xStack DES-7200

Configuration Guide

Version 10.1

D-Link®

DES-7200 Configuration Guide

Revision No.: Version 10.1

Date:

Preface

Version Description

This manual matches the Firmware version 10.1.

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 bolded characters.

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 bolded characters.

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

[ ]: The part enclosed with [ ] means 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.

//:Lines starting with an exclamation mark "//" are annotated.

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**	Descript, prompt, tip or any other necessary supplement or explanation for the operation.

Contents

1 Using Command Line Interface

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 Error Messages
- Using History Commands
- Using Editing Features
- Accessing CLI
- CLI Privilege Configuration

1.1 Command Mode

The management interface of DES-7200 has several modes. The command mode that you are in determines the usable commands.

After you enter a command mode, typing a question mark (?) under the command prompt will list the commands available in this mode.

When a new session connection is set up between you and the switch management interface, you are in user EXEC mode first and can use commands in this mode. In 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 first need to enter privileged EXEC mode. To do this, you shall need input the password for privileged EXEC mode. In privileged EXEC mode, you can use all privileged commands and thus enter global configuration mode.

Using commands in configuration mode (global configuration, interface configuration, and so on) may affect the ongoing configuration. If you have saved the configuration information,

these commands will be saved and 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 methods, prompts, and how to exit methods.Suppose the equipment is named "*DES-7200*" by default.

Summary of main command modes:

Command mode	**Access method**	**Prompt**	**Exit or access next mode**	**About this mode**
User EXEC (User EXEC Mode)	To access the equipment ,first enter this mode.	DES-7200 >	Enter the **exit** command to quit this mode. To enter privileged EXEC mode, enter the **enable** command.	Used for basic test and showing system information
Privileged EXEC (Privileged mode)	From user EXEC mode, enter the **enable** command.	DES-7200 #	To return to the user configuration mode, enter **disable**. To enter global configuration mode, enter the **configure** command.	Used to verify the results of using setting commands and this mode is protected with password.
Global configuration (Global configuration mode.)	From privileged EXEC mode, enter the **configure** command.	DES-7200 (config)#	To exit global configuration command mode and to return to privileged EXEC mode, enter the **end** or **exit** command, or press Ctrl-C. To access the interface configuration mode, enter the interface command. You must indicate to enter to the interface configuration sub_mode in the interface command. To access the VLAN configuration mode, enter the **vlan** *vlan_id* command.	Commands in this mode are used for configuring the global parameters that can affect the whole switch.

Interface configuration (Interface configuration mode)	Enter the **vlan** *vlan-id* global configuration command to access config-vlan mode:	DES-7200 (config-if)#	To return to Privileged EXEC mode, enter **end** or **Ctrl+C.** To return to Global configuration mode, enter **exit** . You must indicate to enter to the interface configuration sub_mode in the interface command.	Configure various interfaces of the equipment in this mode.
Config-vlan (Vlan Mode)	Enter the **vlan** *vlan-id* global configuration command to access config-vlan mode:	DES-7200 (config-vlan)#	To return to Privileged EXEC mode, enter **end** or **Ctrl+C.** To return to Global configuration mode, enter **exit**.	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 ?	Obtains a character string of command keywords beginning with the same. Example: DES-7200# **di?** dir disable
Abbreviated command <Tab>	Obtains complete keywords of commands. Example: DES-7200# **show conf**<Tab> DES-7200# **show configuration**
Prompt the next keyword?	Lists the next keyword associated to the command. Example: DES-7200# **show ?**

Prompt the next variable?	Lists the next variable associated with the keyword. Example: DES-7200(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 running-config** can be abbreviated to:

```
DES-7200# show run
```

If the entered characters are not enough for the system to recognize a command, the system will prompt "Ambiguous command:".

For example, when you want to view information about access-lists, the following text is not complete.

```
DES-7200# show access
% Ambiguous command: "show access"
```

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:

```
DES-7200#configure terminal
DES-7200(config)#interface gigabitEthernet 0/4
DES-7200(config-if)#shutdown        //Use the shutdown command to shut down an interface
DES-7200(config-if)#no shutdown     //Use the no shutdown command to open an interface
```

Most configuration commands have the **default** option, which restores the default setting of the command. Most commands are disabled by default; in this case, the **default** and **no** options generally serve the same purpose. Some commands are enabled by default; in this case the **default** and **no** options serve the different purposes, and the default option is used to enable the command and restore the default settings of the variables..For example, IP routing is enabled on the 3-layer equipment by default, the **default ip routing** command works like **ip routing**, instead of **no ip routing**.

1.5 Understanding CLI Error Messages

The following table lists the error prompt messages when user is using the CLIs management equipment.

Common CLI error messages

Error message	Meaning	How to obtain help
% Ambiguous command: "show c"	If you input insufficient characters in the switch, the switch can not identify the only command.	Re-input the command and a question mark immediately after the ambiguous word. The possible keywords will be listed.
% 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 recently. 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.
DES-7200(config-line)# **history size** *number-of-lines*	Set the number of history commands for the terminal. Range 0 ~ 256. Default value: 10.

Note: Standard terminals like the VT100 family support arrow keys.

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 sliding window to edit the commands that exceed the length of one 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 call complicated commands repeatedly. For details about shortcut keys, see Edit Shortcut Keys.

1.8 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 and 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.

1.9 CLI Privilege Configuration

1.9.1 Introduction to CLI Privilege

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 sub-levels of commands for each mode. By configuring multiple passwords, you can allow different sets of users to have access to specified commands.

For example, if you want to use one command in more levels, you can assign it lower user level. If you want to use one command in less range of levels, you can assign it higher user level. If you want to manage the switch by Telnet, you must set the password for the normal user to verify the validity of the Telnet users.

1.9.2 CLI Privilege Configuration

1.9.2.1 Command authorization

You can authorize command using the following commands:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **privilege mode** [**all**] {**level** *level* | **reset**} *command-string*	Set the privilege level for a command. **mode** - The CLI command mode to which the command to be authorized belongs. For example, **config** indicates the global configuration mode, **exec** indicates the privilege command mode, and **interface** indicates the interface configuration mode. **all -** Change all the privileges of the subcommands of the specified command to the same preivilege level. **level** *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** command. **reset** is used to restore the command execution privilege to the default level. *command* - Specify the command for authorization.

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

1.9.3 Example of CLI Privilege Configuration

1.9.3.1 Command authorization

In the following configuration process, the **reload** command and its subcommands are assigned to level 1 and level 1 is set as a valid level (by setting the password to "test").

```
RedGiant# configure terminal
RedGiant(config)# privilege exec all level 1 reload
RedGiant(config)# enable secret level 1 0 test
RedGiant(config)#End
```

After entering level 1, you can see the command and its subcommands:

```
RedGiant# enable 1
RedGiant>reload ?
```

```
at                reload at a specific time/date
cancel            cancel pending reload scheme
in                reload after a time interval
<cr>
```

1.9.3.2 Privilege Recovery

In the following configuration process, the privileges of the **reload** command and its subcommands are restored to the default values:

```
RedGiant# configure terminal
RedGiant(config)# privilege exec all reset reload
RedGiant(config)# end
At level 1, the privileges of the command have been recovered:
RedGiant# enable 1
RedGiant> reload ?
% Unrecognized command.
```

2 Equipment Management

2.1 Overview

This chapter describes how to manage the equipment:

- Access Control by Command Authorization
- Logon Authentication Control
- System Time Configuration
- Scheduled Restart
- Configuring a System Name and Prompt
- Banner Configuration
- Viewing System Information
- Console Rate Setting
- Using telnet on the Equipment

Note

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

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 or network device. Privilege levels define the commands users can use after they have logged in to a network device.

For 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

DES-7200 has the following commands for setting or changing the passwords at different levels.

Command	Purpose
DES-7200(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 on security password has 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 that is set is the same as the 15-level security password, the system will give a warning message.
DES-7200(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.
DES-7200# **enable** [*level*] and DES-7200# **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 sub-levels of commands for each mode. By configuring multiple passwords, you can allow different sets of users to have access to specified commands.

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

2.2.5 Configuring Line Password Protection

DES-7200 supports 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
DES-7200(config-line)# **password** *password*	Specify the line password
DES-7200(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.

2.2.6 Supporting Session Locking

DES-7200 allows 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
DES-7200(config-line)# **lockable**	Enable the function for locking the line terminal
DES-7200# **lock**	Lock the current line terminal

2.3 Logon Authentication Control

2.3.1 Overview

In the previous section, we describe how to control the access to the switch by configuring the password stored in local files. In addition to local authorization, when users log in to the equipment for management, some servers can also be used to authenticate them according to the user name and password. Currently, the RADIUS server is supported to control the right to manage the switch according to the user name and password inputted at login.

When users login to the equipment, we can authenticate users according to the username and password pairs stored centrally on a RADIUS server instead of local files. The equipment sends the encrypted user information to the RADIUS server for verification, and the server also stores 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

DES-7200 supports 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
DES-7200(config)# **username** *name* [**password** *password* | **password** *encryption-type encrypted password*]	Establish the username identity authentication by using the encryption password.
DES-7200(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
DES-7200(config-line)# **login local**	Set local authentication for line logon in AAA mode.
DES-7200(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 for AAA configuration.

2.4 System Time Configuration

2.4.1 Overview

Every piece of equipment has its system clock, which provides the date (yeah, month, day) and time (hour, minute, second) and the week.When you use the equipment for the first time, you need to first configure the system clock of the equipment to the 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 recording the time when an event occurs.

2.4.2 Setting the System Time and Date

You can configure the system time on the switch manually.After you set the equipment clock, the clock will keep running on the basis of the time you set, and go on even if the equipment is powered off. Hence, after the equipment clock has been set, there is no need to set it again unless you want to calibrate the time on the equipment.

Command	Function
DES-7200# **clock set** *hh:mm:ss date month year* Or DES-7200# **clock set** *hh:mm:ss month date year*	Set the date and clock for the system.

For example, change the system time to 2002-12-25, 08:00:00

```
DES-7200# clock set 10:10:12 20 Jun 2003    //Set the system date and time
DES-7200# show clock                        //Confirm whether the system time change takes
                                            effect
clock: 2003-6-20 10:10:54
```

Abbreviated forms of the English words for months are used for the configuration of months, as detailed below: January/JAN, February/FEB, March /MAR, April /APR, May /MAY, June /JUN, July /JUL, August /AUG, September /SEP, October /OCT, November /NOV and December /DEC.

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:

```
DES-7200# 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, for example). *Modifiers* is the group of 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 type **reload in *10 test***.

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

This command schedules a reload of the software at the specified time. The value must be a specified time in future. The parameter *year* is optional. If you do not provide 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, you do not need to input the year if the current date is between January 1 and November 30.. Because the interval between the reload time and the current time shall not exceed 31 days, you do not need to input the year if the current date is between January 1 and 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 which case, you need to input the year telling 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 restart scheme and then restarts the system before the scheme takes effect, the scheme will be lost. The span from the time in the restart scheme to the current time shall be within 31 days and must be greater than the current system time. Also, after you set reload, you should not set 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
DES-7200# **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). If you have not inputted any year, the current year is used by default.

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):

```
DES-7200# reload at 12:00 11 Nov midday     //Set the system reload time and date
DES-7200# show reload                  //Confirm whether the restart time change takes
                                       effect
Reload scheduled for 2005-01-11 12:00  (in 3 hours 29 minutes)
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
DES-7200# **reload in** *mmm* [*reload-reason*]	Configure the system reload in *mmm* minutes, where the reload reason is described in *reload-reason* (if inputted)
DES-7200# **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):

```
DES-7200# reload in 125 test    //Set the system restart time
```

Or

```
DES-7200# reload in 2:5 test    //Set the system reload time
DES-7200# show reload           //Confirm whether the restart time change takes effect
Reload scheduled  in 2 hours and 4 minutes
Reload reason: test
```

2.5.4 Immediate Restart

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

2.5.5 Deleting the Configured Restart Scheme

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

Command	Function
DES-7200# **reload cancel**	Delete the configured restart scheme.

If no reload scheme is configured, you will see error message for the operation.

2.6 Configuring a System Name and Prompt

2.6.1 Overview

For easy management, you can configure a system name for the switch to identify it. If you configure a system name more than 22 characters, the first 22 characters are used as the system prompt. The prompt varies with the system name. If the system name is empty, the prompt is “DES-7200”. The default switch system name and prompt are both “DES-7200”.

2.6.2 Configuring a System Name

DES-7200 has the following commands to configure the system name in global mode:

Command	Function
DES-7200(Config)# **hostname** *name*	Manually configure a system name. The name must consist of all printable characters, up to 255 of them.

To return to the default hostname, use the **no hostname** command in the global configuration mode. The following example changes the equipment name to DES-7200:

```
DES-7200# configure terminal        //Enter the global configuration mode.
DES-7200(config)# hostname DES-7200      //Set the equipment name to DES-7200
DES-7200(config)#                        //The name has been modified successfully.
```

2.6.3 Configuring a System Prompt

If you have not configured a system prompt, the first 22 characters of the system name are used as the system prompt. The prompt is updated whenever the system name changes. If the system name is empty, the prompt is “DES-7200”. You can configure a system prompt with the **prompt** command in the global configuration mode.

Command	Function
DES-7200# **prompt** *string*	Configure the command-line prompt. The name must consist of all printable characters, up to 22 characters of them.

To return to the default prompt, use the **no prompt** [*string*] command in the global configuration mode.

2.7 Banner Configuration

2.7.1 Overview

When the user logs in to the equipment, you may need to tell the user some useful information. You can achieve it by creating a banner. You can configure a message-of-the-day (MOTD) and a login banner.The message of the day is for all users that connect to the equipment. When a user logs in to the equipment, the message is displayed on the terminal first. By using the daily notice, you can send some urgent messages (for example, that the system is to be shut down) to network users. The login banner also displays on all connected terminals, and it provides some common login messages. The MOTD and login banners are not configured.

2.7.2 Configuring a Message-of-the-Day Login Banner

You can create a single or multi-line message banner that appears on the screen when someone logs in to the equipment. You may configure the message of the day in the global configuration mode:

Command	Function
DES-7200(Config)# **banner motd** *c message c*	Specify the message of the day. For c, enter the delimiting character of your choice, for example, a pound sign (&),

	and press the **Enter** key. Enter the separator and then press Enter. Now, you can start to enter the text, and enter the separator again and then press Enter. Please note that if you enter more characters after the end separator, such characters will be discarded by the system. For message, enter a banner message of up to 255 characters. You cannot use the delimiting character in the message.

To delete the MOTD banner, use the **no banner motd** command in the global configuration mode. The following example describes how to configure an everyday notice. The # symbol is used as the separator, and the text of the notice is “Notice: system will shutdown on July 6th.” See the following configuration example:

```
DES-7200# banner motd #              //Start delimiter
Enter TEXT message. End with the character '#'.
Notice: system will shutdown on July 6th.
#                                    //End delimiter
DES-7200(config)#
```

2.7.3 Configuring a Login Banner

You may configure the logon title message in the global configuration mode:

Command	Function
DES-7200(Config)# **banner login** *c message c*	Specify the text of login banner. For c, enter the delimiting character of your choice, for example, a pound sign (&), and press the **Enter** key. After the delimiter is entered: Press Enter. Now, you can start to enter the text, and enter the separator again and then press Enter. Please note that if you enter more characters after the end separator, such characters will be discarded by the system. For message, enter a banner message of up to 255 characters. You cannot use the delimiting character in the message.

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 switch 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.":

```
DES-7200# banner login #             //Start delimiter
Enter TEXT message. End with the character '#'.
Access for authorized users only. Please enter your password.
#                                    //End delimiter
DES-7200(config)#
```

2.7.4 Displaying a Banner

The message of a banner is displayed on all connected terminals at login. See the following example:

```
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 a MOTD banner, 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 through the command-line interface, such as system information, version, device information, and so on.

2.8.2 Viewing System Information and Version

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

Command	Function
DES-7200# **show version**	Show system information and version

2.8.3 Viewing Hardware Information

Hardware information includes physical device information and slot and module information on the device. The device information 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
DES-7200# **show version devices**	Show the current equipment information

DES-7200# **show version slots**	Show information about the slots and modules of the equipment

2.9 Console Rate Setting

2.9.1 Overview

The equipment comes with a console interface that allows you to manage the equipment. When it is the first time to use the switch, it is required to configure it through the console interface.You can change the rate of the serial interface on the equipment if necessary. Note that the rate of the terminal for equipment management should match the rate of the console of the equipment.

2.9.2 Setting Console Rate

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

Command	Function
DES-7200(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 by default.

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

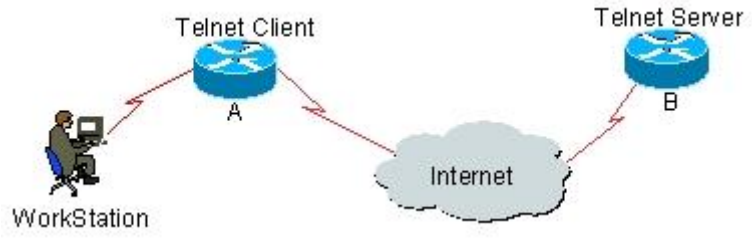
```
DES-7200# configure terminal              //Enter the global configuration mode.
DES-7200(config)# line console 0          //Enter the console line configuration mode
DES-7200(config-line)# speed 57600        //Set the console rate as 57600
DES-7200(config-line)# end                //Return to the privilege mode
DES-7200# 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 Equipment

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 switch A through the terminal emulation program or telnet, and then the user can log onto switch 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 device by using the telnet command on the equipment:

Command	Function
DES-7200# **telnet** *host-ip-address*	Log onto a remote device through telnet.

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

```
DES-7200# 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 by configuring the connection timeout of the device. When the idle time exceeds the set value and there is no input or output, this connection will be interrupted.

2.11.2 Connection Timeout

When there is input for the accepted connection within a specified time, the server will interrupt this connection.

DES-7200 provides commands in the LINE configuration mode to configure the connection timeout:

Command	Function
DES-7200(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, this connection will be interrupted.

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

```
DES-7200# configure terminal            //Enter the global configuration mode.
DES-7200# line vty 0                    //Enter the LINE configuration mode
DES-7200(config-line)#exec-timeout 20   //Set the timeout to 20min
```

2.11.3 Session Timeout

When there is no input 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 become idle.

DES-7200 provides commands in the LINE configuration mode to configure the timeout for the session connected to the remote terminal:

Command	Function
DES-7200(Config-line)#**session-timeout 20**	Configure the timeout for the session connected to the remote terminal on LINE. If there is no input within the specified time, this session will be interrupted.

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

```
DES-7200# configure terminal             //Enter the global configuration mode.
DES-7200# line vty 0                     //Enter the LINE configuration mode
DES-7200(config-line)#session-timeout 20 //Set the session timeout to 20min
```

3 System Upgrade and Maintenance

3.1 Overview

The upgrade and maintenance are the process to upgrade or upload/download files via the main program or CTRL program on the command line interface in two ways: through the network port via the TFTP protocol or through the serial port via the Xmodem protocol.

3.2 Upgrade and Maintenance Method

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

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

3.2.1 Transferring Files by Using the TFTP Protocol

Download files from the host to the equipment, or upload files from the equipment to the host.

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

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

Command	Function
DES-7200# **copy tftp:** *//location/filename* **flash:** *filename*	Download the file *filename* specified by URL on the host to the equipment.

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

Before upload, first 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
DES-7200# **copy flash:** *filename* **tftp:** *//loca tion/filename*	Upload the file *filename* from the equipment to the directory specified by the URL on the host. You can also specify another file name.

3.2.2 Transferring Files by Using the XMODEM Protocol

Download files from the host to the equipment, or upload files from the equipment to the host.

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

Prior to download, first log in to the out-band management interface of the switch by using the Windows HyperTerminal. Then, download the files by using the following command in the privileged mode. Finally, select the “Send File” from the “Transfer” menu on the Windows HyperTerminal on the local host. In the pop-up dialog box, select the file to download for the file name and select the “Xmodem” as the protocol. Click “Send”, and the Windows HyperTerminal will show the transmission process and packets.

Command	Function
DES-7200# **copy xmodem flash**:*filename*	Download a file from the host to the equipment and name it *filename*.

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

Prior to upload, first log in to the out-band management interface of the switch by using the Windows HyperTerminal. Then, upload the files by using the following command in the privileged mode. Finally, select the “Receive File” from the “Transfer” menu on the Windows HyperTerminal on the local host. In the pop-up dialog box, select the storage location for the file to upload and select the “Xmodem” as the reception protocol. Click “Receive”, and the Windows HyperTerminal will further prompt the name of the locally stored file. Click “OK” to start reception.

Command	Function
DES-7200# **copy flash**:*filename* **xmodem**	Upload the file *filename* from the equipment to the host.

3.2.3 Step for Upgrading the Device Programs

You can upgrade the main programs of the master management board, slave management board, and line card by using the TFTP or Xmodem command.

- Steps for upgrading the main program of the management board:

1. Verify that the main program to upgrade has the name of **firmware.bin.**
2. Download the file to the device by using the **copy** command.
3. Wait for the accomplishment of the upgrade of the main program of the master/slave management boards, until the following message appears:

```
Upgrade Slave CM MAIN successful!!
Upgrade CM MAIN successful!!
```

- Steps for upgrading the main program of the line card

1. Verify that the main program to upgrade has the name of **firmware_lc.bin.**
2. Download the file to the device by using the **copy** command.
3. Wait for the accomplishment of the upgrade of the main program of all the line cards, until the following message appears:

```
Upgrade LC MAIN successful!!
```

The CTRL is the boot program on the device, and you can upgrade it in the following way:

- Steps for upgrading the CTRL program of the management board:

1. Verify that the CTRL file to upgrade has the name of **firmware_lc-ctrl.bin.**
2. Download the file to the device by using the **copy** command.
3. Wait for the accomplishment of the upgrade of the CTRL program of the master/slave management boards, until the following message appears:

```
Upgrade Slave CM CTRL successful!!
Plz DO NOT reboot machine, Upgrade CM 'CTRL'...
Upgrade CM CTRL successful!!
```

- Steps for upgrading the CTRL program of the line card

1. Verify that the CTRL file to upgrade has the name of **firmware_lc-ctrl.bin.**
2. Download the file to the device by using the **copy** command.
3. Wait for the accomplishment of the upgrade of the CTRL program of all the line cards, until the following message appears:

```
Upgrade LC CTRL successful!!
```

This upgrades the CTRL programs of all the current line cards in the device.

Caution

1. 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.
2. Do not power off the device before the upgrade is completed. Otherwise, the upgrade program may be lost.

4 Network Communication Detection Tools

4.1 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 DES-7200 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 EXEC mode, only basic ping function can run, which in the privileged EXEC mode, the extended function of ping also can run.

Command	Function
DES-7200# **ping** [*ip*] [*address* [**length** *length*] [**ntimes** *times*] [**timeout** *seconds*]]	Ping network connectivity Test tools

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:

```
DES-7200# 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 and 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:

```
DES-7200# 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
DES-7200#
```

4.2 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**
DES-7200# **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:

```
DES-7200# 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:

```
DES-7200# 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.

5 IP Address and Service Configuration

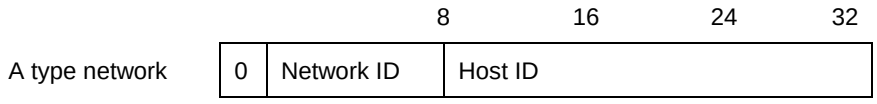
5.1 IP Addressing Configuration

5.1.1 IP Address Overview

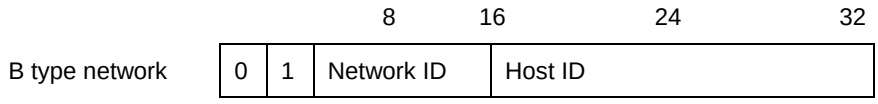
IP address is made up of 32 binary bits and expressed in dotted decimal format for the convenience of writing and describing. When expressed in decimal format, the 32 binary bits are broken into four octets (1 octet = 8 bits). Each octet is separated by a period (dot) in range from 0 to 255 (for example, 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 that address into a network part and a "rest" or local address part. Determined from the high-order bits, IP addresses are classified into four classes.The IP addresses in use can be divided into four categories according to the value in the first several bits of the network portion.

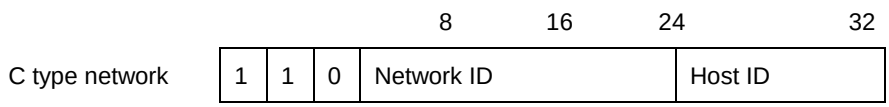
Cass A, has a 7-bit network number and a 24-bit local address. The highest-order bit is set to 0. This allows 128 class A networks.



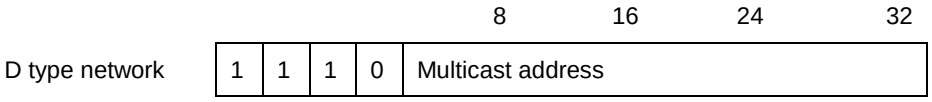
Cass B, has a 14-bit network number and a 16-bit local address. The two highest-order bits are set to 1-0. This allows 16,384 class B networks.



Class C, has a 21-bit network number and a 8-bit local address. The three highest-order bits are set to 1-1-0. This allows 2,097,152 class C networks.



For Class D, the four highest-order bits are set to 1-1-1-0, other bits are used as a multicast address.



Note

No addresses are allowed with the four highest-order bits set to “1111”. These addresses, called "class E", 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 Internet, 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). It 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 interior private network, you do not need to apply for public 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
Class A network	0.0.0.0	Reserved
	1.0.0.0~126.0.0.0	Available
	127.0.0.0	Reserved
Class B network	128.0.0.0~191.254.0.0	Available
	191.255.0.0	Reserved
Class C network	192.0.0.0	Reserved
	192.0.1.0~223.255.254.0	Available
	223.255.255.0	Reserved
Class D network	224.0.0.0~239.255.255.255	Available
Class 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 network. In order to connect the private network to Internet, you need to convert private IP address to valid internet IP address. It describes how to implement address translation in the chapter of “Network Address Translation”. It lists the private network addresses space in the following table, which is defined in RFC 1918.

Class	IP Address Range	Network Numbers
Class A network	10.0.0.0~10.255.255.255	1 Class A network
Class B network	172.16.0.0~172.31.255.255	16 Class B networks
Class C network	192.168.0.0~192.168.255.255	256 Class C networks

For the description of IP address, TCP/UDP port and other network number, please refer to RFC 1166.

5.1.2 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 network requirement.

- Assigning IP Addresses to Network Interfaces (Required)
- Configuring Address Resolution Protocol (ARP) (Optional)
- Configuring IP address mapping to WAN Address (Optional)
- Disabling IP Routing (Optional)
- Configuring Broadcast Packets Handling (Optional)

5.1.2.1 Assigning IP Addresses to Network 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
DES-7200(config-if)# **ip address** *ip-address mask*	Set an IP address for an interface.
DES-7200(config-if)# **no ip address**	Disable 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 Class A network is “255.0.0.0”. You can subnet a network by using network masks. By extending the mask using some of the bits from the host ID portion of the address to create a subnetwork ID, you can reduce hosts capacity of each network and increase subnets at the same time. For this reason, the network masks are also called subnet masks.

Note

Theoretically, bits of subnet masks can be any bits of the host ID portion. DES-7200 only supports continuous subnet masks from left to right which is started from network ID portion.

For interface IP address related configuration, refer to the following tasks which are optional configuration and you can perform them based on the practical requirement.

- Assigning Multiple IP Addresses to Network Interfaces

5.1.2.1.1 Assigning Multiple IP Addresses to Network Interfaces

DES-7200 supports multiple IP addresses per interface. One 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. The secondary IP addresses may be located in the same subnet to the primary address or separated from different subnets. 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 particular network segment. Normally a LAN can be assigned a Class C network, which allows up to 254 hosts. However, when there are more than 254 hosts in the LAN, another class C network address is necessary since one class C network is not enough. Therefore, the equipment 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 aid in the transition to a router-based network of IP layer. For each subnet, each router is assigned an IP address.One IP address is configured in the equipment for each subnet.
- Two subnets of a single network might otherwise be separated by another network. You can create a single network from subnets that are physically separated by another network. By configuring secondary IP addresses, the separated subnets can be re-connected. Note that a subnet cannot appear on more than one active interface of the router at a time.One subnet cannot appear on two or more interfaces in the equipment.

Note

Before configuring secondary IP addresses, you need to confirm that the primary IP address has been configured. If any router on a network segment uses a secondary address, all other routers on that same segment must also use a secondary address from the same network or subnet.If the secondary IP address is configured for a device in the network, the secondary IP address for the same network must be configured for other devices. If other devices have not been configured an IP address yet, you can configure the primary IP address for them.

To assign secondary IP addresses to a network interface, use the following command in interface configuration mode:

Command	Function
DES-7200(config-if)# **ip address** *ip-address mask* **secondary**	Set secondary IP addresses to a network interface.
DES-7200(config-if)# **no ip address** *ip-address* *mask* **secondary**	Disable secondary IP addresses on a network interface.

5.1.2.2 Configuring Address Resolution Protocol (ARP)

For each IP device in a LAN, it uses two kinds of 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 handled in the MAC sub-layer of data link layer, it is normally called MAC address, which represents IP network device of Ethernet. 2) Network address identifies the IP network node on the Internet, and locates the network ID which this node belongs to at the same time.

To implement the inter-communication with other IP devices on the Ethernet, each device has to acquire the 48-bits MAC address of the destination host. ARP is used to locate the Ethernet address associated with a desired IP address. Reversed ARP is used to locate the IP address associated with a desired MAC address. There are two ways of address resolution: Address Resolution Protocol (ARP) and 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 glue together the IP and MAC Address. By an input of an IP address, ARP is used to locate the associated MAC address. One the associated MAC address is found, the corresponding relationship will be stored in ARP cache.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 Ethernet. 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. By an input of an MAC address, RARP is used to locate the associated IP address. RARP is configured on non-disks workstation in general.

Normally, you do not need to configure address resolution protocols on the equipment. Except the case in particular, you do not need to configure address resolution protocols manually. DES-7200 can manage address resolution procedure by performing the following tasks.

- Configuring ARP Statically
- Setting ARP Encapsulations

- Setting ARP Timeout

5.1.2.2.1 Configuring ARP Statically

ARP provides the feature of dynamic mapping from IP address to MAC address. It is not necessary to configure ARP statically in most cases. By Configuring ARP Statically, DES-7200 can respond to the ARP request which is not belonged to its own IP address. DES-7200, with static ARP configured, can respond to the ARP request from other IP addresses.

To configure static ARP, use the following command at global configuration mode:

Command	Function
DES-7200(config)# **arp** *ip-address mac-address arp-type*	Define static ARP
DES-7200(config)# **arp** *ip-address mac-address arp-type* **alias**	Respond the ARP requirement of the IP address
DES-7200(config)# **no arp** *ip-address*	Disable static ARP

5.1.2.2.1 Setting ARP Encapsulations

So far DES-7200 only supports ARP Ethernet II type for ARP encapsulations. It is also expressed as the ARPA keyword in DES-7200.

5.1.2.2.1 Setting ARP Timeout

ARP timeout setting only affects the translation from IP address to MAC address which is learned dynamically. The shorter the ARP timeout is set, the more fresh the mapping entry stored in ARP cache is. For this reason, ARP will occupy much more bandwidth. You do not need to set ARP timeout unless it is needed in particular.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, use the following command at interface configuration mode:

Command	Function
DES-7200(config-if)# **arp timeout** *seconds*	Configure ARP timeout.
DES-7200(config-if)# **no arp timeout**	Restore to default configuration

By default, timeout threshold is 3600 seconds, that is, 1 hour.

5.1.2.3 Disabling IP Routing

IP routing feature 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 lose all the routes of a

router and disable routes forwarding on a router.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
DES-7200(config)# **no ip routing**	Disable IP routing.
DES-7200(config)# **ip routing**	Enable IP routing

5.1.2.4 Configuring Broadcast Packets Handling

A broadcast packet is a data packet destined for all hosts on a particular physical network. DES-7200 supports two kinds of broadcasting: directed broadcasting and flooding. 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. Broadcasts are heavily used by some protocols, including several important Internet protocols. Control of broadcast messages is an essential responsibility of the IP network administrator.Therefore, control and use of broadcast packet is the basic responsibility of a network administrator.

If devices in IP network forward flooding broadcasts, it maybe cause a serious network overload known as a broadcast storm. The equipment provides some protection from broadcast storms by limiting their extent to the local cable. Bridges and switches, because they are Layer 2 devices, forward and propagate 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.

To handle broadcast packets, perform the following tasks according to the network requirement.

- Enabling Directed Broadcast-to-Physical Broadcast Translation
- Establishing an IP Broadcast Address

5.1.2.4.1 Enabling Directed Broadcast-to-Physical Broadcast Translation

An IP directed broadcast packet is an IP packet of which the destination address is an IP subnet broadcast address. For instance, the packet with destination 172.16.16.255 is a directed broadcast packet. But the node which generates the directed broadcast packet is not the member of the destination subnet.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 handle the packet like forwarding unicast packet. After the directed broadcast packet arrives routers directly connected to the subnet, routers translated the directed broadcast packet into the flooding broadcast packet (It refers to the broadcast packet with destination address consisting of all 1s in general.), and send to all hosts within the subnet by means of link layer broadcasting.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 forwarding of IP directed broadcasts on an interface where the broadcast becomes a physical broadcast so that directed broadcasts can be forwarded to the directly-connected network. This command will only affect the directed broadcasts transmission which arrived at the final destination subnet, instead of other directed broadcasts.

You can specify an access list to control which directed broadcasts are forwarded on an interface. When an access list is specified, only those IP 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
DES-7200(config-if)# **ip directed-broadcast** [*access-list-number*]	Enable directed broadcast to physical broadcast translation on an interface.
DES-7200(config-if)# **no ip directed-broadcast**	Disable the translation

5.1.2.4.2 Establishing an IP Broadcast Address

Currently, the most popular way is an address consisting of all 1s (255.255.255.255). DES-7200 can be configured to generate any form of IP broadcast address and receive any form of IP broadcast packets.

To set a different IP broadcast address other than 255.255.255.255, use the following command in interface configuration mode:

Command	Function
DES-7200(config-if)# **ip broadcast-address** *ip-address*	Create a new broadcast address
DES-7200(config-if)# **no ip broadcast-address**	Disable a new broadcast address

5.1.3 Monitoring and Maintaining IP Addressing

To monitor and maintain your network, perform the tasks described in the following sections.

- Clearing Caches and Tables

- Displaying System and Network Status

5.1.3.1 Clearing Caches and Tables

You can remove all contents of a particular cache, table, or database, including: 1) Clearing ARP cache; 2) Clearing the mapping table from hostname to IP address; 3) Clearing the routing tables.

Command	Function
DES-7200# **clear arp-cache**	Clear the ARP cache.
DES-7200# **clear ip route** {*network* [*mask*] | *}	Clearing IP Routing Table

5.1.3.2 Displaying System and Network Status

You can show the contents of the IP routing table, buffer, and database. Such information is very helpful in troubleshooting the network. You also can display information about reachability of local equipment network and discover the routing path that the packets of your device are taking through the network.

Use the following commands in privileged mode to display system and network statistics:

Command	Function
DES-7200# **show arp**	Display the ARP table.
DES-7200# **show ip arp**	Display the IP ARP cache.
DES-7200# **show ip interface** [*interface-type interface-number*]	Show the interface information.
DES-7200# **show ip route** [*network* [*mask*]]	Display the routing table
DES-7200#**show ip route**	Display the current state of the routing table in summary form.
DES-7200# **ping** *ip-address* [**length** *bytes*] [**ntimes** *times*] [**timeout** *seconds*]	Test network node reachability.

5.1.4 IP Addressing Configuration Examples

This chapter provides some IP address configuration examples as follows:

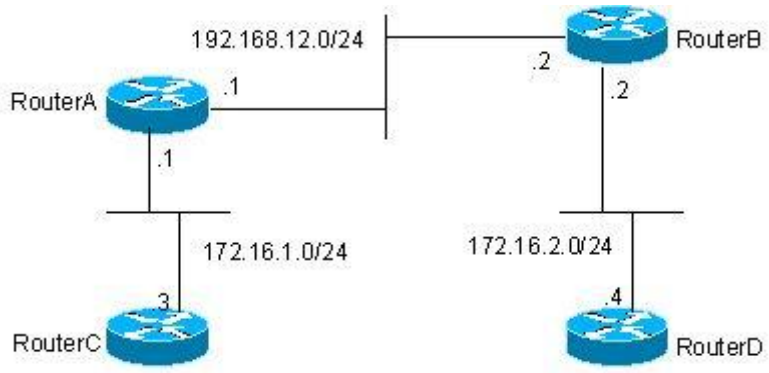
- Secondary IP Addressing Configuration Example

5.1.4.1 Secondary IP Addressing Configuration Example

- **Configuration requirements:**

The IP addresses allocation and network connections as shown in the following Figure 5-1 .

