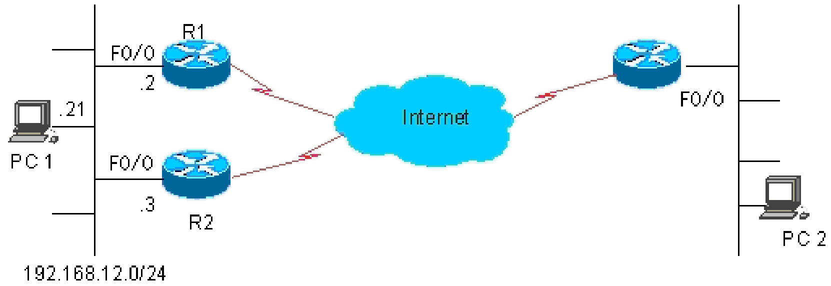
The Virtual Router Redundancy Protocol (VRRP) is designed to work in the active/standby mode to ensure that the function switching can be implemented without affecting internal and external data communication, and the internal network parameters need no modification. Multiple devices within a VRRP group are mapped to a virtual device. The VRRP ensures one and only one device to send packets on behalf of the virtual device at one time, while the host sends packets to that virtual device. The device that forwards packets is elected as the master device. If that device cannot work due to some cause, the one in standby status will be selected to replace it and become the master device. The VRRP enables the host in the LAN seems to use only one router and ensure the router connectivity even when the currently-used first-hop router fails.

The RFC 2338 defines the IP packet format in VRRP type and its working mechanism. The VRRP packets mean a kind of multicast packet with specified destination address, which are sent by the master router in specified time to indicate its operation and are also used to elect the master router. With VRRP, when the router undertaking route forwarding function in the IP LAN fails, another router can automatically take over the operations, thus implementing the hot-backup and error-tolerance of IP routing and ensuring the continuity and reliability of host communication in the LAN. Redundancy is implemented for a VRRP application group through multiple devices, but only one device acts as the master device at any time to undertake the route forwarding function. The others are in the backup roles. The switching between those devices in the VRRP application group is fully transparent for the host in the LAN. The RFC 2338 defines the device switching rules:

1. The VRRP protocol adopts the preempt method to select the master device. First, it compares the VRRP priorities that are set for the interfaces of the routers in a VRRP group. The one with the highest priority becomes the master router and its status will become Master. If the priority of the routers is identical, compare the master IP address of the network interfaces, the one with larger IP address will become the master router and the actual route service will be provided by it.
2. After the master device is elected, the others are in the backup status and monitor the status of the master device through the VRRP packet sent by the master device. In normal operation, the master device sends a VRRP packet at an interval, called advertised packet, to notify the backup devices. The master device is in the normal working status. If the backup device within the group does not receive the packet from the master device for a long time, the status itself will be switched to the Master. If more

than one device within the group becomes Master, repeat the preempt process in step 1. In this process, the device with the maximum priority will be selected as the master device to execute the VRRP backup function.

Figure 46-1 VRRP working principles



Once a master device is elected in a VRRP backup group, the hosts in the LAN will execute route forwarding through that master device. The communication process is illustrated in Figure 47-1. As shown in Figure 47-1, devices R1 and R2 are connected with LAN 192.168.12.0/24 through Ethernet interface Fa0/0, on which the VRRP is configured. All hosts in the LAN use the IP of the virtual device of the VRRP group as the default gateway. The hosts in the LAN only know the virtual router of the VRRP group, while the master router in the VRRP which is implementing the forwarding function is transparent to them. For example, if host PC 1 in the LAN is communicating with host PC 2 in another network, PC 1 will use the virtual router as the default gateway to send packets to the network of PC 2. When receiving the packets, the master router in the VRRP group forwards them to PC 2.In this communication process, PC 1 only feels the virtual device but does not know whether device R1 or R2 is playing the role. The master device is elected between devices R1 and R2 in the VRRP group. Once the master device fails, the other device automatically becomes the master.

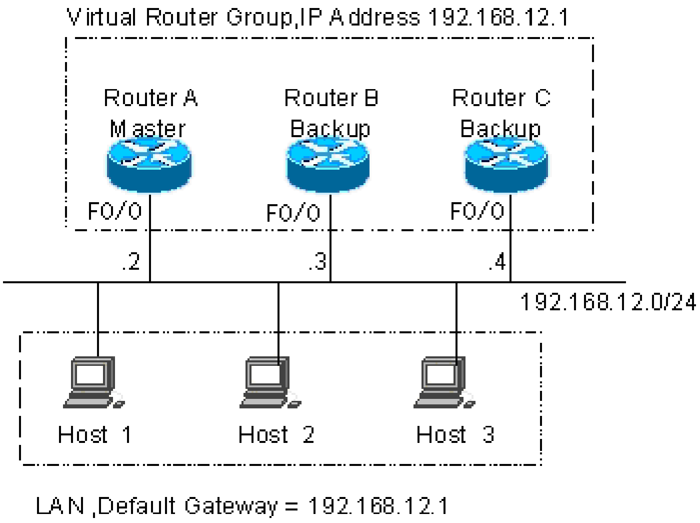
46.2 VRRP Applications

There are two VRRP application modes: basic and advanced. In basic applications, simple redundancy is implemented with a single backup, while in advanced applications multiple backup groups are used to implement both route redundancy and load balancing.

46.2.1 Route Redundancy

The basic VRRP applications are illustrated in Figure 47-2.

Figure 46-2 Basic VRRP applications

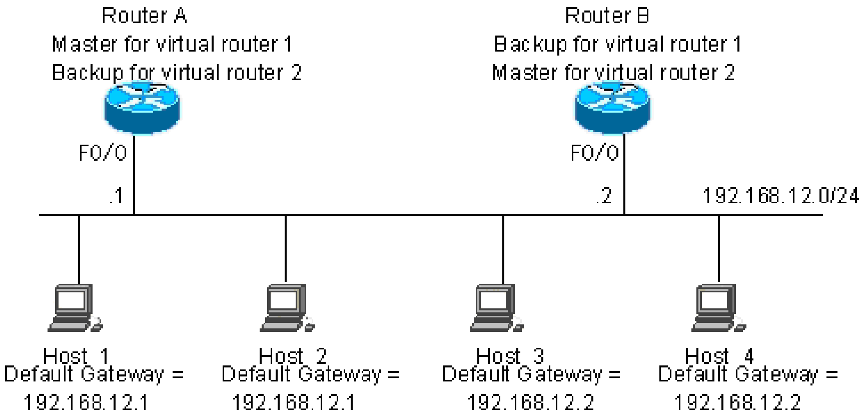


As shown in Figure 47-2, devices A, B and C are connected with the LAN through Ethernet interfaces, on which the VRRP is configured. They are in the same VRRP group with virtual IP address 192.168.12.1. Device A is elected as the master device of the VRRP, and devices B and C are standby. Hosts 1, 2 and 3 in the LAN use the IP address 192.168.12.1 of the virtual router as the gateway.The packets from the hosts in the LAN to other networks will be forwarded by the master device (device A in Figure 47-2). Once device A fails, the master device preempted between devices B and C undertakes the route forwarding function of the virtual device, resulting in simply route redundancy.

46.2.2 Load Balancing

The advanced VRRP applications are illustrated in Figure 47-3.

Figure 46-3 Advanced VRRP applications



As shown in Figure 47-3, two virtual devices are set. For virtual device 1, device A uses the IP address 192.168.12.1 of Ethernet interface Fa0/0 as the IP address of the virtual device, and thus device A becomes the master device and device B standby. For virtual device 2, device B uses the IP address 192.168.12.2 of Ethernet interface Fa0/0 as the IP address of the virtual device, and thus device B becomes the master device and device A standby. In the LAN, hosts 1 and 2 use the IP address 192.168.12.1 of virtual device 1 as the default gateway, while hosts 3 and 4 use the IP address 192.168.12.2 of virtual device 2 as the default gateway. In this VRRP application, device A and router B provide the route redundancy to share the traffic from the LAN, that is, load balancing.

46.3 VRRP Configuration

46.3.1 VRRP Configuration Task List

The VRRP is applicable for the multicast or broadcast LANs, such as Ethernet. The configuration of the VRRP is concentrated on the Ethernet interfaces. The configuration tasks are as follows:

- Enable VRRP backup function (required)
- Set the authentication string of the VRRP backup group (optional)
- Set the broadcast interval of the VRRP backup group (optional)
- Set the preemption mode of device in the VRRP backup group (optional)
- Set the device priority in the VRRP backup group (optional)
- Set a monitored interface for the VRRP backup group
- Set the VRRP broadcast timer learning function (optional)
- Set the description string of device in the VRRP backup group (optional)

Not all of above are required here. The tasks to be completed for a VRRP backup group depend on user demands.

46.3.2 Enabling the VRRP Backup Function

By specifying the backup group number and virtual IP address, you may add a backup in the specified LAN network segment to enable the VRRP backup function of the related Ethernet interfaces.

Command	Purpose
DGS-3610(config-if)**# vrrp** *group* **ip** *ipaddress* [**secondary**]	Enable VRRP
DGS-3610(config-if)**# no vrrp** *group* **ip** *ipaddress* [**secondary**]	Disable VRRP

The range of the backup group number *group* is 1~255. If the virtual IP address *ipaddress* is not specified, the router will not participate in the VRRP backup group. If the **secondary** parameter is not used, the IP address set here will become the master IP address of the virtual router.

Note

If the virtual IP address (Primary or Secondary) of the VRRP group is the same as the IP address (Primary or Secondary) of the Ethernet interface, it is regarded that VRRP group owns the actual IP address of the Ethernet interface, and the priority of the VRRP group is 255. If the corresponding Ethernet interface is available, the VRRP group will become the Master status automatically.

On the NMX-2GEH line card, each interface supports up to 14 VRRP backup groups. If the number of backup groups exceeds 14, the system gives a prompt.

46.3.3 Setting the Authentication String of the VRRP Backup Group

The VRRP supports plaintext password authentication mode and no authentication mode. When the authentication string is set for the VRRP backup group, it is also required to set the VRRP group to be in the plaintext password authentication mode. The members in the VRRP group must be in the same authentication mode to communicate normally. In the plaintext authentication mode, the routers in the same VRRP group must have the same authentication password configured. The plaintext authentication password cannot provide security. It aims only to prevent/prompt the incorrect VRRP configuration.

Command	Purpose
DGS-3610(config-if)# **vrrp** *group* **authentication** *string*	Set the authentication string of the VRRP.
DGS-3610(config-if)# **no vrrp** *group* **authentication** [*string*]	Set no authentication for ARRP

By default, the VRRP is in the no authentication mode. For the plaintext password authentication mode, the length of the plaintext authentication mode cannot be greater than 8 bytes.

46.3.4 Setting the Broadcast Interval of the VRRP Backup Group

Command	Purpose
DGS-3610(config-if)# **vrrp** *group* **timers advertise** *interval*	Set the master device VRRP advertisement interval
DGS-3610(config-if)# **no vrrp** *group* **timers advertise** [*interval*]	Restore default for the master device VRRP advertisement interval

If the current device becomes the master in the VRRP group, it will notify its VRRP status, priority and more information by sending VRRP advertisements in the set interval. By default, this interval is 1 second.

Note

When the VRRP timer learning function is not configured, the same VRRP advertisement interval shall be set for the same VRRP group; otherwise, the routers in the standby status will drop the received VRRP advertisement.

46.3.5 Setting the Preemption Mode of Device in the VRRP Backup Group

If the VRRP group is working in the preemption mode, a device preempts to become the master of the VRRP group once its priority is higher than the Master priority. If the VRRP group is not working in the preemption mode, it does not preempt to become the master of the VRRP group even if its priority is higher than the Master priority. In case the VRRP group is using the Ethernet interface IP address, the setting of the preemption mode does not make sense, because that device has the highest priority and thus automatically become the master in the VRRP group.

Command	**Purpose**
DGS-3610(config-if)# **vrrp** *group* **preempt** [**delay** *seconds*]	Set the preemptive mode for the VRRP group
DGS-3610(config-if)# **no vrrp** *group* **preempt**	Set the non-preemptive mode for the VRRP group

The optional parameter **delay** *seconds* defines the delay for the VRRP router prepares to declare its Master identify, 0 seconds by default. Once the VRRP function is enabled, the VRRP group will work in the preemption mode by default.

46.3.6 Setting the Device Priority in the VRRP Backup Group

The VRRP stipulates that the role of every device in the backup is determined by the priority parameter of the device. In the preemption mode, the device with the highest priority and virtual IP address obtained will become the active (master) device, and the other devices with lower priorities in the same backup group will become the backup (or listening) devices. Once the VRRP function is enabled, the default priority of the VRRP group is 100.

Command	**Purpose**
DGS-3610(config-if)# **vrrp** *group* **priority** *level*	Set the priority of the VRRP backup group.
DGS-3610(config-if)# **no vrrp** *group* **priority** [*level*]	Restore the default of the VRRP priority

The priority level range is 1~254. If the VRRP virtual IP address is the same as the actual IP of the Ethernet interface, the priority of the corresponding VRRP group is 255. Now no matter whether the VRRP group in the preemption mode, the corresponding VRRP group will be in the Master status automatically (as long as the corresponding Ethernet interface is available).

46.3.7 Setting a Monitored Interface for the VRRP Backup Group

After a monitored interface is configured for the VRRP backup group, the system dynamically adjusts the priority of the routing device according to the status of the monitored interface. If the interface is unavailable, the system lowers the priority of the routing device in the VRRP backup group, and another more stable routing device with higher priority becomes active (master) in the VRRP backup group.

Command	**Purpose**
DGS-3610(config-if)# **vrrp** *group* **track** *interface-type number* [*interface –priority*]	Set a monitored interface for the VRRP backup group.
DGS-3610(config-if)# **no vrrp** *group* **track** *interface-type number*	Cancel the setting of a monitored interface for the VRRP backup group.

By default, no monitored interface is set for the VRRP backup group in the system. The value of the parameter **Interface-Priority** ranges from 1-255. In the default status, the value is 10.

Note

A monitored interface can only be a L3 routable logic interface (such as Routed Port, SVI, Loopback and Tunnel).

46.3.8 Setting the VRRP Broadcast Timer Learning Function

Once the timer learning function is enabled, if the current router is a VRRP backup router, it will learn the VRRP advertisement interval from the VRRP advertisement of the master router, with which it calculates the Master router failure judgment interval, instead of the VRRP advertisement interval configured locally. This command may synchronize the VRRP advertisement timer between the Backup device and the Master device.

Command	**Purpose**
DGS-3610(config-if)# **vrrp** *group* **timers learn**	Set the timer learning function
DGS-3610(config-if)# **no vrrp** *group* **timers learn**	Cancel the timer learning function

By default, the VRRP group timer learning function is not set.

Note

In case the advertisement interval in the VRRP advertisement received by the VRRP backup device is inconsistent with the advertisement interval configured locally, the VRRP backup device discards the VRRP advertisement if the timer learning function is not configured on the VRRP backup device; otherwise, the VRRP backup device receives the VRRP advertisement and uses the advertisement interval to calculate the failure judgment interval of the VRRP Master device.

46.3.9 Setting the Description String of a Network Device in the VRRP Backup Group

This command is used to set descriptors for the VRRP group, facilitating VRRP group distinguishing.

Command	Purpose
DGS-3610(config-if)# **vrrp** *group* **description** *text*	Set the description string of the VRRP group
DGS-3610(config-if)# **no vrrp** *group* **description**	Cancel the description string of the VRRP group

By default, the VRRP backup group has no description string configured. The length of the VRRP backup group description string is 80 by maximum.

Note

If spaces are contained in the VRRP backup group description string, quotation marks (") must be used to identify the description string.

46.4 VRRP Monitoring and Maintenance

DGS-3610 series provide the VRRP monitoring and maintenance function through the commands **show vrrp** and **debug vrrp**. The command **show vrrp** is used to check the VRRP status of a local router; the **debug vrrp** is used to check the statuses change of the VRRP group, VRRP advertisement received/sent and VRRP events.

46.4.1 show vrrp

DGS-3610 series provide the following **show vrrp** commands to check the VRRP status of the local router.

Command	Purpose
DGS-3610# **show vrrp** [**brief** | *group*]	Check the current VRRP status

Command	Purpose
DGS-3610# **show vrrp interface** *type number* [**brief**]	Show the VRRP status of the specified network interface

Here are some examples of the command:

1. show vrrp

```
DGS-3610# show vrrp
GigabitEthernet 0/1 - Group 1
State is Backup
Virtual IP address is 192.168.201.1 configured
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 3 sec
Preemption is enabled
min delay is 0 sec
Priority is 100
Master Router is 192.168.201.213 , pritority is 120
Master Advertisement interval is 3 sec
Master Down interval is 9 sec
GigabitEthernet 0/2 - Group 2
State is Master
Virtual IP address is 192.168.201.2 configured
Virtual MAC address is 0000.5e00.0102
Advertisement interval is 3 sec
Preemption is enabled
min delay is 0 sec
Priority is 120
Master Router is 192.168.201.217 (local), priority is 120
Master Advertisement interval is 3 sec
Master Down interval is 9 sec
```

The displayed information above include the Ethernet name, VRRP backup group number configured on the interface, status, priority, preemption mode, VRRP advertisement interval, virtual IP address, virtual MAC address, Master router IP address, Master router priority, Master router advertisement interval, Master router failure judgment interval, current interface monitored by the VRRP backup group and corresponding priority change scale.

The current interface monitored by the VRRP backup group and the corresponding priority change metrics can be shown only after the monitored interface function is enabled.

2. **show vrrp brief** command

```
DGS-3610# show vrrp brief
Interface      Grp Pri Time Own Pre State   Master addr     Group addr
GigabitEthernet0/0 1  100  -    -   P  Backup  192.168.201.213 192.168.201.1
GigabitEthernet0/0 2  120  -    -   P  Master  192.168.201.217 192.168.201.2
```

The information displayed above includes the Ethernet interface name, VRRP group number, priority, timeout period for backup turning into master, same as the interface IP address or not, preemption mode, master device IP address, and VRRP group IP address.

3. **show vrrp interface** command

```
DGS-3610# show vrrp interface GigabitEthernet 0/0
GigabitEthernet 0/0 - Group 1
State is Backup
Virtual IP address is 192.168.201.1 configured
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 3 sec
Preemption is enabled
min delay is 0 sec
Priority is 100
Master Router is 192.168.201.213 , pritority is 120
Master Advertisement interval is 3 sec
Master Down interval is 9 sec
GigabitEthernet 0/0 - Group 2
State is Master
Virtual IP address is 192.168.201.2 configured
Virtual MAC address is 0000.5e00.0102
Advertisement interval is 3 sec
Preemption is enabled
min delay is 0 sec
Priority is 120
Master Router is 192.168.201.217 (local), priority is 120
Master Advertisement interval is 3 sec
Master Down interval is 9 sec
DGS-3610#
```

The displayed information above include the specified Ethernet name, VRRP backup group number configured on the interface, status, priority, preemption mode, VRRP advertisement interval, virtual IP address, virtual MAC address, Master router IP address, Master router priority, Master router advertisement interval, Master router failure judgment interval, current interface monitored by the VRRP backup group and corresponding priority change scale.

46.4.2 debug vrrp

DGS-3610 series provide VRRP status debugging information for local routing devices through the following **debug vrrp** commands.

Command	Purpose
DGS-3610# **debug vrrp error**	Turn on VRRP error prompt debugging switch
DGS-3610# **no debug vrrp error**	Turn off VRRP error prompt debugging switch
DGS-3610# **debug vrrp events**	Turn on the VRRP event debugging switch
DGS-3610# **no debug vrrp events**	Turn off the VRRP event debugging switch
DGS-3610# **debug vrrp packets**	Turn on the VRRP packet debugging switch
DGS-3610# **no debug vrrp packets**	Turning off the VRRP packet debugging switch
DGS-3610# **debug vrrp state**	Turn on the VRRP state debugging switch
DGS-3610# **no debug vrrp state**	Turn off the VRRP status debugging switch
DGS-3610# **debug vrrp**	Enable the IP debug switch
DGS-3610# **no debug vrrp**	Turn off the VRRP debugging switch

Here are some examples of the command:

1. **debug vrrp** command

```
DGS-3610# debug vrrp
DGS-3610#
VRRP: Grp 1 Advertisement priority 120, ipaddr 192.168.201.213
VRRP: Grp 1 Event - Advert higher or equal priority
%VRRP-6-STATECHANGE: FastEthernet 0/0 Grp 1 state Master -> Backup
VRRP: Grp 1 Advertisement from 192.168.201.213 has invalid virtual address 192.168.1.1
%VRRP-6-STATECHANGE: FastEthernet 0/0 Grp 1 state Backup -> Master
DGS-3610#
```

The **debug vrrp** command is equivalent to the joint execution of **debug vrrp errors**, **debug vrrp events**, **debug vrrp packets** and **debug vrrp state**.

2. **debug vrrp errors** command

```
DGS-3610# debug vrrp error
DGS-3610#
VRRP: Grp 1 Advertisement from 192.168.201.213 has invalid virtual address 192.168.1.1
VRRP: Grp 1 Advertisement from 192.168.201.213 has invalid virtual address 192.168.1.1
VRRP: Grp 1 Advertisement from 192.168.201.213 has invalid virtual address 192.168.1.1
```

The above displayed information indicates the VRRP advertisement comes from 192.168.201.213 for VRRP group 1. The virtual IP address 192.168.1.1 in the advertisement is not in local VRRP group 1.

3. **debug vrrp events** command

```
DGS-3610# debug vrrp events
DGS-3610#
VRRP: Grp 1 Event - Advert higher or equal priority
VRRP: Grp 1 Event - Advert higher or equal priority
VRRP: Grp 1 Event - Advert higher or equal priority
DGS-3610#
```

The above displayed information indicates the priority in the VRRP advertisement received by the local VRRP group is not lower than the local priority.

4. **debug vrrp packets** command

```
DGS-3610#debug vrrp packets
DGS-3610#
VRRP: Grp 2 sending Advertisement checksum DD4D
VRRP: Grp 2 sending Advertisement checksum DD4D
VRRP: Grp 2 sending Advertisement checksum DD4D
```

The above displayed information indicates the local VRRP group 2 is sending VRRP advertisement, whose VRRP checksum is 0XDD4D.

```
DGS-3610# debug vrrp packets
DGS-3610#
VRRP: Grp 1 Advertisement priority 120, ipaddr 192.168.201.213
VRRP: Grp 1 Advertisement priority 120, ipaddr 192.168.201.213
VRRP: Grp 1 Advertisement priority 120, ipaddr 192.168.201.213
```

The above displayed information indicates the VRRP advertisement is received from 192.168.201.213 for VRRP group 1, whose priority is 120.