Figure 5-1 Secondary IP address configuration example



It is required to display routes of 172.16.2.0/24 on router C and display routes of 172.16.1.0/24 on router D by configuring RIP routing protocol to RIPv1.

- **Configuration of the Routers:**

RIPv1 does not support Class-based routes, which means masks are not carried in routing advertisement. Subnets of 172.16.1.0/24 and 172.16.2.0/24 are separated by Class C 192.168.12.0/2. Therefore router C and router D can not learn the detailed network information from each other. 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
```

5.2 IP Service Configuration

5.2.1 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.

5.2.2 Managing IP Connections

The IP protocols stack offers a number of services that control and manage IP connections. Internet Control Message Protocol (ICMP) provides many of these services.When there is any problem with the network, the device or access server sends an ICMP message to the host or other devices. 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

5.2.2.1 Enabling ICMP Protocol Unreachable Messages

When the device receives a non-broadcast packet destined to it, and this packet uses the IP that the device cannot handle, the device 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 enable this service if it has been disabled, use the following command in interface configuration mode:

Command	Function
DES-7200(config-if)# **ip unreachables**	Enable the sending of ICMP protocol unreachable and host unreachable messages.
DES-7200(config-if)# **no ip unreachables**	Disable the sending of ICMP protocol unreachable and host unreachable messages.

5.2.2.2 Enabling ICMP Redirect Messages

Routes are sometimes less than optimal. For example, it is possible for the device to be forced to resend a packet through the same interface on which it was received. If the device resends a packet through the same interface on which it was received, it sends an ICMP redirect message to the originator of the packet telling the originator that the gateway to this destination address is another device in the same subnet. Therefore the originator will transmit the packets based on the optimized path afterwards. This feature is enabled by default.

To enable the sending of ICMP redirect messages if this feature was disabled, use the following command in interface configuration mode:

Command	Function
DES-7200(config-if)# **ip redirects**	Enable the sending of ICMP redirect messages. It is enabled by default.
DES-7200(config-if)# **no ip redirects**	Disable the sending of ICMP redirect messages.

5.2.2.3 Enabling ICMP Mask Reply Messages

Occasionally, network devices must 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. DES-7200 can respond to ICMP mask request messages. This function is enabled by default.

To enable the sending of ICMP mask reply messages, use the following command in interface configuration mode:

Command	Function
DES-7200(config-if)# **ip mask-reply**	Enable the sending of ICMP mask reply messages.
DES-7200(config-if)# **no ip mask-reply**	Disable the sending of ICMP mask reply messages.

5.2.2.4 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.

DES-7200 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, the reverse is not true; changing the IP MTU value has no effect on the value of MTU.

Also, all device interfaces on a physical network must have the MTU value for the same protocol.

To set the MTU packet size for a specified interface, use the following command in interface configuration mode:

Command	Function
DES-7200(config-if)# **ip mtu**	Set the IP MTU packet size for an interface.
DES-7200(config-if)# **no ip mtu**	Restore the default setting

5.2.2.5 Configuring IP Source Routing

DES-7200 supports IP source routing. The device examines IP header options on every packet. It supports the IP header options Strict Source Route, Loose Source Route and Record Route, which are defined in RFC 791. If the software finds a packet with one of these options enabled, it performs the appropriate action. If it finds a packet with an invalid option, it sends an ICMP parameter problem message to the source of the packet and discards the packet. DES-7200 supports IP source routing by default.

To enable IP source routing, use the following command in interface configuration mode:

Command	Function
DES-7200(config)# **ip source-route**	Enable IP source routing
DES-7200(config)# **no ip source-route**	Disable IP surce routing

Caution

On DES-7200, you have to use the **trap ip option packet** command to inform the hardware to send the option packet to software due to the restriction of the hardware CMOS chip.

6 Configuring MAC Address

6.1 Managing the MAC Address List

6.1.1 Overview

The MAC address table contains address information that the switch uses to forward traffic between ports. The MAC address table includes these types of addresses: Dynamic address, Static address, Filtering address. We will describe the MAC Address Table in the following sections:

6.1.1.1 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 has been learned by the device, the packet will be sent only to the port associated with the MAC. Otherwise, the packet will be sent to all other ports.

The device updates the address table by adding new dynamic addresses and aging out those that are not in use. For an address in the address table, if the device does not receive any packet 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 current situation. If the aging time is too short, the address in the address table will be aged too early and the address will be an unknown address again for the switch. When the device receives the packet with the destination MAC address, the packet will be broadcast to other ports in the VLAN, introducing needless packets. If the aging time is too long, the address will be aged slowly and the address table will be full rapidly. When the table is full, no new address can be leant, and all other addresses will be unknown addresses before there is room in the table. When the device receives the packet with the destination address, the packet will be broadcast to other ports in the VLAN too and this also introduce some needless packets.

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

6.1.1.2 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 will only be added and deleted manually (instead of learning and aging). Static address will be stored in the configuration file, and will not be lost even if the device reloads.

6.1.1.3 Filtering Address

A filtering address is a MAC address manually added. When the switch receives the packets whose source addresses are the filtering addresses it will directly discard them. Filtering addresses can only be added and deleted manually (instead of aging). 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 filter some invalid users, you can specify their MAC address as filtering addresses, so that these invalid users can not communicate with the outside world through the device.

6.1.1.4 Association between MAC Address and VLAN

All addresses are associated with VLANs. One MAC address can exist in more than one VLANs, and can be associated with more than one port. Each VLAN maintains its own logical address table. A learnt MAC address in one VLAN may be unknown in another VLAN, so it needs learning.

6.1.2 Configuring MAC Address

6.1.2.1 Default Configuration of MAC Address Table

The table shows the default MAC address table configuration:

Item	Default Configuration
Aging time	300 seconds
Dynamic addresses	Automatically learned
Static addresses	No configured
Filtering addresses	No configured

6.1.2.2 Setting the Address Aging Time

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

Command	Function
DES-7200(config)# **mac-address-table aging-time** [*0* |*10-1000000*]	Set the time for how long an address will be stored in the dynamic address table after it is learnt, in seconds within the 101000000 range. The default is 300s. When you set this value 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.

6.1.2.3 Removing Dynamic Address Entries

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

To verify dynamic addresses that have been removed, use the **show mac-address-table dynamic** privileged EXEC command.

6.1.2.4 Adding and Removing Static Address Entries

You add a static address to the address table by specifying the destination MAC address, 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
DES-7200(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. For *interface-id*, specify the interface (physical port or aggregate port) to which the received packet is forwarded. Packets with this destination address received in the specified VLAN are forwarded to the specified interface.

To remove static entries from the address table, 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, the packet is forwarded to the specified port gigabitethernet 1/3.

```
DES-7200(config)# mac-address-table static 00d0.f800.073c vlan 4 interface
gigabitethernet 1/3
```

6.1.2.5 Adding and Removing Filtering Address Entries

You add a filtering address to the address table by specifying the destination MAC address and the VLAN from which it is received. Packets received with this destination address in this VLAN are discarded directly by the device.

Add a filtered address:

Command	Function
DES-7200(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 entries from the address table, 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:

```
DES-7200(config)# mac-address-table filtering 00d0.f800.073c vlan 1
```

6.1.3 Viewing MAC Addresses Table Entries

View information about the MAC address table in the device:

Command	Function
DES-7200# **show mac-address-table**	Show all types of MAC addresses (including dynamic address, static address and filtering address)
DES-7200# **show mac-address-table aging-time**	Show the current aging time
DES-7200# **show mac-address-table Dynamic**	Show only dynamic MAC addresses
DES-7200# **show mac-address-table static**	Show only static MAC addresses
DES-7200# **show mac-address-table filtering**	Show only filtering MAC addresses
DES-7200# **show mac-address-table interface**	Show all types of MAC addresses for the specified interface
DES-7200# **show mac-address-table vlan**	Show all types of MAC addresses for the specified VLAN
DES-7200# **show mac-address-table count**	Show the number of MAC addresses present in MAC address table:

The following examples show MAC addresses:

```
Show the MAC address table:
DES-7200# 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 number of MAC addresses present in MAC address table:

```
DES-7200# 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 effective address space of the MAC address table in the 5700 series device is 16384.

Show the current aging time:

```
DES-7200# show mac-address-table aging-time
Aging time    : 300
```

6.2 Configuring MAC Address Notification

6.2.1 Overview

If you want to know 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, there may be times when lots of MAC address changes occur (such as when the device is powered on), resulting in increase of network traffic. In order to decrease the network load, you can set the time interval of sending MAC address notifications. All the notification messages in the interval time will be bundled in one trap, so one notification trap includes many MAC address changing information so as to reduce network traffic.

At the same time when the switch generates MAC address notification traps, they will be recorded in the MAC address notification history list. If you do not specify the NMS for receiving the traps or you do not receive the traps in time, you can view the address changing information by displaying the MAC address notification history list.

MAC address notification traps are associated with the interface, and there is a global switch for these traps. When the global switch is turned off, the switch will not send any MAC address notification traps on any interface.This interface will only generate a MAC address change notification if 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.

6.2.2 Configuring MAC Address Notification Traps

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
DES-7200(config)# **snmp-server host** *host-addr* **traps** { **version** {*1*|*2c*}} *community-string*	Specify the recipient NMS of the trap message. *host-add*: Specifies the address of the recipient. **version -** Specify the version of the Trap to send. Specify the authentication alias event record type attached on the Trap
DES-7200(config)#**snmp-server enable traps**	Allows the switch to send Trap.
DES-7200(config)# **mac-address-table notification**	Turn on the MAC address notification global switch.
DES-7200(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.
DES-7200(config-if)# snmp trap mac-notification {added | removed}	Enable the MAC address notification trap on the specified interface. **added**: Enable the MAC notification trap 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** 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 traps on a specified interface, use the **no snmp trap mac-notification** {**added** | **removed**} command in the interface configuration mode.

This example shows how to specify 192.168.12.54 as the NMS IP address with the community string to be **public**, and enable the switch to send MAC address notification traps to the NMS, and set the interval time to 40 seconds with the history-size to be 100, and enable notification trap whenever a MAC address is added or deleted on the specified port gigabitethernet 1/3.

```
DES-7200(config)# snmp-server host 192.168.12.54 traps public
```

```
DES-7200(config)# snmp-server enable traps
DES-7200(config)# mac-address-table notification
DES-7200(config)# mac-address-table notification interval 40
DES-7200(config)# mac-address-table notification  history-size 100
DES-7200(config)# interface gigabitethernet 1/3
DES-7200(config-if)# snmp trap mac-notification added
DES-7200(config-if)# snmp trap mac-notification removed
```

6.2.3 Viewing MAC Address change Notification information

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
DES-7200# **show mac-address-table notification**	Show the global configuration of MAC address change notification function
DES-7200# **show mac-address-table notification interface**	Show the enable status of MAC address change notification on the interface
DES-7200# **show mac-address-table notification history**	Show MAC address change notification traps History List

The following examples show how to view the MAC address change notices.

View the global configuration for MAC address notification:

```
DES-7200# show mac-address-table notification
MAC Notification Feature : Enabled
Interval(Sec): 2
Maximum History Size : 154
Current History Size : 2
DES-7200# 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
DES-7200# 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
```

6.3 IP and MAC Address Binding

6.3.1 Overview

Address binding allows you to bind an IP address to a MAC address. If you have bound an IP address with a specified MAC address, when the device receives packets with the same IP address and a different source MAC address bound for the IP address, it will discard these packets.

You can impose a strict policy to authenticate users on the device with address binding. Notice that the control of device input through address binding has priority over 802.1X, port-based security and ACL.

6.3.2 Configuring IP and MAC Address Bind

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

Command	Function
DES-7200(config)# **address-bind** *ip-address mac-address*	Configure the IP and MAC address binding

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

6.3.3 Viewing the IP and MAC Address Binding Table

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

```
DES-7200# show address-bind
IP Address     Binding MAC Addr
----------    ----------------------
3.3.3.3        00d0.f811.1112
3.3.3.4        00d0.f811.1117
```

7 Configuring Interfaces

7.1 Overview of Interface Types

This chapter provides the classification of interfaces used in DES-7200 as well as a precise definition of each type.Interfaces on DES-7200 are classified into two types:

- L2 Interfaces
- L3 Interfaces (available in layer 2 devices)

7.1.1 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

7.1.1.1 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.

7.1.1.1.1 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.

7.1.1.1.2 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.

7.1.1.1.3 Hybrid port

The Hybrid port can belong to multiple VLANs, and 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.

7.1.1.2 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.

7.1.2 L3 Interfaces

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

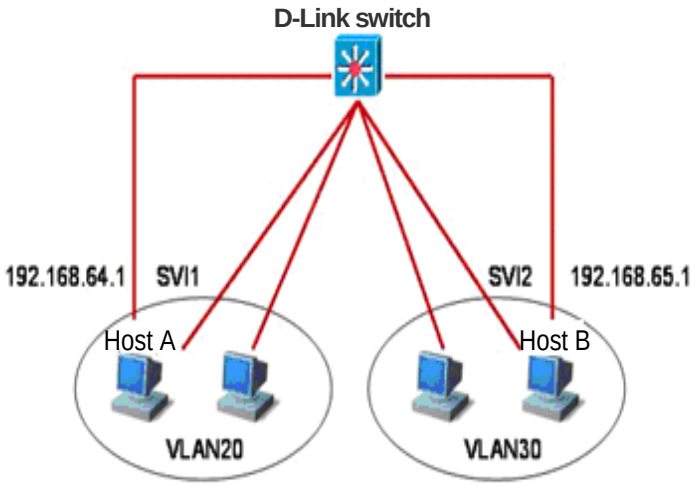
- SVI (Switch virtual interface)
- Routed Port
- L3 Aggregate Ports

7.1.2.1 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.

Figure 7-1



7.1.2.2 Routed Port

A Routed Port is a physical port, for example, 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 routing purposes.Note that using the **no switchport** interface configuration command will close and restart this port and delete all the layer 2 features from this port.

Caution

However, when a port is a member port of an L2 Aggregate Port, the **switchport/ no switchport** commands will not work.

7.1.2.3 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, considers 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, making the connection more reliable.

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

7.2 Configuring Interfaces

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

7.2.1 Numbering Rules for Interfaces

The number of a switch port consists of a slot number and port number 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 top downwards, 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 or electrical 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.

7.2.2 Using Interface Configuration Commands

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

Command	Function
DES-7200(config)# **interface** *interface ID*	Input **interface** to enter interface configuration mode. You may also set the 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:

```
DES-7200(config)# interface gigabitethernet 2/1
DES-7200(config-if)#
```

You may set interface attributes in interface configuration mode.

7.2.3 Using the interface range Command

7.2.3.1 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 interface parameters you enter apply to all interfaces within the range.

Command	Function
DES-7200(config)# **interface range** {*port-range* | **macro** *macro_name*}	Enter an interface range. You may use the **interface range** command to specify ranges. 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 ranges with a comma. Be sure that all interface ranges in a command contain the same type of interfaces.

When using the **interface range** command, note

Effective range format is:

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

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

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

```
DES-7200# configure terminal
DES-7200(config)# interface range fastethernet 1/1 - 10
DES-7200(config-if-range)# no shutdown
DES-7200(config-if-range)#
```

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

```
DES-7200# configure terminal
DES-7200(config)# interface range fastethernet 1/1-5, 1/7-8
DES-7200(config-if-range)# no shutdown
DES-7200(config-if-range)#
```

7.2.3.2 Configuring and Using Macro Definition for Interface Range

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

Command	Function
DES-7200(config)# **define interface-range** *macro_name interface-range*	Define the macro for interface range. Name of the interface-range macro, up to 32 characters. Macro definition may cover more than one range. All ranges in the same macro definition can contain but one type of interfaces.
DES-7200(config)# **interface range macro** *macro_name*	The macro will be saved in the memory. When you use the **interface range** command, you can use the defined macro-name to replace the interface-range string.

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, note

Effective range format is:

– **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.

This example defines the macro for fastethernet1/1-4 by using the **define interface-range** command:

```
DES-7200# configure terminal
DES-7200(config)# define interface-range resource
fastethernet 1/1-4
DES-7200(config)# end
```

This example defines a macro for multiple ranges:

```
DES-7200# configure terminal
DES-7200(config)# define interface-range ports1to2N5to7
fastethernet 1/1-2, 1/5-7
DES-7200(config)# end
```

This example uses macro ports1to2N5to7 to set a specified range of interfaces:

```
DES-7200# configure terminal
DES-7200(config)# interface range macro ports1to2N5to7
DES-7200(config-if-range)#
```

This example deletes macro ports1to2N5to7:

```
DES-7200# configure terminal
DES-7200(config)# no define interface-range ports1to2N5to7
DES-7200# end
```

7.2.4 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 medium, the attributes like connection status, speed, duplex, and flow control will be determined by the medium. When you change the medium, the attributes will take their default values. Change the default values 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 to be Aggregate Port must have the same media type. Otherwise, they cannot be added to the AP. The port type of Aggregate Port cannot be changed.

Command	Function
DES-7200(config-if)# **medium-type** { **fiber** | **copper** }	Set the medium type for a port.

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

```
DES-7200# config terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# medium-type fiber
DES-7200(config-if)# end
```

7.2.5 Setting Interface Description and Management Status

You may give an interface a particular name (description) to help you remember its functions. You may name the interface what you want to do with it, for example, if you want to reserve Gigabitethernet 1/1 for the exclusive use of user A, you may set its description to “Port for User A”.

Command	Function
DES-7200(config-if)# **description** *string*	Describe the interface in no more than 32 characters

This example sets the description of Gigabitethernet 1/1:

```
DES-7200# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# description PortForUser A
DES-7200(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, an interface will send and receive no more frames and cease to perform all its functions. You can also restart an interface shut down by setting its management status. The management status of an interface can be **up** or **down**. When a port is shut down, it enters into the status **down**; otherwise, it is in the status **up**.

Command	Function
DES-7200(config-if)# **shutdown**	Shut down an interface.

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

```
DES-7200# configure terminal
DES-7200(config)# interface gigabitethernet 1/2
```

```
DES-7200(config-if)# shutdown
DES-7200(config-if)# end
```

7.2.6 Setting Speed, Duplexing, and Flow Control for Interfaces

The section deals with the setting of speed, duplexing, and flow control for interfaces.

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

Command	Function
DES-7200(config-if)# **speed** {**10** | **100** | **1000** | **auto** }	Select a speed or set it to **auto**. Note: 1000 applies only to gigabit interfaces.
DES-7200(config-if)# **duplex** {**auto** | **full** | **half** }	Set duplex mode
DES-7200(config-if)# **flowcontrol** {**auto** | **on** | **off** }	Set flow control mode. Note: When **speed**, **duplex**, and **flowcontrol** are all set to non-auto, the interface will stop auto-negotiation.

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

```
DES-7200# configure terminal
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# speed 1000
DES-7200(config-if)# duplex full
DES-7200(config-if)# flowcontrol off
DES-7200(config-if)# end
```

7.2.7 Configuring Interface MTU

When a heavy throughout of data interchange 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 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 aphysical port. The SVI interface currently does not support the MTU setting.

Command	Function
DES-7200(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:

```
DES-7200# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# mtu 64
DES-7200(config-if)# end
```

7.2.8 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 Traffic 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 1~4093
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
Aggregate port	None
Storm Control	Off
Port protection	Off
Port Security	Off

7.2.8.1 Configuring Switch Ports

7.2.8.1.1 Configuring Access/Trunk Port

This section is devoted to the setting of working modes (access/trunk port) of Switchport and setting in each mode.

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

Command	Function
DES-7200(config-if)# **switchport mode** {**access** | **trunk** }	Set the operation mode of the port.

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

```
DES-7200# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)# interface gigabitethernet 1/2
DES-7200(config-if)# switchport mode access
DES-7200(config-if)# end
```

Command	Function
DES-7200(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

```
DES-7200# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)# interface gigabitethernet 2/1
DES-7200(config-if)# switchport access vlan 100
DES-7200(config-if)# end
```

Set the native VLAN of the trunk port.

Command	Function
DES-7200(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.

```
DES-7200# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)# interface gigabitethernet 2/1
DES-7200(config-if)# switchport trunk native vlan 10
DES-7200(config-if)# end
```

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

Command	Function
DES-7200(config-if)# **switchport port-security**	Set the port-security.

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

```
DES-7200# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)# interface gigabitethernet 2/1
DES-7200(config-if)# switchport port-security
DES-7200(config-if)# end
```

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

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

```
DES-7200# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)# interface gigabitethernet 2/1
DES-7200(config-if)# switchport access vlan 100
DES-7200(config-if)# speed auto
DES-7200(config-if)# duplex auto
DES-7200(config-if)# flowcontrol auto
DES-7200(config-if)# switchport port-security
DES-7200(config-if)# end
```

7.2.8.1.2 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
switchport hybrid allowed vlan [[**add**] [**tagged	untaged**]] **|remove**] *vlist*	Set the output rule for the port

```
DES-7200# configure terminal
DES-7200(config)# interface g 0/1
DES-7200(config-if)# switchport mode hybrid
DES-7200(config-if)# switchport hybrid native vlan 3
DES-7200(config-if)# switchport hybrid allowed vlan untagged 20-30
```

```
DES-7200(config-if)# end
DES-7200# show running interface g 0/1
```

7.2.8.2 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.

7.2.8.3 Clearing Interface Statistics and Then Resetting It

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
DES-7200# **clear counters** [*interface-id*]	Clear interface statistics.
DES-7200# **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.

```
DES-7200# clear counters gigabitethernet 1/1
```

7.2.9 Configuring L3 Interfaces

Configuring L3 Interfaces:

Command	Function
DES-7200(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.
DES-7200(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.

```
DES-7200# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)# interface gigabitethernet 2/1
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 192.20.135.21 255.255.255.0
DES-7200(config-if)# no shutdown
DES-7200(config-if)# end
```

7.2.9.1 Configuring SVI

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

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

Configuring SVI:

Command	Function
DES-7200(config)# **interface vlan** *vlan-id*	Enter SVI interface configuration mode.

Then, you can configure the properties related to SVI. For detailed information, please refer to *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.

```
DES-7200# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)# interface vlan 100
DES-7200(config-if)# ip address 192.168.1.1 255.255.255.0
DES-7200(config-if)# end
```

7.2.9.2 Configuring Routed Ports

This section deals with how to create and configure a 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
DES-7200(config-if)# **no switchport**	Shut down the interface and then change it to L3 mode.
DES-7200(config-if)# **ip address** *ip_address subnet_mask*	Configure the IP address and subnet mask.

Caution

No layer switching can be performed 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 and IP address to it.

```
DES-7200# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)# interface fastethernet 1/6
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 192.168.1.1 255.255.255.0
DES-7200(config-if)# no shutdown
DES-7200(config-if)# end
```

7.2.9.3 Configuring L3 Aggregate Ports

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

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

Command	Function
DES-7200(config-if)# **no switchport**	Shut down the interface and change it to L3 mode.
DES-7200(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.

```
DES-7200# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)# interface aggregateport 2
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 192.168.1.1 255.255.255.0
DES-7200(config-if)# no shutdown
DES-7200(config-if)# end
```

7.3 Showing Interface Configuration and Status

This section covers interface status display and gives examples. You may view interface status by using **show** in privileged EXEC mode. To show interface status, use the following commands.

Command	Function
DES-7200# **show interfaces** [*interface-id*]	Show all the statuses of a specified interface and its configuration information.
DES-7200# **show interfaces** *interface-id* **status**	Show the status of an interface.
DES-7200# **show interfaces** [*interface-id*] **switchport**	Show the administrative and operational status information of an switch interface (non-routing interface).
DES-7200# **show interfaces** [*interface-id*] **description**	Show the description and status of a specified interface.
DES-7200# **show interfaces** [*interface-id*] **counters**	Show the statistics of a specified port.

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

```
DES-7200# 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.

```
DES-7200# 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.

```
DES-7200# 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:

```
DES-7200# 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:

```
DES-7200# show interfaces gigabitethernet 1/2 description
Interface               Status    Administrative    Description
--------------------  ---------   ---------------    ----------------
gigabitethernet 2/1     down        down            Gi 2/1
```

This example shows statistics of the interfaces.

```
DES-7200# 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
```

8 Configuring Aggregate Port

This chapter explains how to configure an aggregate port on DES-7200.

8.1 Overview

8.1.1 Understanding Aggregate Port

Multiple physical connections can be bound into a logical connection, which is called an aggregate port (referred to as AP below). DES-7200 provide the AP function that complies with the IEEE802.3ad standard. This function can be used to expand the link bandwidth to provide higher connection reliability.

When a member link in the AP is disconnected, the system will automatically allocate the traffic of the member 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 8-1 Typical AP configurations

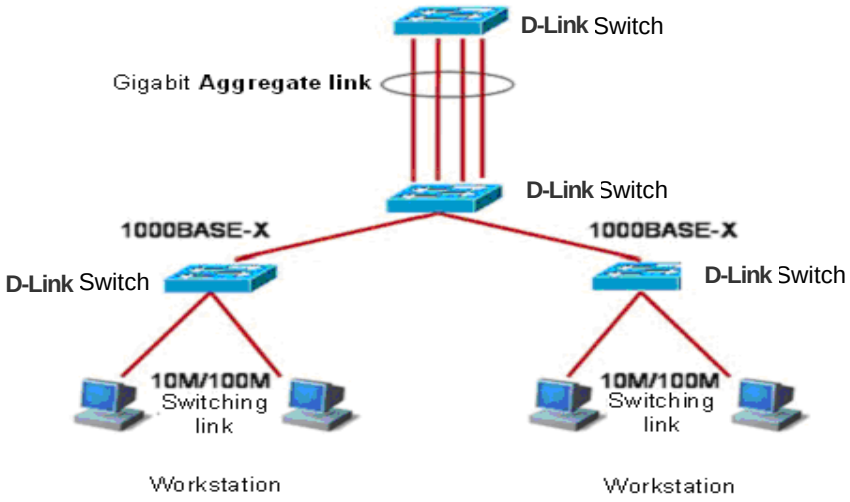


Figure 8-2

Note

The DES-7200 series device supports up to 128 APs, each of which includes up to eight ports.

8.1.2 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 based traffic balancing means that the messages are distributed onto the links 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 the process to distribute the packets to every member link of the AP according to the destination MAC addresses of the packets. Packets with the same 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 method is used for the L3 packets. If L2 packets are received when this method is used, the traffic is balanced automatically according to the source or destination MAC address of the L2 packets.

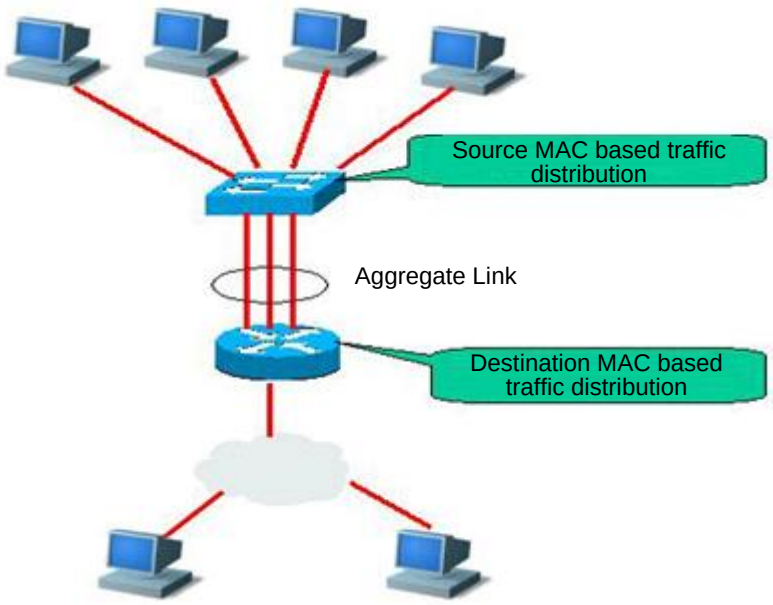
The traffic balancing based on source + destination IP addresses is the process to distribute the packets according to their source + destination IP addresses. This traffic balancing method is used for the L3 packets. If L2 packets are received when this method is used, the traffic is balanced according 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 style should be set according to the actual network environments, so that the traffic can be evenly distributed to the links for maximum utilization 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 inside the network (such as four PCs on the top of the diagram). The source MAC addresses of all the packets that the devices outside the network (such as two PCs at the bottom of the diagram) send through the router are the

MAC address of the gateway. In order to distribute the traffic between the router and other hosts to other links, the traffic balancing should be based on the destination MAC address. However, the traffic balancing should be based on the source MAC address in the switch.

Figure 8-3 AP traffic balancing



8.2 Configuring Aggregate Port

8.2.1 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-2 AP interface	None
Traffic balancing	Traffic is distributed according to the source MAC addresses of the incoming packets. The default value of traffic balancing for the 5700 series switch is traffic balancing based on the source MAC address + destination MAC address of the incoming packet.

Caution

The default traffic balancing method of the DES-7200 switches is: based on source MAC + destination MAC of the incoming packets.

8.2.2 Configuration Guide for Aggregate Port

The ports added to the AP must work in the full duplex mode.

The rates of the AP member ports must be the same.

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 feature.

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.

8.2.3 Configuring Aggregate Port

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

Command	Function
DES-7200(config-if-range)# **port-group** *port-group-number*	Add the interface into an AP (create the AP as well if it does 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 into the members of layer-2 AP 5.

```
DES-7200# configure terminal
DES-7200(config)# interface range gigabitEthernet 0/1
DES-7200(config-if-range)# port-group 5
DES-7200(config-if-range)# end
```

The command DES-7200(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).

8.2.4 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):

```
DES-7200# configure terminal
DES-7200(config)# interface aggretegateport 3
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 192.168.1.1 255.255.255.0
DES-7200(config-if)# end
```

8.2.5 Configuring Traffic Balancing of Aggregate Port

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

Command	Function
DES-7200(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 incoming 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 incoming 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. 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

8.3 Showing Aggregate Port

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

Command	Function
DES-7200# **show aggregateport** [*port-number*]{**load-balance | summary**}	Show the AP settings.

```
DES-7200# show aggregateport load-balance
Load-balance : Source MAC address
DES-7200# show aggregateport 1 summary
AggregatePort MaxPorts SwitchPort Mode   Ports
------------- -------- ---------- ------
Ag1             8        Enabled    ACCESS
```

9 Port-based Flow Control

9.1 Storm Control

9.1.1 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 streams 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 stream becomes normal again. This prevents excessive flood packets from entering the LAN to for a storm.

9.1.2 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 a port by percentage, this percentage applies to all the ports and any other settings will not take effect.

In the interface configuration mode, use the following command to configure storm control:

Command	Function
DES-7200(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 using the no storm-control broadcast, no storm-control multicast, or no storm-control unicast command.

The following example enables the multicast storm control on GigabitEthernet 0/1 and set the allowed rate to 4M.

```
DES-7200# configure terminal
DES-7200(config)# interface GigabitEthernet 0/1
DES-7200(config-if)# storm-control multicast 4096
DES-7200(config-if)# end
```

9.1.3 Viewing the Enable Status of Storm Control

To view the storm control status of the interface, use the following command:

Command	Function
DES-7200# **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:

```
DES-7200# 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:

```
DES-7200# 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
```

9.2 Protected Port

9.2.1 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 conducted through the L3 device. 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.

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 by doing so).

The device supports the Aggregated Port to be set 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.

9.2.2 Configuring the Protected Port

Set one port as the protection port:

Command	Function
DES-7200(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.

```
DES-7200# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)# interface gigabitethernet 0/3
DES-7200(config-if)# switchport protected
DES-7200(config-if)# end
```

9.2.3 Showing Protected Port Configuration

Command	Function
DES-7200(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.

```
DES-7200# show interfaces gigabitethernet 0/3 switchport
Interface   Switchport  Mode   Access Native Protected   VLAN lists
---------   ----------  ----   ------ -----  --------   ----
GigabitEthernet 0/3  enabled   Trunk  1   1    Enabled    ALL
```

9.3 Port Security

9.3.1 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 secure 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 secure addresses on a port. If you set the maximum value to 1 and configure one secure 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 secure address. Of course you can also designate the MAC address without binding the IP address.

You can add the secure addresses on the port in the following ways:

You can manually configure all the secure 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 secure address on this port till the total number reaches the maximum value. Note that, however, the automatically-learned secure addresses will not be bound with the IP address. On the same port, if you have configured a secure address bound up with the IP address, the port cannot be added with any secure address by automatic learning.

Manually configure some secure addresses, and let the device to learn the rest.

When a port is configured as a secure port and the maximum number of its secure addresses is reached, a security violation occurs if the port receives a packet whose source address is not one of the secure addresses on the port. When security violations occur, you can set the following methods for handling them:

protect: When the maximum number of secure addresses is reached, the secure port discards the packet of unknown addresses (none of which are among the secure addresses of the port).This is the default method for handling exceptions.

restrict: In the case of violation, a Trap notification is sent

shutdown: In the case of violation, the port is shut down and a Trap notification is sent.

9.3.2 Configuring Port Security

9.3.2.1 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 secure addresses	128
Secure address	None
Handling mode for violations	Protect

Caution

For the devices of this series, up to 1024 secure addresses are supported globally if IP is not bound, and each port supports up to 84 secure addresses if IP is bound.

9.3.2.2 Port Security Configuration Guide

The following restrictions apply 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 secure 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 secure addresses.

The secure 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 secure address not bound with the IP address will fail (the secure address bound with the IP address has a high priority).

9.3.2.3 Configuration of Secure Ports and Violation Handling Modes

In the interface configuration mode, configure secure ports and violation handling modes by using the following commands:

Command	Function
DES-7200(config-if)# **switchport port-security**	Enable the port security function of this interface.
DES-7200(config-if)# **switchport port-security maximum** *value*	Set the maximum number of secure addresses on the interface. The range is between 1 and 1000 and the default value is 128.
DES-7200(config-if)# **switchport port-security violation**{**protect** | **restrict** | **shutdown**}	Set the violation handling mode: **protect**: Protected port. When the number of secure addresses if full, the security port will discard the packets from unknown address (that is, not any among the secure addresses of the port). **restrict**: In the case of violation, a Trap notification is sent **shutdown**: In the case of violation, the port is shut down and a Trap notification is sent. When a port is closed because of violation, you can recover it from the error status by using 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**. Use the command **no switchport port-security maximum** to recover to the default maximum value. Use 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 to be set is 8 and the violation handling mode is set to **protect**.

```
DES-7200# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)# interface gigabitethernet 0/3
DES-7200(config-if)# switchport mode access
DES-7200(config-if)# switchport port-security
DES-7200(config-if)# switchport port-security maximum 8
DES-7200(config-if)# switchport port-security violation protect
DES-7200(config-if)# end
```

Note

If the secure address mac+ip has been configured on the secure port, the exception handling rule for the port will not take effect.

9.3.2.4 Configuration of Secure Addresses on the Secure Port

In the interface configuration mode, add secure addresses for secure ports by using the following commands:

Command	Function
DES-7200(config-if)# **switchport port-security mac-address** *mac-address* [**ip-address** *ip-address*]	Manually configure the secure address on the interface. **ip-address** (optional): IP address bound up with the secure address.

In the interface configuration mode, you can use the command **no switchport port-security mac-address** *mac-address* to delete the secure address of this interface.

The example below describes how to configure a secure address for interface fasttethernet 0/3: 00d0.f800.073c and bind it with an IP address: 192.168.12.202.

```
DES-7200# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)# interface gigabitethernet 0/3
DES-7200(config-if)# switchport mode access
DES-7200(config-if)# switchport port-security
DES-7200(config-if)# switchport port-security mac-address 00d0.f800.073c ip-address
192.168.12.202
DES-7200(config-if)# end
```

9.3.2.5 Configuration of Aging Time for Secure Addresses

You can configure the aging time for all the secure addresses on an interface. To enable this function, you need to set the maximum number of secure addresses. In this way, you can make the device automatically add or delete the secure addresses on the interface.

In the interface configuration mode, configure the aging time for secure addresses by using the following command:

Command	Function
DES-7200(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 secure 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 secure address of the port. The default value of *Time* is 0.

In interface configuration mode, use **no switchport port-security aging time** to disable the port security aging. Use 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 secure addresses:

```
DES-7200# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)# interface gigabitthernet 0/3
DES-7200(config-if)# switchport port-security aging time 8
DES-7200(config-if)# switchport port-security aging static
DES-7200(config-if)# end
```

9.3.3 Viewing Port Security Information

In the privileged mode, you can view the security information of a port by using the following commands.

Command	Function
DES-7200#**show port-security interface** [*interface-id*]	View the port security configuration information of an interface.
DES-7200#**show port-security address**	View the secure address information.
DES-7200# **show port-security address** [*interface-id*]	Show the secure address information on an interface.
DES-7200# **show port-security**	Show the statistics of all the security ports, including the maximum number of secure addresses, the number of current addresses, and violation handling mode.

The example below shows the port security configuration on interface **gigabitethernet 0/3**:

```
DES-7200# 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 secure addresses in the system.

```
DES-7200# 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 secure address on one interface. The instance below shows the secure address on interface gigabitstethernet 0/3.