5. **debug vrrp state** command

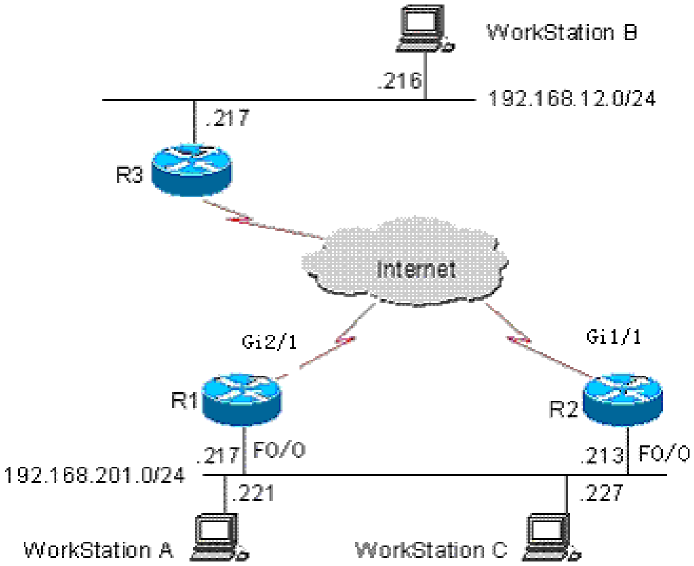
```
DGS-3610# debug vrrp state
VRRP State debugging is on
DGS-3610#
%VRRP-6-STATECHANGE: GigabitEthernet 0/0 Grp 2 state Master -> Backup
%VRRP-6-STATECHANGE: GigabitEthernet 0/0 Grp 2 state Backup -> Master
DGS-3610# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
DGS-3610(config)# interface GigabitEthernet 0/0
DGS-3610(config-if)# no shutdown
DGS-3610(config-if)# end
DGS-3610#
%VRRP-6-STATECHANGE: GigabitEthernet 0/0 Grp 2 state Master -> Init
DGS-3610#
```

The above displayed information indicates the VRRP group status on GigabitEthernet 0/0 is shifting among Master, Backup and Init.

46.5 Example of Typical VRRP Configuration

In the connections shown in Figure 47-4, VRRP backup is configured on devices R1 and R2 to provide the VRRP service for internal network segment 192.168.201.0 /24. Device R3 is not configured with VRRP but just the common routing functions. The configurations below provide the related VRRP settings of devices R1 and R2.

Figure 46-4 Network connection with VRRP



In the configuration example below, the configurations of device R3 remain unchanged,The configuration on device R3 is shown below:

```
!
!
hostname "R3"
!
!
!
interface FastEthernet 0/0
no switchport
ip address 192.168.12.217 255.255.255.0
!
interface GigabitEthernet 1/1
no switchport
ip address 60.154.101.5 255.255.255.0
!
interface GigabitEthernet 2/1
no switchport
ip address 202.101.90.61 255.255.255.0
!
router ospf
network 202.101.90.0 0.0.0.255 area 10
network 192.168.12.0 0.0.0.255 area 10
network 60.154.101.0 0.0.0.255 area 10
!
!
!
end
```

46.5.2 Example of Single VRRP Backup Group

Establish the connections according to Figure 47-4. In this configuration example, user workstation group (192.168.201.0/24) uses the backup group that is composed of routers R1 and R2, and points its gateway to the virtual router IP address 192.168.201.1 of the backup group. The remote user workstation group (in network 192.168.12.0 /24) is accessed via the virtual router 192.168.201.1. Here router R1 is set as the VRRP Master device. In normal cases, device R1 is the active router to function as the gateway (192.168.201.). When device R1 becomes unreachable due to power-off or failure, device R2 takes its place to function as the gateway (192.168.201.1). The configurations for devices R1 and R2 are described as follows.

Configurations on device R1:

```
!
!
hostname "R1"
!
!
interface FastEthernet 0/0
no switchport
ip address 192.168.201.217 255.255.255.0
vrrp 1 priority 120
vrrp 1 timers advertise 3
vrrp 1 ip 192.168.201.1
!
interface GigabitEthernet 2/1
no switchport
ip address 202.101.90.63 255.255.255.0
!
router ospf
network 202.101.90.0 0.0.0.255 area 10
network 192.168.201.0 0.0.0.255 area 10
!
Configurations on device R2:
!
hostname "R2"
!
interface FastEthernet 0/0
no switchport
ip address 192.168.201.213 255.255.255.0
vrrp 1 ip 192.168.201.1
vrrp 1 timers advertise 3
!
interface GigabitEthernet 1/1
no switchport
ip address 60.154.101.3 255.255.255.0
!
!
router ospf
network 60.154.101.0 0.0.0.255 area 10
network 192.168.201.0 0.0.0.255 area 10
!
!
end
```

As shown above, routers R1 and R2 are in the same VRRP backup group 1, point to the same virtual router IP address (192.168.201.1) and are both in the VRRP preemption mode.Since the VRRP backup group priority of device R1 is 120 but that of R2 is the default value 100, device R1 acts as the VRRP Master in normal cases.

46.5.3 Example of Monitored Interface Configuration of VRRP

Establish the connections according to Figure 47-4. In this configuration example, user workstation group (192.168.201.0/24) uses the backup group that is composed of routers R1 and R2, and points its gateway to the virtual router IP address 192.168.201.1 of the backup group. The remote user workstation group (in network 192.168.12.0 /24) is accessed via the virtual router 192.168.201.1. Here router R1 is set as the VRRP Master device. Different from the above configuration example, router R1 is configured with VRRP to monitor interface GigabitEthernet 2/1. In normal cases, device R1 is the active device to function as the gateway (192.168.201.1). When device R1 becomes unreachable due to power-off or failure, device R2 takes its place to function as the gateway (which is just the virtual device address 192.168.201.1). Especially, when the WAN interface GigabitEthernet 2/1 of device R1 is unavailable, device R1 will decrease its priority in the VRRP backup group so that device R2 has the chance to become active and functions as the virtual gateway (192.168.201.1). If the WAN interface GigabitEthernet 2/1 of device R1 resumes normal, device R1 restores its priority in the VRRP backup group, becomes active and functions as the virtual gateway once again. The configurations for devices R1 and R2 are described as follows.

Configurations on device R1:

```
!
!
hostname "R1"
!
!
interface FastEthernet 0/0
no switchport
ip address 192.168.201.217 255.255.255.0
vrrp 1 priority 120
vrrp 1 timers advertise 3
vrrp 1 ip 192.168.201.1
vrrp 1 track GigabitEthernet 2/1 30
!

interface GigabitEthernet 2/1
no switchport
ip address 202.101.90.63 255.255.255.0
!
router ospf
network 202.101.90.0 0.0.0.255 area 10
network 192.168.201.0 0.0.0.255 area 10
!
!
end
Configurations on device R2:
!
!
hostname "R2"
!
interface FastEthernet 0/0
no switchport
ip address 192.168.201.213 255.255.255.0
vrrp 1 ip 192.168.201.1
vrrp 1 timers advertise 3
!
interface GigabitEthernet 1/1
no switchport
ip address 60.154.101.3 255.255.255.0
!
router ospf
```

```
network 60.154.101.0 0.0.0.255 area 10
network 192.168.201.0 0.0.0.255 area 10
!
!
end
```

As shown above, devices R1 and R2 are in the same VRRP backup group 1, use the same VRRP backup group authentication mode (no authentication), point to the same virtual IP address (192.168.201.1) and are both in the VRRP preemption mode. The VRRP Advertisement interval for devices R1 and R2 are 3 seconds. In normal cases, since the VRRP backup group priority of device R1 is 120 but that of R2 is the default value 100, device R1 acts as the VRRP Master in normal cases. If device R1 in the Master status finds its WAN interface GigabitEthernet 2/1 is unavailable, device R1 decreases its priority in the VRRP backup group from 90 to 30, so that device R2 can become the Master. If router R1 finds its WAN interface GigabitEthernet 2/1 becomes available later, it increases its priority in VRRP backup group from 30 to 120, so that device R1 becomes the master once again.

46.5.4 Example of Multiple VRRP Backup Groups

Besides the single backup group, DGS-3610 series also allow multiple VRRP backup groups configured on the same Ethernet interface. There are obvious benefits for using multiple backup groups. It is possible to implement load balancing through mutual backup to offer more stable and reliable network services.

Establish the connections according to Figure 47-4. In this configuration example, user workstation group (192.168.201.0/24) is using the backup group that is composed of routers R1 and R2. Some user workstations (such as A) point its gateway to the virtual IP address 192.168.201.1 of backup group 1, while the others (such as C) point its gateway to the virtual IP address 192.168.201.2 of backup group 2. Device 1 acts as the master in backup group 1 and standby in backup group 1; device 2 acts as the standby in backup group 2 and master in backup group 1. The configurations for devices R1 and R2 are described as follows.

Configurations on device R1:

```
!
!
hostname "R1"
!
interface FastEthernet 0/0
no switchport
ip address 192.168.201.217 255.255.255.0
vrrp 1 timers advertise 3
vrrp 1 ip 192.168.201.1
vrrp 2 priority 120
vrrp 2 timers advertise 3
vrrp 2 ip 192.168.201.2
vrrp 2 track GigabitEthernet 2/1 30
!
```

```
interface GigabitEthernet 2/1
no switchport
ip address 202.101.90.63 255.255.255.0
!
router ospf
network 202.101.90.0 0.0.0.255 area 10
network 192.168.201.0 0.0.0.255 area 10
!
!
end
Configurations on device R2:
!
!
hostname "R2"
!
!
interface Loopback 0
ip address 20.20.20.5 255.255.255.0
!
interface FastEthernet 0/0
no switchport
ip address 192.168.201.213 255.255.255.0
vrrp 1 ip 192.168.201.1
vrrp 1 timers advertise 3
vrrp 1 priority 120
vrrp 2 ip 192.168.201.2
vrrp 2 timers advertise 3
!
interface GigabitEthernet 1/1
no switchport
ip address 60.154.101.3 255.255.255.0
!
router ospf
network 60.154.101.0 0.0.0.255 area 10
network 192.168.201.0 0.0.0.255 area 10
!
!
!
end
```

It is shown that devices R1 and R2 are mutual backup, and the two are acting as the master devices in VRRP backup groups 1 and 2 respectively to provide different virtual gateway functions.

46.6 VRRP Diagnosis and Troubleshooting

In case of VRRP faults, it is possible to troubleshoot through checking configurations and debugging information. Here is some common fault analysis.

Symptom: Unable to ping the virtual IP address

Analysis:

- Ensure that at least one router in the backup group is active.
- If it is possible to ping the virtual IP address from other network devices, the causes may be the VRRP status changing needs some time (although brief). Execute the **show vrrp** command to check the VRRP information and confirm this.
- If the local network device is in the same network segment of the virtual router, check whether ARP table of the local network device contains the APP entry for the IP virtual address. If no, check the network lines.
- If the local network device is not in the same network segment of the virtual router, make sure the local network device has a router to the virtual IP address.

Symptom: multiple master devices in the same VRRP backup group

Analysis:

- In the same VRRP backup group, the Ethernet interfaces of those routers are in different VRRP group authentication modes.
- In the same VRRP backup group, the Ethernet interfaces of those routers are in the plaintext password VRRP group authentication mode, but the authentication strings are not the same.
- In the same VRRP backup group, the cables the Ethernet interfaces of some routers may be disconnected, since the routers fail to detect that.
- In the same VRRP backup group, the VRRP advertisement interval is inconsistent and the timer learning function is not configured.
- In the same VRRP backup group, the virtual IP for the routers are not the same.

47 RLDP Configuration

47.1 About RLDP

47.1.1 Understanding RLDP

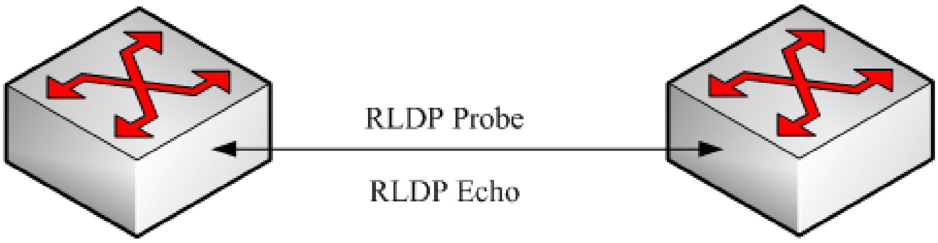
The Rapid Link Detection Protocol (RLDP) is one of D-Link's proprietary link protocol designed to detect Ethernet link fault quickly.

General Ethernet link detection mechanism only makes use of the status of the physical connections and detects the connectivity of the link via the auto-negotiation of the physical layer. This detection mechanism has restrictions and sometimes cannot provide reliable link detection information for users. For example, if the fiber receiving cable on the optical interface is misconnected, the related interface of the device is "linkup" physically but actually the corresponding layer-2 link cannot work for communications due to the existence of the optical converter. Here is another example. There is an intermediate network between two Ethernet devices. Due to the existence of the network transmission relay devices, the same problem may occur if those relay devices are faulty.

The RLDP enables easy detection of Ethernet device link fault, including the one-way link fault, two-way link fault and loop link fault.

The RLDP implements the detection by exchanging the RLDP packets at the two ends of the link, as shown below:

Figure 47-1



The RLDP defines two protocol packets: Probe packet and Echo packet. The RLDP sends the Probe packet of this port to the port with RLDP configured and in linkup status on regular basis, and waits for the Echo packet from the neighbor port and waits for the Probe packet sent by the neighbor ports. If a link is correct both physically and logically, a port shall be able to receive the Echo packet of the neighbor port as well as the Probe packet of the neighbor port. Otherwise, the link is considered abnormal.

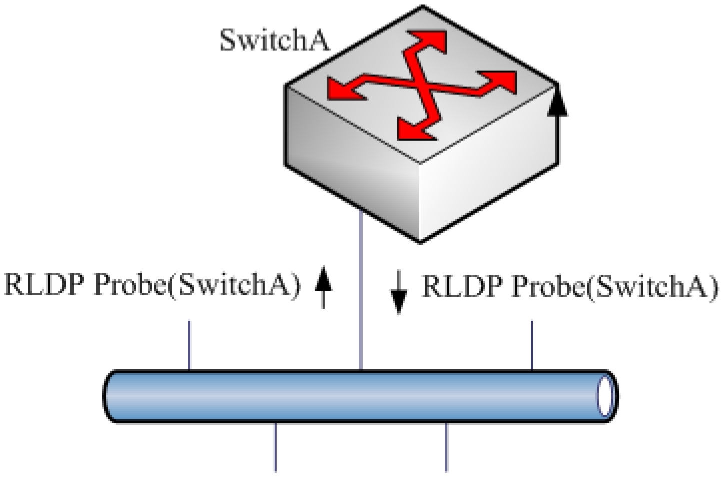
Note

To make use of the one-way detection and two-way detection functions of the RLDP, it is necessary to ensure the RLDP is enabled on the ports at both ends of the link. And, it is not allowed for a port with RLDP enabled to connect multiple neighbor ports. Otherwise, the RLDP cannot detect the health conditions of every neighbor link.

47.1.2 Typical Application

Loop detection:

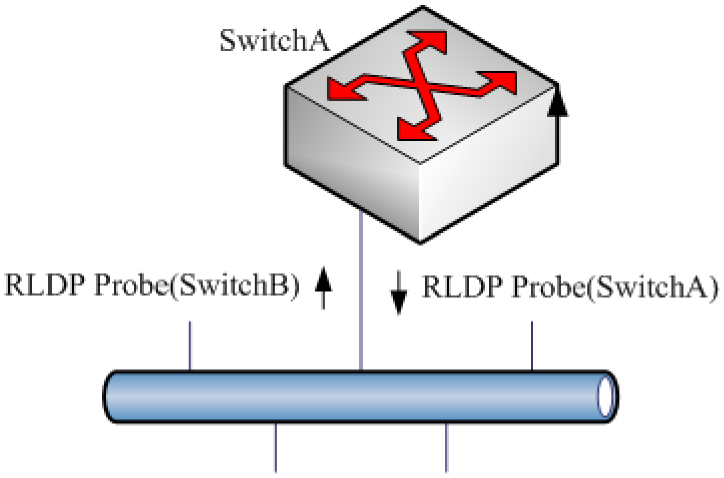
Figure 47-2 Loop detection



The so-called loop fault means that a loop appears on the links connected with the port. As shown above, on a port the RLDP receives the RLDP packet sent from its machine, so the port is considered as loop fault. The RLDP deals with the fault according to the user configurations, including alarming, setting port violation, turning off the SVI with that port and turning off the port learning forwarding.

One-way link detection:

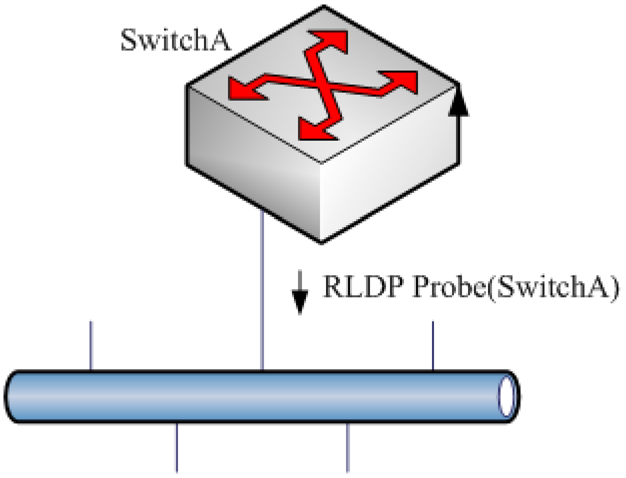
Figure 47-3 One-way link detection



The so-called one-way link detection means the link connected with the port can receive packet only or send packets only (due to misconnection of the optical receiving line pair, for example). As shown above, the RLDP only receives the detection packet from the neighbor port on a port, so it is considered one-way link fault. The RLDP deals with the fault accordingly according to the user configurations. In addition, if the port cannot receive any RLDP detection packet, it is also considered one-way link fault.

Two-way link detection:

Figure 47-4 Two-way link detection



This means that a fault occurs at the frame transmission/receiving at both ends of the link. As shown above, the port of the device sends the RLDP probe packet but has never received the Echo packet or the Probe packet from the neighbors. So, it is considered two-way link fault. From the nature of the fault, the two-way fault actually includes the one-way fault.

Note

If the party at one of the two link ends has not enabled the RLDP, the diagnosis also shows two-way or one-way link fault. So, in configuring two-way link detection or one-way link detection, the administrator needs to make sure that the RLDP is enabled at both ends to avoid the incorrect diagnosis information.

47.2 Configuring RLDP

The following sections describe how to configure RLDP.

- Default value of RLDP
- Configure global RLDP
- Configure port RLDP
- Configure detection vlan
- Configure RLDP detection interval
- Configure the RLDP maximum detection times
- Restore the RLDP status of the interface

47.2.1 Default Value of RLDP

Global RLDP status	DISABLE
Port RLDP status	DISABLE
Detection interval	2S
Maximum detection times	3

Caution

- The RLDP can be configured only on the basis of the switching interface (including AP) and the routing interface.
- All RLDP frames are untagged.
- In the RLDP fault processing type, the block function and the STP are mutually exclusive. In other words, if the fault processing type configured on the port is **block**, it is recommended to disable STP; otherwise, since the STP cannot recognize one-way link, possibly the STP allows port forwarding but the RLDP is configured with port blocking.

47.2.2 Configuring Global RLDP

The port RLDP works only when the global RLDP is enabled.

In the global configuration mode, follow these steps to enable RLDP:

Command	**Function**
DGS-3610(config)# **rldp enable**	Turn on the global RLDP function switch.
DGS-3610(config)# **end**	Return to the privileged mode.

The **no** option of the command turns off the global *RLDP*.

47.2.3 Configuring Port RLDP

The RLDP operation is port-based, so the user needs to explicitly configure specific ports that need RLDP running. In configuring the port RLDP, you need to specify the diagnosis type and the troubleshooting method for the port at the same time. The diagnosis types include unidirection-detect, bidirection-detect and loop-detect. The troubleshooting methods include warning, block, shutdown-port, and shutdown-svi.

In the configuration mode, follow these steps to configure port RLDP:

Command	**Function**
DGS-3610(config)# **interface** *interface-id*	Enter the interface mode.
DGS-3610(config-if)# **rldp port** {**unidirection-detect** | **bidirection-detect** | **loop-detect** } {**warning** | **shutdown-svi** | **shutdown-port** | **block**}	Enable the RLDP on the port and configure the diagnosis type and troubleshooting method at the same time.
DGS-3610(config-if)# **end**	Return to the privileged mode.

The **no** option of the command disables the RLDP on the port and the configured detection types one by one.

In the example below, the RLDP is configured on GigabitEthernet 0/5, and multiple diagnosis types and troubleshooting methods are specified:

```
DGS-3610# configure terminal
DGS-3610(config)# interface gigabitEthernet 0/5
DGS-3610(config-if)# rldp port unidirection-detect
shutdown-svi
DGS-3610(config-if)# rldp port bidirection-detect warning
DGS-3610(config-if)# rldp port loop-detect block
DGS-3610(config-if)# end
DGS-3610# show rldp interface gigabitEthernet 0/5
port state     : normal
local bridge    : 00d0.f822.33ac
neighbor bridge : 0000.0000.0000
neighbor port   :
```

```
unidirection detect information:
action : shutdown svi
state  :  normal
bidirection detect information :
action : warnning
state  :  normal
loop detect  information    :
action : block
state  :  normal
```

Several precautions in configuring port detection:

- The routing interface does not support the shutdown-svi error handling method, so this method is not executed when a detection error occurs.
- In configuring loop detection, the neighbor devices downward connected with the port cannot enable the RLDP detection; otherwise, the port cannot have correct detection.
- If the block method is configured on the aggregated port and a link detection error occurs, do not change the member port relations of the aggregate port before the port reset detection; otherwise, the forwarding status of the member interface may have unexpected effects of forwarding status.
- If the RLDP detects link error, the system gives an alarm prompt. The user can send the alarm information to the log server by configuring the log function. At least 3 levels of log shall be ensured.

47.2.4 Configuring Detection vlan

RLDP loop detection is vlan-based. After RLDP loop detection is enabled, the user must specify the vlan range of the detection. For an access port, the system can only detect the vlan the port belongs to. For a trunk port, the removed vlan cannot be executed even if the detection function is configured.