```
DES-7200# 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.

```
DES-7200# 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
```

10 Configuring VLAN

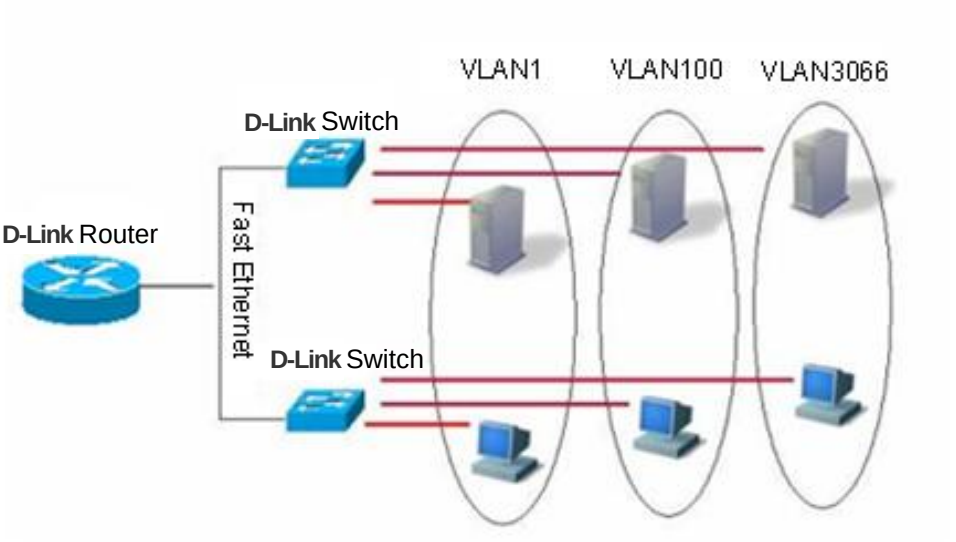
This chapter describes how to configure IEEE802.1q VLAN.

10.1 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 entire network supports multiple VLANs. When you add, delete, and modify a user, you do not need to modify the network configuration physically.

Figure 10-1



Same as a physical network, the VLAN is usually connected to an IP subnet.A typical example: 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. DES-7200 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.

10.1.2 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.

The DES-7200 series devices support 4093 VLANs.

10.1.3 VLAN Member Type

You can determine the frames that can pass a port and the number of VLANs that the port can belong 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 can belong 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).

10.2 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 removed.

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

10.2.1 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.

10.2.2 Default SPAN Configuration

Parameter	Default value	Range
VLAN ID	1	1-4093
VLAN Name	VLAN xxxx, where xxxx is the VLAN ID	No range
VLAN State	Active	Active, Inactive

10.2.3 Creating/Modifying a VLAN

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

Command	Function
DES-7200(config)# **vlan** *vlan-id*	Enter one VLAN ID. If you enter a new VLAN ID, the device will create it for you. If you enter an existing VLAN ID, the device modifies the appropriate VLAN.
DES-7200(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:

```
DES-7200# configure terminal
DES-7200(config)# vlan 888
DES-7200(config-vlan)# name test888
DES-7200(config-vlan)# end
```

10.2.4 Deleting a VLAN

You cannot delete the default VLAN (VLAN 1).

In the privileged mode, you can delete a VLAN.

Command	Function
DES-7200(config)# **no vlan** *vlan-id*	Enter one VLAN ID to delete it.

10.2.5 Assigning Access Ports to the VLAN

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

In the privileged mode, you can assign a port to a VLAN.

Command	Function
DES-7200(config-if)# **switchport mode access**	Define the VLAN member type of the interface (L2 ACCESS port)
DES-7200(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:

```
DES-7200# configure terminal
DES-7200(config)# interface fastethernet 1/10
DES-7200(config-if)# switchport mode access
DES-7200(config-if)# switchport access vlan 20
DES-7200(config-if)# end
```

The following example shows how to verify the configuration:

```
DES-7200(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
```

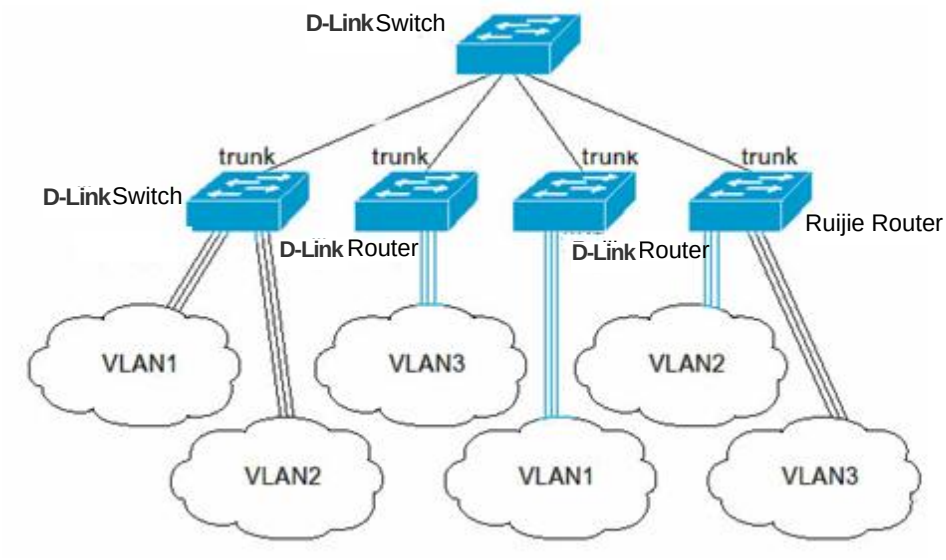
10.3 Configuring VLAN Trunks

10.3.1 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 can transmit the traffics of multiple VLANs.

The Trunk of DES-7200 is encapsulated according to the 802.1Q standard. The following diagram shows one network connected with trunks.

Figure 10-2



You can set one common Ethernet port or one Aggregate Port to be 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**
DES-7200(config-if)# **switchport mode access**	Set one interface to the access mode
DES-7200(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.

10.3.2 Configuring a Trunk Port

10.3.2.1 Trunk Port Basic Configuration

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

Command	Function
DES-7200(config-if)# **switchport mode trunk**	Define the interface type to be a L2 trunk port.
DES-7200(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.

10.3.3 Defining the Allowed VLAN List of a Trunk Port

By default, a trunk port transmits traffic for all VLANs (ID 1-4094) that the device supports. 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
DES-7200(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 the allowed VLAN list contains all the supported VLANs; **add** means to add the specified VLAN list to the allowed 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:

```
DES-7200(config)# interface fastethernet 1/15
DES-7200(config-if)# switchport trunk allowed vlan remove 2
DES-7200(config-if)# end
```

```
DES-7200# 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
```

10.3.4 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
DES-7200(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, it will be automatically removed with the tag 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.

10.4 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:

```
DES-7200# 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

DES-7200#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
```

11 Protocol VLAN

11.1 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 matches none of the protocol group configurations on the input port, the VLAN ID will be assigned based on the VLAN category of the port.
3. If the packet is a TAG packet, its VLAN category 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 with the same type of protocol into the same VLAN.0020

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

RNGOS supports both global IP address-based VLAN classification technology, and the port-wide packet type and Ethernet type-based VLAN classification.

Because IP address-based VLAN classification is a global configuration, it will apply to all the Trunk interfaces once you have configured it.

1. If the incoming packet has no VLAN ID, and its IP address matches the configured IP address, this packet will be classify into the configured VLAN.
2. If the incoming packet has no VLAN ID, and its packet type and Ethernet type respectively match those you configured on the input port, this packet will be classified into the configured VLAN.

IP address-based VLAN classification takes precedence over 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 incoming packet matches them both, the IP address-based VLAN classification takes effect.

You should configure VLAN, and the Trunk, Access and AP attributes of the port before configuring the Protocol VLAN. If you have configured Protocol VLAN for the Trunk interface, the allowed VLAN list for the Trunk interface of the packet must include all the VLANs related to the Protocol VLAN.

11.2 Protocol VLAN Configuration

11.2.1 Default Protocol VLAN

No Protocol VLAN is configured by default.

11.2.2 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 <***1-4093***>**	Configure IP address, subnet mask and VLAN classification
no protocol-vlan ipv4 *address mask address*	Undo IP address allocation
no protocol-vlan ipv4	Undo all IP address allocations
end	Exit the VLAN mode
show protocol-vlan ipv4	Show configured IP addresses

Note

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

Available VLAN IDs may vary with the product.

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

```
DES-7200# configure terminal
DES-7200(config)# protocol-vlan ipv4 192.168.100.3 mask 255. 255.255.0 vlan 100
DES-7200(config-vlan)# end
DES-7200# show protocol-vlan ipv4
ip              mask            vlan
--------------  --------------   -----

192.168.100.3   255.255.255.0   100
```

11.2.3 Configuring Profile for 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 <*1-16***>** **frame-type** [*type*] **ether-type** [*type*]	Configuring profile for packet type and Ethernet type
no protocol-vlan profile <*1-16***>**	Delete an profile
no protocol-vlan profile	Clear all profiles
end	Exit the VLAN mode
show protocol-vlan profile	Show all profiles
show protocol-vlan profile <*1-16***>**	Show a profile

For example:

```
DES-7200# configure terminal
DES-7200(config)# protocol-vlan profile 1 frame-type ETHERII ether-type EHTER_AARP
DES-7200(config)# protocol-vlan profile 2 frame-type SNAP ether-type 0x809b
DES-7200(config-vlan)# end
DES-7200# 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 become effective until the profile is applied to the port.
2. Before a profile is updated, this profile must be deleted first and configured again.
3. Different products support different numbers of profiles.

11.2.4 Applying Profile

To do so, use he following commands:

Command	Description
configure terminal	Enter configuration mode
interface *[interface ID]*	Enter the interface mode
protocol-vlan profile <*1-16***> vlan** *<1-4093>*	Apply a profile to this interface
no protocol-vlan profile	Clear all profiles on this port

no protocol-vlan profile <*1-16***>**	Clear a profile on this port
end	Exit the interface mode

The following example applies profile 1 and profile 2 to the GE interface 1 of Slot 3. The VLAN categories are VLAN 101 and 102:

```
DES-7200# configure terminal
DES-7200(config)# interface gi 3/1
DES-7200(config-if)# protocol-vlan profile 1 vlan 101
DES-7200(config-if)# protocol-vlan profile 2 vlan 102
DES-7200(config-if)# end
DES-7200# 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

Any profile can be applied to each interface.

Different VIDs can be specified for the same profile on different interfaces.

11.3 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

```
DES-7200# 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
```

12 Private VLAN

12.1 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 device, 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 possible for 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 port and community port of the secondary VLAN in the same private VLAN.

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 community 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 for the secondary VLAN.

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

12.2 Private VLAN Configuration

12.2.1 Default Private VLAN Setting

No Private VLAN is configured by default.

12.2.2 Configuring VLAN as a Private VLAN

Configure using the following commands:

Command	Description
configure terminal	Enter configuration mode
vlan *vid*	Enter configuration mode
private-vlan{community | isolated| primary}	Configure private VLAN type
no private-vlan{community | isolated | primary}	Undo private VLAN configuration
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 interface 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:

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:

```
DES-7200# configure terminal
DES-7200(config)# vlan 303
DES-7200(config-vlan)# private-vlan community
DES-7200(config-vlan)# end
DES-7200# show vlan private-vlan community
VLAN Type  Status    Routed   Interface   Associated VLANs
--- ----   --------  ------   ---------   ------------------
303 comm   inactive  Disabled             no association
DES-7200#configure terminal
DES-7200(config)#vlan 404
DES-7200(config-vlan)# private-vlan isolated
DES-7200(config-vlan)# end
DES-7200# show vlan private-vlan
```

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

12.2.3 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:

```
DES-7200# configure terminal
DES-7200(config)# vlan 202
DES-7200(config-vlan)# private-vlan association 303-307,309,440
DES-7200(config-vlan)# end
DES-7200# 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.

12.2.4 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:

```
DES-7200# configure terminal
DES-7200(config)# interface vlan 202
DES-7200(config-if)# private-vlan mapping add 303-307,309,440
DES-7200(config-if)# end
DES-7200#
```

Note

Primary VLAN and Secondary VLAN in this process are associated.

12.2.5 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:

```
DES-7200# configure terminal
DES-7200(config)# interface gigabitEthernet 0/2
DES-7200(config-if)# switchport mode private-vlan host
DES-7200(config-if)# switchport private-vlan host-association
202 203
DES-7200(config-if)# end
DES-7200#
```

Note Primary VLAN and Secondary VLAN in this process are associated.

12.2.6 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	Undo mixing of all the secondary VLANs.

Following example to describe how to configure:

```
DES-7200# configure terminal
DES-7200(config)# interface gigabitEthernet 0/2
DES-7200(config-if)# switchport mode private-vlan promiscuous
DES-7200(config-if)# switchport private-vlan mapping 202 add 203
DES-7200(config-if)# end
```

Note Primary VLAN and Secondary VLAN in this process are associated.

12.3 Private VLAN Showing

12.3.1 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

```
DES-7200# 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      202
```

13 802.1Q Tunneling

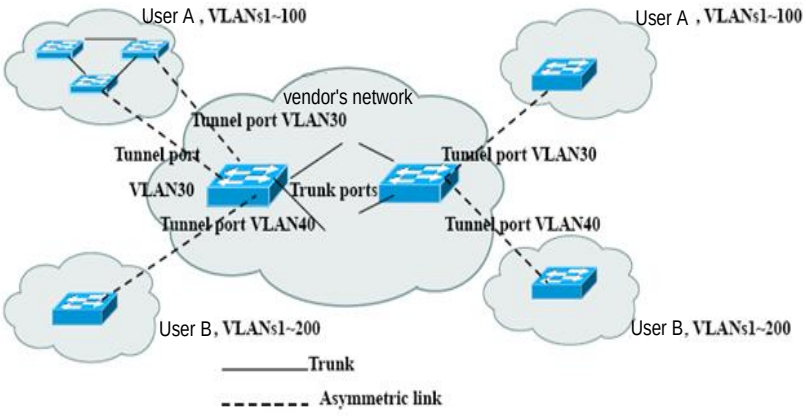
13.1 Understanding 802.1Q Tunneling

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 isolated. 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 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.

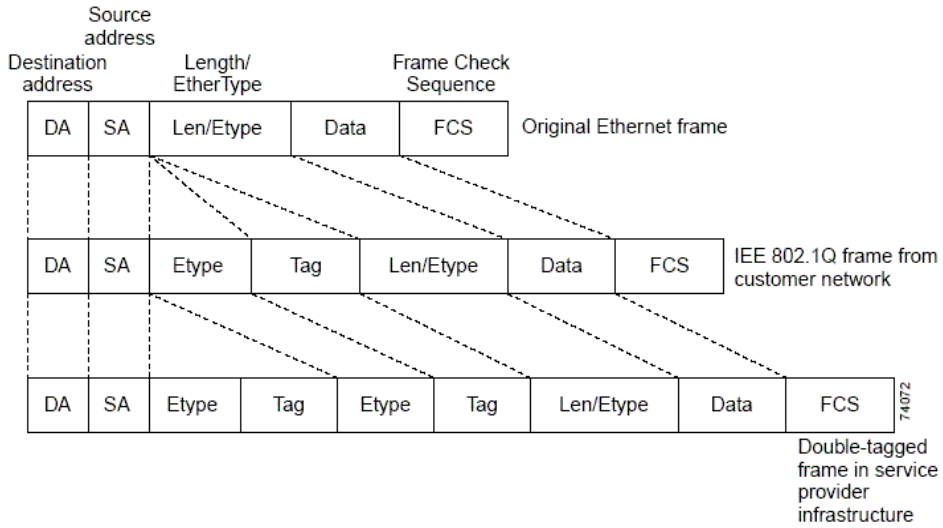
The switching traffic of the user goes from one of its TRUNK port, carrying normal 802.1Q tags, to a tunnel port of the edge device of the vendor. Such an asymmetrical connection between the user and vendor is called the asymmetrical link, because one end is to a Trunk port while the other end to a tunnel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

Figure 13-1



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 dual-tagging process.

Figure 13-2



When the dual-tagged frames go out of 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 enveloped 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.

13.2 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

13.2.1 Default Configurations of the 802.1Q Tunneling

By default, the 802.1Q tunneling function is disabled.

13.2.2 802.1Q 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 maximum frame length.

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 frame length increases from 1518 to 1522.

Uplink port: The Up-link port is used to connect the vendor device or uplink device in other user networks. For example, the Trunk Ports of the vendor network in Figure 13-1 . The Uplink port is actually a special Trunk port except that the packets that go out of the Uplink port are tagged. The packets that go out of 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. We know that the tag of Ethernet frame includes four fields: TPID, User Priority, CFI and VLAN ID. The default TPID value for S2128G and S3750E are 0x8100 as specified in the IEEE802.1Q protocol. In the devices from some vendors the TPID value in the outer tag in the packet is set as 0x9100 or

other values. In order to be compatible with these devices, S2128G and S3750E devices provide port-based packet TPID configuration function. Users can configure the TPID value for the ports on their own. When these ports receive packets, they will replace the TPID in the outer VLAN Tag of the packet with the user-defined values.

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.

13.2.3 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.

13.2.4 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 the user.
switchport mode dot1q-tunnel	Set the port 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:

```
DES-7200(config)# interface fastEthernet 0/1
```

```
DES-7200(config-if)# switchport access vlan 22
DES-7200(config-if)# switchport mode dot1q-tunnel
DES-7200(config)# end
```

13.2.5 Configuring an Uplink 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 mode uplink	Configure the port as an uplink port
end	Exit from interface mode

The following example demonstrates how to configure a tunnel port:

```
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# switchport mode up-link
DES-7200(config)# end
```

13.2.6 Configuring TPID Value in Vendor Tag

In the global configuration mode, type in **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 enter 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:

```
DES-7200(config)# interface gigabitethernet 0/1
DES-7200(config-if)# frame-tag tpid 9100
DES-7200(config)# end
DES-7200# show frame-tag tpid interface gigabitethernet 0/1
Port     tpid
-------- -------------
Gi0/1    0x9100
```

13.2.7 Configuring Priority Duplication of User Tag

In the global configuration mode, type in **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.

Note

S23/S37 series devices do not support configuration of the priority duplication function for the user tag.

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

```
DES-7200(config)# interface gigabitethernet 0/1
DES-7200(config-if)# inner-priority-trust enable
DES-7200(config)# end
DES-7200# show inner-priority-trust interface gigabitethernet 0/1
Port     inner-priority-trust
------   --------------------
Gi0/1    enable
```

14 Super VLAN Configuration

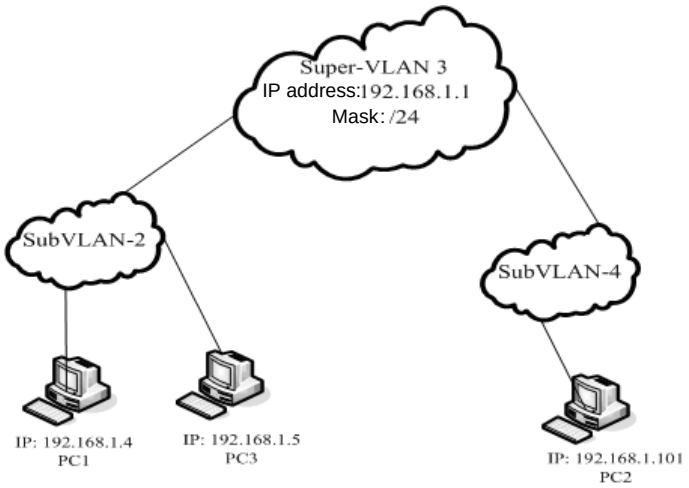
This chapter describes the Super VLAN configuration of DES-7200.

14.1 Overview

Super VLAN is a method for VLAN division. Super VLAN, also called VLAN set, 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 interoperation between layers 3 of layer 2 isolated ports. By default, the ARP agent function is enabled for Super VLAN and Sub VLAN.

The Super VLAN technology saves lots of IP addresses, because it just assigns one IP addresses to the Super VLAN that includes several sub VLANs, saving addresses and making network management easy.

Figure 14-1



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 form Super VLAN3. An IP address 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 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 interfaces.
- 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 supported.

14.2 Configuring Super VLAN

Using following command to configure Super VLAN.

Command	Function
DES-7200# **configure**	Enter the global configuration mode.
DES-7200(config)# **vlan** *vlan-id*	Enter VLAN configuration mode
DES-7200(config-vlan)# **supervlan**	Enable the SuperVLAN function
DES-7200(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**.

14.3 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
DES-7200# **configure**	Enter configuration mode
DES-7200(config)# **vlan** *vlan-id*	Enter VLAN configuration mode
DES-7200(config-vlan)# **supervlan**	Set this VLAN as a Super VLAN
DES-7200(config-vlan)# **subvlan** *vlan-id-list*	Specify several sub VLANs and add them to the Super VLAN.
DES-7200(config-vlan)# **exit**	Exit the global mode.

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

14.4 Setting Address Range of Sub VLAN

The user can configure address range for each sub VLAN, so that the device understands 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
DES-7200# **configure**	Enter configuration mode
DES-7200(config)# **vlan** *vlan-id*	Enter VLAN configuration mode
DES-7200(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.
DES-7200(config-vlan)# **end**	Return to the privilege mode.
DES-7200# **show run**	Verify the configurations made in the previous steps.

Note: Users can delete old configurations using **no subvlan-address-range**.

14.5 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
DES-7200# **configure**	Enter configuration mode
DES-7200(config)# **interface vlan** *vlan-id*	Enter the SVI mode
DES-7200(config-vlan)# **ip address** *ip mask*	Set an IP address for the virtual interface
DES-7200(config-vlan)# **end**	Return to the privilege mode.
DES-7200# **show run**	Verify the configurations made in the previous steps.

14.6 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
DES-7200# **configure**	Enter configuration mode
DES-7200(config)# **vlan** *vlan-id*	Enter the VLAN mode
DES-7200(config-vlan)# **proxy-arp**	Enable the ARP agent function for VLAN
DES-7200(config-vlan)# **end**	Return to the privilege mode.
DES-7200# **show run**	Verify the configurations made in the previous steps.

The ARP agent function can be disabled for VLAN using **no proxy-arp**.

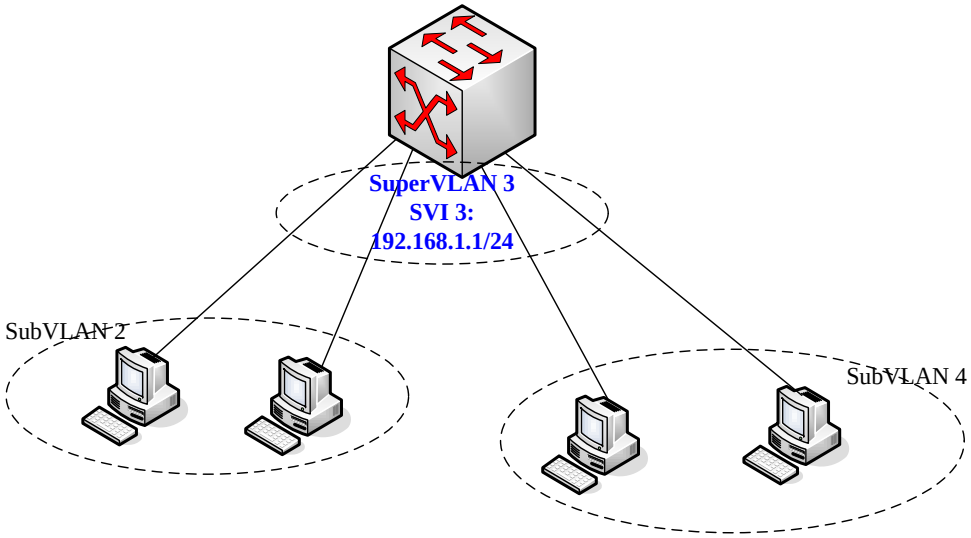
14.7 Showing Super VLAN Setting

Show the Super VLAN setting using the following command.

Command	Function
DES-7200# **show supervlan**	Show Super VLAN setting

14.8 Configuration Example

Figure 14-2



In the above diagram, Super VLAN is used. 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 under 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 under Sub VLAN 4

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

Add a member port for Sub VLAN2

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

Add a member port for Sub VLAN4

```
switchport access vlan 4
!
```

Create a virtual layer 3 interface that correspond to Super VLAN

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

15 DHCP Relay Configuration

15.1 Overview

15.1.1 Understanding DHCP

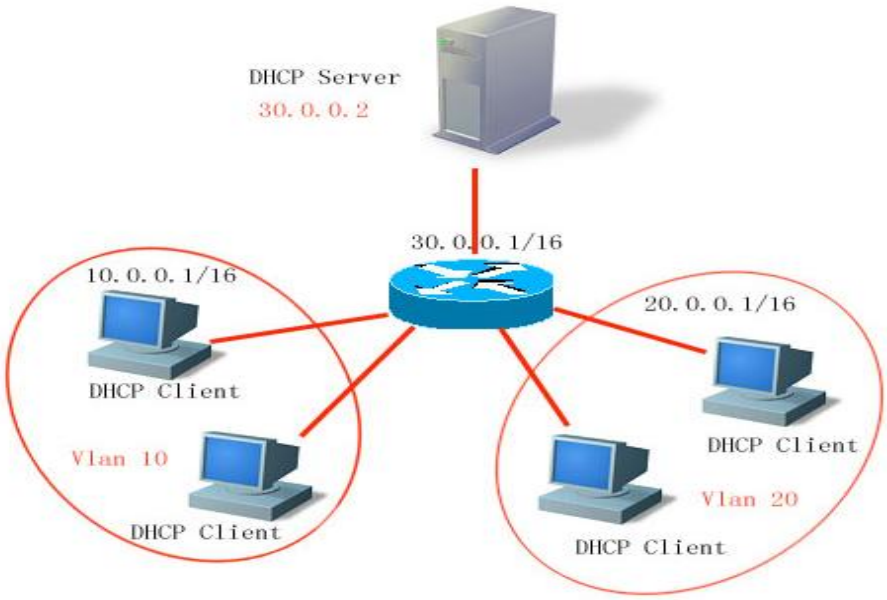
The DHCP is widely used to dynamically allocate the reusable network resources, for example, IP address.

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.

15.1.2 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 15-1



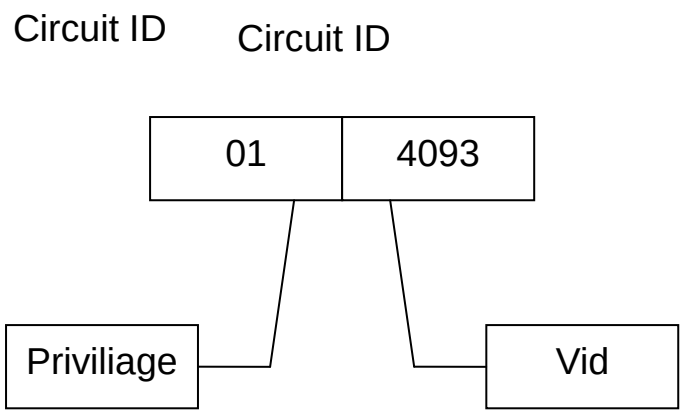
VLAN 10 and VLAN 20 correspond to the 10.0.0.1/16 and 20.0.0.1/16 networks respectively, while the DHCP Server is located on the 30.0.0.1/16 network. To have a dynamic IP management on the 10.0.0.1/16 and 20.0.0.1/16 networks through the DHCP Server at 30.0.0.2, just enable the DHCP Relay Agent on the device that functions as the gateway, and specify the DHCP Server IP as 30.0.0.2.

15.1.3 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. DES-7200 provides two types of relay agent information. One is the relay agent information option dot1x that is combined with the 802.1x/SAM application scheme, the other is relay agent information option82 that is combined with the port VID, slot, port of user and device MAC information. Depicted below are the contents in the option, format, and typical application schemes when the two schemes are used:

1. relay agent information option dot1x: This application scheme requires combination of 802.1x authentication and RG-SAM. RG-SAM assigns different IP privileges to devices during 802.1x authentication. They are combined with VID to which DHCP client belongs to form the Circuit ID sub-option. When DHCP relay is uploaded to the DHCP server, combine with the configuration of DHCP server, so that IP with different privileges can be assigned to users with different privileges. The Circuit ID is in the following format, where the privilege and vid fields respectively have two bytes:

Figure 15-2



2. 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 15-3

Agent Circuit ID

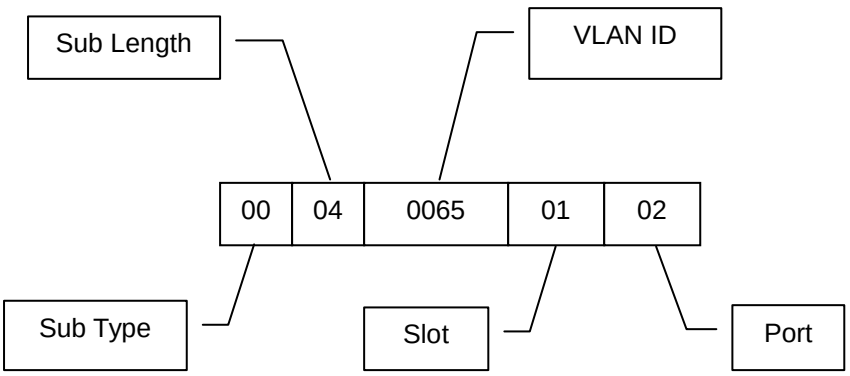
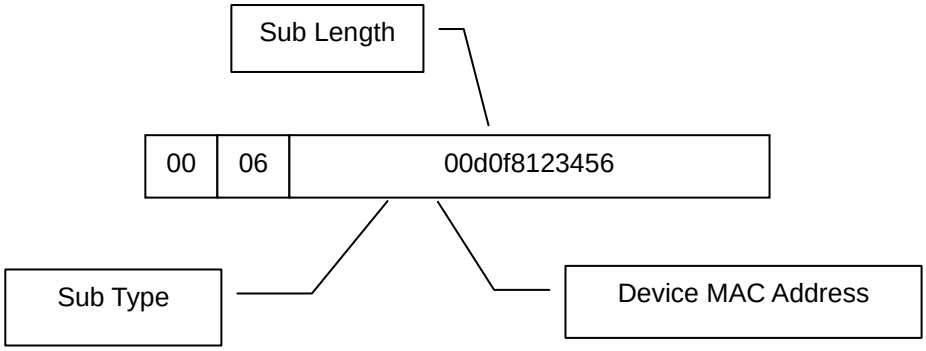


Figure 15-4

Agent Remote ID



15.1.4 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.

15.2 Configuring DHCP

15.2.1 Configuring DHCP Relay Agent

In the global configuration mode, configure the DHCP relay agent by performing the following steps.

Command	Function
DES-7200(config)# **service dhcp**	Enable the DHCP agent
DES-7200(config)# **no service dhcp**	Disable the DHCP agent

15.2.2 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
DES-7200(config)# **IP helper-address** *A.B.C.D*	Add a global DHCP server address
DES-7200(config-if)# **IP helper-address** *A.B.C.D*	Add the DHCP server address of an interfaceThis command must be set under the layer 3 interface.
DES-7200(config)# **no IP helper-address** *A.B.C.D*	Delete a global DHCP server address
DES-7200(config-if)# **no IP helper-address** *A.B.C.D*	Delete the DHCP server address of an interface

15.2.3 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
DES-7200(config)# **ip dhcp relay information option dot1x**	Enable the DHCP option dot1x function
DES-7200(config)# **no ip dhcp relay information option dot1x**	Disable the DHCP option dot1x function

15.2.4 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:

```
DES-7200# config
DES-7200(config)# ip access-list extended DenyAccessEachOtherOfUnauthrize
DES-7200(config-ext-nacl)# permit ip any host 192.168.3.1    //Packet that can be sent
to the gateway
DES-7200(config-ext-nacl)# permit ip any host 192.168.4.1
DES-7200(config-ext-nacl)# permit ip any host 192.168.5.1
DES-7200(config-ext-nacl)# permit ip host 192.168.3.1 any
```

//Allow communication of packets with IP address as the gateway address

```
DES-7200(config-ext-nacl)# permit ip host 192.168.4.1 any
DES-7200(config-ext-nacl)# permit ip host 192.168.5.1 any
DES-7200(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

```
DES-7200(config-ext-nacl)# deny ip 192.168.3.0  0.0.0.255  192.168.4.0  0.0.0.255
DES-7200(config-ext-nacl)# deny ip 192.168.3.0  0.0.0.255  192.168.5.0  0.0.0.255
DES-7200(config-ext-nacl)# deny ip 192.168.4.0  0.0.0.255  192.168.4.0  0.0.0.255
DES-7200(config-ext-nacl)# deny ip 192.168.4.0  0.0.0.255  192.168.5.0  0.0.0.255
DES-7200(config-ext-nacl)# deny ip 192.168.5.0  0.0.0.255  192.168.5.0  0.0.0.255
DES-7200(config-ext-nacl)# deny ip 192.168.5.0  0.0.0.255  192.168.3.0  0.0.0.255
DES-7200(config-ext-nacl)# deny ip 192.168.5.0  0.0.0.255  192.168.4.0  0.0.0.255
DES-7200(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
DES-7200(config)# **ip dhcp relay information option dot1x access-group** *acl-name*	Apply DHCP option dot1x acl
DES-7200(config)# **no ip dhcp relay information option dot1x access-group** *acl-name*	Cancel the applied DHCP option dot1x acl.

15.2.5 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
DES-7200(config)# **ip dhcp relay information option82**	Enable the DHCP option82 function
DES-7200(config)# **no ip dhcp relay information option82**	Disable the DHCP option82 function.

15.2.6 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
DES-7200(config)# **ip dhcp relay check** *server-id*	Enable the DHCP relay check server-di function
DES-7200(config)# **no ip dhcp relay check** *server-id*	Disable the DHCP relay check server-id function

15.2.7 DHCP Configuration Example

The following commands enable the dhcp relay function and add two groups of server addresses:

```
DES-7200# configure terminal
DES-7200(config)# service dhcp                      //Enable the dhcp relay function
DES-7200(config)# ip helper-address 192.18.100.1    //Add a global server address
DES-7200(config)# ip helper-address192.18.100.2     //Add a global server address
DES-7200(config)# interface GigabitEthernet 0/3
DES-7200(config-if)# ip helper-address 192.18.200.1 //Add an interface server address
DES-7200(config-if)# ip helper-address 192.18.200.2 // Add an interface server address
DES-7200(config-if)# end
```

15.3 Other Notes 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.

15.3.1 Notes 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.

15.3.2 Notes 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.

15.4 Showing DHCP Configuration

Show the DHCP configuration using the **show running-config** command in the privilege mode.