Command	**Function**
DGS-3610(config)# **interface** *interface-id*	Enter the interface mode.
DGS-3610(config)# **rldp loop-detect vlan allowed** *line*	Configure the range of detected vlans, supporting line configuration.

You can delete the detected vlans through the no form of the command.

47.2.5 Configuring RLDP Detection Interval

The port with the RLDP function enabled will send the RLDP Probe packets periodically.

In the global configuration mode, follow these steps to configure the RLDP detection interval:

Command	**Function**
DGS-3610(config)# **rldp detect-interval** *interval*	Configure the detection interval within the range 2-15s, 3s by default.
DGS-3610(config)# **end**	Return to the privileged mode.

The **no** option of the command restores default.

47.2.6 Configure the RLDP Maximum Detection Times

If the port with RLDP enabled cannot receive packets from neighbors in the maximum detection period (maximum detection times X detection interval), that port will be diagnosed as faulty. See the Overview for details of the fault types.

In the global configuration mode, follow these steps to configure the RLDP maximum detection times:

Command	**Function**
DGS-3610(config)# **rldp detect-max** *Num*	Configure the maximum detection times, **num** ranges 2-10, 2 by default.
DGS-3610(config)# **end**	Return to the privileged mode.

The **no** option of the command restores default.

Note

The maximum detection times only take effect in unidirection link detection and bidirection link detection, and will not take effect if only loop detection is enabled on a port.

47.2.7 Restoring the RLDP Status of the Port

The port with shutdown-port troubleshooting method configured cannot resume the RLDP detection actively after a fault occurs. If the user confirms the fault is removed, run the recovery command to restart the RLDP on the shutdown port. This command sometimes can be executed to resume other ports with detection errors.

In the privileged mode, follow these steps to resume the RLDP detection of the port:

Command	**Function**
DGS-3610# **rldp reset**	Make any port with RLDP detection failure resume the detection.

Note

The **errdisable recover** command can be used in the global configuration mode to restart, instantly or at fixed time, the RLDP detection of the port that is set as the violation port by RLP.

47.3 Viewing RLDP Information

The following RLDP-related information can be viewed:

- View the RLDP status of all ports
- View the RLDP status of the specified port

47.3.1 Viewing the RLDP Status of All Ports

In the privileged mode, run the following commands to view the RLDP global configuration and the port detection information with RLDP detection configured:

Command	Function
DGS-3610# **show rldp**	View the RLDP global configuration and the port detection information with RLDP detection configured

In the example below, the **show rldp** command is used to view the detection information of all RLDP ports:

```
DGS-3610# show rldp
rldp state            : enable
rldp hello interval   : 2
rldp max hello        : 3
rldp local bridge     : 00d0.f8a6.0134
------------------------------------------------
interface GigabitEthernet 0/1
port state:normal
neighbor bridge       : 00d0.f800.41b0
neighbor port         : GigabitEthernet 0/2
unidirection detect information:
action                : shutdown svi
state                 : normal

interface GigabitEthernet 0/24
port state:error
neighbor bridge       : 0000.0000.0000
neighbor port         :
bidirection detect information :
action                : warnning
state                 : error
```

As shown above, port GigabitEthernet 0/1 is configured with unidirection detection. No error is detected now, and the port status is normal. Port GigabitEthernet 0/24 is configured with bidirection detection, and bidirection fault is detected.

47.3.2 Viewing the RLDP Status of a Specified Port

In the privileged mode, run the following command to view the RLDP detection information of a specified port:

Command	**Function**
DGS-3610# **show rldp interface** *interface-id*	View the RLDP detection information of *interface-id*.

In the example below, the **show rldp interface GigabitEthernet** *0/1* command is used to view the RLDP detection information of port fas0/1:

```
DGS-3610# show rldp int GigabitEthernet 0/1
port state     :error
local bridge    : 00d0.f8a6.0134
neighbor bridge : 00d0.f822.57b0
neighbor port   : GigabitEthernet 0/1
unidirection detect information:
action: shutdown svi
state :  normal
bidirection detect information :
action : warnning
state :  normal
loop detect  information    :
action: shutdown svi
state :  error
```

As shown above, the port GigabitEthernet 0/1 is configured with three detection types: unidirection detection, bidirection detection and loop detection. The troubleshooting methods are shutdown-svi and warning. Error is found in loop detection so the current port status is error. Accordingly, the SVI of the port is shutdown.

48 TPP Configuration

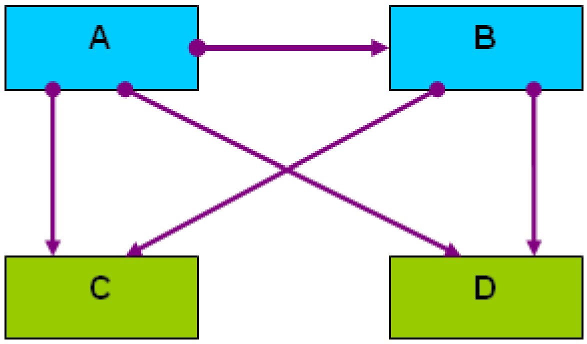
48.1 TPP Overview

The Topology Protection Protocol (TPP) is a topology stability protection protocol. The network topology is rather fragile. Illegal attacks in the network may cause abnormal CPU utilization on network devices, frame path blocked and so on. These are apt to cause network topology turbulence. The topology protection aims to stabilize the network topology by detecting the abnormalities (such as high CPU utilization and frame buffer abnormal) and detecting the abnormalities of neighbor devices. The interaction with neighbor devices is implemented by sending specific exception advertisement. This function has rather high priority and can effectively prevent network topology turbulence.

48.2 TPP Application

The topology protection is generated to address the network topology turbulence that my be caused in the MSTP or VRRP and other distributed network protocol. The MSTP, VRRP and other protocols work with the message notification mechanism to automatically maintain the network topological structure and automatically adapt to the topological change in the network. This on the other hand results in the aptness to attacks. When malicious network attacks arrive, transient interruption of timed messages may be caused due to high CPU utilization or frame path blocking, causing error fluctuation of the network topology and great harm to the normal communication in the network. The topology protection function minimizes such unnecessary fluctuations. It works with the other distributed protocols (such as MSTP and VRRP,) to make the network more stable and reliable.

Figure 48-1



As shown in the above dual-core topology, A and B are the L3 convergence devices, and C and D are the L2 access devices. A is the MSTP root bridge. The topology protection functions of all the devices are enabled.

The CPU of the L3 convergence device A is extremely busy due to network attack, resulting in failure of sending BPDU packets. The topology protection function detects the exception and sends the exception advertisement packet to its neighbors. B, C, and D all receive the advertisement and adopt the anti-vibration measures.

The CPU of B is extremely busy under the attack of a large number of packets and cannot send or receive packets normally. After detecting the exception, B sends the exception advertisement to all its neighbors. A receives the exception advertisement but does not process it further because B finds the exception has not effect on B according to its source. The downstream C and D receive the exception advertisement and perform further defense activities to ensure the reliability of the network topology, because they find the exception will affect the topology calculation.

48.3 TPP Configuration

Configuring TPP involves global function configuration and port function configuration. The global function configuration is used to enable the topology protection function of the device. By default, the global topology protection function is enabled. Here, it will detect the running conditions of the local and neighbor devices and perform treatment for the exceptions that occur. However, it does not notify the local running conditions to neighbor devices. The port function configuration is used to enable the topology protection function of the port. When the topology protection function is enabled on the port, it indicates that the opposite neighbor device is concerning about the running conditions of this machine. When the local device becomes abnormal, this will be notified to the opposite neighbor device of the port. By default, the topology protection function is disabled on all ports.

Note

The topology protection function is suitable for the point-to-point link network, and adjacent network devices must enable the topology protection function. Besides, during the TPP configuration, you often need to use CPU topology-limit to configure the threshold for CPU utilization detection. When the CPU utilization exceeds the threshold, the system generates the topology protection advertisement. We suggest a middle to high value, such as 50–70, so that the TPP can judge the network conditions more accurately. If the value is too small, the network topology may not switch when it needs to switch due to TPP alarm. If the value is too large, the system may be too busy to generate a TPP alarm, causing the TPP invalid.

48.3.1 Configuring Global Topology Protection

The global topology protection function is enabled by default. The **no** option of the command disables the global topology protection.

The configuration commands are as follows:

Command	Function
DGS-3610> **enable**	Enter the privileged mode.
DGS-3610# **config terminal**	Enter the global configuration mode.
DGS-3610(config)# **topology guard**	Enable the global topology protection
DGS-3610(config)# **end**	Exit to the privileged mode.
DGS-3610# **copy running-config startup-config**	Save the configuration.

The **no topology guard** command diables the global topology protection function on the device.

48.3.2 Configuring the Topology Protection on Port

The configuration commands are as follows:

Command	Function
DGS-3610> **enable**	Enter the privileged mode.
DGS-3610# **config terminal**	Enter the global configuration mode.
DGS-3610(config)# **interface gi** *0/1*	Enter the interface configuration mode.
DGS-3610(config-if)# **tp-guard port enable**	Enable the port topology protection function.

Command	Function
DGS-3610(config-if)# **end**	Exit to the privileged mode.

The **no tp-guard port enable** command disables the topology protection on the port. This command is suitable only on layer-2 switching ports and routing ports.It is inapplicable to AP member ports.

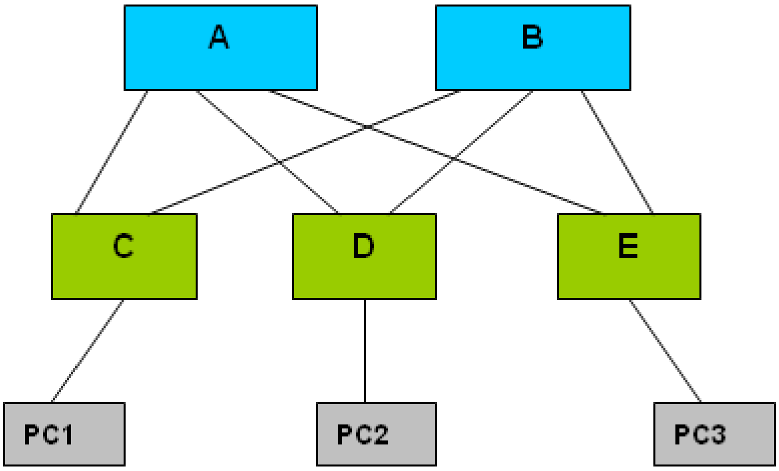
Note

The global topology protection is the global switch for the topology protection. When it is enabled, the device detects the running parameters of its own and monitors the running parameters of neighbor devices at the same time. When exception appears locally, it sends exception notification messages to the neighbor devices. When the port topology protection function is enabled, it sends exception notification message to neighbor devices if exception occurs locally.

48.4 Typical TPP Configuration Examples

The figure below shows a dual-core networking topology:

Figure 48-2



As shown in the figure, A and B are L3 convergence devices, while C, D and E are L2 access devices.

The MSTP is enabled on A, B, C, D, and E, and VRRP is enabled on A and B. The topology protection function enables the MSTP and VRRP to operate more reliable, avoiding unnecessary vibration of the network topology.

The global topology protection function is enabled on A, B, C, D, and E, and the topology protection function is enabled on all the ports..

48.5 Viewing TPP Information

The following TPP-related information can be viewed:

View the TPP configuration and status of devices

48.5.1 Viewing the TPP Configuration and Status of Devices

In the privileged mode, run the following command to view the TPP configuration and status of the device:

Command	Function
DGS-3610# **show tpp**	View the TPP configuration and status of the device

```
DGS-3610#show tpp
tpp state        : enable
tpp local bridge : 00d0.f822.35ad
-----------------------------------
```

49 File System Configuration

49.1 Overview

The file system is an organization for storing and managing the files on the auxiliary storage devices. The switch provides the serial Flash as the auxiliary storage device to store and manage the NM operating system files and configuration files of the switch.

The file data is stored as logs on the serial Flash and each file has a file header for recording the basic information of the file. When the storage device is full with no more space for other operations, the file system automatically de-fragments the storage device and recycles the trash. This is for providing sufficient space for file operations. This is done in a very short period without your perception. To make the most of the limited space, the file system provides the data compression function and the data node index.

49.2 Configuring File System

The following sections describe how to configure the file system.

- Changing Directories
- Copying Files
- Showing Directories
- Formatting the System
- Creating directories
- Moving Files
- Showing the Current Working Path
- Removing Files
- Deleting Empty Directories

49.2.1 File System Configuration Guide

The command keyword is not case sensitive, while the file name is case sensitive, and the maximum size of the file name is 4096.

None of all the file names and paths support the wildcard.

49.2.2 Changing Directories

It means the shifts from the current director to the specified directory.

In the privileged mode, use this command through the following steps:

Command	Function
DGS-3610# **cd** *directroy*	Enter the specified directory.
DGS-3610# **cd** ../	Enter the higher-level directory
DGS-3610# **cd** ./	Enter the current-level directory

The following example shows how to enter the **DOCUMENT** directory in the **MNT** directory at the root:

```
DGS-3610# cd mnt/document
```

After that, the operations will be performed in the **MNT/DOCUMENT** directory.

49.2.3 Copying Files

This copies files to a directory or a file.

In the privileged user mode, copy files to a directory or files by executing the **copy** command:

Command	Function
DGS-3610# **copy flash:** *filename* **flash:** *directoryname*	Copy files to the specified directory
DGS-3610# **copy flash:** *filename* **sour** *directoryname*	Copy files to the specified file

The following example shows how to copy a file to a directory and another file:

```
DGS-3610# copy flash:config.tex flash:tmp/
DGS-3610# copy flash:con_bak.txt flash:config.text
```

49.2.4 Showing Directories

This shows the contents of the current working directory or specified directory:

Command	Function
DGS-3610# **dir**	Show the contents in the current directory
DGS-3610# **dir** *directory*	Show the contents in the specified directory

The following example shows the contents of the current directory and specified directory:

```
DGS-3610# dir
DGS-3610# dir ../bak
```

49.2.5 Formating the System

In the privileged user mode, format the device managed and operated by the file system through the following command:

Command	Function
DGS-3610# **makefs dev** *devname* **fs** *fs_name*	Format the device named **dev** for the file system named **fs_name**

The following example formats the first MTD device in the **dev** directory for the jffs2 file system:

```
DGS-3610# makefs dev /dev/mtd/mtdblock/1 fs jffs2
```

The above example formats a device in the mtdlbock directory for the jffs2 file system, clearing the data on the device for use by the file system.

49.2.6 Creating Directories

In the privileged mode, create a required directory in the specified location through the following steps:

Command	Function
DGS-3610# **mkdir** *directoryname*	Create directories

The following example creates a **BAK** directory in the root directory:

```
DGS-3610# mkdir bak
```

49.2.7 Moving Files

In the privileged user mode, move the specified files to the specified directory:

Command	Function
DGS-3610# **rename flash:** *old_filename* **flash**: *new_filename*	Name the file named as **old_filename** to **new_filename**.

49.2.8 Showing the Current Working Path

In the privileged user mode, show the current working path through the following steps:

Command	Function
DGS-3610# **pwd**	Show the current working paths

49.2.9 Removing Files

In the privileged user mode, delete a file permanently through the following step:

Command	**Function**
DGS-3610# **del** *filename*	Delete the specified file.

The following example deletes the temporary file named **large.c** in the **MNT** directory:

```
DGS-3610# del mnt/large.c
```

49.2.10 Deleting Empty Directories

In the privileged user mode, delete an empty directory permanently through the following step:

Command	**Function**
DGS-3610# **rmdir** *directoryname*	Delete an empty directory

The above example deletes an empty directory named **MNT**.

```
DGS-3610# rmdir mnt
```

50 Log Configuration

50.1 Overview

During the operation of a device, various state changes occur such as the link status up/down, and various events occur such as receiving abnormal packets and handling exceptions. Our product provides a mechanism to generate packets of a fixed format (log packet) in case of status change or event occurring. These packets can be displayed in related windows (such as console and VTY) or recorded in related media (memory buffer, FLASH), or sent to a group of log servers in the network for the administrators to analyze and locate problems. Meanwhile, in order to make it easy for administrators to read and manage log packets, these log packets can be labeled time stamps and serial numbers, and is graded according to the priority of log information.

50.1.1 Log Packet Format

The log packet format of Rujie products is as follows:

<priority> seq no: timestamp sysname

%ModuleName-severity-MNEMONIC: description

They are: <priority> Sequential number timestamp device name module name-severity – information type: abbre: information contents

Priority value = Device value *8 + Severity

Example:

```
<189> 226:Mar  5 02:09:10 S3250 %SYS-5-CONFIG_I: Configured from console by console
```

Caution

The priority field is not attached to the log packets that are printed in the user window. It only appears in the log packets that are sent to the Syslog Server.

50.2 Log Configuration

50.2.1 Log Switch

The log switch is turned on by default. If it is turned off, the device will not print log information in the user window, or send log information to the syslog server, or record the log information in the related media (memory buffer, flash).

To turn on or off the log switch, run the following command in the global configuration mode:

Command	Function
DGS-3610(config)# **logging on**	Turn on the log switch
DGS-3610(config)# **no logging on**	Turn off the log switch

Caution

Do not turn off the log switch in general case. If you are worrying about too much information printed, you can reduce it by setting different displaying levels for device log information.

50.2.2 Configuring the Log Information Displaying Device

When the log switch is turned on, the log information will be displayed on the console and also sent to different displaying devices. To configure a different displaying device for receiving logs, run the following commands in the global configuration mode or privileged user level:

Command	Function
DGS-3610(config)# **logging buffered** [*buffer-size* | *level*]	Record log in memory buffer
DGS-3610# **termninal monitor**	Allow log to be displayed on VTY window
DGS-3610(config)# **logging** *host*	Send log information to the syslog sever in the network
DGS-3610(config)# **logging file flash:***filename* [*max-file-size*] [*level*]	Record log on extended FLASH

Logging Buffered will record log information in the memory buffer. The memory buffer for log is used in recycled manner. That is, when it is full, the oldest information will be overwritten. To show the log information in the memory buffer, run **show logging** at the privileged user level. To clear the log information in the memory buffer, run **clear logging** at the privileged user level.

Terminal Monitor allows log information to be displayed on the current VTY (such as the Telnet window).

Logging Host specifies the address of the syslog server that will receive the log information. Our product allows the configuration of at most 5 syslog servers. The log information will be sent to all the syslog servers at the same time.

⚠ **Caution**

To send the log information to the syslog server, it is required to turn on the timestamp switch or sequential number switch of the log information. Otherwise, log information will not be sent to the syslog server.

Logging File Flash: Record log information in FLASH. The filename for log shall not have any extension to indicate the file type. The extension of the log file is fixed as **txt**. Any configuration of extension for the filename will be refused.

The More flash: show the contents of a log file in the flash with the **Filename** command.

⚠ **Caution**

Some devices support extended FLASH. If the device has extended FLASH, the log information will be recorded there. If the device has no extended FLASH, the log information will be recorded in the serial FLASH.

50.2.3 Enabling the Log Timestamp Switch of Log Information

To add or delete timestamp in log information, run the following command in the global configuration mode:

Command	**Function**
DGS-3610(config)# **service timestamps** *message-type* [**uptime** | **datetime**]	Enable the timestamp in the log information
DGS-3610(config)# **no service timestamps** *message-type*	Disable the timestamp in the log information

The timestamp are available in two formats: device uptime and device datetime. Select the type of timestamp.

Message type: log or debug. The **log** type means the log information with severity levels of 0-6. The **debug** type means that with severity level 7.

⚠ **Caution**

If the current device has no RTC, the configured time is invalid, and the device automatically uses the startup time as the time stamp for the log information.

50.2.4 Enabling Switches in Log System

By default, the system name is not included in the log information. To add or remove the system name in the log information, perform the following commands in the global configuration mode.

Command	Function
DGS-3610(config)# **no service sysname**	Cancel the system name from the log packet.
DGS-3610(config)# **service sysname**	Add the system name for the log packet.

50.2.5 Enabling Log Statistics

By default, the log statistics function is disabled. To enable or disable the log statistics function, perform the following commands in the global configuration mode.

Command	Function
DGS-3610(config)# **no logging count**	Disable the log statistics function and delete the statistics information
DGS-3610(config)# **logging count**	Enable the log statistics function

50.2.6 Enabling the Sequential Number Switch of Log Information

By default, the log information has no sequential number. To add or delete sequential number in log information, run the following command in the global configuration mode:

Command	Function
DGS-3610(config)# **no service sequence-numbers**	Delete sequential number in the log messages
DGS-3610(config)# **service sequence-numbers**	Add sequential number in the log messages

50.2.7 Configuring the Log Information Displaying Level

To limit the number of log packets displayed on different devices, you can set the severity level of log information allowed to be displayed on those devices.

To configure the log information displaying level, run the following command in the global configuration mode:

Command	**Function**
DGS-3610(config)# **logging console** *level*	Set the level of log information allowed to be displayed on the console
DGS-3610(config)# **logging monitor** *level*	Set the level of log information allowed to be displayed on the VTY window (such as telnet window)
DGS-3610(config)# **logging buffered** [*buffer-size* | *level*]	Set the level of log information allowed to be recorded in memory buffer
DGS-3610(config)# **logging file flash:***filename* [*max-file-size*] [*level*]	Set the level of log information allowed to be recorded in the extended FLASH
DGS-3610(config)# **logging trap** *level*	Set the level of log information allowed to be sent to the Syslog Server

The log information of DGS-3610 series falls into the following 8 levels.

Keyword	**Level**	**Description**
Emergencies	0	Be emergent The system cannot work normally.
Alerts	1	The problem against which you need to take measures immediately
Critical	2	Be important.
Errors	3	Error information
warnings	4	Warning information
Notifications	5	Common, but important, You need to focus on it.
informational	6	Explanation information
Debugging	7	Debug information

The smaller the value is, the higher the level is. The level-0 information is at the highest level.

If the level of the log information allowed to be displayed on a specified device is configured, all the information at the equal or lower level can be displayed. If the **logging console 6** command is configured, all the log information at level 6 or a lower level can be displayed on the console.

By default, the level of the log information allowed to be displayed on the console is set to 7.

By default, the level of the log information allowed to be displayed in the VTY window is set to 7.

By default, the level of the log information to be sent to the Syslog Server is set to 6.

By default, the level of the log information allowed to be recorded in the memory buffer is set to 7.

By default, the level of the log information allowed to be recorded in the extended FLASH is set to 6.

The privileged command **show logging** can be used to show the level of log information allowed to be displayed on different devices.