```
DES-7200# show running-config
Building configuration...
Current configuration : 1464 bytes
Software version 10.1.00(1), Release(11758)(Fri Mar 30 12:53:11 CST 2007 -nprd
hostname DES-7200
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
```

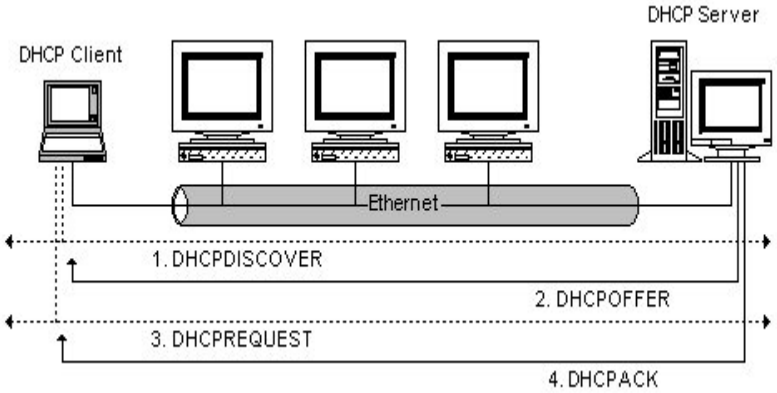
16 DHCP Snooping Configuration

16.1 DHCP Snooping Overview

16.1.1 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 16-1



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.

16.1.2 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 interface: 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: Many users in the network where DHCP is used will set IP addresses by themselves. This makes it difficult to maintain the network and makes users who obtain IP addresses using DHCP unable to 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 user entry. This creates a user database for 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 inspection 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.

16.1.3 Relationship between DHCP Snooping and ARP Detectation

ARP detectation 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.

16.1.4 Other Notes 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.

16.2 DHCP Snooping Configuration

16.2.1 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
DES-7200# **configure terminal**	Enter configuration mode
DES-7200(config)# [**no**] **ip dhcp snooping**	Enable and disable DHCP snooping

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

```
DES-7200# configure terminal
DES-7200(config)# ip dhcp snooping
DES-7200(config)# end
DES-7200#
```

16.2.2 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
DES-7200# **configure terminal**	Enter configuration mode
DES-7200(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:

```
DES-7200# configure terminal
DES-7200(config)# ip dhcp snooping verify mac-address
```

```
DES-7200(config)# end
DES-7200#
```

16.2.3 Configuring Static DHCP Snooping User

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

Command	Description
DES-7200# **configure terminal**	Enter configuration mode
DES-7200(config)# [**no**] **ip dhcp snooping bindingmac-addrees vlan** *vlan_id* **ip** *ip-address***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:

```
DES-7200# configure terminal
DES-7200(config)# ip dhcp snooping binding 00d0.f801.0101 vlan 1 ip 192.168.4.243
interface gigabitEthernet 0/9
DES-7200(config)# end
DES-7200#
```

16.2.4 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
DES-7200# **configure terminal**	Enter configuration mode
DES-7200(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:

```
DES-7200# configure terminal
DES-7200(config)# ip dhcp snooping database write-delay 3600
DES-7200(config)# end
```

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.

16.2.5 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
DES-7200# **configure terminal**	Enter configuration mode
DES-7200(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:

```
DES-7200# configure terminal
DES-7200(config)# ip dhcp snooping database write-to-flash
DES-7200(config)# end
```

16.2.6 Configuring Port as TRUST Port

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

Command	Description
DES-7200# **configure terminal**	Enter configuration mode
DES-7200(config)# **interface** *interface*	Enter the interface configuration mode.
DES-7200(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:

```
DES-7200# configure terminal
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# ip dhcp snooping trust
DES-7200(config-if)# end
DES-7200#
```

Caution

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

16.2.7 Clearing Dynamic User Information from DHCP Snooping Database

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

Command	Description
DES-7200# **clear ip dhcp snooping binding**	Clear information from the current database

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

```
DES-7200# clear ip dhcp snooping binding
```

16.3 Showing DHCP Snooping Configuration

16.3.1 Showing DHCP snooping

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

Command	Description
DES-7200# **show ip dhcp snooping**	Show configuration information of DHCP snooping.

For example:

```
DES-7200# 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
```

16.3.2 Showing DHCP Snooping Database Information

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

Command	Description
DES-7200# **show ip dhcp snooping binding**	View the static user information in the DHCP Snooping binding database

For example:

```
DES-7200# show ip dhcp snooping binding
MacAddress  IpAddress   Lease(sec) Type  VLAN  Interface
------------------ --------------- ---------- -------------
00d0.f801.0101 192.168.4.243 -  static 1 GigabitEthernet 0/9
```

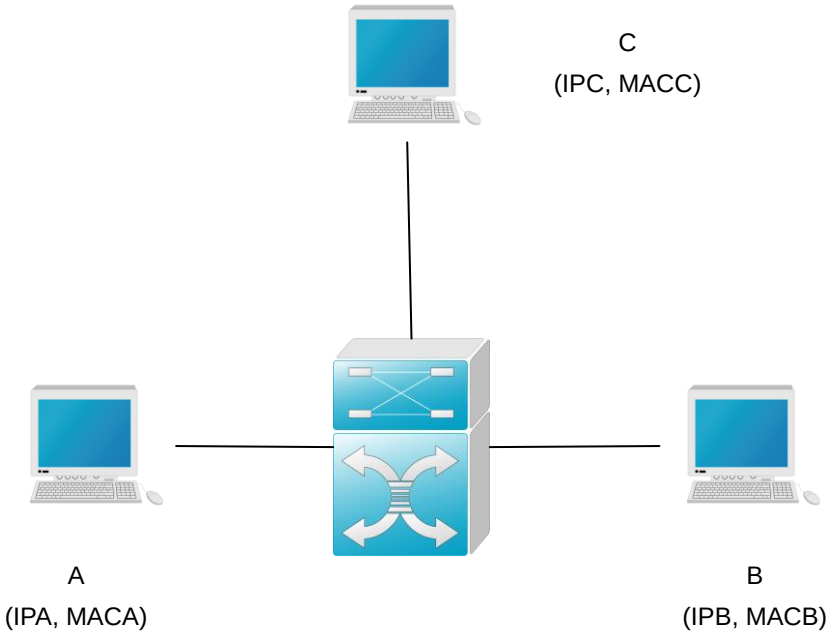
17 Dynamic ARP Inspection Configuration

17.1 Understanding DAI

DAI, an acronym of Dynamic ARP Inspection, Refers to validity inspection of received ARP packets. Illegal ARP packets will be discarded.

17.1.1 Understanding ARP Spoofing Attack

ARP itself does not check the validity of incoming ARP packets, a drawback of ARP. This way, attackers can launch ARP spoofing attacks easily by exploiting the drawback of the protocol. The most typical one is the man in the middle attack, which is described as follows:



As shown in the diagram, devices A, B and C are connected to DES-7200 and located in the same subnet. Their IP and MAC addresses are respectively represented by (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 will cause the corresponding relationship of ARP entries in device A and device B incorrect. The policy is to broadcast ARP response to the network continuously. The IP address in this response is IPA/IPB, and the MAC address is MACC. Then, ARP entries (IPB and MACC) will 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 man in the middle attack.

17.1.2 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 untrust 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 check according to the DHCP snooping binding database. For details, refer to the configuration guide DHCP Snooping Configuration.

17.1.3 Understanding DAI Global Switch

Typically, the 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.

17.1.4 Interface Trust Status and Network Security

ARP packets are check according to the trust status of each port on the device. DAI check is ignored for the packets that are received through trust ports and are considered legal ARP packets. DAI check will be performed strictly for the ARP packets that are received through untrust ports.

In a typical network configuration, layer 2 port connected to the network device should be set as a trust port, and layer 2 port connected to the host device should be set as an untrust port.

Note: Incorrectly configuring a layer 2 port as an untrust port may affect normal communication of the network.

For specific configuration commands, refer to ip arp inspection trust, show ip arp inspection interface.

17.1.5 Restricting Rate of ARP Packets

Because DAI validity check consumes certain CPU resources, the rate of ARP packets is restricted, namely 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 untrust port is 15. This restriction does not apply to the trust port. To configure this rate restriction, use the ip arp inspection limit-rate command in the layer 3 interface configuration mode.

For specific configuration commands, refer to ip arp inspection limit-rate show ip arp inspection interface

17.2 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 Global DAI Function (required)
- Enabling DAI Packet Check Function for Specified VLAN (required)
- Set Trust Status of Port (optional)
- Set Maximum Receiving Rate of ARP Packets for a Port (optional)

- Related Configuration of DHCP Snooping Database (optional)

17.2.1 Enabling Global DAI Function

This feature is disabled by default.

DAI-related security check will be performed against ARP packets only when the global DAI function is enabled.

If this global switch is enabled, the words **ip arp inspection** can be seen using **show running-config**.

Command	Function
DES-7200(config)# **ip arp inspection**	Enable the global DAI function
DES-7200(config)# **no ip arp inspection**	Disable the global DAI function

17.2.2 Enabling 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 has enabled VLAN vid, DAI-related security check will be skipped for the ARP packets with vlan-id = vid (ARP packet rate restriction is not skipped).

show ip arp inspection vlan can be used to check whether the DAI packet check function has been enabled for all VLANs.

To configure the DAI packet check function for VLAN, execute the following commands in the interface configuration mode:

Command	Function
DES-7200(config)# **ip arp inspection vlan** *vlan-id*	Turn on the DAI packet check function switch for VLAN *vlan-id*
DES-7200(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

17.2.3 Set Trust Status of Port

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 check further. Otherwise, the validity of the current ARP packet will be check using 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
DES-7200(config-if)# **ip arp inspection trust**	Set the port as a trust port
DES-7200(config-if)# **no ip arp inspection trust**	Set the port as an untrust port

17.2.4 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 default ARP packet receiving rate of each untrust switching port is 15 ARP packets per second. By default, this does not apply to trust switching ports.

If the number of ARP packets received through this port within one second exceeds this threshold, the following packets will be discarded.

The rate restriction of each layer 2 interface can be viewed by using 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
DES-7200(config-if)# **ip arp inspectionlimit-rate**{ *<1-2048>* **| none**}	Set the maximum ARP packet receiving rate for a port, in packets/second **none**: There is no restriction
DES-7200(config-if)# **no ip arp inspection limit-rate**	Restore the default setting

17.2.5 Related Configuration of DHCP Snooping Database

Refer to *DHCP Snooping Configuration*.

If DHCP Snooping database is not configured, all the ARP packets pass inspection.

17.3 Showing DAI Configuration

17.3.1 Showing Whether DAI Function Is Enabled for VLAN

To show the enabling status of VLAN, execute the following command in the global configuration mode:

Command	Function
DES-7200(config)# **show ip arp inspection vlan**	Show the enabling status of each VLAN

17.3.2 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
DES-7200(config)# **show ip arp inspection interface**	Show the DAI configuration of each layer 2 interface (including trust status and rate restriction)

18 Configuring MSTP

18.1 MSTP Overview

18.1.1 STP and RSTP

18.1.1.1 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 prevent 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 one 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 set by administrators automatically. 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 1s to re-span the topology tree once the network topology changes (it takes about 50s for conventional STP protocol).

18.1.1.2 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 message)
- Port ID (the port ID that sends this message).
- 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.

Once 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 promulgated 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.

18.1.1.3 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 subsequent extensibility protocol use. 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

18.1.1.4 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 the sending of the BUDU message 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 message. Once it is timeout, the message will be discarded.

18.1.1.5 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.

Figure 18-1 , Figure 18-2 and Figure 18-3 below show the roles of various ports:

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 18-1

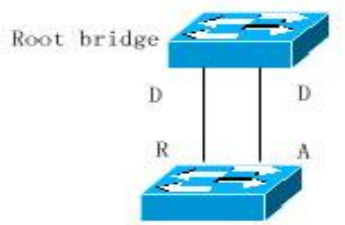


Figure 18-2

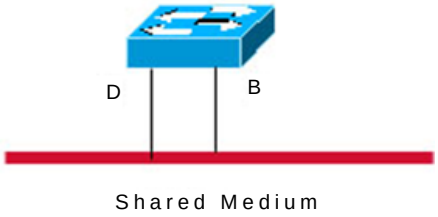
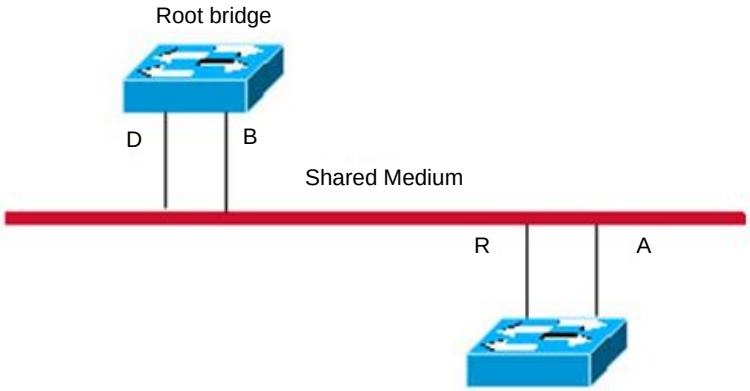


Figure 18-3



Each port takes three port states to indicate whether the data packet is forwarded, to control the topology of the whole spanning tree.

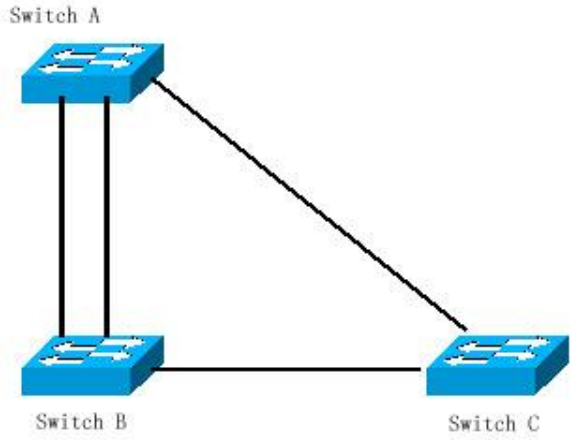
- Discarding: It will neigh forward the received frame nor learn about the source Mac address.
- Learning: It will not forward the received frame, but learn about the source Mac address, so it is a transitional status.
- Forwarding: It will forward the received frame and learn about the source Mac address.

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.

18.1.1.6 Spanning of Network Topology Tree (Typical Application Solution)

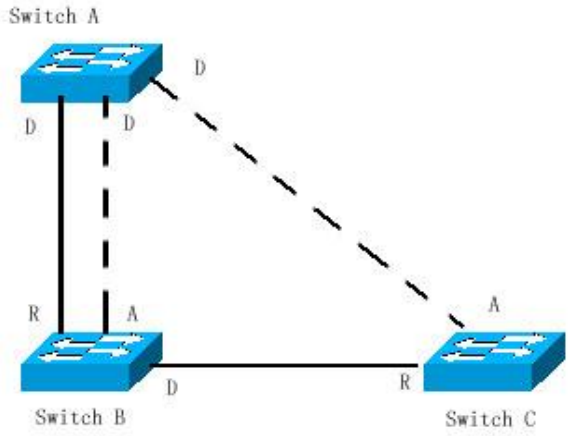
We now describe how the STP and RSTP protocol spans a tree-type structure by the mixed network topology. As is shown in Figure 18-4 below, the bridge IDs of the Switch A, B and C are assumed to be increasing. Namely, the Switch A presents the highest priority. There is the 1000M link between switch A 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 produce the broadcast storm if all these links are active.

Figure 18-4



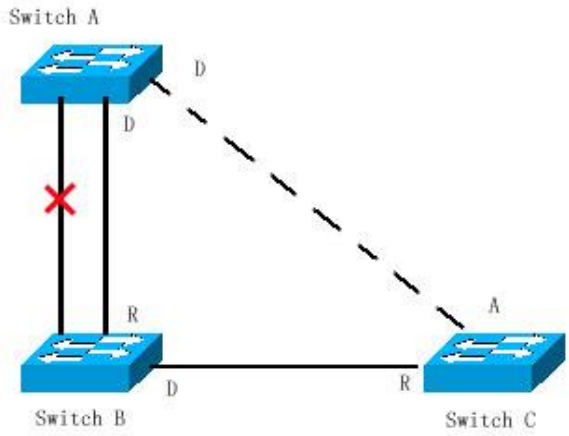
If all of three Switches open the Spanning Tree protocol, they will select the root bridge as the Switch A by switching the BPDU. Once Switch B detects that two ports are connected to Switch A, it will select the port with the highest priority as the root port, while another one is selected as the Alternate 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 18-5 after the port roles are selected.

Figure 18-5



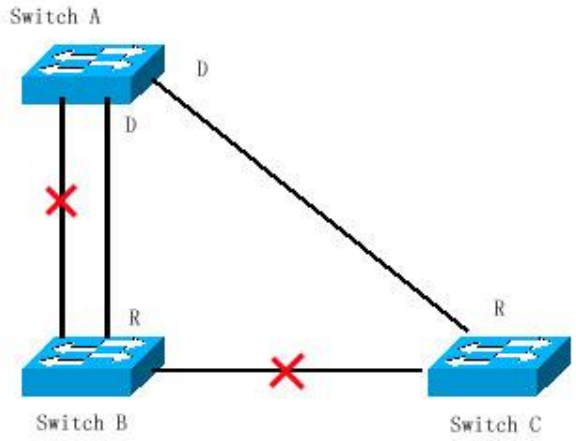
If the failure of the active path between Switch A and Switch B occurs, the alternate path will take action immediately to generate corresponding Figure 18-6 .

Figure 18-6



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 18-7 .

Figure 18-7



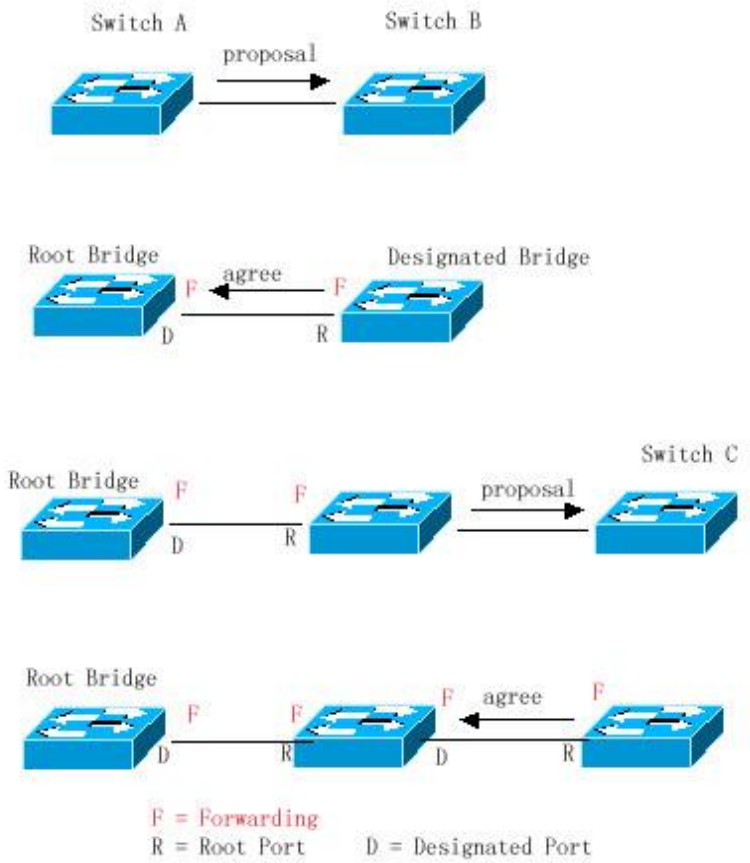
18.1.1.7 Quick Convergence of RSTP

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 18-8 , the Switch A will send the proposal message 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 message is the Root Port, and then sends the Agree message 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 18-8



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 18-9 , 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 18-9

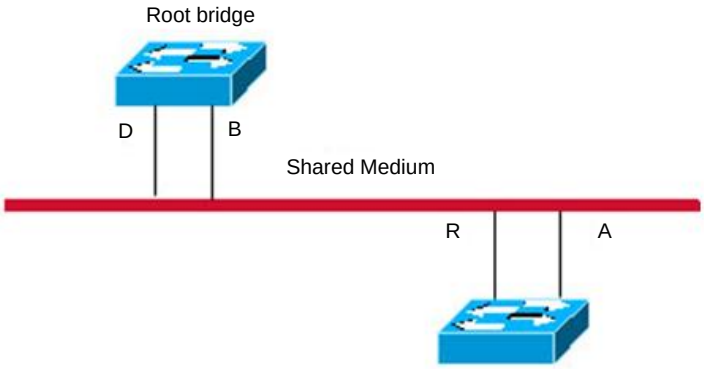
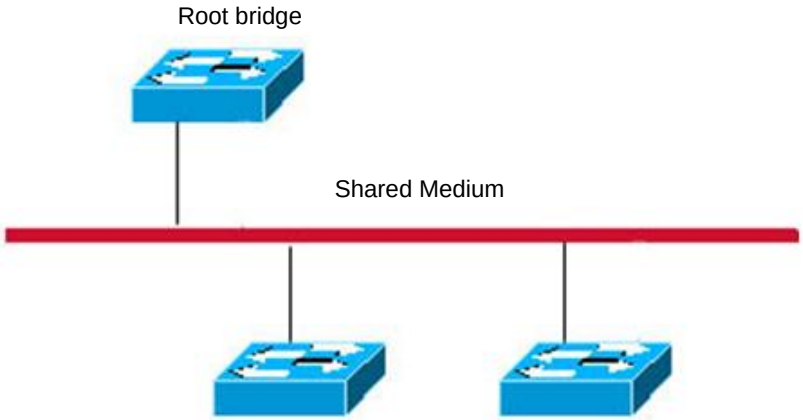
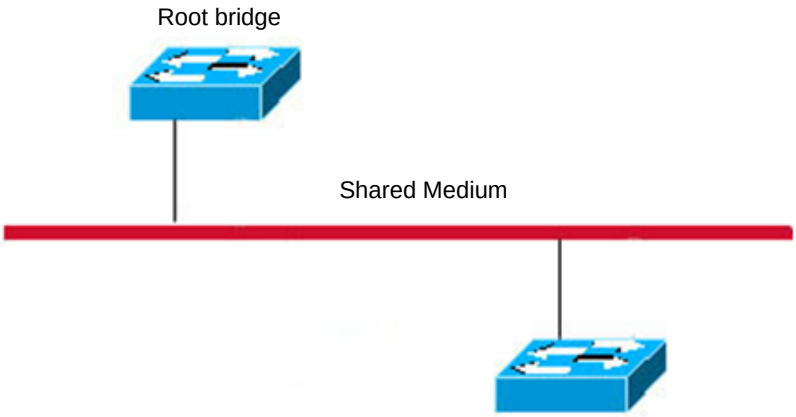


Figure 18-10



In addition, the following figure is a point-to-point connection and should be differentiated by users carefully.

Figure 18-11



18.1.1.8 Compatibility of RSTP and STP

The RSTP protocol is completely compatible with the STP protocol, and will judge whether the bridge connected with supports the STP protocol or the RSTP protocol by the version number of received BPDU automatically. 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 18-12 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 18-13 .

Figure 18-12

Protocol Migration

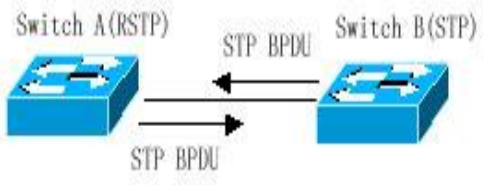
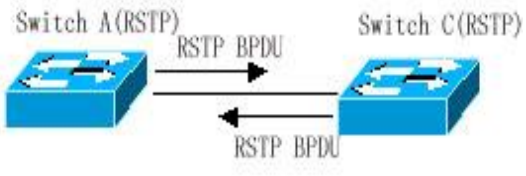


Figure 18-13



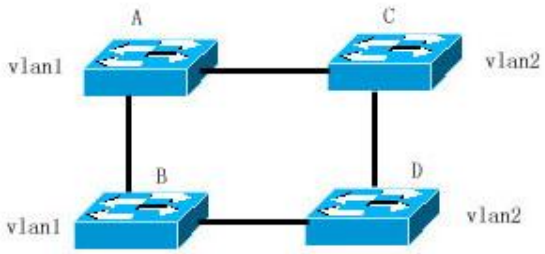
18.1.2 MSTP Overview

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:

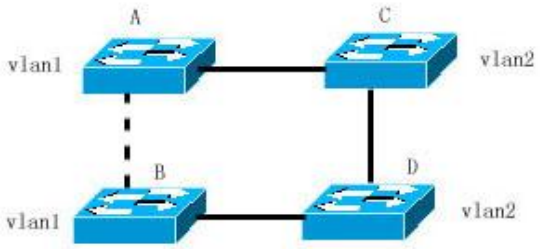
As shown in Figure 18-14 , devices A and B are located in Vlan1, and devices C and D in Vlan2. They form a loop.

Figure 18-14



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 18-15). 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.

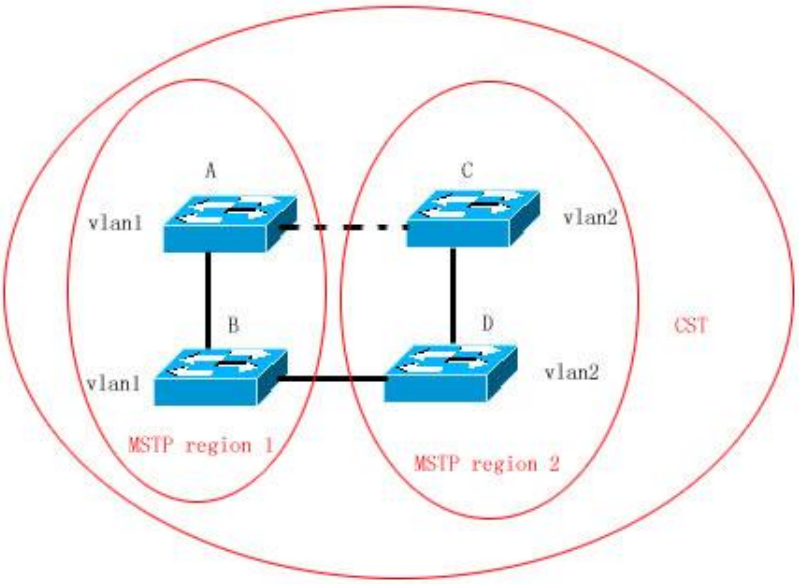
Figure 18-15



The MSTP is developed to address 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).

By this algorithm, above network can form the topology as Figure 18-16 : 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 18-16



In this way, it prevents the form of loop and has no effect on the communication among the same vlans.

18.1.2.2 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, 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 with 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 open the MSTP to ensure the stability and convergence of the network topology.

18.1.2.3 Spanning Tree within MSTP region (IST)

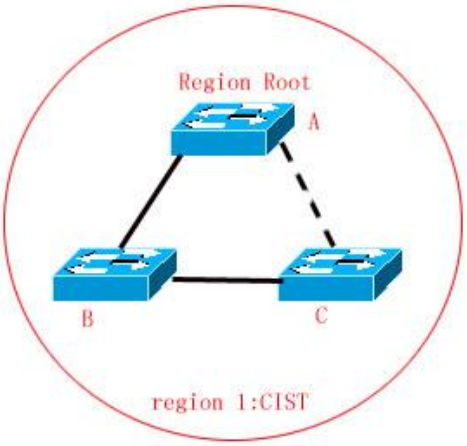
After the MSTP region is partitioned, each region will select separate root bridge of various instances and the port role of various ports for each device according to such parameters as the bridge priority and port priority. Finally, it will specify whether this port is FORWARDING or DISCARDING within this instance for the port role.

In this way, the IST (Internal Spanning Tree) is formed 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.

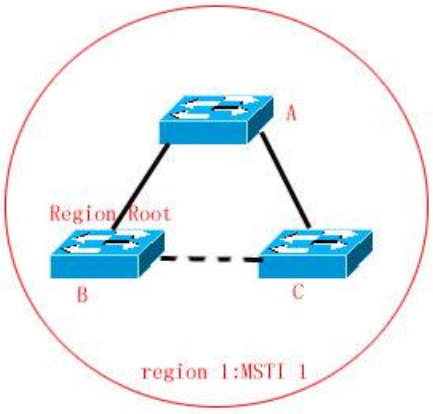
As is shown in Figure 18-17 , device A with the highest priority is selected as the Region Root in the CIST (instance 0). Then, the path between devices A and C are DISCARDING according to other parameters. Hence, for the vlan group of the instance 0, only the path from switch A to B and device B to C is available, which breaks the loop of the vlan group.

Figure 18-17



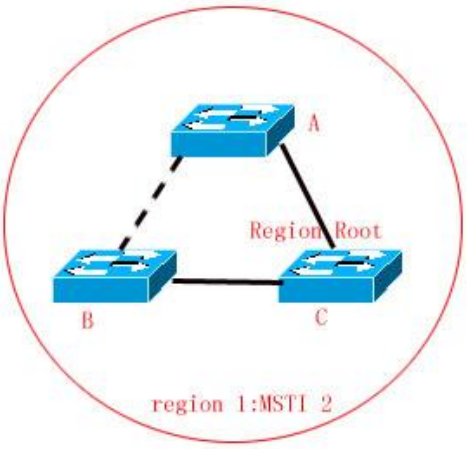
As is shown in Figure 18-18 , switch C with the highest priority is selected as the Region Root in the MSTI 1 (instance 1). Then, the path between switch A and B is DISCARDING according to other parameters. Hence, for the vlan group of the instance 1, only the path from switch A to B and switch A to C is available, which breaks the loop of the vlan group.

Figure 18-18



As is shown in Figure 18-19 , switch B with the highest priority is selected as the Region Root in the MSTI 2 (instance 2). Then, the path between switch B and C is DISCARDING according to other parameters. Hence, for the vlan group of the instance 2, only the path from switch A to B and switch B to C is available, which breaks the loop of the vlan group.

Figure 18-19



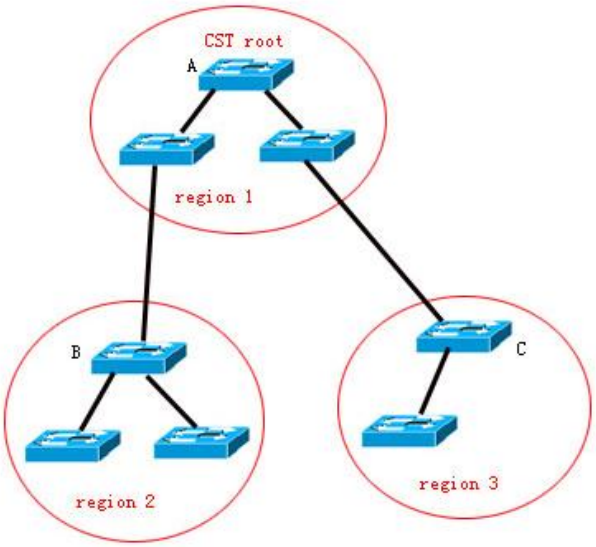
It should note that the MSTP protocol doesn't concern with which vlan the port is of, so users should configure corresponding path cost and priority for related port according to actual vlan configuration, to prevent the MSTP protocol from breaking the loop unexpected.

18.1.2.4 Spanning Tree between MSTP regions (CST)

For CST, each MSTP region is equivalent to a 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 18-20 , 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 18-20



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!

18.1.2.5 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.

18.1.2.6 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.

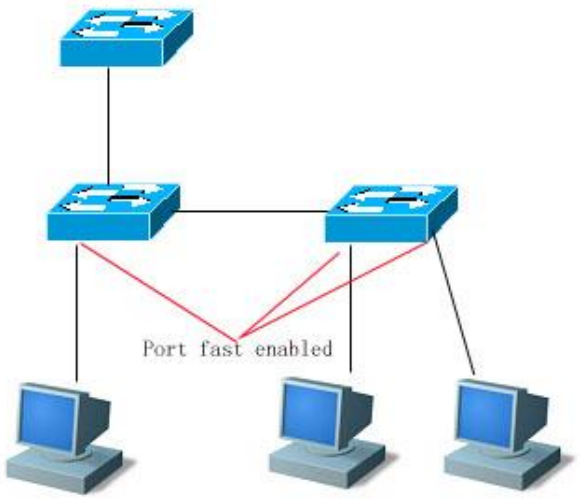
Each device that runs STP or RSTP is an independent region, and does not form the same region with any other device.

18.2 Overview of Optional Features of MSTP

18.2.1 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 18-21



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.

18.2.2 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 open 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.

18.2.3 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.

18.2.4 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, this period of time is monitored for TC-BPDU packets. 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.

18.2.5 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 point-to-point connection to the remote switch 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.

18.2.6 Understanding Invalid Length Filtering for BPDU

When the Ethernet length field of BPDU exceeds 1500, this BPDU frame is discarded in order to avoid receiving invalid BPDU packets.

18.3 Configuring MSTP

18.3.1 Default Configuration of Spanning Tree

The following lists the default configuration of the Spanning Tree.

Item	Default value
Enable State	Disable, the STP is not opened.
STP MODE	MSTP
STP Priority	32768
STP port Priority	128
STP port cost	Judged according to the port rate automatically.
Hello Time	2 seconds
Forward-delay Time	15 seconds
Max-age Time	20 seconds
Default calculation method of the Path Cost	Long integer
Tx-Hold-Count	3
Link-type	Determined by the dual status of the port automatically.
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.

18.3.2 Open and Close 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
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **spanning-tree**	Open the Spanning tree protocol.
DES-7200(config)# **end**	Return to the privileged EXEC mode.
DES-7200# **show spanning-tree**	Check the configuration entities.
DES-7200# **copy running-config startup-config**	Save the configuration.

If you close the Spanning Tree protocol, use the global configuration command **no spanning-tree** to set.

18.3.3 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, taking that some manufacturers will not develop by the standard completely into consideration, 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 to the RSTP or STP mode from the MSTP mode, all information about 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
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **spanning-tree mode mstp/rstp/stp**	Switch the Spanning Tree mode.
DES-7200(config)# **end**	Return to the privileged EXEC mode.
DES-7200# **show spanning-tree**	Check the configuration entries.
DES-7200# **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.

18.3.4 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 various 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
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(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.
DES-7200(config)# **end**	Return to the privileged EXEC mode.
DES-7200# **show running-config**	Check the configuration entries.
DES-7200# **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.

18.3.5 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 various instances on one port, by which various instances 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
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** *interface-id*	Enter he configuration mode of this interface, the legal interface contains the physical port and the Aggregate Link.
DES-7200(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.
DES-7200(config-if)# **end**	Return to the privileged EXEC mode.
DES-7200# **show spanning-tree** [**mst** *instance-id*] **interface** *interface-id*	Check the configuration entries.
DES-7200# **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.

18.3.6 Configuring Path Cost of 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 various instances on one port, by which various instances can run separate spanning tree protocol.

In the privileged mode, perform these steps to configure the port path cost:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** *interface-id*	Enter he configuration mode of this interface, the legal interface contains the physical port and the Aggregate Link.
DES-7200(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.
DES-7200(config-if)# **end**	Return to the privileged EXEC mode.
DES-7200# **show spanning-tree** [**mst** *instance-id*] **interface** *interface-id*	Check the configuration entities.
DES-7200# **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.

18.3.7 Configuring Default Calculation Method of Path Cost (path cost method)

If 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
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
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(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.
DES-7200(config)# **end**	Return to the privileged EXEC mode.
DES-7200# **show running-config**	Check the configuration entries.
DES-7200# **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.

18.3.8 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
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **spanning-tree hello-time** *seconds*	Configure the hello_time, whose value range is 1-10s, 2s by default.
DES-7200(config)# **end**	Return to the privileged EXEC mode.
DES-7200# **show running-config**	Check the configuration entries.
DES-7200# **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.

18.3.9 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
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **spanning-tree forward-time** *seconds*	Configure the forward delay time, whose value range is 4-30s, 15s by default.
DES-7200(config)# **end**	Return to the privileged EXEC mode.
DES-7200# **show running-config**	Check the configuration entries.
DES-7200# **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.

18.3.10 Configuring Max-Age Time

The number of seconds a switch waits without receiving spanning-tree configuration messages before attempting a reconfiguration The default value is 20s.

In the privilege mode, perform these steps to configure the Max-Age Time:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **spanning-tree max-age** *seconds*	Configure the max age time, whose value range is 6-40s, 20s by default.
DES-7200(config)# **end**	Return to the privileged EXEC mode.
DES-7200# **show running-config**	Check the configuration entries.
DES-7200# **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** to set.

Caution

Each of Hello Time, Forward-Delay Time and Max-Age Time has a value range. There is constraint relationship between them: 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.

18.3.11 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
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(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.
DES-7200(config)# **end**	Return to the privileged EXEC mode.
DES-7200# **show running-config**	Check the configuration entries.
DES-7200# **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.

18.3.12 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 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
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** *interface-id*	Enter the interface configuration mode.
DES-7200(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.
DES-7200(config-if)# **end**	Return to the privileged EXEC mode.
DES-7200# **show running-config**	Check the configuration entries.
DES-7200# **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.

18.3.13 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
DES-7200# **clear spanning-tree detected-protocols**	Forcibly check versions of all the ports
DES-7200# **clear spanning-tree detected-protocols interface** *interface-id*	Execute the version check forcibly to a specific port.

18.3.14 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
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **spanning-tree mst configuration**	Enter the configuration mode.
DES-7200(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 transferred to the instance 0 automatically.
DES-7200(config-mst)# **name** *name*	Specify the MST configuration name, this string can present up to 32 bytes.
DES-7200(config-mst)# **revision** *version*	Specify the MST revision number, whose range is 0-65535. The default value is 0.
DES-7200(config-mst)# **show**	Check the MST configuration entries.
DES-7200(config-mst)# **end**	Return to the privileged EXEC mode.
DES-7200# **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:

```
DES-7200(config)# spanning-tree mst configuration
DES-7200(config-mst)# instance 1 vlan 10-20
DES-7200(config-mst)# name region1
DES-7200(config-mst)# revision 1
DES-7200(config-mst)# show
Multi spanning tree protocol : Enable Name [region1]
Revision 1
Instance Vlans Mapped
-------- ---------------------
0 1-9,21-4094
1 10-20
-------------------------------
DES-7200(config-mst)# exit
DES-7200(config)#
```

18.3.15 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**
DES-7200# **configure terminal**	Enter the global configuration mode.

DES-7200(config)# **spanning-tree max-hops** *hop-count*	Configure the Maximum-Hop Count, whose range is 1-40, 20 by default.
DES-7200(config)# **end**	Return to the privileged EXEC mode.
DES-7200# **show running-config**	Check the configuration entries.
DES-7200# **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.

18.4 Configuring Optional Features of MSTP

18.4.1 Default Setting of Optional Features for Spanning Tree

All the optional features are disabled by default.

18.4.2 Opening Port Fast

This port will execute the forwarding directly after the Port Fast is opened. However, the Port Fast operational state will be disabled for the BPDU is received, to participate in the STP algorithm and execute the forwarding normally.

In the privileged mode, perform these steps to configure the **Port Fast**:

Command	**Function**
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** *interface-id*	Enter the configuration mode of this interface, the legal interface contains the physical port and the Aggregate Link.
DES-7200(config-if)# **spanning-tree portfast**	Open the portfast of this interface.
DES-7200(config-if)# **end**	Return to the privileged EXEC mode.
DES-7200# **show spanning-tree interface** *interface-id* **portfast**	Check the configuration entries.
DES-7200# **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 open the portfast of all ports.

18.4.3 Enabling BPDU Guard

If the BPDU is received from this port, the opened BPDU guard will enter the error-disabled status.

In the privileged mode, perform these steps to configure the BPDU guard:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **spanning-tree portfast Bpduguard default**	Open the BPDU guard globally.
DES-7200(config)# **interface** *interface-id*	Enter the configuration mode of this interface, the legal interface contains the physical port and the Aggregate Link.
DES-7200(config-if)# **spanning-tree portfast**	Open the portfast of this interface.
DES-7200(config-if)# **end**	Return to the privileged EXEC mode.
DES-7200# **show running-config**	Check the configuration entries.
DES-7200# **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 open 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.

18.4.4 Enabling BPDU Filter

Corresponding port will not transmit or receive the BPDU after the BPDU filter is opened.

In the privilege mode, perform these steps to configure the BPDU Filter for the port:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **spanning-tree portfast bpdufilter default**	Open the BPDU filter globally.

DES-7200(config)# **interface** *Interface-id*	Enter he configuration mode of this interface, the legal interface contains the physical port and the Aggregate Link.
DES-7200(config-if)# **spanning-tree portfast**	Open the portfast of this interface.
DES-7200(config-if)# **end**	Return to the privileged EXEC mode.
DES-7200# **show running-config**	Check the configuration entries.
DES-7200# **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 close the BPDU guard.

18.4.5 Enabling Tc_Protection

In the privileged mode, perform these steps to configure tc_protection:

Command	**Function**
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **spanning-tree tc-protection**	Enable tc-protection
DES-7200(config)# **end**	Return to the privileged EXEC mode.
DES-7200# **show running-config**	Check the configuration entries.
DES-7200# **copy running-config startup-config**	Save the configuration.

To disable Tc_Protection, use the global configuration command **no spanning-tree tc-protection**.

18.5 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
DES-7200# **show spanning-tree**	Show parameter information of MSTP and topology information of the spanning tree
DES-7200# **show spanning-tree mst configuration**	Show the configuration information of the MST region.
DES-7200# **show spanning-tree mst** *instance-id*	Show the MSTP information of this instance.
DES-7200# **show spanning-tree mst** *instance-id* **interface** *interface-id*	Show the MSTP information of corresponding instance for specified interface.
DES-7200# **show spanning-tree interface** *interface-id*	Show the MSTP information of all instances for specified interface.
DES-7200# **show spanning-tree forward-time**	Show forward-time
DES-7200# **show spanning-tree Hello time**	Show Hello time
DES-7200# **show spanning-tree max-hops**	Show max-hops
DES-7200# **show spanning-tree tx-hold-count**	Show tx-hold-count
DES-7200# **show spanning-tree pathcost method**	Show pathcost method

19 Log Configuration

19.1 Overview

During the operation of a device, there are various state changes, such as the link status up/down, and various events occurring, such as receiving abnormal message and handling abnormities. DES-7200 log provides a mechanism to generate messages of fixed format (log message) in case of status change or event occurring. These messages can be displayed in related windows (console, VTY, etc.) 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 messages, these log messages can be labeled time stamps and serial numbers, and is graded according to the priority of log information.

19.1.1 Log Message Format

The format of the DES-7200 log message is as follows:

<priority> seq no timestamp sysname : %severity: description

They are: <priority> Sequential number timestamp device name severity – information type: contents

Priority value = Device value *8 + Severity

Example:

<190>0008 2005-05-08 09:26:15 R2690: %6: Reload requested by Administrator. Reload Reason :Reload command

Caution

The priority field is not attached to the log messages that are printed in the user window. It only appears in the log messages that are sent to the syslog server.

19.2 Log Configuration

19.2.1 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
DES-7200(config)# **logging on**	Turn on the log switch
DES-7200(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 many information printed, it is possible to reduce it by setting different displaying levels for device log information.

19.2.2 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 device. To configure a different displaying device for receiving logs, run the following commands in the global configuration mode or privileged user level:

Command	Function
DES-7200(config)# **logging buffered** [*buffer-size* | *level*]	Record log in memory buffer
DES-7200# **termninal monitor**	Allow log to be displayed on VTY window
DES-7200(config)# **logging** *host*	Send log information to the syslog sever in the network
DES-7200(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. DES-7200 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: filename command shows the contents of the log file in the flash.

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.

19.2.3 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
DES-7200(config)# **service timestamps** *message-type* [**uptime** | **datetime**]	Enable the timestamp in the log information
DES-7200(config)# **no service timestamps** *message-type*	Disable the timestamp in the log information

The timestamp are available in two formats: device uptime and device date. Select the type of timestamp as appropriate.

Message type: log or debug. The "log" type means the log information with severity levels 0-6. The "debug" type means that with severity level 7.

19.2.4 Turning on 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
DES-7200(config)# **no service** sequence-numbers	Delete sequential number in the log messages
DES-7200(config)# **service** *sequence-numbers*	Add sequential number in the log messages

19.2.5 Configuring the Log Information Displaying Level

To limit the number of log messages displayed on different devices, it is possible to set the severity level of log information that is 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
DES-7200(config)# **logging console** *level*	Set the level of log information that is allowed to be displayed on the console
DES-7200(config)# **logging monitor** *level*	Set the level of log information that is allowed to be displayed on the VTY window (such as telnet window)
DES-7200(config)# **logging buffered** [*buffer-size* | *level*]	Set the level of log information that is allowed to be recorded in memory buffer
DES-7200(config)# **logging file flash:***filename* [*max-file-size*] [*level*]	Set the level of log information that is allowed to be recorded in extended flash
DES-7200(config)# **logging trap** *level*	Set the level of log information that is allowed to be sent to syslog server

The log information of the DES-7200 is classified into the following 8 levels:

Level Keyword	Level	Description
Emergencies	0	Emergency case, system cannot run normally
Alerts	1	Problems that need immediate remedy
Critical	2	Critical conditions
Errors	3	Error message
Warnings	4	Alarm information
Notifications	5	Information that is normal but needs attention
informational	6	Descriptive information

Debugging	7	Debugging messages

Lower value indicates higher level. That is, level 0 indicates the information of the highest level.

When the level of log information that can be displayed is set for the specified device, the log information that is at or below the set level will be displayed. For example, after the command **logging console 6** is executed, all log information at or below level 6 will be displayed on the console.

By default, the log information that is allowed to be displayed on the console is at level 7.

By default, the log information that is allowed to be displayed on the VTY window is at level 7.

By default, the log information that is allowed to be sent to the syslog server is at level 6.

By default, the log information that is allowed to be recorded in the memory buffer is at level 7.

By default, the log information that is allowed to be recorded in the extended flash is at level 6.

The privileged command **show logging** can be used to show the level of log information allowed to be displayed on different devices.

19.2.6 Configure the log information device value

The device value is one of the parts that form the priority field in the messages 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
DES-7200(config)# **logging facility** *facility-type*	Configure the log information device value
DES-7200(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 the DES-7200 is 23.

19.2.7 Configuring the Source Address of Log Messages

By default, the source address of the log messages sent to the syslog server is the address of the port that sends the messages. It is possible to fix the source address for all log messages through commands.

It is possible to directly set the source IP address of the log messages or the remote port of the log messages.

To configure the source address of the log messages, run the following command in the global configuration mode:

Command	Function
DES-7200(config)# **logging source interface** *interface-type interface-number*	Configure the source port of log information
DES-7200(config)# **logging source ip** *A.B.C.D*	Configure the source IP address of log messages

19.2.8 Setting and Sending User Log

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
DES-7200(config)# **logging userinfo**	Set user login/logoff log.
DES-7200(config)# **logging userinfo command-log**	Send a log when a configuration command is executed

19.3 Log Monitoring

To monitor log information, run the following commands in the privileged user mode:

Command	Function
DES-7200# **show logging**	View the log messages in memory buffer as well as the statistical information of logs
DES-7200# **clear logging**	Clear the log messages in the memory buffer
DES-7200# **more flash:***filename*	View the log files in the extended flash

19.3.1 Examples of Log Configurations

Here is a typical example to enable the logging function:

```
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# ip address 192.168.200.42 255.255.255.0
DES-7200(config-if)# exit
DES-7200(config)# service sequence-numbers          //Enable sequence number
DES-7200(config)# service timestamps debug datetime //Enable debug information
                                                    timestamp, in date format
DES-7200(config)# service timestamps log datetime //Enable log information timestamp,
                                                    in date format
DES-7200(config)# logging 192.168.200.2             //Specify the syslog server address
logging trap debugging                              //The log information of all levels
                                                    will be sent to syslog server
DES-7200(config)# end
```

20 DHCP Overview

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.

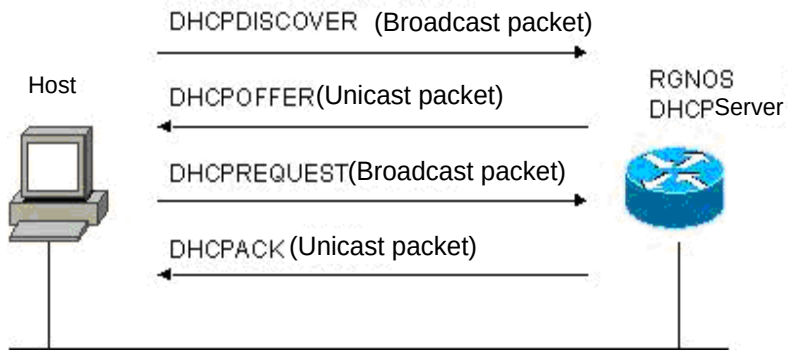
Among the three methods mentioned above, only dynamic assignment allows reuse of address that the client does not need any more.

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 DES-7200 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



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.

Use of the DHCP server of DES-7200 during network construction 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 current version of DES-7200 supports the DHCP client over Ethernet interface, FR, PPP and HDLC interfaces. 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 (compulsory)
- Configuring DHCP Excluded Addresses (compulsory)
- Configuring DHCP Address Pool (compulsory)
- Binding Address Manually (optional)
- Configuring Client Boot File (optional)
- Configuring Number of Packet Ping Operations (optional)
- Configuring Packet Ping Timeout (optional)

- Configuring DHCP Client over Ethernet Interface (optional)

20.5.1 Enabling DHCP Server and Relay Agent

In the firmware v10.1, the DHCP server and the DHCP relay share the service dhcp command by default. However, these two functions are mutually exclusive. Switching of these two functions depends on whether a DHCP address pool has been configured. To enable the DHCP server and the relay agent, execute the following commands in the global configuration mode:

Command	Function
DES-7200(config)# **service dhcp**	Enable the DHCP server and the DHCP relay agent
DES-7200(config)# **no service dhcp**	Disable the DHCP server and the relay agent

Note

The products prior to firmware v10.1 do not support all the servers and relays. In these systems, therefore, the **service dhcp** command is degraded to be used for opening the relays or servers supported by the current product.

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
DES-7200(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
DES-7200(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 Configuring 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. The DES-7200 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
DES-7200(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 “DES-7200(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
DES-7200(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
DES-7200(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, it cannot use this address when the lease period expires.

To configure the address lease period, execute the following commands in the address pool configuration mode:

Command	Function
DES-7200(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
DES-7200(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
DES-7200(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
DES-7200(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
DES-7200(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
DES-7200(dhcp-config)# **network** *network-number mask*	Configure the network number and mask for the DHCP address pool

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
DES-7200(config)# **ip dhcp pool** *name*	Define the name of address pool and enter the DHCP configuration mode
DES-7200(dhcp-config)# **host** *address*	Define an IP address for the client
DES-7200(dhcp-config)# **hardware-address** *hardware-address type* DES-7200(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
DES-7200(dhcp-config)# **client-name** *name*	(Optional) Define the client name using standard ASCII characters. Don't include domain name in the client name.

20.5.14 Configuring Number of Packet Ping Operations

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
DES-7200(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
DES-7200(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

The DES-7200 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
DES-7200(config-if)# **ip address dhcp**	Configure as obtaining an IP address using DHCP

20.5.17 Configuring DHCP Client on PPP Encapsulated Link

The DES-7200 supports the PPP-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
DES-7200(config-if)# **ip address dhcp**	Configure as obtaining an IP address using DHCP

20.5.18 Configuring DHCP Client on FR Encapsulated Link

The DES-7200 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
DES-7200(config-if)# **ip address dhcp**	Configure as obtaining an IP address using DHCP

20.5.19 Configuring DHCP Client on HDLC Encapsulated Link

The DES-7200 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
DES-7200(config-if)# **ip address dhcp**	Configure as obtaining an IP address using DHCP

Note

In some products of firmware v10.1, the client supports to obtain an IP address on the point-to-point connection encapsulated by PPP, HDLC, and FR using 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.

DES-7200 provides three clear commands. To clear information, execute the following commands in the command execution mode:

Command	Function
DES-7200# **clear ip dhcp binding** { *address* | ***** }	Clear DHCP address binding information
DES-7200# **clear ip dhcp conflict** { *address* | *}	Clear DHCP address conflict information
DES-7200# **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
DES-7200# **debug ip dhcp server**	Debug the DHCP server

To show the working status of the DHCP server, execute the following commands in the command execution mode:

Command	Function
DES-7200# **show ip dhcp binding** [*address*]	Show DHCP address binding information
DES-7200# **show ip dhcp conflict**	Show DHCP address conflict information
DES-7200# **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
DES-7200# **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
DES-7200# **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 dlink.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 dlink.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.dlink.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 dlink.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 DNS Configuration

21.1 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 from the host name to the IP address: 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 to improve the query efficiency. Furthermore, the DNS adopts the hierarchy structure.

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 DES-7200 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.

21.2 Configuring Domain Name Resolution

21.2.1 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
Status Host List	Void
Maximum number of DNS servers	6

21.2.2 Enabling DNS Resolution Service

This section describes how to enable the DNS resolution service.

Command	Function
DES-7200(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.

```
DES-7200(config)# ip domain-lookup
```

21.2.3 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
DES-7200(config)# **ip name-server** *ip-address*	Add the IP address of the DNS Server. The switch will add a DNS Server when thisCommand is executed every time. If the domain name can't be obtained from the first Server, the switch 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.

21.2.4 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
DES-7200(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.

21.2.5 Clearing Buffer Table of Dynamic Host Names

This section describes how to clear the buffer table of dynamic host names. If the command **clear host** or **clear host** * is entered, the dynamic buffer table will be cleared. Otherwise, only the entries of specified domain names will be cleared.

Command	Function
DES-7200# **clear host** [*word*]	Clear the buffer table of dynamic host names. The host names configured statically will not be removed.

21.2.6 Showing Domain Name Resolution Information

This section describes how to display relevant configuration information of DNS.

Command	Function
DES-7200# **show hosts**	View related parameters of the DNS.

```
DES-7200# 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
```

21.2.7 Application examples

Ping the host with specified domain name:

```
DES-7200# 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
```

22 NTP Configuration

22.1 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.

22.2 Configuring NTP

This chapter describes how to configure the NTP client in the system implementation.

- Configuring Global Security Authentication Mechanism for the NTP
- Configuring the NTP to synchronize with server
- Disabling NTP Function

22.2.1 Configuring Global Security Authentication Mechanism for the NTP

The NTP client of DES-7200 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 message is verified by the trusted key, which is specified by the command **ntp authentication-key** or **ntp trusted-key**.

22.2.2 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.

The current version in DES-7200 can support the authentication key up to 1024 and only one key can be set for each server for secure communication.

22.2.3 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*	Specify 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.

22.2.4 Configuring NTP Server

No NTP server is configured by default. DES-7200'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. *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.

22.2.5 Disabling receiving NTP Messages 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.

22.2.6 Enabling/Disabling NTP

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.

22.2.7 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.

DES-7200 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.

22.3 Display of NTP Information

22.3.1 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.

22.3.2 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.

22.4 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 DES-7200 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.

```
DES-7200(config)# no ntp
DES-7200(config)# ntp authentication-key 6 md5 wooooop
DES-7200(config)# ntp authenticate
DES-7200(config)# ntp trusted-key 6
DES-7200(config)# ntp server 192.168.210.222 key 6
DES-7200(config)# ntp synchronize
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# ntp disable
DES-7200(config-if)# no ntp disable
```

23 UDP-Helper Configuration

23.1 UDP-Helper Configuration

23.1.1 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 acts like a relay.

When the UDP-Helper is used, the destination UDP port number of received broadcast messages will be identified. If this number matches the port number to be forwarded, the destination IP address of messages 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 messages from 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.

23.2 Configuring UDP-Helper

23.2.1 Default Configuration of UDP-Helper

Table 23-1 Default Configuration of UDP-Helper

Attribute	Default value
Function of relay and forwarding	Off
UDP port for relay and forwarding	When enabling the UDP-Helper, the UDP broadcast messages from Ports 69, 53, 37, 137, 138 and 49 are relayed and forwarded by default.
Destination Server for delay and forward	None

23.2.2 Enable the Function of Relay and Forward for UDP-Helper

Command	Function
DES-7200(config)# **udp-helper enable**	TheCommand **udp-helper enable** is used to enable the function of relay and forward for UDP broadcast message. This function is disabled by default.

The command **no udp-helper enable** is used to disable the function of relay and forward 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 messages, the broadcast messages from 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.

23.2.3 Configuring Destination Server for Relay and Forward

Command	Function
DES-7200(config-if)# **ip helper-address** *192.168.100.1*	Configure the destination server to which the UDP broadcast messages are relayed and forwarded. By default, it is not configured.

The command **no ip helper-address** can be used to remove the destination server for relay and forward.

Note

1. At most 20 destination servers can be configured for an interface.
2. If the destination server for relay and forward 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.

23.2.4 Configuring UDP Port Requiring Relay and Forward

Command	Function
DES-7200(config)# **ip forward-protocol udp** *134*	Configure the UDP port requiring delay and forward. 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 messages from 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 forward.

Note

- Only when the function of delay and forward 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 delay and forward is enabled, the function of forwarding the broadcast UDP messages 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 forward are supported by the switch.
- Two ways can be used to configure the default ports, for example, the commands **ip forward-protocol udp domain** and **ip forward-protocol udp** *53* do the same thing.

24 Configuring SNMP

24.1 SNMP Related Information

24.1.1 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-server mode, including three parts as follows:

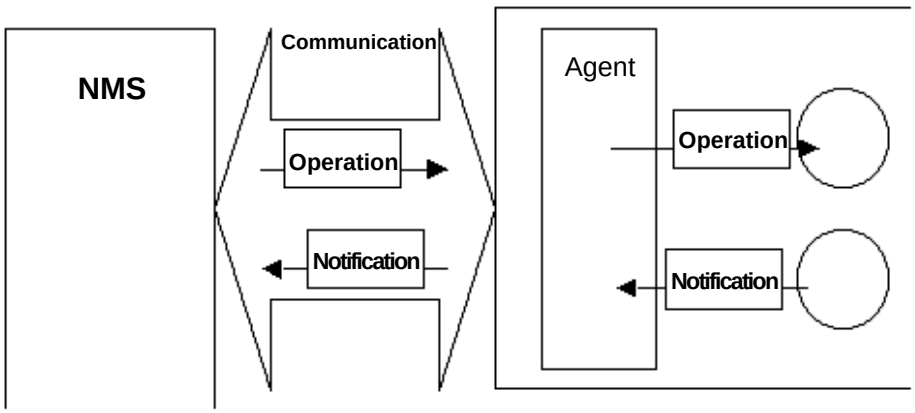
- SNMP network manager
- SNMP agent
- MIB (management information base)

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. DES-7200 has developed a suit of software (Star View) for network management against 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.

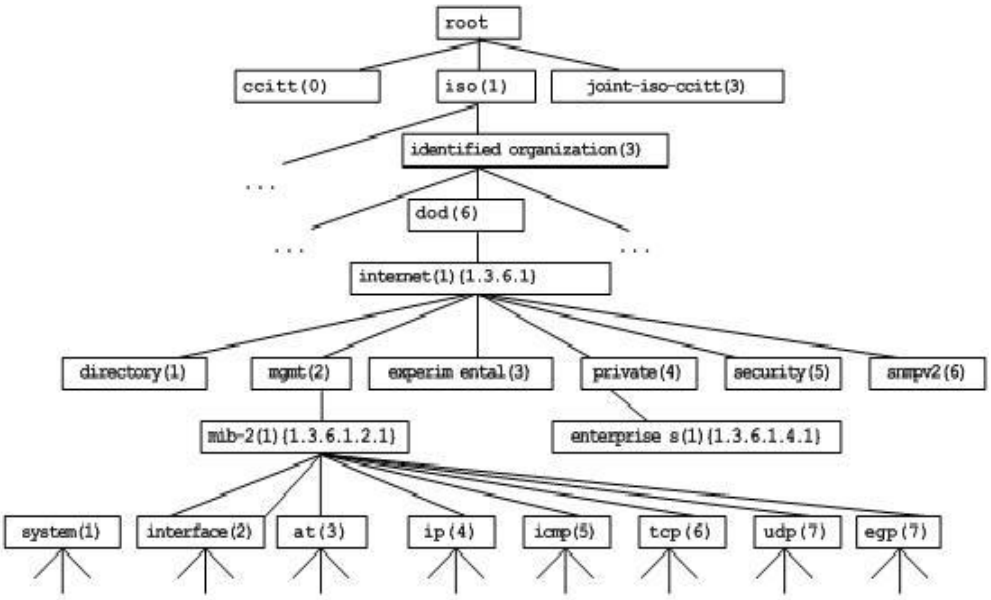
The relation of the NMS and Agent can be indicated as follows:

Figure 24-1 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 24-2 MIB tree hierarchy



24.1.2 SNMP 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 come from a valid data source.
  3. Encrypting packets to ensure the data confidentiality.

Both the SNMPv1 and SNMPv2C use 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 retrieval 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-handling 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.

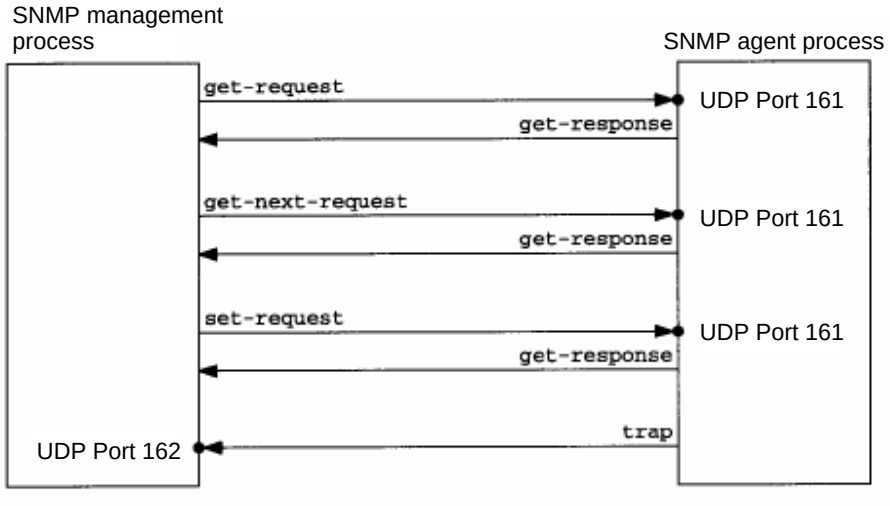
24.1.3 SNMP Management Operations

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 messages are sent from the NMS to the Agent, and the last two messages 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 24-3 Message 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.

24.1.4 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 access 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.

Model	Level	Authentication	Encryption	Description
SNMPv1	noAuthNoPriv	Community string	None	Insures the data confidentiality through Community string.
SNMPv2c	noAuthNoPriv	Community string	None	Insures the data confidentiality through Community string.
SNMPv3	noAuthNoPriv	User Name	None	Insures 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.
SNMPv2c	noAuthNoPriv	Community string	None	Insures the data confidentiality through Community string.
SNMPv3	noAuthNoPriv	User Name	None	Insures 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.

24.1.5 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 and unambiguous identifier named SNMP Engine ID.

SNMP Engine ID is an OCTET STRING (5~32 octets), defined in RFC3411:

- The first four octets are assigned with the private enterprise number in HEX by IANA.
- The fifth octet indicates how the rest (6th and following octets) are formatted.

  0: Reserved

  1: The following 4 octets are for IPv4 address

  2: The following 16 octets are for IPv6 address

  3: The following 6 octets are for MAC address

  4: Texts, assigned by product providers, 27 octets at most

  5: Hexadecimal number, assigned by product providers, 27 octets at most

6-127: Reserved

128-255: Special Form assigned by product providers

24.2 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.

24.2.1 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 messages without matched 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 rights 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
DES-7200(config)# **snmp-server community** *string* [**view** *view-name*] [**ro** | **rw**] **[host** *host-ip*]	Set the community string and the access.

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 access. To remove the community name and its access authority, run the command **no snmp-server community** in the global mode.

24.2.2 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
DES-7200(config)# **snmp-server view** *view-name oid-tree* {**include | exclude**}	Create an MIB view to including or excluding associated MIB objects.
DES-7200(config)# **snmp-server group** *groupname* {**v1** | **v2c** |**v3** {**auth** | **noauth** | **priv**}} [**read** *readview*] [**write** *writeview*]	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 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.

24.2.3 Configuring SNMP Users

You can implement the security management through the security model, first you shall configure user information. Only valid users of NMS can communicate with the SNMP agent on the switch.

For the SNMPv3 users, specify the safety 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
DES-7200(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.

24.2.4 Configuring SNMP Host Address

In special cases, Agent may also proactively send messages to NMS. To configure NMS host address that the Agent proactively sends messages to, execute the following commands in the global configuration mode:

Command	Function
DES-7200(config)# **snmp-server host *host-addr* traps {version {1|2c |3 [auth | noauth | priv]}** *community-string* [*type*]	Set the address of SNMP host, message type, community string (user name in SNMPv3) and safety level (supported only be SNMPv3).

24.2.5 Configuring SNMP Agent Parameters

You can configure the basic agent parameters for SNMP, including the contact 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
DES-7200(config)# **snmp-server contact** *text*	Configure the contact of the system
DES-7200(config)# **snmp-server location** *text*	Configure the location of the system
DES-7200(config)# **snmp-server chassis-id** *number*	Configure the sequential number of the system

24.2.6 Defining Maximum Message Length of SNMP Agent

In order to enhance network performance, user can configure the maximum size of packet allowed by SNMP agent. Run the following command in the global configuration mode:

Command	Function
DES-7200(config)# **snmp-server packetsize** *byte-count*	Set the maximum size of packet allowed by SNMP agent.

24.2.7 Shielding SNMP Agent

The SNMP agent service is a service provided by the DES-7200 and can be enabled or disabled at any time. To disable it, run the following command in the global configuration mode:

Command	Function
DES-7200(config)# **no snmp-server**	Disable the SNMP agent service.

24.2.8 Disable SNMP Agent

DES-7200 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
DES-7200(config)# **no enable service snmp-agent**	Disable the SNMP agent service.

24.2.9 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 critical 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
DES-7200(config)# **snmp-server enable traps** [*type*] [*option*]	Allow Agent to sent trap proactively.
DES-7200(config)# **no snmp-server enable traps** [*type*] [*option*]	Forbid Agent to sent trap proactively.

24.2.10 Configuring 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 and the Link status of the interface changes, the SNMP will send the LinkTrap. Otherwise, it will not.By default, this function is enabled.

Command	Function
DES-7200(config)# **interface** *interface-id*	Enter the interface configuration mode.
DES-7200(config-if)# **no snmp-server enable traps** [*type*] [*option*]	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.

```
DES-7200(config)# interface gigabitEthernet 1/1
DES-7200(config-if)#no snmp trap link-status
```

24.2.11 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
DES-7200(config)# **snmp-server trap-source** *interface*	Specify the source port for sending Trap messages.
DES-7200(config)# **snmp-server** queue-length *length*	Specify the length of each Trap message queue.
DES-7200(config)# **snmp-server** trap-timeout *seconds*	Specify the interval for sending Trap messages.

24.3 SNMP Monitoring and Maintenance

24.3.1 Checking Current SNMP Status

To monitor the SNMP status and troubleshoot SNMP configurations, the DES-7200 has monitoring commands for SNMP, with which it is possible to easily check the SNMP status of the current network device. In the privileged user mode, execute **show snmp** to check the current SNMP status.

```
DES-7200# 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 message
Get-next PDUs	Get-next message
Set-request PDUs	Set-request message
Too big errors (Maximum packet size 1500)	Too large response message
No such name errors	Not in the specified managed unit
Bad values errors	Wrong value type specified
General errors	General error
Get-response PDUs	Get-response message
SNMP trap PDUs	SNMP trap message

24.3.2 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:

```
DES-7200# 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
```

24.3.3 Viewing SNMP User

To view the SNMP users configured on the current agent, run the command **show snmp user** in the privileged user mode:

```
DES-7200# 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
```

24.3.4 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:

```
DES-7200# 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:

```
DES-7200# show snmp view
default(include) 1.3.6.1
test-view(include) 1.3.6.1.2.1
```

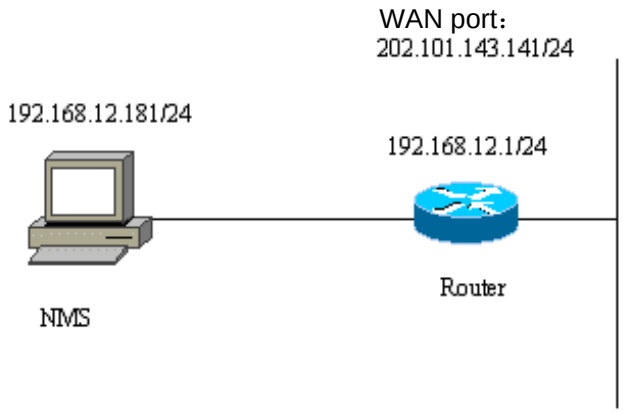
24.4 SNMP Configuration Example

24.4.1 Typical 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 24-4 Typical Networking Diagram of SNMP



■ **Detailed configuration of the router**

Enable the SNMP agent service:

```
DES-7200(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 router, and then the NMS can monitor the SNMP for the router. However, just read-only access is configured; the NMS can not modify the router's configuration but monitor its running. Other configurations are optional.

If the read-write access is required, it can be configured as follows:

```
DES-7200(config)# snmp-server community private RW
```

Followings are basic agent parameters to configure the SNMP of router. The NMS can get basic system information of the router via these parameters. This configuration is optional:

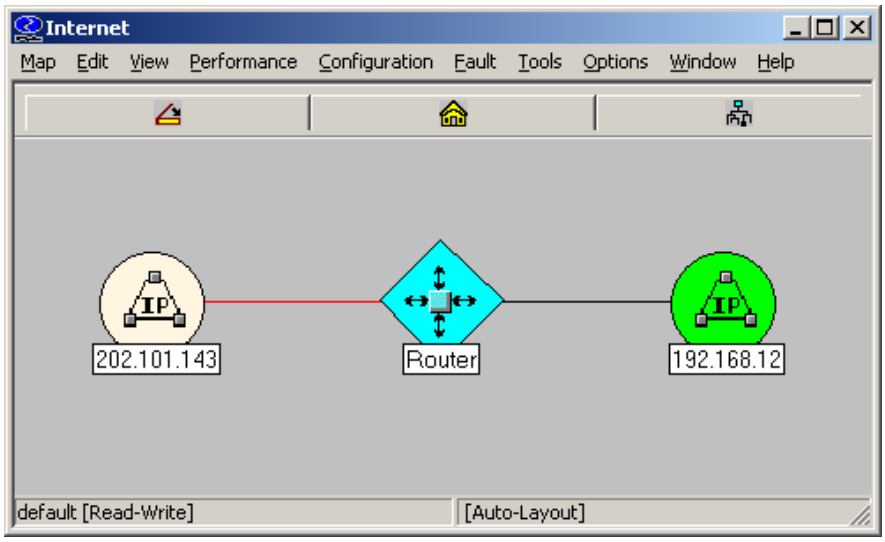
```
DES-7200(config)# snmp-server location fuzhou
DES-7200(config)# snmp-server contact wugb@i-net.com.cn
DES-7200(config)# snmp-server chassis-id 1234567890
0987654321
```

The following configuration is optional; the router is allowed to send some Trap messages to the NMS proactively.

```
DES-7200(config)# snmp-server enable traps
DES-7200(config)# snmp-server host 192.168.12.181 public
```

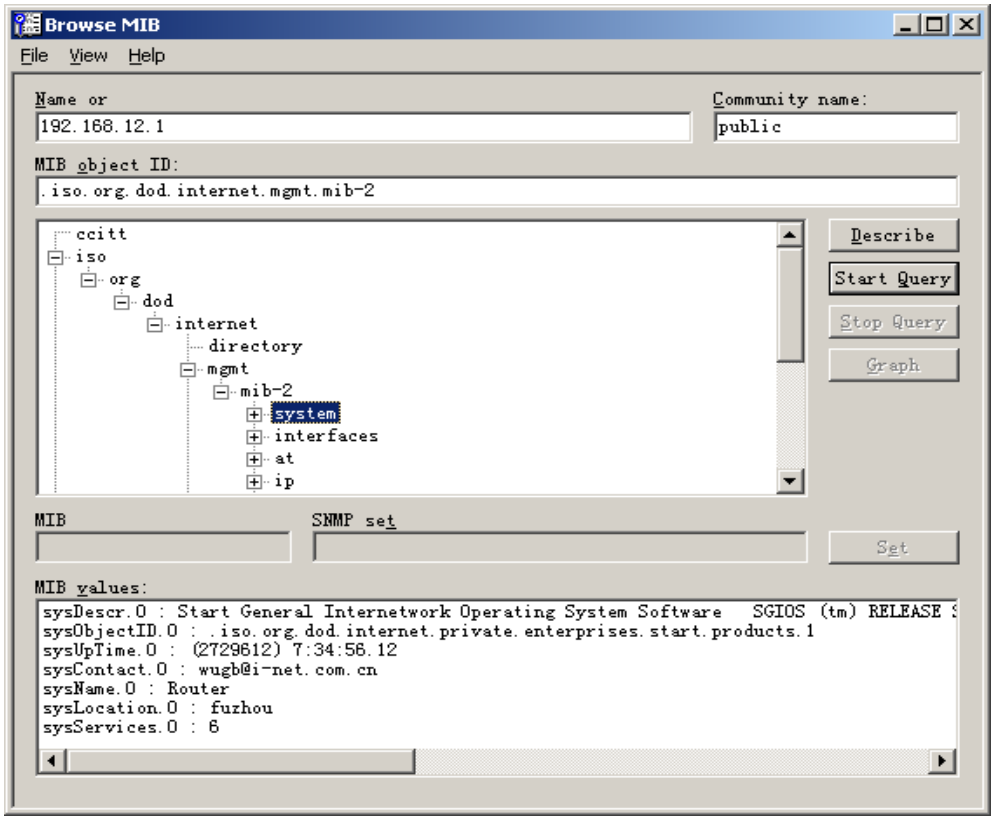
The SNMP agent is configured for the router by the above configuration. Then, the NMS can monitor and manage the router. Take HP OpenView as an example and a network topology is coming into being as follows:

Figure 24-5 Network topology diagram



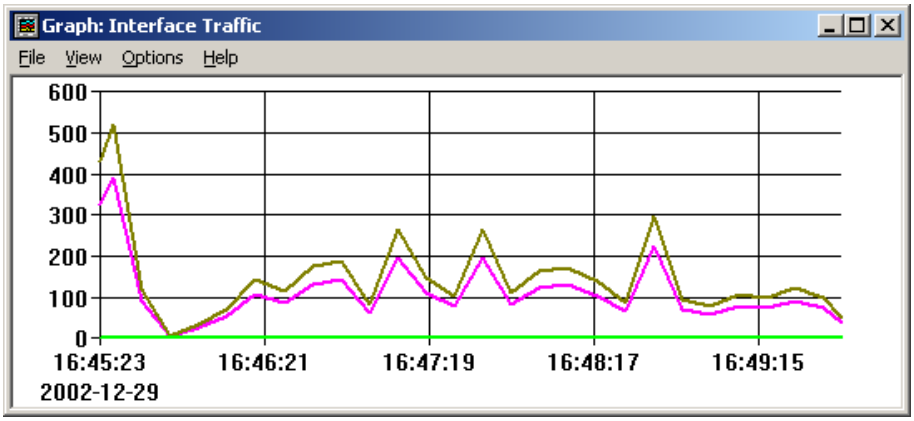
Now it is possible to query or set the managed units in the network device. Click the TOOL->SNMP MIB Brower menu on the HP OpenView to display the following dialog box. Enter the IP address 192.168.12.1 in the Name field and "public" in the Community Name field. Select the specific managed unit of the 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 24-6 Interface of MIB query



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 24-7 Statistics graph of interface traffic



24.4.2 Example of SNMP Access List Association Control

DES-7200 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:

```
DES-7200(config)# access-list 1 permit 192.168.12.181
DES-7200(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.

24.4.3 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.