50.2.8 Configuring the Log Information Device Value

The device value is one of the parts that form the priority field in the packets sent to the syslog server, indicating the type of device that generates the information.

To configure the log information device value, run the following command in the global configuration mode:

Command	Function
DGS-3610(config)# **logging facility** *facility-type*	Configure the log information device value
DGS-3610(config)# **no logging facility** *facility-type*	Restore the default of the log information device value

The meanings of various device values are described as below:

Numerical Code	Facility
0	kernel messages
1	user-level messages
2	mail system
3	system daemons
4	security/authorization messages
5	messages generated internally by syslogd
6	line printer subsystem
7	network news subsystem
8	UUCP subsystem
9	clock daemon
10	security/authorization messages
11	FTP daemon
12	NTP subsystem
13	log audit

14	log alert
15	clock daemon
16	local use 0 (local0)
17	local use 1 (local1)
18	local use 2 (local2)
19	local use 3 (local3)
20	local use 4 (local4)
21	local use 5 (local5)
22	local use 6 (local6)
23	local use 7 (local7)

The default device value of our products is 23.

50.2.9 Configuring the Source Address of Log Packets

By default, the source address of the log packets sent to the syslog server is the address of the interface that sends the packets. It is possible to fix the source address for all log packets through commands.

It is possible to directly set the source IP address of the log packets or the remote port of the log packets.

To configure the source address of the log packets, run the following command in the global configuration mode:

Command	Function
DGS-3610(config)# **logging source interface** *interface-type interface-number*	Configure the source port of log information
DGS-3610(config)# **logging source ip** *A.B.C.D*	Configure the source IP address of log messages

50.2.10 Setting the Function of Sending User Logs

By default, no log is output when a user logs in or out and executes configuration commands. To output user login/logoff logs or configuration command logs, execute the following commands in the global configuration mode:

Command	Function
DGS-3610(config)# **logging userinfo**	Set user login/logoff log.
DGS-3610(config)# **logging userinfo command-log**	Send a log when a configuration command is executed

50.3 Log Monitoring

To monitor log information, run the following commands in the privileged user mode:

Command	Function
DGS-3610# **show logging**	View the log packets in memory buffer as well as the statistical information of logs
DGS-3610# **show logging count**	View the statistical information of logs in every module
DGS-3610# **clear logging**	Clear the log packets in the memory buffer
DGS-3610# **more flash:***filename*	View the log files in the extended flash

Caution

The format of the time stamp in the output result of **show logging count** is the format in the latest log output.

50.3.1 Examples of Log Configuration

Here is a typical example to enable the logging function:

```
DGS-3610(config)# interface gigabitEthernet 0/1
DGS-3610(config-if)# ip address 192.168.200.42 255.255.255.0
DGS-3610(config-if)# exit
DGS-3610(config)# service sequence-numbers        //Enable sequence number
DGS-3610(config)# service timestamps debug datetime //Enable debug information
                                                  timestamp, in date format
DGS-3610(config)# service timestamps log datetime  //Enable log information timestamp
in the date format
DGS-3610(config)# logging 192.168.200.2    //Specify the syslog server address
DGS-3610(config)# logging trap debugging       //Send the log information at all levels
to the syslog server
DGS-3610(config)# end
```

51 POE Management Configuration

51.1 Overview

PoE (Power Over Ethernet) is a mechanism that provides 45V~-57V DC to the remote PD devices (IP Phone, WLAN AP and Network Camera) via twisted pair cables.

The PSE (Power Sourcing Equipment) can transmit both data and current at the same time via Category 3/5 twisted pair cables (1, 3, 2, 6), with a maximum distance of 100m.

The switch supporting POE can provide the statistics of the power condition of each port and the entire device, which can be shown through a query command. At the same time, it also provides overtemperature protection. When the temperature inside the switch exceeds 80 Celsius degrees, the switch will trigger protection by turning off the PoE power supply to all ports. When the temperature inside the switch is lower than 60 Celsius degrees, the switch will restore the PoE power supply for all ports.

Caution The switches supporting POE include DGS-3610-26P

51.2 POE Configuration Management

This section includes:

- Remote power supply configuration
- Enabling/disabling the remote power supply of the port
- Setting the minimum allowed voltage of the POE system
- Setting the maximum allowed voltage of the POE system
- Power management mode of the switch
- Disconnection detection mode
- Showing the port/system status

51.2.1 Remote Power Supply Configuration

The switch supporting POE can automatically detect whether the device connected to a port is a standard PD device and provide supply power to the standard PD device.

You can enable or turn off the remote power supply of a port, set the minimum allowed voltage of the POE system, set the maximum allowed voltage of the POE system, set the power management mode of the switch, and set the disconnection detection mode through the command line.

Table 51-1 Remote Power Supply Configuration

Device	Configuration	Default	Description
Switches supporting PoE	Enable/disable the PoE of a port	Enabled	-
	Set the maximum power of the power supply for the port	15.4w	-
	Set the minimum allowed voltage of the POE system	45v	-
	Set the maximum allowed voltage of the POE system	57v	-
	Power management mode of the switch	Auto	-
	Disconnection detection mode	AC	-
PD device	Correct connection with the electrical interface of the POE device	-	-

51.2.2 Enabling/Disabling the PoE of a Port

You can enable or disable the PoE feature of a port according to network requirements through the following commands. By default, the PoE is enabled. Please make the following configuration in the global mode.

Table 51-2 Enabling/Disabling the PoE Feature of a Port

Command	Description
configure	Enter the configuration mode
interface gigabitEthernet ***interface-id***	Select the port, enter the interface configuration mode, and specify the physical port to be configured.
poe enable | no poe enable	Enable/disable the PoE of a port
end	Return to privileged EXEC mode

show run	Verify the configuration of the steps above
copy running-config startup-config	Save the settings into the parameter file.

For example, enable/disable the PoE of interface 1 on line card 1:

```
DGS-3610#
DGS-3610# configure
DGS-3610(config)#interface gigabitEthernet  1/1
DGS-3610(config-if)# poe enable
DGS-3610(config-if)# no poe enable
DGS-3610(config-if)# end
DGS-3610#
```

51.2.3 Setting the Minimum Allowed Voltage of the POE System

Currently, the Ethernet interface of the switch supporting POE can provide the minimum allowed voltage of 45V. You can set the minimum allowed voltage according to the actual need, within the range of 45v~47v. When the output voltage is lower than the minimum allowed value due to reasons such as power faults, the device will automatically turn off the power supply of the devices connected at all ports.

You can execute the following commands to set the minimum allowed voltage of the power supply of the port. Configure in the global mode.

Table 51-3 Setting the minimum allowed voltage of POE

Command	Description
configure	Enter the configuration mode
poe-power lower ***lower*** **| no poe-power lower**	Set the minimum allowed voltage of the POE system/restore the minimum allowed voltage to the default value
end	Return to privileged EXEC mode
show run	Verify the configuration of the steps above
copy running-config startup-config	Save the settings into the parameter file.

By default, the minimum output power of a port is 45v.

For example, set the minimum output power of the system to 46v.

```
DGS-3610#
DGS-3610# configure
DGS-3610(config)# poe-power lower 46
DGS-3610(config)# end
DGS-3610#
```

51.2.4 Setting the Maximum Allowed Voltage of the POE System

The Ethernet interface of the switch supporting POE can provide the maximum allowed voltage of 57V. You can set the maximum allowed voltage according to the actual need, within the range of 55v~57v. When the output voltage is higher than the maximum allowed value due to reasons such as power faults, the device will automatically turn off the power supply of the devices connected at all ports.

You can execute the following commands to set the maximum allowed voltage of the power supply of the port. Configure in the global mode.

Table 51-4 Setting the Maximum Allowed Voltage of the POE System

Command	Description
configure	Enter the configuration mode
poe-power upper upper | no poe-power upper	Set the maximum allowed voltage of the POE system/restore the maximum allowed voltage to the default value
end	Return to privileged EXEC mode
show run	Verify the configuration of the steps above
copy running-config startup-config	Save the settings into the parameter file.

By default, the maximum output power of a port is 57v.

For example, set the maximum output power of the system to 56v.

```
DGS-3610#
DGS-3610# configure
DGS-3610(config)# poe-power upper 56
DGS-3610(config-if)# end
DGS-3610#
```

51.2.5 Setting the Power Management Mode of the Switch

The power management mode of the switch is used to allocate the power to the PD devices. When one PD device is connected to the equipment, the equipment allocates power to the external PD device according to the power supply management mode, if the current power allocated has not exceeded the no_connect limit. POE has one limit: no_connect. When the power allocated from the equipment exceeds the no_connect limit, the equipment does not supply power to any new PD devices.

Currently, the PoE device uses the auto power management mode.

In the Auto mode, the power is allocated according to the detected port PD type. In the Auto mode, the equipment allocates power to classes 1~3 PD devices as follows: class1~4W, class2~7W, lass3~15.4W and class0~15.4W.

This configuration is automatically performed by the switch without any user intervention.

51.2.6 Disconnection Detection Mode

The equipment supporting POE checks whether a previously connected device has been disconnected through disconnection detection. The equipment supports two detection modes: AC and DC. In the AC detection mode, the connected PD device is disconnected when the current of a port is smaller than a fixed value for the specified period. The DC detection mode works by detecting the voltage feature of the port.

You can execute the following command to set the disconnection detection mode. Please make the following configuration in the global mode. You can also set this mode for a particular device.

Table 51-5 Disconnecting Detection Mode

Command	Description
configure	Enter the configuration mode
poe disconnect-mode {**ac** | **dc**} | **no poe disconnect-mode**	Set the disconnect detection mode/restore the disconnect detection mode to the default value
end	Return to privileged EXEC mode
show run	Verify the configuration of the steps above
copy running-config startup-config	Save the settings into the parameter file.

By default, the disconnection detection mode is the AC mode.

For example, set the disconnectiong detection mode to DC:

```
DGS-3610#
DGS-3610# configure
DGS-3610(config)# poe-disconnect-mode dc
DGS-3610(config-if)# end
DGS-3610#
```

51.2.7 Showing the Power Supply Status of the Port/System

The equipment supporting POE will scan the ports and the status of the entire POE system periodically, and save all the status information. You can view interface status by executing the **show** command in the privileged EXEC mode.

Command	Description
show poe interfaces gigabitEthernet [*interface-id*]	Show the power supply status of the specified port
show poe interfaces	Show the power supply status of all POE ports (the 24 ports that the POE system can power)
show poe powersupply	Show the power supply status of the entire POE system
show running-config interface [*interface-id*]	Show the configuration of the current running interface.