```
DES-7200(config)# snmp-server view v3userview 1.3.6.1.2.1 include
DES-7200(config)# snmp-server group v3usergroup v3 priv read v3userview write v3userview
```

```
DES-7200(config)# snmp-server user v3user v3usergroup v3 auth md5 md5-auth priv des56
des-priv
DES-7200(config)# snmp-server host 192.168.65.199 traps version 3 priv v3user
```

25 Configuring RMON

25.1 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.

25.1.1 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.

25.1.2 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.

25.1.3 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.

25.1.4 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.

25.2 List of RMON Configuration Tasks

25.2.1 Configuring Statistics

One of these commands can be used to add a statistic entry.

Command	Function
DES-7200(config-if)# **rmon collection stats** *index* [**owner** *ownername*]	Add a statistic entry.
DES-7200(config-if)# **no rmon collection stats** *index*	Remove a statistic entry.

The current version of DES-7200 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.

25.2.2 Configuring History Control

One of these commands can be used to add an entry for history control.

Command	Function
DES-7200(config-if)# **rmon collection history** *index* [**owner** *ownername*] [**buckets** *bucket-number*] [**interval** *seconds*]	Add an entry of history control.
DES-7200(config-if)# **no rmon collection history** ***i****ndex*	Remove an entry of history control.

The current version of DES-7200 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.

25.2.3 Configuring Alarm and Event

One of these command can be used to configure the alarm form:

Command	Function
DES-7200(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.
DES-7200(config)# **rmon event** *number* [**log**] [**trap** *community*] [*description-string*]	Add an entry of Event.
DES-7200(config)# **no rmon alarm** *number*	Remove an alarm.
DES-7200(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 -2147483647.

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.

25.2.4 Showing RMON status

Command	Function
DES-7200(config)# **show rmon alarms**	Show the Alarm
DES-7200(config)# **show rmon events**	Show the Event
DES-7200(config)# **show rmon history**	Show the History
DES-7200(config)# **show rmon statistics**	Show the Statistics

25.3 RMON Configuration Examples

25.3.1 Example of Configuring Statistics

If you want to get the statistics of Ethernet Port 3 , use the following commands:

```
DES-7200(config)# interface gigabitEthernet 0/3
DES-7200(config-if)# rmon collection stats 1 owner zhangsan
```

25.3.2 Example of Configuring History

Use the following commands if you want to get the statistics of Ethernet Port 3 every 10 minutes:

```
DES-7200(config)# interface gigabitEthernet 0/3
DES-7200(config-if)# rmon collection history 1 owner zhangsan interval 600
```

25.3.3 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”.

```
DES-7200(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
DES-7200(config)# rmon event 1 log trap rmon description "ifInNUcastPkts is too much "
owner zhangsan
```

25.3.4 Example of Showing rmon Status

25.3.4.1 show rmon alarms

```
DES-7200# 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
```

25.3.4.2 show rmon events

```
DES-7200# 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
```

25.3.4.3 show rmon history

```
DES-7200# 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
```

25.3.4.4 show rmon statistics

```
DES-7200# 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
```

26 RIP Routing Protocol Configuration

26.1 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 240 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 router 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 DES-7200 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.

26.2 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 summary (optional)
- Configuring RIP Authentication (optional)
- Adjusting the RIP Timer (optional)
- Configuring the RIP Route Source Address Validation (optional)

For the following topics, see the *IP Routing "Protocol Independent" Feature Configuration* chapter.

- Filtering the RIP route information
- VLSMs (for RIPv2)

26.2.1 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
DES-7200(config)# **router rip**	Create the RIP routing process
DES-7200(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.

26.2.2 Configuring 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 advertisement via unicast for the RIP, execute the following commands in the RIP routing process configuration mode:

Command	Function
DES-7200(conf-router)# **neighbor** *ip-address*	Configure the packet unicast for the RIP

By using this command, you can also control which port is allowed to advertise the RIP route update packets, restrict a port from advertising 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, 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.

26.2.3 Configuring Split Horizon

When multiple routers 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
DES-7200(config-if)# **no ip split-horizon**	Disable split horizon
DES-7200(config-if)# **ip split-horizon**	Enable split horizon

For frame relay encapsulation, the port has split horizon disabled by default. For frame relay sub-interface and X.25 encapsulation, split horizon is enabled by default. Encapsulation of all other types has split horizon enabled. Therefore, you must pay attention to the use of split horizon in practice.

26.2.4 Defining the RIP Version

The DES-7200 supports RIP version 1 and version 2, where RIPv2 supports authentication, key management, route summary, CIDR and VLSMs. For the information about the key management and VLSMs, see the *IP Routing "Protocol Independent" Feature Configuration* chapter.

By default, the DES-7200 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 to receive and send the packets of a particular version, execute the following commands in the routing process configuration mode:

Command	Function
DES-7200(config-router)# **version** {**1** | **2**}	Defining the RIP Version

The following 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 particular version, execute the following commands in the interface configuration mode:

Command	Function
DES-7200(config-if)# **ip rip send version 1**	Specify to send the packets of only RIPv1
DES-7200(config-if)# **ip rip send version 2**	Specify to send the packets of only RIPv2
DES-7200(config-if)# **ip rip send version 1 2**	Specify to send the packets of RIPv1 and RIPv2

To configure a port to receive the packets of only a particular version, execute the following commands in the interface configuration mode:

Command	Function
DES-7200(config-if)# **ip rip receive version 1**	Specify to receive the packets of only RIPv1
DES-7200(config-if)# **ip rip receive version 2**	Specify to receive the packets of only RIPv2
DES-7200(config-if)# **ip rip receive version 1 2**	Specify to receive the packets of RIPv1 and RIPv2

26.2.5 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
DES-7200(config-router)# **no auto-summary**	Disable automatic route summary
DES-7200(config-router)# **auto-summary**	Enable automatic route summary

26.2.6 Configuring RIP Authentication

The RIPv1 does not support authentication. If the router 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.

DES-7200 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
DES-7200(config-if)# **ip rip authentication key-chain** *key-chain-name*	Apply the key chain and enable RIP authentication
DES-7200(config-if)# **ip rip authentication mode** {**text** | **md5**}	Configure the RIP authentication for the interface Mode: plain-text or MD5

For the configuration management of the key chain, see the "Key Authentication Management" section in *IP Routing "Protocol Independent" Feature Configuration*.

26.2.7 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
DES-7200(config-router)# **timers basci 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 240 seconds.

Note

The routers connected in the same network must have the same RIP timers.

26.2.8 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
DES-7200(config-router)# **no validate-update-source**	Disable source address validation
DES-7200(config-router)# **validate-update-source**	Enable source address validation

26.3 RIP Configuration Examples

This section provides three RIP configuration examples:

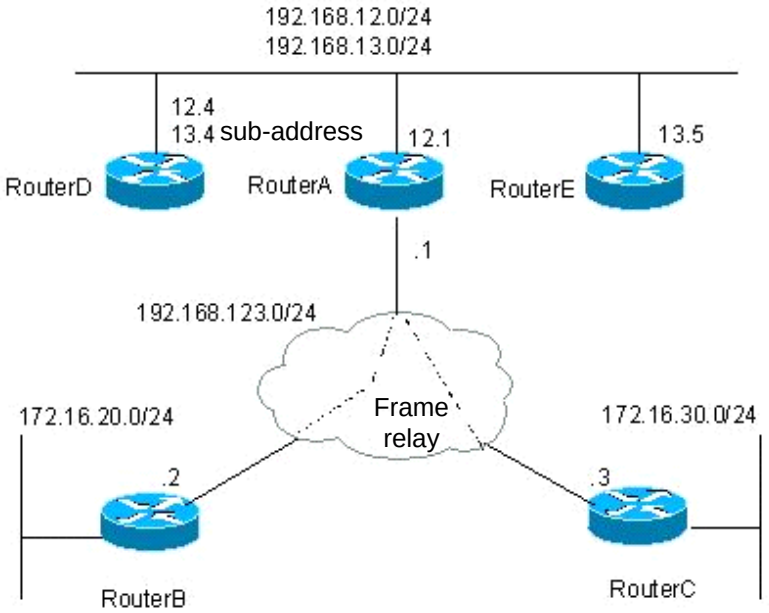
- Example of Configuring Split Horizon
- Example of configuring RIP unicast update packets

26.3.1 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 26-1 shows IP address distribution and equipment connection, where RouterD is configured with a sub-address.

Figure 26-1 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 interface

```
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 interface

```
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 interface

```
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 interface

```
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 interface

```
interface FastEthernet0/0
ip address 192.168.13.5 255.255.255.0
```

Configuring RIP route protocol

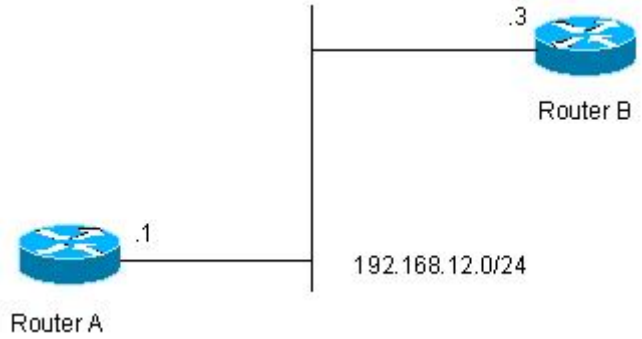
```
router rip
version 2
network 192.168.13.0
```

26.3.2 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 26-2 .

Figure 26-2 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 infinite
send-lifetime 00:00:00 Dec 4 2000 infinite
key 2
```

```
key-string keyb
accept-lifetime 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 keya
accept-lifetime infinite
send-lifetime 00:00:00 Dec 4 2000 00:00:00 Dec 5 2000
key 2
key-string keyb
accept-lifetime infinite
send-lifetime 00:00:00 Dec 4 2000 infinite
```

Configuring Ethernet interface

```
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

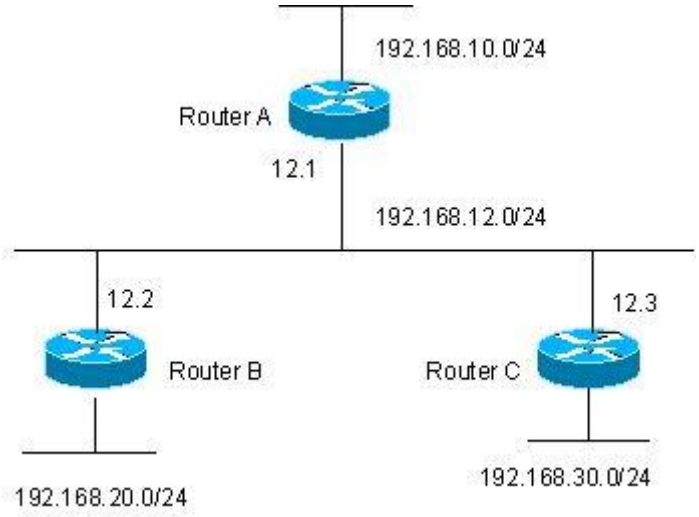
```
router rip
version 2
network 192.168.12.0
```

26.3.3 Example of Configuring Packet Unicast for the RIP

- **Configuration requirements:**

All the three routers are connected on the LAN, and all run the RIP routing protocol. Figure 26-3 shows the IP address allocation and connection of the equipment.

Figure 26-3 Example of Configuring Packet Unicast for the RIP



Following are to be implemented via the configuration of RIP message 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 interface

```
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
```

27 OSPF Routing Protocol Configuration

27.1 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 router will generate the link status notification, in which includes all link statuses of this router.
- All routers switch the link status information in the multicast way, and each of the routers 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 router 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 still. If any changes occur on the network, the OSPF advertises the changes via the link status, but only the changed ones. The routers involved in the changes will have the Dijkstra algorithm run again, with a new shortest path tree created.

A group of routers 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 routers 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 router belong at least to two areas, one of which must be the backbone area;
3. ASBR (Autonomous System Boundary Routers): It is the router between which the OSPF route domain exchanges the external route domain.

- The DES-7200 implements the OSPF by fully complying with the OSPF v2 defined in RFC 2328. The main features of the OSPF implemented by the DES-7200 are described as below:
- Stub area——The definition of the sub area is fully supported;
- Route redistribution——Redistribution to the RIP route protocol is 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;
- Currently, DES-7200 does not support the following function, but will support them in future versions;
- OSPF line on-demand support, as defined in RFC 1793

27.2 OSPF Configuration Task List

The configuration of OSPF should be cooperated with various routers (including internal routers, 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, packets both sent and received do not need authentication, and the interface does not belong to any area of the autonomous system. When you change the default parameters, you must ensure that the routers 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: No authentication. Authentication password: No password specified.
Area	Authentication type : No authentication. Default metric 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 automatically; Default automatic cost is 100Mbps
Default route generation	Disable 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: Inter-area route information: External route information:
Database filter	Disabled. All interfaces can receive the status update message.
Neighbor change log	Enable
Neighbor	None
Neighbor database filter Disabled.	All outgoing LSAs are sent to the neighbor.
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 5 seconds The least interval between two calculating operations: 10 seconds
Optimal path rule used to calculate the external routes	Using the rules defined in RFC1583

27.2.1 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 advertises the link status of the interface to the outside. Currently, we support one OSPF routing process.

To create the OSPF routing process, you can perform the following steps:

Command	Meaning
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **ip routing**	Enable the IP routing (if disabled)
DES-7200(config)# **router ospf 1**	Enable OSPF and enter OSPF route configuration mode.
DES-7200(config-router)# **network** *address wildcard-mask* **area** *area-id*	Define an IP address range for an area.
DES-7200(config-router)# **End**	Return to the privileged EXEC mode.
DES-7200# **show ip protocol**	Display the routing protocol that is running currently.
DES-7200# **write**	Save the configuration.

Note

In the Network command, the 32 “bit wildcards” have the values contrary to the masks, where “1” means that the bit will not be compared, and “0” means that the bit will be compared. However, if it is defined by using the mask, the DES-7200 will also be automatically translated into the bit wildcard. As long as the interface address matches the IP address range defined by the Network command, the interface belongs to the specified area.

To disable the OSPF protocol, use the **no router ospf** [*process-id*]command. The example shows how to start the OSPF protocol:

```
DES-7200(config)# router ospf 1
DES-7200(config-router)# network 192.168.0.0 255.255.255.0 area 0
```

```
DES-7200(config-router)# end
```

27.2.2 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
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **ip routing**	Enable the IP routing (if disabled)
DES-7200(config)# **interface** *[interface-id]*	Enter the interface configuration mode.
DES-7200(config-if)# **ip ospf cost** *cost-value*	(Optional) Define the interface cost
DES-7200(config)# **ip routing retransmit-interval** *seconds*	(Optional) Set the link status retransmission interval;
DES-7200(config)# **ip routing transmit-delay** *seconds*	(Optional) Set the transmit delay for the link status update packets;
DES-7200(config)# **ip routing hello-interval** *seconds*	(Optional) Set the hello packet send interval, which must be the same for all the nodes of the entire network;
DES-7200(config)# **ip routing dead-interval** *seconds*	(Optional) Set the dead interval for the adjacent router, which must be the same for all the nodes of the entire network;
DES-7200(config)# **ip routing priority** *number*	(Optional) The priority is used to select the dispatched routers (DR) and backup dispatched routers (BDR).
DES-7200(config)# **ip routing authentication [message-digest | null]**	(Optional) Set the authentication type on the network interface.
DES-7200(config)# **ip routing authentication-key** *key*	(Optional) Configure the key for text authentication of the interface

DES-7200(config-if)#**ip ospf message-digest-key** *keyid* **md5** *key*	(Optional) Configure the key for MD5 authentication of the interface
DES-7200(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.
DES-7200(config-if)#**End**	Return to the privileged EXEC mode.
DES-7200#**show ip ospf** [*process-id*] **interface** [*interface-id*]	Display the routing protocol that is running currently.
DES-7200# **write**	(Optional) Save the configuration.

You can use the **no** form of the above commands to cancel or restore the configuration to the default.

27.2.3 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 Non-broadcast Multi-access (NBMA) network. The NBMA requires direct communication all routers interconnected. Only fully meshed network 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, without needing to configure the neighbors, neither election of the designated router;
- Small cost, without needing the fully meshed topology

To configure the network type, execute the following commands in the interface configuration mode:

Command	Function
DES-7200(config-if)# **ip ospf network {broadcast | non-broadcast | {point-to-multipoint [non-broadcast]}| point-to-point }**	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 abnormality will occur, for instance, the neighbor is Full and the calculation of the routing is incorrect.

27.2.3.2 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 sees 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
DES-7200(config-if)# **ip ospf network point-to-multipoint**	Configure the point-to-multipoint network type for an interface
DES-7200(config-if)# **exit**	Exit to the global configuration mode
DES-7200(config)# **router ospf 1**	Enter the routing process configuration mode
DES-7200(config-router)# **neighbor** *ip-address* **cost** *cost*	Specify the cost of the neighbor (optional)

Note

Although the OSPF point-to-point 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.

27.2.3.3 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
DES-7200(config-if)# **ip ospf network non-broadcast**	Specify the network type of the interface to be the NBMA type
DES-7200(config-if)# **exit**	Exit to the global configuration mode
DES-7200(config)# **router ospf 1**	Enter the routing process configuration mode

DES-7200(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**
DES-7200(config-if)# **ip ospf point-to-multipoint non-broadcast**	Specify the network type of the interface to be the point-to-multipoint non-broadcast type
DES-7200(config-if)# **exit**	Exit to the global configuration mode
DES-7200(config)# **router ospf 1**	Enter the routing process configuration mode
DES-7200(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.

27.2.3.4 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
DES-7200(config-if)# **ip ospf network broadcast**	Specify the type of the interface to be the broadcast network type
DES-7200(config-if)# **ip ospf priority** *priority*	(Optional) Specify the priority of the interface

27.2.4 Configuring the OSPF Area Parameters

To configure area authentication, stub area, and default route summary cost, you need to use the command for configuring the areas.

Area authentication is configured to avoid the learning of non-authenticated and invalid routers and the advertisement 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
DES-7200(config-router)#**area** *area-id* **authentication**	Set plain-text authentication as the authentication mode for the area
DES-7200(config-router)#**area** *area-id* **authentication**	Set MD5 authentication as the authentication mode for the area
DES-7200(config-router)#**area** *area-id* **authentication**	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
DES-7200(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 routes in the area. To configure a full stub area, you still have to configure the full stub area parameters on the border router of the stub area in addition to the basic configuration of stub area. You do not need to change the configuration of other routers.

27.2.5 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 routers 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
DES-7200(config-router)# **area** *area-id* **nssa** [**no-redistribution**] [**no-summary**] [**default-information-originate**[metric][metric-type]]	(Optional) Define a NSSA
DES-7200(config-router)#**area** *area-id* **authentication** **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.

27.2.6 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
DES-7200(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.

27.2.7 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
DES-7200(config-router)# **summary-address** *ip-address mask*[**not-advertise | tag** *tag-id* **|**]	Configure the external summary route

27.2.8 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
DES-7200(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 router. 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*".

27.2.9 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
DES-7200(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 advertise it to all routers within the stub area.

27.2.10 Using the Loopback address as the route ID

The OSPF routing process always uses the largest interface IP address as the router ID. If the interface is disabled or the IP address does not exist, the OSPF routing process must calculate the router 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 router ID. If there are multiple loopback interfaces, the largest IP address is selected as the router 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
DES-7200(config)# **interface loopback 1**	Create the loopback interface
DES-7200(config-if)# **ip address** *ip-address mask*	Configure the Loopback IP address

27.2.11 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 the DES-7200 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
DES-7200(config-router)#**distance** {[**inter-area** *dist1*] [**inter-area** *dist2*] [**external** *dist3*]}	Change the OSPF management distance

27.2.12 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
DES-7200(config-router)#**timers spf** *spf-delay spf-holdtime*	Configure the route calculation timer

27.2.13 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 switch. 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
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **router ospf 1**	Enable OSPF and enter OSPF route configuration mode.
DES-7200(config-router)# **timers lsa-group-pacing** *seconds*	(Optional) Change the LSAs group pacing.
DES-7200(config-router)**# End**	Return to the privileged EXEC mode.
DES-7200# **show running-config**	Verify whether the content is correct.

DES-7200# **write**	(Optional) Save the configuration.

To restore the default value, use the **no timers lsa-group-pacing** in **the** router configuration mode.

27.2.14 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**
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **router ospf 1**	Enable OSPF and enter OSPF route configuration mode.
DES-7200(config-router)#**auto-cost [reference-bandwidth** *ref-bw***]**	(Optional) Set the default cost based on the bandwidth on an interface.
DES-7200(config-router)**# End**	Return to the privileged EXEC mode.
DES-7200# **show ip protocol**	Display the routing protocol that is running currently.
DES-7200# **write**	(Optional) Save the configuration.

To disable route cost, use the **no ip ospf cost** or **auto-cost** command.

27.2.15 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 the MTU of the neighbor against 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
DES-7200(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.

27.2.16 Configuring to prohibit an interface from sending the OSPF interface parameters

To prevent other routes in the network from dynamically learning the route information of the router, you can set the specified network interface of the router 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
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **router ospf 1**	Enter the routing protocol configuration mode (currently RIP and OSPF are supported)
DES-7200(config-router)# **passive-interface** *interface-id*	(Optional) Set the specified interface as passive interface.
DES-7200(config-router)# **passive-interface default**	(Optional) Set all the network interfaces as passive
DES-7200(config-router)# **end**	Return to the privileged EXEC mode.
DES-7200(config-router)# **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 re-enable tall network interfaces, use the keyword **default.**

27.3 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
DES-7200# **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.
DES-7200# **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.
DES-7200# **show ip ospf** [*process-id*] [*area-id*] **database** [**adv-router** *ip-address*]	
DES-7200# **show ip ospf** [*process-id*] [*area-id*] **database** [**self-originate**]	
DES-7200# **show ip ospf** [*process-id*] [*area-id*] **database** [**database-summary**]	
DES-7200# **show ip ospf** [*process-id*] [*area-id*] **database** [**router**] [*link-state-id*]	
DES-7200# **show ip ospf** [*process-id*] [*area-id*] **database** [**router**] [**adv-router** *ip-address*]	
DES-7200# **show ip ospf** [*process-id*] [*area-id*] **database** [**router**] [**self-originate**]	
DES-7200# **show ip ospf** [*process-id*] [*area-id*] **database** [**network**][*link-state-id*]	
DES-7200# **show ip ospf** [*process-id*] [*area-id*] **database** [**network**] [*link-state-id*] [**adv-router** *ip-address*]	
DES-7200# **show ip ospf** [*process-id*] [*area-id*] **database** [**network**][*link-state-id*] [**self-originate**]	
DES-7200# **show ip ospf** [*process-id*] [*area-id*] **database** [**summary**] [*link-state-id*]	
DES-7200# **show ip ospf** [*process-id*] [*area-id*] **database** [**summary**] [*link-state-id*] [**adv-router** *ip-address*]	

DES-7200# **show ip ospf** [*process-id*] [*area-id*] **database** [**summary**] [*link-state-id*] [**self-originate**]	
DES-7200# **show ip ospf** [*process-id*] [*area-id*] **database** [**asbr-summary**] [*link-state-id*]	
DES-7200# **show ip ospf** [*process-id*] [*area-id*] **database** [**asbr-summary**] [*link-state-id*] [**adv-router** *ip-address*]	
DES-7200# **show ip ospf** [*process-id*] [*area-id*] **database** [**asbr-summary**] [*link-state-id*] [**self-originate**]	
DES-7200# **show ip ospf** [*process-id*] [*area-id*] **database** [**external**] [*link-state-id*]	
DES-7200# **show ip ospf** [*process-id*] [*area-id*] **database** [**external**] [*link-state-id*] [**adv-router** *ip-address*]	
DES-7200# **show ip ospf** [*process-id*] [*area-id*] **database** [**external**] [*link-state-id*] [**self-originate**]	
DES-7200# **show ip ospf** [*process-id*] [*area-id*] **database** [**nssa-external**] [*link-state-id*]	
DES-7200# **show ip ospf** [*process-id*] [*area-id*] **database** [**nssa-external**] [*link-state-id*] [**adv-router** *ip-address*]	
DES-7200# **show ip ospf** [*process-id* [*area-id*] **database**[**nssa-external**] [*link-state-id*][**self-originate**]	
DES-7200# **show ip ospf** [*process-id*] **border-routers**	Show the route information when specified processes reach the ABR and ASBR.
DES-7200# **show ip ospf interface** [*interface-name*]	Show the information on the OSPF interface
DES-7200# **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
DES-7200# **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.

```
DES-7200# 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
DES-7200# 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
DES-7200# 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 router 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.

```
DES-7200# 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, oip->type = BROADCAST
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, router type, area information, area summary, and other related information.

```
DES-7200# show ip ospf
Routing Process "ospf 1" with ID 192.168.1.1
```

```
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 route 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
rea 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 192.168.1.1
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
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
umber of non-default external LSA 0
External LSA database is unlimited.
umber of LSA originated 0
Number of LSA received 0
Log Neighbor Adjency Changes : Enabled
Number of areas attached to this router: 0
```

27.4 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

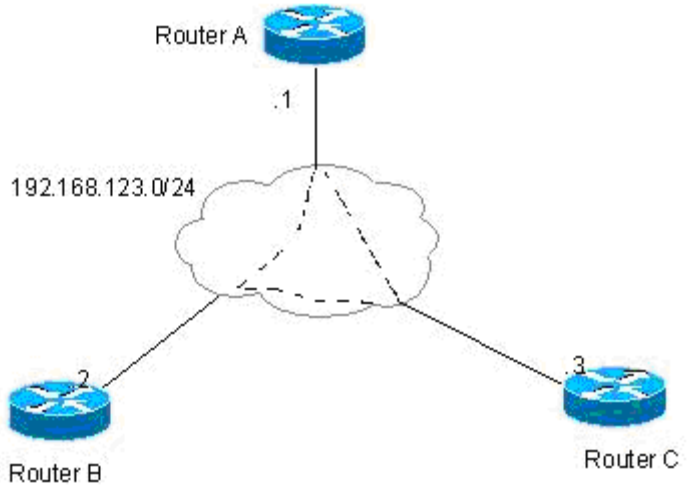
- Example of configuring route summary
- OSPF ABR, ASBR Configuration Examples
- Example of configuring OSPF stub area
- Example of configuring OSPF virtual connection

27.4.1 Example of configuring the OSPF NBMA network type

- **Configuration requirements:**

The three routers must be fully connected in a meshed network via frame relay. Each router has only one frame relay line, which has the same bandwidth and PVC rate. Figure 27-1 shows the IP address allocation and connection of the equipment.

Figure 27-1 Example of configuring the OSPF NBMA network type



Requirement: 1) The NBMA network type is configured among router A, B and C, 2) The router A is the designated router, and the router B is the backup designated router, 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 Switch 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 Switch 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 Switch 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

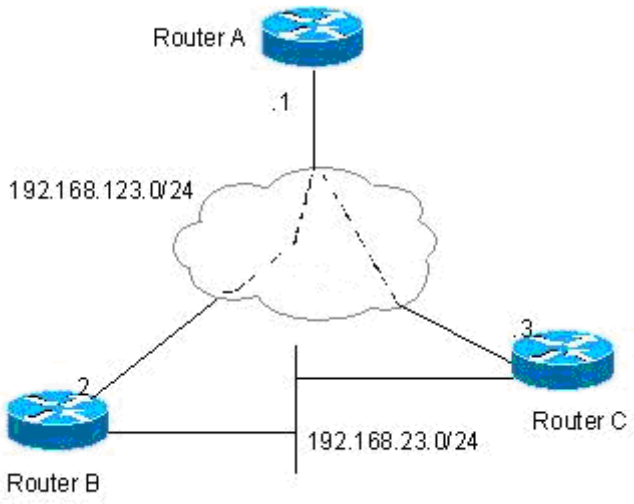
```
router ospf 1
network 192.168.123.0 0.0.0.255 area 0
neighbor 192.168.123.1 10
neighbor 192.168.123.2 5
```

27.4.2 Example of configuring the OSPF point-to-multipoint board network type

- **Configuration requirements:**

The three routers must be fully interconnected via frame relay. Each router has only one frame relay line, which has the same bandwidth and PVC rate. Figure 27-2 shows the IP address allocation and connection of the equipment.

Figure 27-2 Example of Configuring the OSPF Point-to-Multipoint Network Type



Requirements: 1) The point-to-multipoint network should be configured among routers A, B, and C.

- **Concrete Configuration of Routers**

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 Switch 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 Switch 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 Switch 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 router 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 router A:

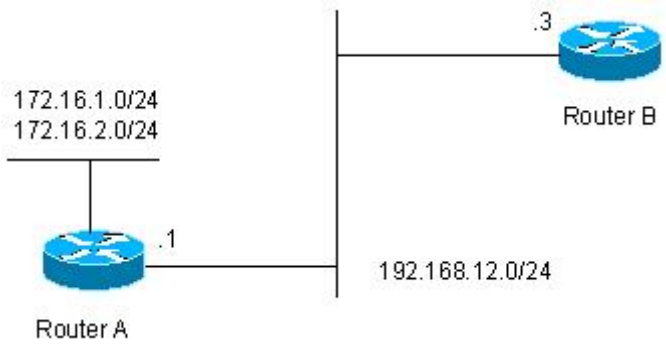
```
router ospf 1
neighbor 192.168.123.2 cost 100
neighbor 192.168.123.3 cost 200
```

27.4.3 Example of configuring OSPF authentication

- **Configuration requirements:**

Two routers are connected via the Ethernet and run the OSPF routing protocol, with the MD5 authentication used. The connection diagram among routers and the assignment of IP addresses are shown as in Figure 27-3 .

Figure 27-3 Example of configuring OSPF authentication



■ **Concrete Configuration of Routers**

The authentication configuration of the OSPF involves two parts:

1. Specifying the authentication mode of the area in the routing configuration mode;
2. 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 Switch 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 Switch 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

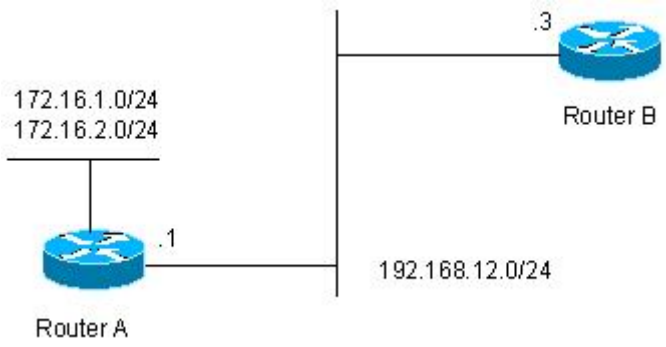
```
router ospf 1
network 192.168.12.0 0.0.0.255 area 0
area 0 authentication message-digest
```

27.4.4 Example of configuring route summary

■ **Configuration requirements:**

The two routers are connected via Ethernet. Figure 27-4 shows the IP address allocation and connection of the equipment.

Figure 27-4 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 route 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 Routers**

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 Switch 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 Switch B:

#Configuring Ethernet interface

```
interface FastEthernet0/0
ip address 192.168.12.2 255.255.255.0
```

#Configuring OSPF routing protocol

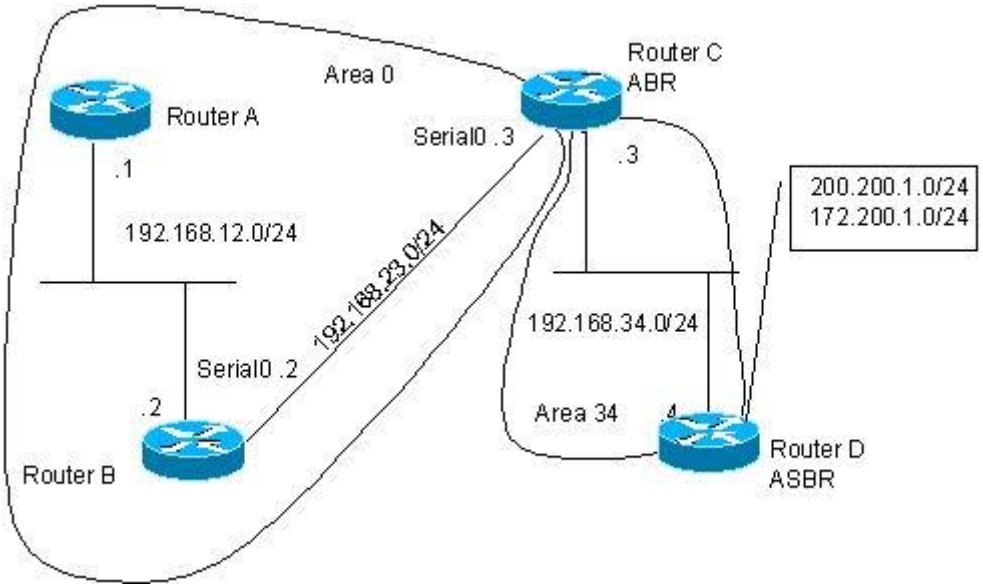
```
router ospf 1
network 192.168.12.0 0.0.0.255 area 0
```

27.4.5 OSPF ABR, ASBR Configuration Examples

■ **Configuration requirements:**

Four routers 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 27-5 shows the IP address allocation and connection of the equipment.

Figure 27-5 Example of configuring OSPF ABR and ASBR



As is shown in above figure, the router A and router B are of the area internal routers, the router C is of the ABRs, and the router 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 routers so that all OSPF routers can learn the external routes, which must carry the “34” tag and be Type-I.

■ **Concrete Configuration of Routers**

When the OSPF redistributes the routes of other sources, the default type is type II and it does not carry any tag.

Configuration of Switch 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 Switch 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 Switch 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 Switch 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 Router 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 Router B, you can see the link status database as shown below. Please note that the tag of the external link has become “E1”.

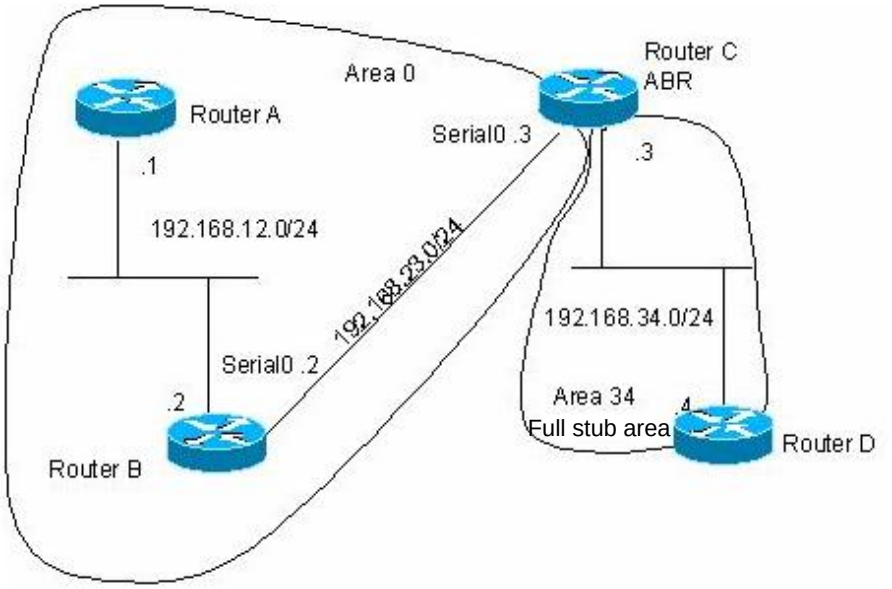
```
RouterB#show ip ospf 1 database
OSPF Router process 1 with ID (192.168.23.2) (Process ID 100)
             Router Link States (Area 0)

Link ID          ADV Router     Age    Seq#      Checksum Link count
192.168.23.2    192.168.23.2    155    0x8000000A 0xD617   3
192.168.34.3    192.168.34.3    156    0x80000001 0x2CF3   2
192.168.65.55   192.168.65.55   237    0x80000062 0x555E   1
192.168.101.1   192.168.101.1   237    0x8000000B 0x7D16   2

             Net Link States (Area 0)
Link ID          ADV Router     Age    Seq#      Checksum
192.168.12.55   192.168.65.55   237    0x80000004 0x91B2

             Summary Net Link States (Area 0)
Link ID         ADV Router     Age    Seq#      Checksum
192.168.34.0    192.168.34.3    70    0x80000003 0x3B05

             Summary ASB Link States (Area 0)
  Link ID       ADV Router     Age    Seq#      Checksum
200.200.1.1     192.168.34.3    65    0x80000001 0xA98F

             AS External Link States
Link ID         ADV Router     Age    Seq#      Checksum Tag
172.200.1.0     200.200.1.1    122    0x80000001 0x1104   34
200.200.1.0     200.200.1.1    122    0x80000001 0xA355   34
RouterB#
```

27.4.6 Example of configuring OSPF stub area

- **Configuration requirements:**

Four routers 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 27-6 shows the IP address allocation and connection of the equipment.

Figure 27-6 Example of configuring OSPF stub area



The requirement 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 Routers**

Only the routers 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 routers in the area. In order to show the inter-area routing in the router D, the router C advertises a 192.168.30.0/24 network.

The configuration of router 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 Switch 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 Switch 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 Switch 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 router D by the ospf is shown as follows:

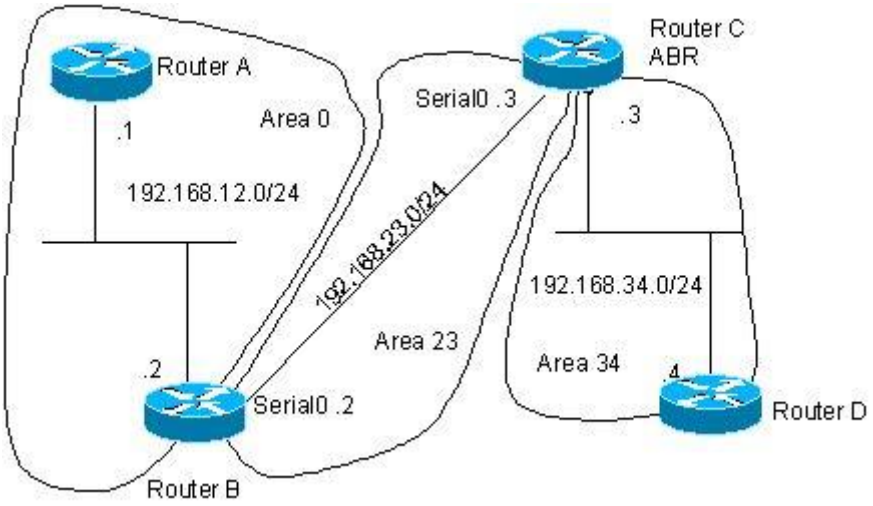
```
O 192.168.30.0/24 [110/1786] via 192.168.34.3, 00:00:03, FastEthernet0/0
O*IA 0.0.0.0/0 [110/2] via 192.168.34.3, 00:00:03, FastEthernet0/0
```

27.4.7 Example of configuring OSPF virtual connection

- **Configuration requirements:**

Four routers 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 27-7 shows the IP address allocation and connection of the equipment.

Figure 27-7 Example of configuring OSPF virtual connection



The purpose is to allow router D to learn the routes of 192.168.12.0/24 and 192.168.23.0/24.

■ **Concrete Configuration of Routers**

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 router 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 router 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 Switch 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 router 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
```

28 Overview of BGP Protocol

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

28.1 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.**

28.2 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

28.3 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.