For example, show the power status of the gigabitethernet 0/2 port:

```
Interface : Gi0/2
Port power enabled : ENABLE
Port connect status : OFF
Port PD Class : no PD devices
Port max power : 15.4W
Port current power : 0 mW
Port peak power : 0 mW
Port current : 0 mA
Port voltage : 48V
Port trouble cause : normal
```

Note: Port trouble cause means the power-down cause, as below:

Port trouble cause	Description
normal	Normal power supply (red/green); AC/DC detects that the equipment is disconnected (LED off), Disable (LED off)
overload during start-up	Power supply start-up, finding that the current is too large or is disconnected (red/orange)
port off due to overload event	PD device is disconnected due to overload (LED orange)
short circuit event	PD device is disconnected due to short circuit (LED red)
voltage is out of established bounds	Output voltage is turned off due to out of bounds (LED red)
temperature rise too high	Turned off due to high-temperature protection (LED red)
power overload	Turned off due to power management (LED orange)

The following example shows the power supply status of the POE system:

```
DGS-3610# show poe powersupply

PSE Total Power :1200.0 W
PSE Total Power Consumption : 0 W
PSE Available Power : 1200.0 W
PSE Peak Value : 0 W
PSE Min Allow Voltage : 45 V
PSE Max Allow Voltage : 57 V
PSE Disconnect Sense Mode : ac
```

The remote power supply of S7600P-48GT is PSE. The following exmaple shows the power status of the POE system of S7600 products:

```
External Power Mangement: auto
External PSE Total Power: 1200.0 W
External PSE Total Power Consumption : 0 W
External PSE Total Remain Power Consumption : 1200.0 W
External PSE Peak Value : 0 W
External PSE Min Allow Voltage : 45V
External PSE Max Allow Voltage : 57V
External PSE SYS Voltage: 48 V
External PSE Disconnect Sense Mode : ac
```

52 Stack Management

52.1 Understanding Stack

52.1.1 Overview

The stack technology is for centralized management and port expansion. You can connect multiple separate switches into a centralized stack system by using stack ports and stack cables. Its advantages are:

Flexible port density expansion: The number of ports in a stack system is the total of the ports of all member devices in the stack. You can flexibly add or reduce ports according to the size of the network, without discarding the old devices, for maximum investment protection.

Easy user management: The stack system is logically a device and one node in a network, managed through a single IP address, for saving IP addresses and easy management.

52.1.2 Hardware Structure

Special ports and cables are usually needed to form a stack system. DGS-3610 series provide multiple hardware solutions for choice:

- Stack module: A dedicated stack module can provide a high-bandwidth and low-cost stack solution. To use this solution, you need the special stack cables, whose lengths restrict the distances between stack member devices.
- Common module: A common module can provide a high-bandwidth and long-distance stack solution. To adopt this solution, you do not need special stack cables. However, its disadvantage is that it has a high cost.
- Fixed port: A fixed port can provide a low-cost and long-distance stack solution. To use this solution, you do not need special stack cables. However, its disadvantage is that it has low bandwidth.

⚠ **Caution**

All the DGS-3610 series switches support stack.

The switch stack system supports eight member devices, which are connected through the stack module or stack cables. For how to install the stack, see the hardware manual of the specific product.

52.1.3 Starting and Stopping a Stack

If no stack module is inserted in the slot of a switch in the start process, the switch works in the standalone mode. If a stack module is inserted, the switch detects whether the stack link is connected. If yes, the switch works in the stack mode. If the switch finds that the switch link is not connected for some time, it works in the standalone mode.

In the stack environment, if the stack cable connection is interrupted, the management of the stack will fail, and the system will send a log to the user:

```
STACKMODULE-LINKSTATUS-CHANGED: Link loss is detected in the stack loop.
Device [2] loss has been detected, system will reset.
```

If the connectivity of the stack cable recovers in 10 seconds, the stack environment will recover, and the system will send a log to the user:

```
STACKMODULE-LINKSTATUS-CHANGED: Link recover is detected in the stack loop.
```

If the connection remains interrupted for more than 10 seconds, the stack cannot work normally, and the stack system will restart to create the stack again.

When the network traffic is excessively heavy, the management of the stack will fail. In this case, you do not need to restart the switch. When the network traffic decreases, the switch in the stack environment will restore its normal working.

The stack does not support hot plugging, which means that you cannot insert, remove or replace any member devices when the stack is running. If you do so, the stack system will restart to establish another stack. In the stack environment that is working stably, if any switch is powered off and is restarted, all other switches in the stack will automatically restart and make another selection to establish a new stack.

⚠ **Caution**

When the stack is running, if you insert, remove or replace the member devices, the stack will reset and another election will be made to establish a new stack.

52.2 Configuring a Stack

52.2.1 Default Configuration

The stack attribute of the device is configured as below:

Attribute	Default value
Stack interface	Stack module
Device priority	1

Attribute	Default value
Device description	SWITCH

52.2.2 Identifying Stack Member Device According to the Device Number

The host in the stack system is selected according to device priorities. The one with the highest priority is selected as the host. When two member devices have the same priority, they are selected according to their MAC addresses. The one with a smaller MAC address is selected as the host. After you configure the priority of a device, you must restart it to put the setting into effect.

After the stack is established, you can only execute out-band management through the serial port of the host. Therefore, you are recommended to first select a host before you establish a stack, and set it to have a high priority in the standalone mode, so that it is elected as the host in the stack. The priorities of the devices are 1-10 from high to low, defaulted to 1. For the detailed setting methods, see **Configuring the Device Priority**. When the stack is started, you can use the **show member** command to show the information of the stack members. You can determine the devices in the stack and their sequence according to their MAC addresses.

You are recommended to arrange the devices stacked from device 1 to device N, and connect them according to the above rule.

⚠ **Caution**

In a stack, you can only execute out-band management through the serial port of the host. Therefore, you are recommended to first select a host before you establish a stack, and set it to have a high priority in the standalone mode, so that it is elected as the host in the stack.

52.2.3 Configuring the Device Priority

Run the following commands in the global configuration mode:

Command	Description
DGS-3610(config)# **device-priority** [*member*] *priority*	*member:* 1-MAX, configuring the member device. *priority:* 1-10, specifying the priority of the device. By default, 1 is configured for a member device.

Configuration Examples: Specify the priority of the member device 2 to 8:

```
DGS-3610(config)# device-priority 2 8
```

Caution

After configuration is completed, you need to execute the **write** command to save it. After the stack is reset, the priority takes effect only after a new stack system is established.

52.2.4 Configuring Device Description

For easier memory, you can set a description for a stack member. In the global configuration mode, execute the following command to configure it:

Command	Description
DGS-3610(config)# **device-description** [**member** *member*] *description*	*member:* 1-MAX, configuring the member device. *description:* Its length is 31, and it indicates the description of the device. By default, 1 is configured for a member device.

Configuration Examples: Specify the description of member equipment 2 to **D-Link**:

```
DGS-3610(config)# device-description member 2 D-Link
```

52.2.5 Saving Parameters

The stack information configured with the following commands can be saved into the member device:

```
device-priority [member] priority
device-description [member member] description
stack on
```

Such configuration information is moved as the member device is moved. Other system configuration information is only saved in the primary device, moving as the primary device moves.

52.3 Showing Stack Information

In the privileged mode, you can view the stack information with the following commands.

Command	Description
DGS-3610# **show version devices**	Show the system device information
DGS-3610# **show version slots**	Show the slot information.
DGS-3610# **show version**	Show the version of the stack system

Command	Description
DGS-3610# **show member** [*member*]	Show the stack information of the member device. *member:* 1-MAX, configuring the specified member device.

Note

The display information of partial examples in this manual may include the content of other product series (such as the product model and description). For detailed display information, refer to actual equipment information used.

Examples: Show all kinds of information of the stack system

```
DGS-3610#show version devices
   Device  Slots  Description
   ------  -----  --------------------
   1       3      DGS-3610-26
   2       3      DGS-3610-52
   3       3      DGS-3610-26
   4       3      DGS-3610-26
   5       3      DGS-3610-26
   6       3      DGS-3610-26
   7       3      DGS-3610-26
   8       3      DGS-3610-52

DGS-3610#show version slots
   Device  Slot  Ports  Max Ports  Module
   ------  ----  -----  ---------  ---------------------------------
   1       0     24     24     DGS-3610-26_Static_Module
   1       1     1      1          DEM-412CX
   1       2     0      1
   2       0     48     48         DGS-3610-52_Static_Module
   2       1     1      1      DEM-412CX
   2       2     1      1      DEM-412CX
   3       0     24     24     DGS-3610-26_Static_Module
   3       1     1      1      DEM-412CX
   3       2     1      1      DEM-412CX
   4       0     24     24     DGS-3610-26_Static_Module
   4       1     1      1      DEM-412CX
   4       2     1      1      DEM-412CX
   5       0     24     24     DGS-3610-26_Static_Module
   5       1     1      1      DEM-412CX
   5       2     1      1      DEM-412CX
   6       0     24     24     DGS-3610-26_Static_Module
   6       1     1      1      DEM-412CX
   6       2     0      1
   7       0     24     24     DGS-3610-26_Static_Module
   7       1     1      1      DEM-412CX
   7       2      1     1       DEM-412CX
   8       0      48    48      DGS-3610-52_Static_Module
   8       1      1     1       DEM-412CX
   8       2      1     1       DEM-412CX

DGS-3610#show version
System description      : DGS-3610-26 Gigabit Ethernet Switch
System start time       : 2007-4-23 17:39:11
System hardware version : 1.0
System software version : v10.2.00(2), Release(39975)
System BOOT version     : 10.1.11330
System CTRL version     : 10.1.11330
System Serial Number    : 1234942570002
Device information:
  Device-1
    Hardware version : 1.0
    Software version : v10.2.00(2), Release(39975)
    BOOT version     : 10.1.11330
    CTRL version     : 10.1.11330
    Serial Number    : 1234942570002
  Device-2
    Hardware version : 1.0
    Software version : v10.2.00(2), Release(39975)
    BOOT version     : 10.1.11330
    CTRL version     : 10.1.11330
    Serial Number    : 1234942570001
  Device-3
    Hardware version : 1.0
    Software version : v10.2.00(2), Release(39975)
    BOOT version     : 10.1.11330
    CTRL version     : 10.1.11330
    Serial Number    : 1234942570003
  Device-4
    Hardware version : 1.0
    Software version : v10.2.00(2), Release(39975)
    BOOT version     : 10.1.11330
    CTRL version     : 10.1.11330
    Serial Number    : 1234942570004
  Device-5
    Hardware version : 1.0
    Software version : v10.2.00(2), Release(39975)
    BOOT version     : 10.1.11330
    CTRL version     : 10.1.11330
    Serial Number    : 1234942570005
  Device-6
    Hardware version : 1.0
    Software version : v10.2.00(2), Release(39975)
    BOOT version     : 10.1.11330
    CTRL version     : 10.1.11330
    Serial Number    : 1234942570006
  Device-7
    Hardware version : 1.0
    Software version : v10.2.00(2), Release(39975)
    BOOT version     : 10.1.11330
    CTRL version     : 10.1.11330
    Serial Number    : 1234942570007
  Device-8
    Hardware version : 1.0
    Software version : v10.2.00(2), Release(39975)
    BOOT version     : 10.1.11330
    CTRL version     : 10.1.11330
    Serial Number    : 1234942570008

DGS-3610#show member
Member   Mac Address     Priority Software Version    Hardware    Version   Description
------   -------------- -------- ---------------- ------------- -------- ------------
1        00d0.f810.3323  1       V10.2.00(2), Release(39975)   1.0      SWITCH
2        00d0.f822.33aa  1       V10.2.00(2), Release(39975)   1.0      SWITCH
3        00d0.f822.33ae  1       V10.2.00(2), Release(39975)   1.0      SWITCH
4        00d0.f822.33b0  1       V10.2.00(2), Release(39975)   1.0      SWITCH
5        00d0.f822.33b2  1       V10.2.00(2), Release(39975)   1.0      SWITCH
6        00d0.f824.23b4  1       V10.2.00(2), Release(39975)   1.0      SWITCH
7        00d0.f833.44b4  1       V10.2.00(2), Release(39975)   1.0      SWITCH
8        00d0.f855.33ae  1       V10.2.00(2), Release(39975)   1.0      SWITCH
```