28.4 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**
Router(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).
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

The **neighbor update-source** command can be used to select any valid interface to establish the TCP connection. The key function of this command is to provide available Loopback interface, which makes the connection to the IBGP Speaker more stable.

By default, it is required to directly connect with BGP Peers physically, to establish the EBGP connection. To establish the EBGP Peers among non-direct-connected External BGP Speakers, the **neighbor ebgp-multihop** command can be used.

Caution

It is necessary to present the non-default routing to reach the opposite party among peers.

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.

28.5 Configuring Management Strategy for BGP

Once the routing strategy (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 strategies. Traditional measure is to close it and reestablish new BGP connection.

This product supports to implement new routing strategy 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 strategy which has an effect on the input route information as the input route strategy (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 strategy 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 strategy.

If the input route strategy changes, its operation will be more complicated than that of the output route strategy: For the implement of the output routing strategy is based on the route information table of this BGP Speaker. The implement of the input routing strategy 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 strategy, 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 strategy in future.

At present, there is a standard implement method referred to as the Route Refresh Performance, which can support to modify the route strategy without the storage of the original route information. This product supports the route refreshing performance.

If the input route strategy 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 strategy.

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 strategy changes.

28.6 Configuring Synchronization between BGP and IGP

For it will pass through this AS and reach anther 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.

28.7 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.

28.8 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.

28.9 Configuring Path Attribute for BGP

28.9.1 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).
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 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.

28.9.2 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.

28.9.3 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.

28.9.4 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.

28.9.5 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.

28.9.6 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.

28.10 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.

28.11 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.

28.12 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.

28.13 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.
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.

28.14 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.

28.15 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.

28.16 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.

28.17 Protocol Independent Configuration

28.17.1 route-map Configuration

The BGP protocol applies the Route-map strategy on a large scale. For the configuration of the Route-map strategy, refer to the Protocol Independent Configuration Part in this manual.

28.17.2 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.

28.17.2.1 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.

28.17.2.2 Application Example of Regular Expression

At present, the equipment **show ip bgp** presents the content below:

```
DES-7200# 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:

```
DES-7200# 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
```

28.18 BGP Configuration Examples

The following lists the BGP configuration.

28.18.1 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

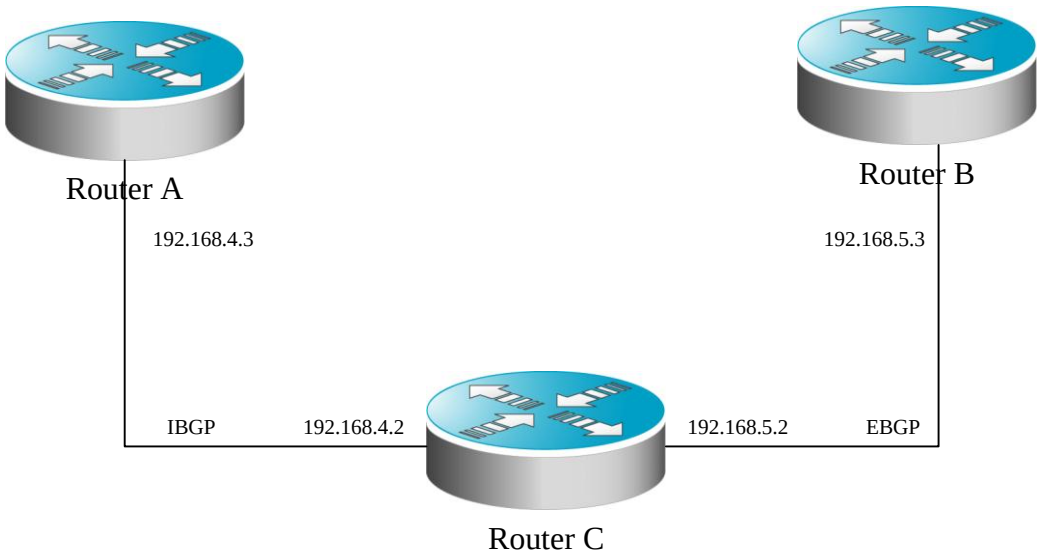
neighbor 131.108.200.1 remote-as 167

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 routers is shown as follows:

Configuration of Router A :

```
!
router bgp 100
 neighbor 192.168.4.2 remote-as 100
```

Configuration of Router B:

```
!
router bgp 100
 neighbor 192.168.4.3 remote-as 100
 neighbor 192.168.5.3 remote-as 200
```

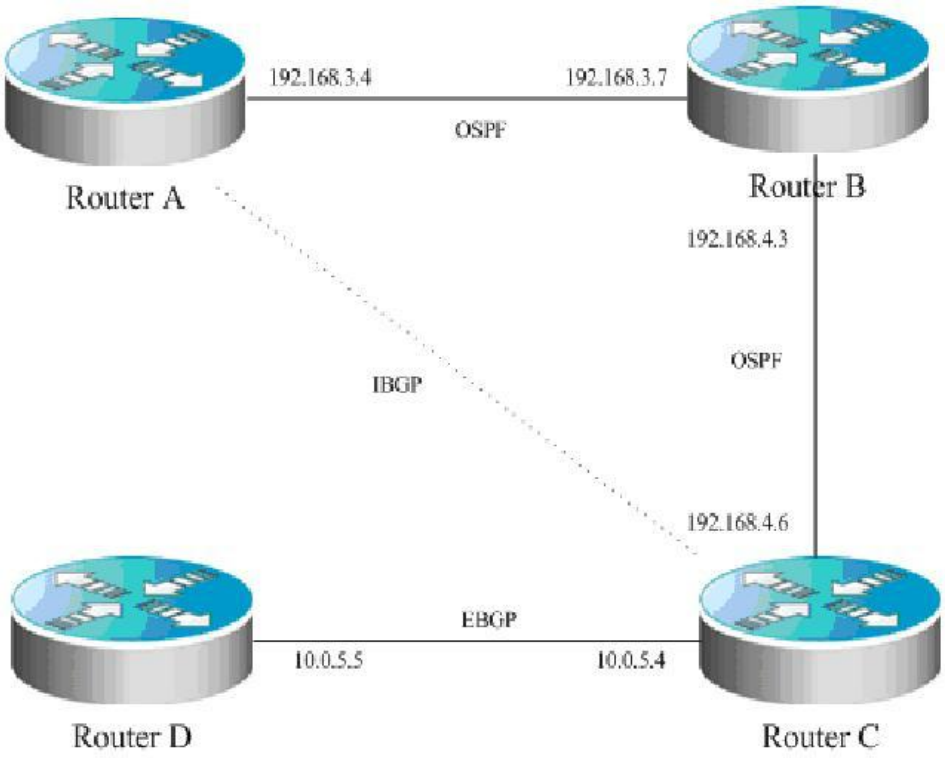
Configuration of Router C:

```
!
router bgp 200
 neighbor 192.168.5.2 remote-as 100
```

28.18.2 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.

28.18.3 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* 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 passes through the **as-path access-list** *3 filter.*

28.18.4 Configuring Aggregate Route

Use the **aggregate-address** command to configure the static 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 aggregate route will not be advertised

28.18.5 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.

28.18.6 Configuring Route Reflector

When the route reflector is configured, it is necessary to use the **bgp client-to-client reflection** command to open 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
```

28.18.7 Configuring peergroup

Here will take the configuration of **peergroup** for IBGP and EBGP as an example.

28.18.7.1 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
```

28.18.7.2 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
```

28.18.8 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.*

29 Guide for Configuring Policy-Based Routing

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 redistribution 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**
DES-7200(config)# **route-map** *route-map-name* [**permit** | **deny**] *sequence*	Define the route map
DES-7200(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
DES-7200(config-route-map)# **match ip address** *access-list-number*	Match the address in the access list
DES-7200(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
DES-7200(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
DES-7200(config-route-map)# **set ip next-hop** *ip-address* [*weight*][*ip-address*[*weight*]]	Set the next-hop IP address of the packets
DES-7200(config-route-map)# **set interface** *intf_name*	Set the egress interface
DES-7200(config-route-map)# **set default interface** *intf_name*	Set the default egress interface

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
DES-7200(config-if)# **ip policy route-map** [*name*]	Use the specified route-map for filtering on the interface
DES-7200(config-if)# **no ip policy** *route-map* [*name*]	Cancel the route-map applied on the interface

5. Use policy-based routing for the locally sent packets

Command	Function
DES-7200(config-if)# **ip local policy route-map** [*name*]	Use the specified route-map for filtering of locally sent packets

DES-7200(config-if)# **no ip local policy** *route-map* [*name*]	Cancel policy-based routing for local packets

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.

```
DES-7200(config)# access-list 1 permit any
DES-7200(config)# route-map name
DES-7200(config-route-map)# match ip address 1
DES-7200(config-route-map)# set ip next-hop 192.168.5.5
DES-7200(config-route-map)# int f 0/0
DES-7200(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**
DES-7200(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**
DES-7200(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:

1. [**no**] **ip policy route-map**
2. **match ip address**
3. **set ip next-hop**
4. **set ip default next-hop**

Restrictions:

On the firmware v10.0, 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.

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.

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.

The deny option of the ACE has a different behavior from that of CISCO, for which the matching starts from the next ACL. Since the chip does not offer adequate support, we perform the normal forwarding. Also, to meet the matching sequence of the policy-based routing, the “deny any any” means to skip the next ACL and then start matching.

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.

When working in the redundancy backup mode, the first solved nexthop takes effect. If none of the nexthops is resolved, the drop action is set. If the first nexthop is not resolved, but later connection is made, this will also take effect.

Policy-based routing on the equipment:

Supported commands:

1. [**no**] **ip policy route-map**
2. **ip local policy route-map**
3. **match ip address**
4. **match length**
5. **set ip next-hop**
6. **set ip default next-hop**
7. **set tos**
8. **set prefrence**

30 Configuring Protocol-Independent Features

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 the DES-7200 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
DES-7200(config)# **ip route** [**vrf** *vrf_name*] *network mask* {*ip-address* | *interface-type interface-number* } [*distance*] [**tag** *tag*] [**permanent**]	Configure static routes
DES-7200(config)# **no ip route** *network mask*	Delet Static Route
DES-7200(config)# **ip static route-limit** *number*	Specify the maximum number of static routes
DES-7200(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, the DES-7200 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 the DES-7200:

Route source	Default management distance
Directly connected networks	0
Static route	1

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 the DES-7200 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 network-wide 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
DES-7200(config)# **ip default-network** network	Configure the default network
DES-7200(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)

30.1.4 Configuring the Default Gateway

When the device does not know which destination address to forward the packets, it sends the packets to the default gateway. You can view this by using the show ip redirects command.

To configure the default gateway, execute the following command in the global configuration mode. The **no** form of this command deletes the default gateway.

Command	Description
Ip default-gateway *ip-address*	Set the default gateway

To view the default gateway set, execute the following command.

Command	Description
show ip redirects	Show the default gateway

This command is only supported on the L2 device.

30.2 Route Redistribution

30.2.1 Configuring Route Redistribution

To support the routers to run multiple routing protocol processes, the DES-7200 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
DES-7200(config)# **route-map** *route-map-name* [**permit** | **deny**] *sequence*	Define the route map *sequence* : 0-65535

DES-7200(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, 3000-3199*
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
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
Route(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**
DES-7200(config-route-map)# **set level** {**stub-area** | **backbone** | **level-1** | **level-1-2** | **level-2**}	Specify the area of route inputted
DES-7200(config-route-map)# **set metric** *metric*	Set the metric for route redistribution

DES-7200(config-route-map)# **set metric-type** {**type-1** | **type-2 | external** | **internal**}	Set the type for route redistribution
DES-7200(config-route-map)# **set tag** *tag*	Set the tag for route redistribution
DES-7200(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**
DES-7200(config-router)# **redistribute** *protocol* [**metric** *metric*] [**metric-type** *metric-type*] [**match internal** | **external** *type* | **nssa-external** *type*] [**tag** *tag*] [**route-map** *route-map-name*] [**subnets**]	Set route redistribution *Protocol* (protocol type): bgp, connected, isis, rip, static
DES-7200(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 Configuring 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
DES-7200(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.
DES-7200(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
DES-7200(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 not allow 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.
DES-7200(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 Configuring Route Redistribution

- **Configuration requirements:**

One router exchanges route information with other routers 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.

```
DES-7200(config)# ip route 172.16.1.0 255.255.255.0 172.200.1.2
DES-7200(config)# ip route 192.168.1.0 255.255.255.0 172.200.1.2
DES-7200(config)# ip route 192.168.2.0 255.255.255.0 172.200.1.4
!
DES-7200(config)# router rip
```

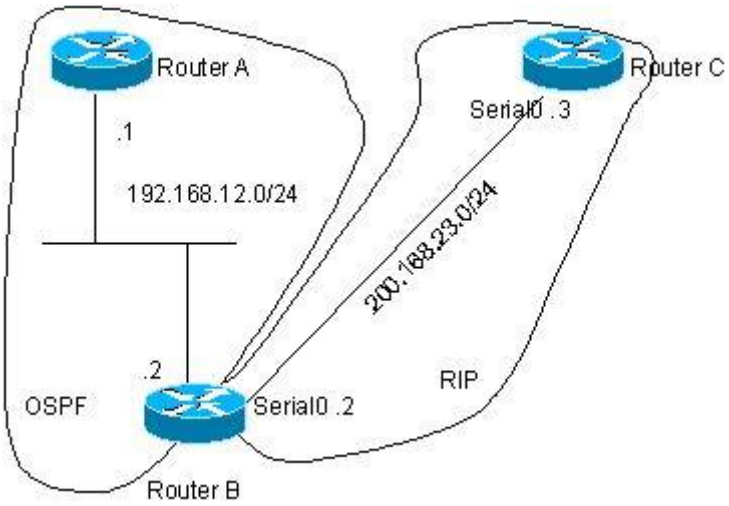
```
DES-7200(config-router)# version 2
DES-7200(config-router)# redistribute static
DES-7200(config-router)# network 192.168.34.0
DES-7200(config-router)# distribute-list 10 out static
DES-7200(config-router)# no auto-summary
!
DES-7200(config)# access-list 10 permit 192.168.1.0
DES-7200(config)# access-list 10 permit 172.16.1.0
```

30.2.3.2 Example of Configuring 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:

```
DES-7200(config)# interface gigabitEthernet 0/0
DES-7200(config-if)# ip address 192.168.10.1 255.255.255.0
DES-7200(config)# interface loopback 1
DES-7200(config-if)# ip address 192.168.100.1 255.255.255.0
DES-7200(config-if)# no ip directed-broadcast
!
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# ip address 192.168.12.55 255.255.255.0
!
DES-7200(config)# router ospf 1
DES-7200(config-router)# network 192.168.10.0 0.0.0.255 area 0
DES-7200(config-router)# network 192.168.12.0 0.0.0.255 area 0
DES-7200(config-router)# network 192.168.100.0 0.0.0.255 area 0
```

Configuration of router B:

```
DES-7200(config)# interface gigabitEthernet 0/0
DES-7200(config-if)# ip address 192.168.12.5 255.255.255.0
!
DES-7200(config)# interface Serial 1/0
DES-7200(config-if)# ip address 200.168.23.2 255.255.255.0
```

#Configure OSPF and set the redistribution route type

```
DES-7200(config)# router ospf
DES-7200(config-router)# redistribute rip metric 100 metric-type 1 subnets
DES-7200(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

```
DES-7200(config)# router rip
DES-7200(config-router)# redistribute ospf metric 2
DES-7200(config-router)# network 200.168.23.0
DES-7200(config-router)# distribute-list 10 out ospf
DES-7200(config-router)# no auto-summary
```

#Define an access list

```
DES-7200(config)# access-list 10 permit 192.168.10.0
```

Configuration of router C:

```
DES-7200(config)# interface gigabitEthernet 0/0
DES-7200(config-if)# ip address 200.168.30.1 255.255.255.0
!
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# ip address 200.168.3.1 255.255.255.0
!
DES-7200(config)# interface Serial 1/0
DES-7200(config-if)# ip address 200.168.23.3 255.255.255.0
DES-7200(config)# router rip
DES-7200(config-router)# network 200.168.23.0
DES-7200(config-router)# network 200.168.3.0
DES-7200(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.

```
!
DES-7200(config)# router ospf
DES-7200(config-router)# redistribute rip subnets route-map redrip
DES-7200(config-router)# network 192.168.12.0 0.0.0.255 area 0
!
DES-7200(config)# access-list 20 permit 200.168.23.0
!
DES-7200(config)# route-map redrip permit 10
DES-7200(config-route-map)# match metric 4
DES-7200(config-route-map)# set metric 40
DES-7200(config-route-map)# set metric-type type-1
DES-7200(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.
DES-7200(config)# router rip
DES-7200(config-router)# version 2
DES-7200(config-router)# redistribute ospf route-map redospf
DES-7200(config-router)# network 200.168.23.0
!
DES-7200(config)# route-map redospf permit 10
DES-7200(config-route-map)# match tag 10
DES-7200(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
- 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
DES-7200(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.

DES-7200(config)# **no ip ref ecmp load-balance {[crc32_lower | crc32 upper] [dip] [port] [udfnumber]}**	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:

```
DES-7200(config)#ip ref ecmp load-balance crc32_lower dip port udf 50
```

31 Configuring IPv6

31.1 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 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 Message Header

The design principle of new IPv6 message header is to minimize the overhead. For this reason, some non-critical fields and optional fields are removed from the message header and placed into the extended message 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 message header is more efficient for the router forwarding, for instance, there is no check sum in the IPv6 message 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**

31.1.1 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 800:0:0:0:0:0:1 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 : 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.

31.1.2 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 set 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 set 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.

Note The broadcast address is not defined in the IPv6.

The following will introduce these types of addresses one-by-one:

31.1.2.1 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.

31.1.2.2 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

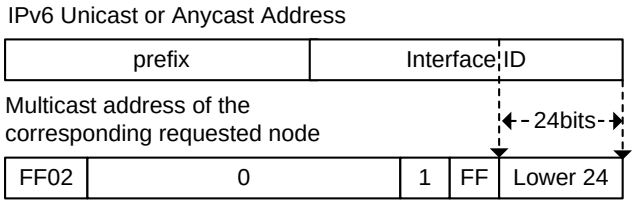
If they are routers, it is necessary to add the multicast address FF02::2 of all routers for the local link.

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 31-1



31.1.2.3 Anycast Addresses

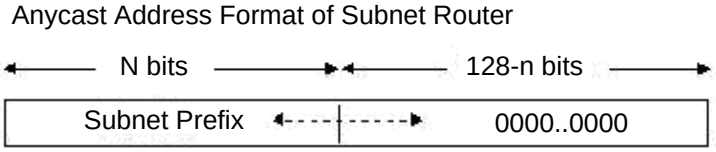
The anycast address is similar with the multicast address as more than one node shares an anycast address. The difference is that only one node expects to receive the data packet of the anycast address, while all nodes of the multicast address members expect to receive all packets sending to this address. 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 router, 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.

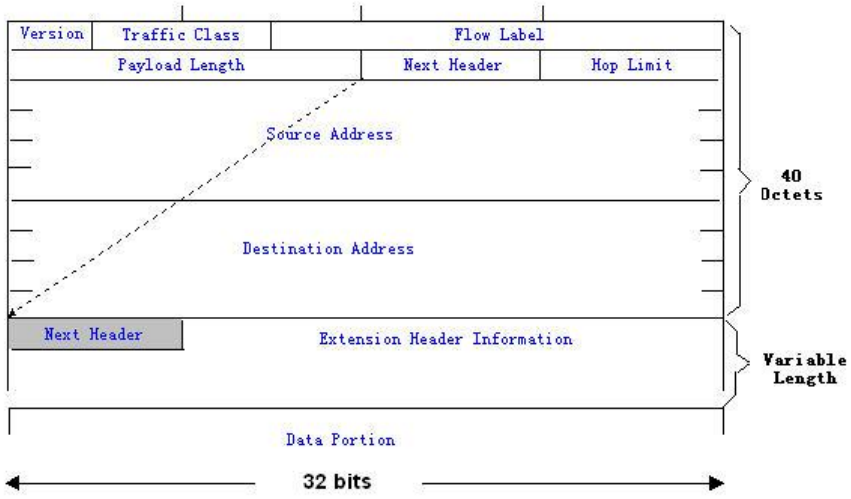
Figure 31-2



31.1.3 IPv6 Packet Header Structure

The format of the IPv6 packet header is shown as the figure below:

Figure 31-3



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.

31.1.4 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.

31.1.5 IPv6 Neighbor Discovery

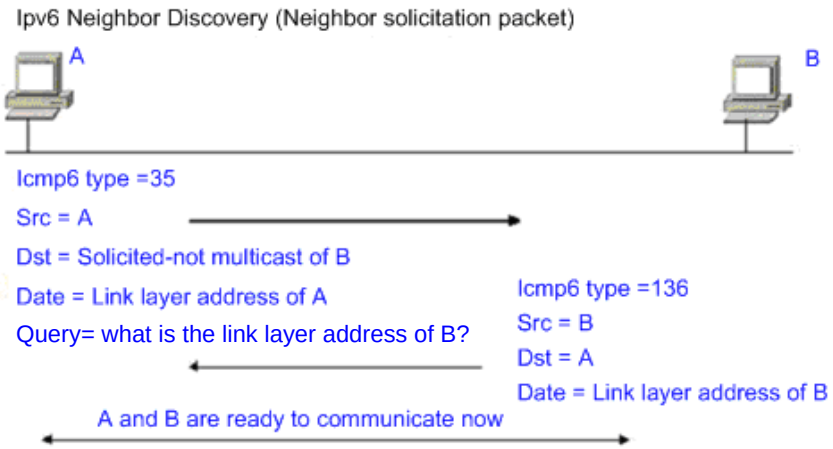
The IPv6 neighbor discovery processing makes use of the message of the ICMPv6 and the multicast addresses of the solicited neighbor to obtain the link layer address of the neighbor at the same link, and verify the reachability of the neighbor as well as maintain the status of the neighbor. These types of messages are briefly described respectively below.

31.1.5.1 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 31-4



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.

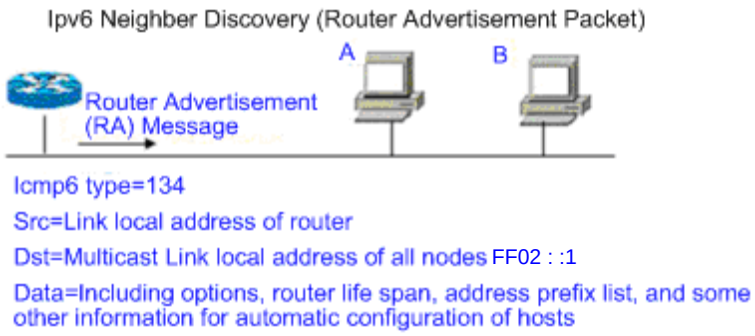
Furthermore, the neighbor solicitation message in the stateless address auto-configuration can also be used to detect the unique of the address, namely the address conflict detect. At this time, the source address of the message is unassigned address (: :).

31.1.5.2 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 31-5



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.

31.2 IPv6 Configuration

The following will introduce the configuration of various function modules of the IPv6 respectively:

31.2.1 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*/*prefix-length* **[eui-64]**command to delete the configured address. The following is an example of the configuration of the IPv6 address:

```
DES-7200(config)# interface vlan 1
DES-7200(config-if)# ipv6 enable
DES-7200(config-if)# ipv6 address fec0:0:0:1::1/64
DES-7200(config-if)# end
DES-7200(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
Joined group address(es):
ff02:1::2
ff01:1::1
ff02:1::1
ff02:1::1:ff00:1
INET6: fec0:0:0:1::1 , subnet is fec0:0:0:1::/64
Joined group address(es):
ff02:1::2
ff01:1::1
ff02:1::1
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
```

31.2.2 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 router 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:

```
DES-7200(config)# interface vlan 1
DES-7200(config-if)# ipv6 redirects
DES-7200(config-if)# end
DES-7200# 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
Joined group address(es):
ff02:1::2
ff01:1::1
ff02:1::1
ff02:1::1:ff00:1
INET6: fec0:0:0:1::1 , subnet is fec0:0:0:1::/64
Joined group address(es):
ff02:1::2
ff01:1::1
```

```
ff02:1::1
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
```

31.2.3 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 31-1 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:

```
DES-7200(config)# ipv6 neighbor fec0:0:0:1::100 vlan 1 00d0.f811.1234
DES-7200(config)# end
DES-7200# 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
```

31.2.4 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:

```
DES-7200(config)# interface vlan 1
DES-7200(config-if)# ipv6 nd dad attempts 3
DES-7200(config-if)# end
DES-7200# 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
Joined group address(es):
ff02:1::2
ff01:1::1
ff02:1::1
ff02:1::1:ff00:1
INET6: fec0:0:0:1::1 , subnet is fec0:0:0:1::/64
```

```
Joined group address(es):
ff02:1::2
ff01:1::1
ff02:1::1
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
```

31.2.5 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 preferred-lifetime*] | [**at** *valid-date preferred-date*] | **infinite** | **no-advertise**]]	(Optional) Set the address prefix to be advertised in the router advertisement (RA) message.

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. For the guide of concrete commands, refer to the *IPv6 Command Reference*.

31.3 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.
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.

```
DES-7200# 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
Joined group address(es):
ff02:1::2
ff01:1::1
ff02:1::1
ff02:1::1:ff00:1
INET6: fec0:1:1:1::1 , subnet is fec0:1:1:1::/64
Joined group address(es):
ff02:1::2
ff01:1::1
ff02:1::1
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

```
DES-7200# 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.

```
DES-7200# 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
```

32 Configuring IPV6 Tunnel

32.1 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 messages in IPv4 messages. 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 to 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:

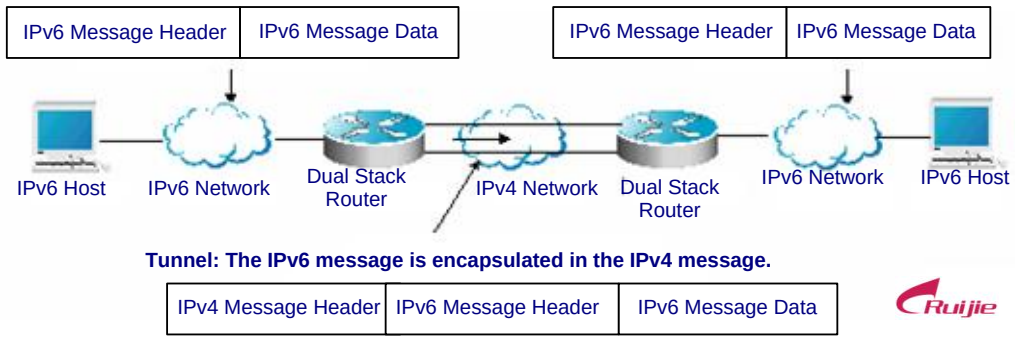
Tunnel Type	**Reference**
Manually Config Tunnel	RFC2893
automatic 6to4 Tunnel	RFC3056
Intra-Site Automatic Tunnel Addressing Protocol(ISATAP)	draft-ietf-ngtrans-isatap-22

Caution

Interconnecting the isolated IPv6 network through the IPv6 tunnel technology is not the ultimate IPv6 network architecture, but a transitional technology. The structure formed by connecting isolated IPv6 networks with the IPv6 tunnel technology is not the final network architecture of the IPv6. Ihe technology is only for transition.

The model to use the tunnel technology is shown in the following figure:

Figure 32-1



The features of various tunnels are respectively introduced below.

32.1.2 Manually Configured Tunnel (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 for 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.

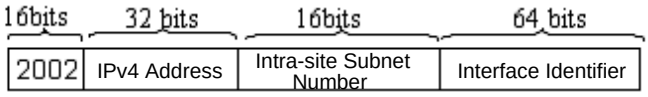
On a tunnel interface, you must manually configure the IPv6 address, source IPv4 address (tunnel source) and destination IPv4 address (tunnel destination) of the tunnel. The nodes at the two end of the tunnel must support the IPv6 and IPv4 protocol stacks. In practical application, tunnels to be manually 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.

32.1.3 Automatic 6to4 Tunnel (Automatic 6to4 Tunnel)

The automatic 6to4 tunnel technology allows isolated IPv6 networks to be interconnected via IPv4 networks. The difference between the automatic 6to4 tunnel and manual configured tunnel technologies is as follows: A manual 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 routers of 6to4 need not be configured in pairs. The IPv4 addresses embedded in an IPv6 address will be used to look for the other end of the automatic tunnel. The 6to4 tunnel can be taken as a point -to-multipoint tunnel. The automatic 6to4 tunnel can be configured on an Area Border Router of one isolated IPv6 network. For each message, it will automatically build a tunnel connecting to an Area Border Router in another IPv6 network. The destination address of a tunnel is the IPv4 address of an Area Border Router in the IPv6 network at the other end. The IPv4 address will be extracted from the destination IPv6 address of the message. The destination IPv6 address starts at the prefix 2002::/16 in the following form:

Figure 32-2



IPv6 6to4 Address Format

The 6to4 address is an address for automatic 6to4 tunnel technology. The IPv4 address embedded in it are 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 message 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 with 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 (i.e., 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 of the sites must have one connect to one of their shared IPv4 networks at least. This IPv4 network can be an Internet network or a internal backbone network of an organization. The key is that 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.

32.1.4 ISATAP Automatic Tunnel (ISATAP Tunnel)

Intra-site Automatic Tunnel Addressing Protocol (ISATAP) is a type of 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 in the following condition: The pure IPv6 network inside a site is not ready for use yet and an IPv6 message need be transferred internally in the site. For example, a few of IPv6 hosts for test need communicate with each other inside the site. By an 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 message, allowing the ISATAP host to be automatically configured inside the site. At the same time, the ISATAP router performs the function that an intra-site ISATAP host and external IPv6 host forward messages.

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.

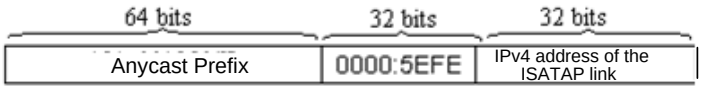
- ISATAP interface identifier

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. Where, the value of the first 32 bits of the interface identifier is **0000:5EFE**, which means 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. An ISATAP address structure is shown in the following figure:

Figure 32-3



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

32.2 IPv6 Tunnel Configuration

32.2.1 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 port and destination port IPv4 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

You cannot configure manual tunnels with the same Tunnel Source and Tunnel Destination. 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.
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, then 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.

See the “Verifying the IPv6 Tunnel Configuration and Monitoring” section to check the working status of the tunnel. Refer to the section *Verifying IPv6 Tunnel Configuration and Mmonitoring* to check the working states of the tunnel.

32.2.2 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 at the two end 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 will not 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.
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, i.e., the tunnel interface specified in the above Step 2.
End	Return to the privileged EXEC 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.

32.2.3 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 the

IPv4 address of the interface referenced by the tunnel source address. Refer to the above chapters and sections for the 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 message 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.
no ipv6 nd suppress-ra	By default, it is disabled to send router advertisement messages on an interface. Use the command to enable the function, allowing the ISATAP host to be automatically configured.
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.

32.3 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.
show ipv6 route	View the IPv6 router table.

1. View the information of a tunnel interface.

```
DES-7200# 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.

```
DES-7200# 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
```

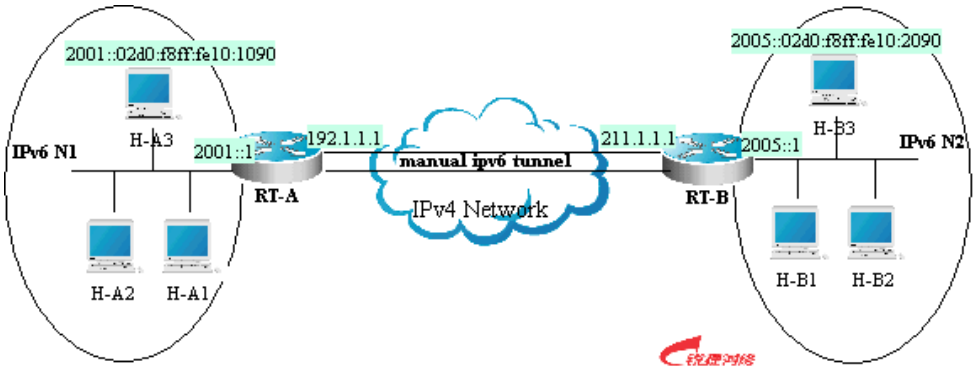
32.4 IPv6 Tunnel Configuration Instances

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

32.4.1 Manual IPv6 Tunnel Configuration Instance

Figure 32-4



As shown in the above figure, IPv6 networks N1 and N2 are isolated by the IPv4 network. Now, the two networks are interconnected by configuring a manual tunnel. For example, the H-A3 host in N1 can access the H-B3 host in N2.

In the figure, RT-A and RT-B are routers that support the IPv4 and IPv6 protocol stacks. The configuration of the tunnel is performed on the Area Border Routers (RT-A and RT-B) in N1 and N2. Note that the manual tunnel must be configured symmetrically. Namely, the manual tunnel should be configured on RT-A and RT-B.

The concrete configurations related to the tunnel are respectively as follows:

Prerequisite: Suppose the routes of IPv4 are connected. In the following content, no more route configuration condition about IPv4 is listed.

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

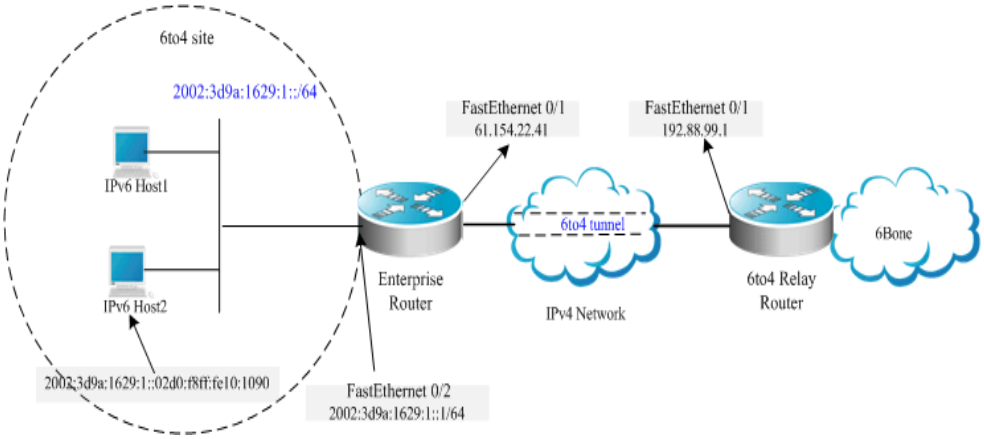
```
interface Tunnel 1
tunnel mode ipv6ip
ipv6 enable
tunnel source FastEthernet 2/1
tunnel destination 192.1.1.1
```

#Configure the route to the tunnel

```
ipv6 route 2001::/64 tunnel 1
```

32.4.2 6to4 Tunnel Configuration Instance

Figure 32-5



As shown in the above figure, an IPv6 network (6to4 site) uses a 6to4 tunnel to access the IPv6 backbone network (6bone) via the 6to4 relay router.

As introduced above, the 6to4 tunnel technology is used to interconnect isolated IPv6 networks and they can access 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 will be used to look for 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 form is 3d9a:1629

192.88.99.1 in the hex form 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 will not work normally.

The following is 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

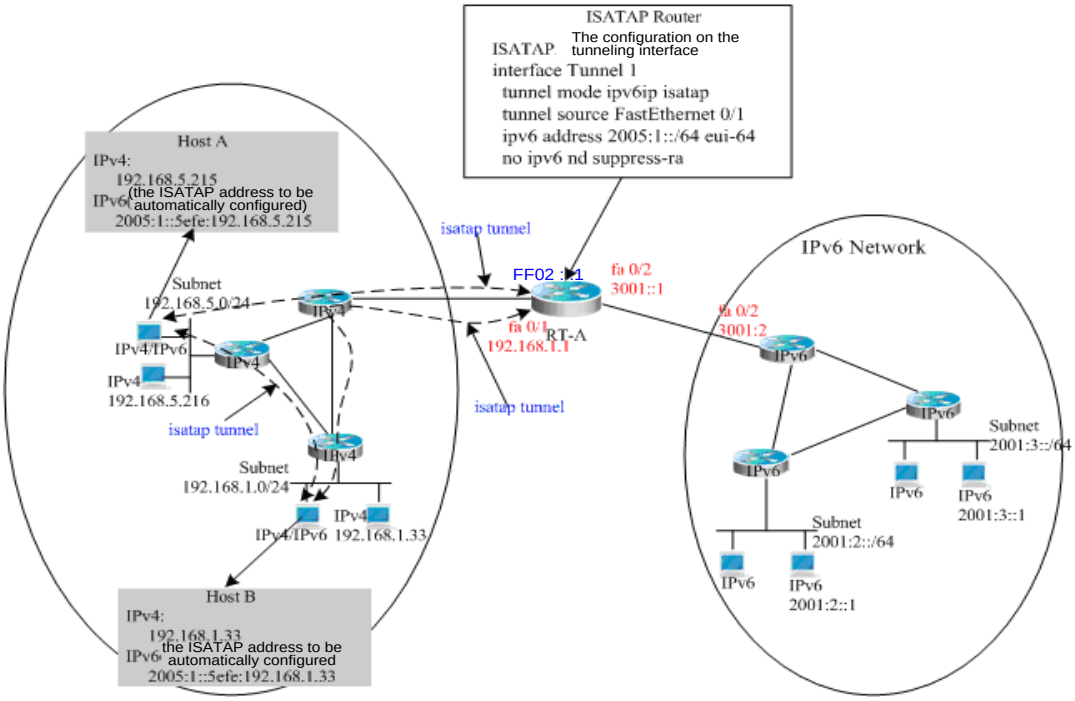
```
interface Tunnel 1
tunnel mode ipv6ip 6to4
ipv6 enable
tunnel source FastEthernet 0/1
```

Configure the route to the tunnel

```
ipv6 route 2002::/16 Tunnel 1
```

32.4.3 ISATAP Tunnel Configuration Instance

Figure 32-6



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 two following functions inside the ISATAP site:

- Receive a router request message from the ISATAP host inside the site and then respond with a router advertisement message for the ISATAP host inside the site to be automatically configured.
- Be responsible for the message forwarding function 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 message. After receiving the message, the hosts will be automatically configured and they also 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 message to the ISATAP router RT-A via the ISATAP tunnel and then RT-A forwards the message 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

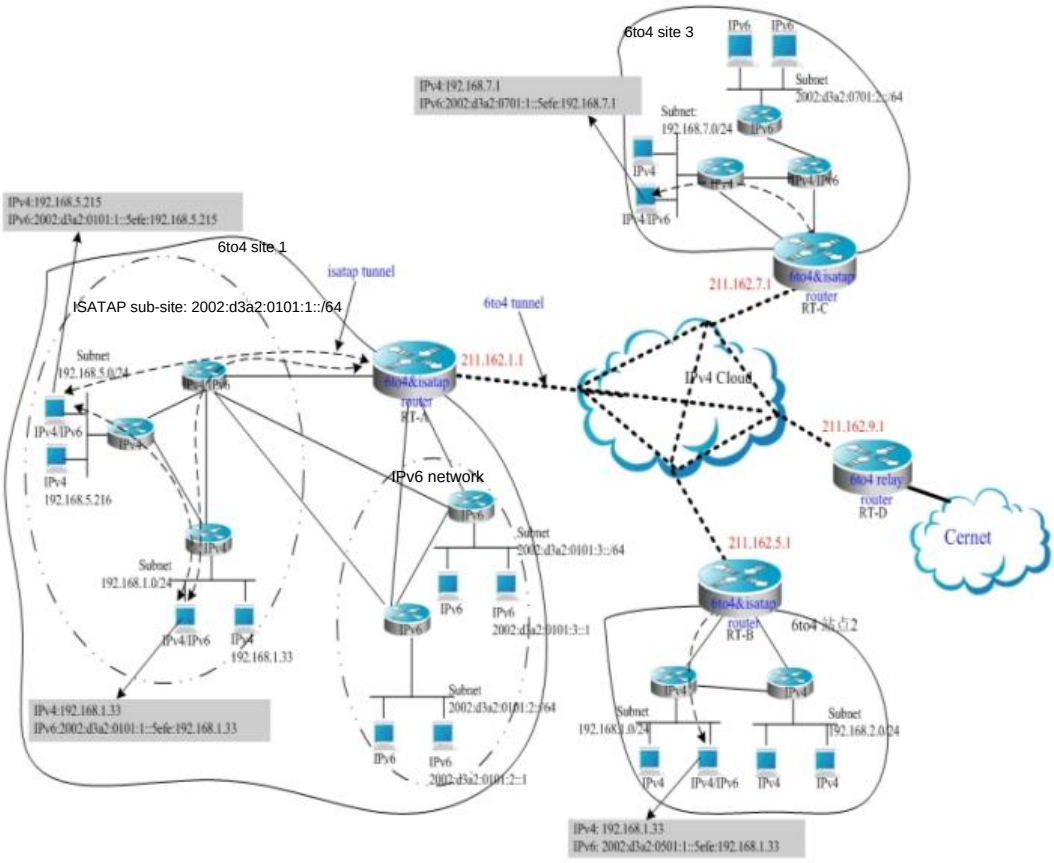
```
interface FastEthernet  0/2
no switchport
ipv6 address 3001::1/64
```

Configure the route to the IPv6 network

```
ipv6 route 2001::/64 3001::2
```

32.4.4 Configuration Instance for Composite Application of ISATAP and 6to4 Tunnels

Figure 32-7



Note

In the above figure, it is an instance about composite application of 6to4 tunnel and ISATAP tunnels. By use of 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, by use of 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 the addresses of 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 network

```
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 siteinterface 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 network

```
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 tunnel interfaceinterface 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 network

```
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 network

```
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
```

33 Configuring OSPFv3

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.

33.1 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.

33.1.1 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 of networks and address information. In contrast to the IPv4, the IPv6 uses a 128-bit IP address structure and makes the design of LSAs modified accordingly. Now, 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 is allowed to be generated for each device in each area. While in the OSPFv3, multiple

Router-LSAs are allowed to 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, they use a prefix structure to describe destination network information.

- 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, it uses a prefix structure to describe destination network information.

- NSSA-LSA (Type 7)

Their function is 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 link local 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 change 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, link local flooding scopes occur. Type 8 Link-LSAs is the type that can flood only inside a ink local flooding scope.

- Handling an unknown LSA type

This is an improvement made by the OSPFv3 based on the OSPFv2.

In the OSPFv2, during the time when establishing a adjacency relation, you need synchronize databases. At this time, if there is an irrecognizable LSA type in the database description message, then you are unable to normally establish the adjacency relation. If there is an unrecognizable LSA type in a link-state updating message, 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.

33.1.2 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 it is allowed to run multiple OSPF entities on a same links, then different devices connected by this link can select to participate in the running of an OSPF entity. The OSPFv2 does not support the function.

33.1.3 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 to use it 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.

33.1.4 Authentication Mechanism Setting

The OSPFv2 itself supports the 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 future, we will support the IPSec authentication mechanism.

33.2 OSPFv3 Basic Configuration

The OSPFv3 protocol of DES-7200 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;

To be implemented:

- 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 message sending interval	10 seconds
	Dead interval:	4 times the hello interval.
	LSA sending delay	1 seconds
	LSA retransmit interval.	5 seconds
	Priority	1
	MTU check of database description messages	Enable

Virtual Link	Virtual Link	Undefined
	hello message sending interval	10 seconds
	Dead interval:	4 times the hello interval.
	LSA sending delay	1 seconds
	LSA retransmit interval.	5 seconds
Area Configuration	Area	Undefined
	stub and NSSA area default router cost	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 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:
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 appropriae process.

33.3 Configuring OSPFv3 Interface Parameter

In the interface configuration mode, you can modify parameter values of an interface to meet practice application needs.

To configure an OSPFv3 interface parameter, run the following commands in the interface configuration mode:

Command	Function
ipv6 router ospf area *area-id* [**tag** *tag-name*| **instance** *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 message on an interface. For all nodes in the whole network, the vale must be 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 will be impossible to establish the adjacency relation. These parameters include the following: **instance, hello-interval and dead-interval.**

33.4 Configuring OSPFv3 Area Parameter

The OSPF protocol applies the concept of “hierarchical structure”, allowing a network to be divided into a group of parts connected through a “backbone” in mutual independence. These parts are called Areas. The backbone part is called Backbone Area and always 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 messages 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, then we can design the area as a stub area.

If an area is designed as a stub area, then 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

about little route information, reducing the system resources to be required to run the OSPF protocol.

If a device inside a stub area need reach outside AS, then 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.

A NSSA is extended from a stub Area and also block 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*	Configure a normal area.
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.

33.4.1 Configurring OSPFv3 Virtual Connection

In the OSPF, all areas must connect to the backbone area to ensure the communication with other areas.I f some areas cannot connect to the backbone area, then they must use virtual connections to connect the backbone area.

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 same to that of a normal interface. You must ensure that the configurations of **instance, hello-interval** and **dead-interval** configured at the two ends of the virtual connection are identical.

33.5 Configuring OSPFv3 Route Information Convergence

The switches in a network have to maintain all the routing information of the whole networks without route summarization. After convergence is used, some information can be integrated to alleviate the burden on the L3 equipment and network bandwidth. The larger the networks are, the more important the route summarization becomes.

Layer 3 devices of D-Link Corporation support two route convergence configurations: inter-area convergence and eternal route convergence.

33.5.1 Configuring Area Convergence

The ABR of the OSPF need tell the information of the routes in one area to other areas. If the route address of the area is continuous, then 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.

33.5.2 Configuring External Route Convergence

In the firmware v10.1, currently our products do not support the configuration of external route convergence.

Caution

Currently, our products do not support external route convergence with the tag parameter.

33.6 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, then the automatically calculated interface cost value of the network interface is 100/10=10.

Currently, the setting of the bandwidth for network interfaces of DES-7200 is defaulted to 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.

33.7 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 design conditions, you can use 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 a database, to make the refresh, aging, check and calculation as synchronous as possible 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.

If you need adjust OSPF LSA information pace, then run the following command in the OSPFv3 configuration mode:

33.7.1 Configuring OSPFv3 Route Redistribution

Route information retribution can reattribute the route information of one route protocol to another route protocol.

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 routing protocol. You can set the conditions of redistribution. Currently, the OSPFv3 supports static, connect, rip, bgp and isis route redistribution. At present, the OSPFv3 supports static routes, connect routes, rip, bgp and isis route distribution..
default-metric *number*	Configure the default measurement value of distribution 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.

33.7.2 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, then this network interface will receive/send no OSPF message.

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.

33.8 OSPFv3 Debug and Monitoring

The OSPFv3 process supports plenty of debug commands and monitoring commands.

33.8.1 OSPFv3 Debug Command

In the privileged configuration mode, use 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 will affect the performance of the system in a certain extent.

Therefore, after running debug commands, be sure to use undebug commands to protect the performance of the system.

33.8.2 OSPFv3 Monitoring Command

In the privileged configuration mode, use 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 [*process-tag*] **database** [**lsa-type** [**adv-router** *router-id*]]	Show the database information of the OSPFv3 process
show ipv6 ospf interface [*interface-type interface-number*]	Show the interface information of the OSPFv3 process
show ipv6 ospf neighbor[*process-tag*] [**detail**] [*neighbor-id* | *interface-type interface-number* [*neighbor-id*]]	Show the neighbor information of the OSPFv3 process.
show ipv6 ospf [*process-tag*] **route**	Show the OSPFv3 route information.
show ipv6 ospf [*process-tag*] **topology** [**area** *area-id*]	Show each area topology of the OSPFv3.
show ipv6 ospf [*process-tag*] **virtual-links**	Show the virtual link information of the OSPFv3 process.

34 Configuring IGMP Snooping

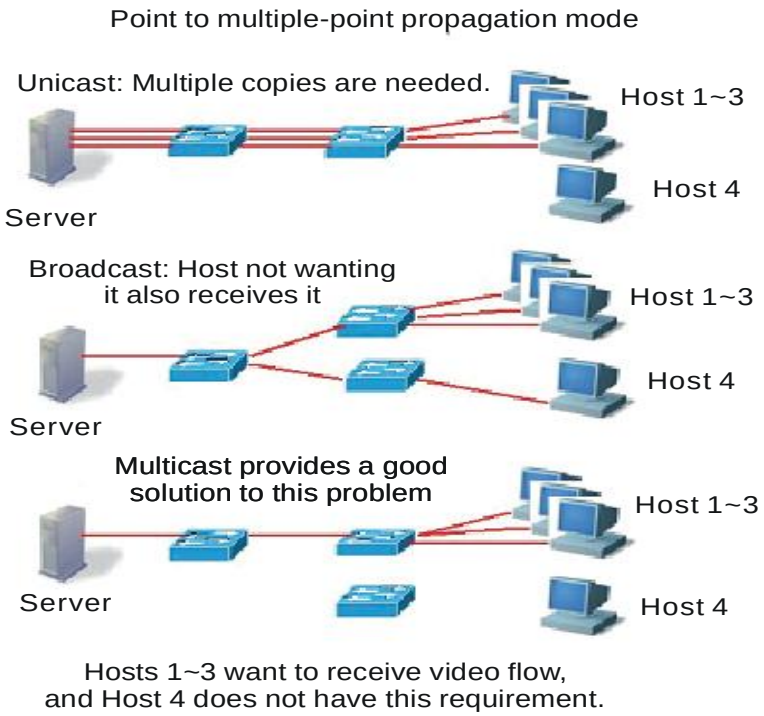
34.1 Overview

34.1.1 Understanding IGMP

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

On the Internet, the one point to multiple-point multimedia services such as video conference and video on demand (VOD) 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 34-1



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 router connected to the host. Through this protocol, the host tells 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 the 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 if 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.

34.1.2 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 certain 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.

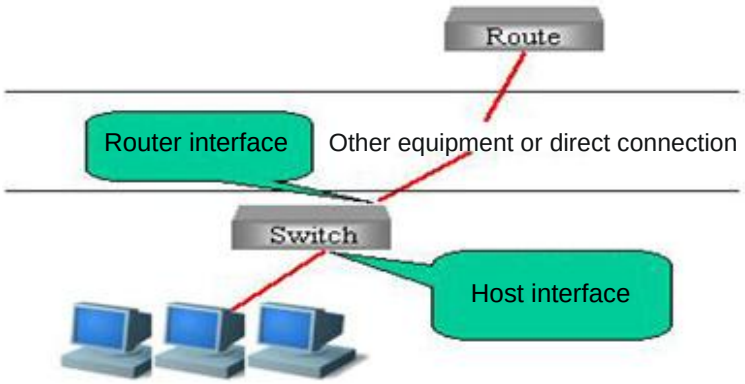
The function of IGMP Snooping is to solve this problem. It can enable the video flow to be forwarded only to the port where the register user is located, without influencing other users.

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 Snooping is “eavesdrop”. 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 applied port. 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.

34.1.3 Understanding Router Interface

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

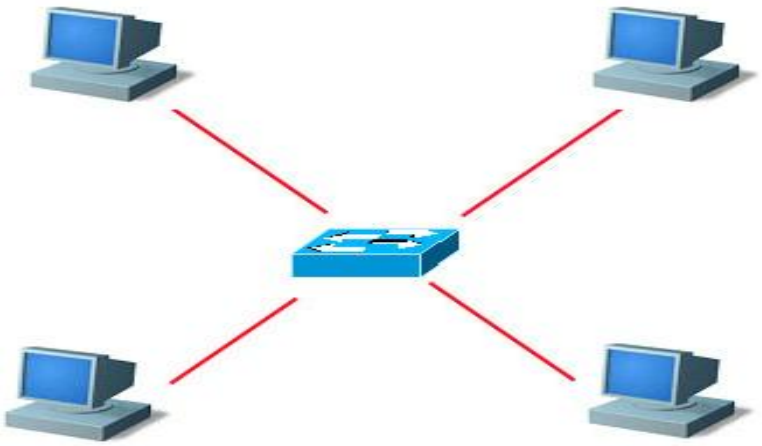
Figure 34-2



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, and IGMP Query messages received from non-router interface will be discarded. How to configure route connection, see the Configuring Router Interface section.

Note: 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:

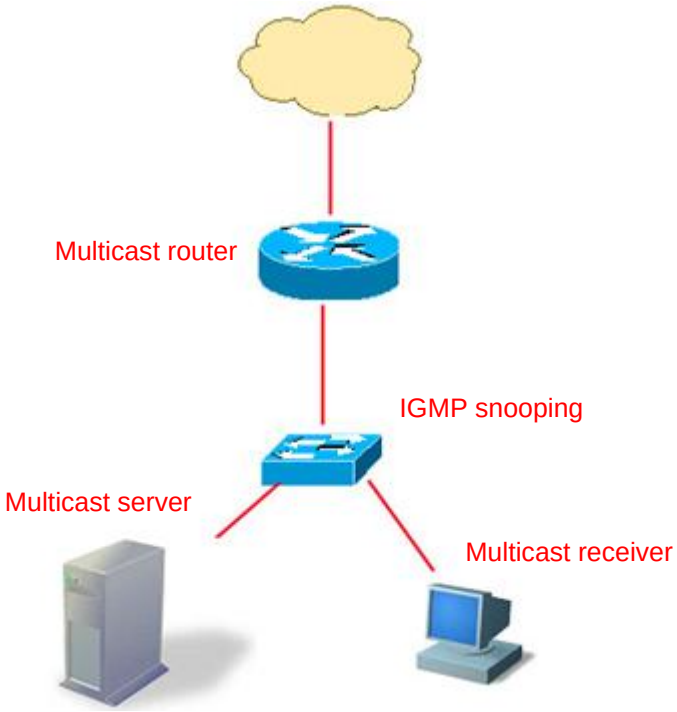
Figure 34-3



In this network environment, there is no multicast router, and these four PC can be both multicast flow senders and multicast flow receivers. Here, 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 34-4



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. Our switch can configure the router interface to make sure which multicast data needs forwarding, and which multicast data needs filtering, to satisfy the network administrator's requirements.

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 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. The administrator is recommended to directly configure one static multicast entry for the route connection interface (Please see Configuring IGMP snooping Static Member) to ensure stable forwarding of the multicast traffic.

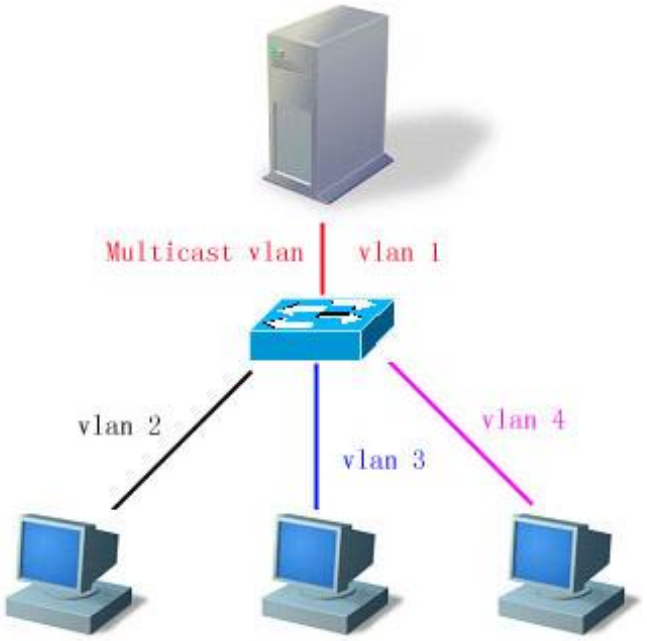
34.1.4 Understanding Operation Modes of IGMP Snooping

DISABLE mode: In this mode, IGMP Snooping does not function, that is, the switch does not "snoop" the IGMP message or multicast frame between the host and the router 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 34-5



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 DES-7200 strengthens the network application flexibility, enabling it to adapt to different network environment.

34.1.5 Understanding Source Port Check

DES-7200 support IGMP source port check function which can 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.

34.1.6 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.

34.1.7 Understanding IGMP Snooping Suppression

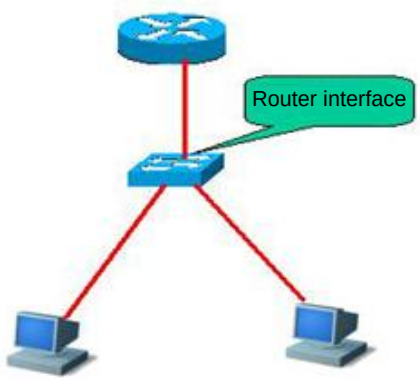
For the devices enabled with IGMP Snooping, every group address may have multiple IGMP users. When every user joins the group and receives the Query message, it will send a Report packet. For every Report packet, DES-7200 will forward it to the multicast router. In this way, when the multicast router sends a Query to the port enabled with the Snooping device, it will receive multiple Report packets. To reduce 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 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.

34.1.8 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 34-6



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.

34.2 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 the Aging Time of the Route Interface in Dynamic Learning
- 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 Snooping Suppression
- Configuration IGMP Filtering

34.2.1 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.
SVGL Multicast Vlan	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 possible that your expected requirement cannot be met. 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.

34.2.2 Configuring IGMP Profiles

Let us first describe a IGMP Profile entry, which can define a set of multicast address ranges and permit/deny actions for use by subsequent “multicast address range for SVGL mode”, “route connection interface filtering multicast data range” and “IGMP Filtering range”. Note that: After an IGMP Profile is already associated with a function, 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
DES-7200(config)# **ip igmp profile** *profile-number*	Enter IGMP Profile mode, and allocate a number for identification. The range is 1–65535.
DES-7200(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.
DES-7200(config-profile)# **range** *ip multicast-address*	Add one or more multicast address ranges.

DES-7200# **end**	Save the configuration.

To delete one of the IGMP profiles, use **no ip igmp profile** *profile number*.

To delete one of the ranges in the file, use **no range** *ip multicast address*.

This example shows the profile configuration process:

```
DES-7200(config)# ip igmp profile 1
DES-7200(config-profile)# permit
DES-7200(config-profile)# range 224.1.1.1 225.1.1.1
DES-7200(config-profile)# range 226.1.1.1
DES-7200(config-profile)# end
DES-7200# 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 will be to permit the multicast addresses 224.1.1.1 to 225.1.1.1, and 226.1.1.1, while all other multicast addresses are denied.

34.2.3 Configuring Router Interface

The router interface is the port for the multicast router to connect switch port (it does not refer to the port connecting video server). When the source port check is on, 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 it to let the switch dynamically snoop the IGMP query/dvmrp 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**
DES-7200(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 it to let the switch dynamically learn the router interface. Use the no form of the corresponding no command to disable the dynamic learning and clear all router interfaces learned through dynamic learning. By default, dynamic learning is disabled
DES-7200(config)# **end**	Return to the privileged mode.

This example sets the Ethernet interface 1/1 as the router interface, and configures the automatic learning router interface:

```
DES-7200# configure terminal
```

```
DES-7200(config)# ip igmp snooping vlan 1 mrouter interface gigabitEthernet 0/7
DES-7200(config)# ip igmp snooping vlan 1 mrouter learn pim-dvmrp
DES-7200(config)# end
DES-7200# show ip igmp snooping mrouter
Vlan    Interface        State       IGMP profile
----    ---------        ------      -------------
1   GigabitEthernet 0/7   static          0
1   GigabitEthernet 0/12  dynamic         0
DES-7200# show ip igmp snooping mrouter learn
Vlan   learn method
----   ------------------
1      pim-dvmrp
```

34.2.4 Configuring Range of Multicast Frame Forwarding by Router Interface

As the router interface default is to forward the multicast data flow as the member of all multicast addressed within this VLAN. 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 forwarding of the route interface connected by performing the following steps:

Command	Function
DES-7200(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.
DES-7200(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 forwarding by the router interface:

```
DES-7200# configure terminal
DES-7200(config)# ip igmp Snooping vlan 1 mrouter interface gigabitEthernet 0/7 profile
1
DES-7200(config)# end
DES-7200# show ip igmp Snooping mrouter
Vlan    Interface        State    IGMP profile
----    ---------        ------   -------------
1   GigabitEthernet 0/7   static       1
1   GigabitEthernet 0/12  dynamic      0
```

34.2.5 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 within the aging time, the route interface learnt will be deleted. The following commands can set the aging time within the 1-3600s range.

In the configuration mode, configure the range of the multicast frame forwarding of the route interface connected by performing the following steps:

Command	Function
DES-7200(config)# **ip igmp snooping dyn-mr-aging-time** *time*	Configure the dynamic router port aging time, *Time:* <1-3600> The default is 300s.
DES-7200(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:

```
DES-7200# configure terminal
DES-7200(config)# ip igmp snooping dyn-mr-aging-time 100
DES-7200(config)# end
```

34.2.6 Configuring IVGL Mode

In the configuration mode, enable IGMP Snooping and set its mode as IVGL mode by performing the following steps:

Command	Function
DES-7200(config)# **ip igmp Snooping ivgl**	Enable IGMP Snooping and set it to the IVGL mode.
DES-7200(config)# end	Return to the privileged mode.

This examples enables IGMP Snooping and sets it to the IVGL mode:

```
DES-7200# configure Terminal
DES-7200(config)# IP igmp Snooping ivgl
DES-7200(config)# end
```

34.2.7 Configuring SVGL Mode

In the configuration mode, enable IGMP Snooping and set its mode as SVGL mode by performing the following steps:

Command	Function
DES-7200(config)# **ip igmp snooping svgl**	Enable IGMP Snooping and configure it as the SVGL mode.
DES-7200(config)# **end**	Return to the privileged mode.

This example enables IGMP Snooping, and sets it to the SVGL mode,

```
DES-7200# configure Terminal
DES-7200(config)# iP igmp snooping svgl
DES-7200(config)# end
```

34.2.8 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
DES-7200(config)# **ip igmp snooping ivgl-svgl**	Enable IGMP Snooping and configure it as the IVGL, SVGL coexistence mode
DES-7200(config)# **end**	Return to the privileged mode.

This examples enables IGMP Snooping and sets it to the IVGL mode:

```
DES-7200# configure Terminal
DES-7200(config)# iP igmp snooping ivgl-svgl
DES-7200(config)# end
```

34.2.9 Configuring DISABLE Mode

In the configuration mode, set IGMP Snooping to the DISABLE mode by performing the following steps:

Command	Function
DES-7200(config)# **no ip igmp snooping**	Disable IGMP Snooping
DES-7200(config)# **end**	Return to the privileged EXEC mode.

34.2.10 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 privileged mode, you can set the maximum response period for Query packets by performing the following steps:

Command	Function
DES-7200(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.
DES-7200(config)# **end**	Return to the privileged EXEC mode.

Use **no ip igmp snooping query-max-response-time** to restore its default value.

34.2.11 Configuring Source Port Check

In the configuration mode, set source port check by performing the following steps:

Command	Function
DES-7200(config)# **ip igmp Snooping source-check port.**	Open source port check.
DES-7200(config)# **end**	Return to the privileged EXEC mode.

You can disable source port check by using the **no ip igmp snooping source-check port** command.

34.2.12 Configuring Source IP Check

In the privileged mode, you can set igmp snooping source IP check by performing the following steps:

Command	Function
DES-7200(config)# **ip igmp snooping source-check default-server** *address*	Enable source IP check and add the multicast-source IP entry.
DES-7200(config)# **ip igmp snooping limit-ipmc vlan** *vid* **address** *address* **server** *address*	Add multicast addresses—source IP address (multicast server address) corresponding entry

DES-7200(config)# **end**	Return to the privileged EXEC mode.

You can disable source IP check by using the **no ip igmp snooping source-check default-server** command.

The above 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.

```
DES-7200# configure Terminal
DES-7200(config)# ip igmp snooping source-check default-server 192.1.1.1
DES-7200(config)# ip igmp snooping limit-ipmc vlan 1 address 224.1.1.1 server 192.1.2.3
DES-7200(config)# end
```

34.2.13 Configuring Fast-Leave

In the configuration mode, set **igmp snooping fast-leave** by performing the following steps:

Command	Function
DES-7200(config)# **ip igmp snooping fast-leave enable**	Enable the fast-leave function on the switch.
DES-7200(config)# **end**	Return to the privileged EXEC 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:

```
DES-7200# configure Terminal
DES-7200(config)# ip igmp snooping fast-leave enalbe
DES-7200(config)# end
```

34.2.14 Configuring IGMP Snooping Suppression

In the configuration mode, set **igmp snooping suppression** by performing the following steps:

Command	Function
DES-7200(config)# **ip igmp snooping suppression enable**	Enable the suppression function on the switch.
DES-7200(config)# **end**	Return to the privileged EXEC mode.

You can disable the Suppression function by using the **no ip igmp snooping suppression enable** command.

The following example enables the Suppression function:

```
DES-7200# configure Terminal
DES-7200(config)# ip igmp snooping suppression enalbe
DES-7200(config)# end
```

34.2.15 Configuring Static Members of IGMP Snooping

When igmp snooping is enabled, you can statically configure a port to receive a specific multicast stream, disregard of various IGMP packets.

In the configuration mode, set the static member of IGMP Snooping by performing the following steps:

Command	Function
DES-7200(config)# **ip igmp Snooping ivgl**	Enable IGMP Snooping and set it to the **IVGL** mode.
DES-7200(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
DES-7200(config)# **end**	Return to the privileged EXEC 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:

```
DES-7200# configure Terminal
DES-7200(config)# ip igmp snooping vlan 1 static 224.1.1.1 interface GigabitEthernet 0/7
DES-7200(config)# end
DES-7200(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)
```

34.2.16 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 satisfies 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
DES-7200(config)# **interface** *interface-id*	Enter the configuration interface.
DES-7200(config-if)# **ip igmp snooping filter** *profile-number*	(Optional) apply the profile to this port. The profile number range is 1- 65535.
DES-7200(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.
DES-7200(config-if)# **end**	Return to the privileged EXEC mode.

34.3 Viewing IGMP Snooping Information

Related to the information of IGMP snooping, please refer to the following information:

- Viewing Current Mode
- View Router Interface Information
- Viewing Dynamic Forwarding Table
- Viewing Source Port Check Status
- Viewing IGMP Profile
- Viewing IGMP Filtering

34.3.1 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
DES-7200# **show ip igmp snooping**	View the current operation mode of IGMP Snooping and global configuration.

The following example uses the **show ip igmp snooping** command to view the IGMP Snooping configuration information:

```
DES-7200# 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)
```

34.3.2 Viewing and Clearing IGMP snooping Statistics

In the privileged mode, view and clear the IGMP Filtering statistics by using the following commands:

Command	Function
DES-7200# **show ip igmp snooping statistics** [**vlan** *vlan-id*]	View the IGMP Snooping statistics
DES-7200# **clear ip igmp snooping statistics**	Clear the IGMP Snooping statistics

The following example uses the **show ip igmp snooping statistics** command to view the IGMP Snooping router interface information:

```
DES-7200# 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
```

34.3.3 View Router Interface Information

In the privileged mode, view the IGMP Filtering router interface information by using the following command:

Command	Function
DES-7200# **show ip igmp snooping mrouter**	Show the route connection port information of IGMP Snooping

The following example uses the **show ip igmp snooping** command to view the IGMP Snooping router interface information:

```
DES-7200# show ip igmp snooping mrouter
Vlan    Interface          State       IGMP profile number
----    --------           -------     -------------------
1   GigabitEthernet 0/7    static       1
1   GigabitEthernet 0/12   dynamic      0
```

34.3.4 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
DES-7200# **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:

```
DES-7200# 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)
```

34.3.5 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
DES-7200# **show ip igmp snooping**	View the current operation mode of IGMP Snooping and global configuration.

34.3.6 Viewing IGMP Profile

In the privileged mode, view the IGMP Profile information by using the following command:

Command	Function
DES-7200# **show ip igmp profile** *profile-number*	View the IGMP Profile information.

34.3.7 Viewing IGMP Filtering

In the privileged mode, view the IGMP Filtering configuring information by using the following command:

Command	Function
DES-7200# **show ip igmp snooping interface** *interface-id*	View IGMP Filtering configuration information.

The following serves to view IGMP Filtering information.

```
DES-7200# show ip igmp snooping interface GigabitEthernet 0/7
Interface         Filter Profile number     max-groups
----------       ----------------------    -----------
GigabitEthernet 0/7          1               4294967294
```

34.3.8 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 *"Configuring Secure ACLs*". Address binding, source port check and ACL share the filtering domain masks. The total number of templates available depends on the specific products. As the number of filtering domain masks is limited, these three functions will influence one another. Enable the address binding function needs to occupy two masks, enabling the source port check occupies two masks, and the usable masks of 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 the ACL can reduce two masks. If the address binding and source port check are concurrently enabled, then the number of usable masks by ACL is reduced by 4, and only four are left. Contrarily, if the ACL uses multiple masks and the number of left masks cannot satisfy 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 time, the system prompts: source port check applying failed for hardware out of resources. In this case, you should release other templates, disable and then enable source port check.

35 Configuring IGMP

35.1 IGMP Overview

The IP multicast is a network technology that enables one or many senders (multicast source) to send a single packet to multiple receivers at the same time.The multicast source sends packets to the specific multicast group, and only the hosts with addresses in the multicast group can receive the packets.Multicast can save much network bandwidth, because any link in the network only has one single packet no matter how many destination addresses.

The IANA-specified type D network addresses are used for multicast. Type D network addresses have the highest bit 1110. So, the multicast address range is 224.0.0.0 - 239.255.255.255. However, not all addresses can be used by the users because some are reserved for the use of protocols or other addresses. For example, 224.0.0.1 indicates all multicast host addresses, and 224.0.0.2 indicates multicast device addresses.

Any host as a member of a multicast group or not can act as a multicast source. However, only a member of a multicast group can receive multicast frames. The members in a multicast group are dynamic, and hosts can join or leave a group dynamically. Multicast frames are forwarded in the network by multicast device on which the multicast routing protocol runs.

To join the IP multicast, the multicast hosts and device have to support the IGMP operations. The host uses this protocol notify the multicast membership to the devices that have direct network connections with it, to determine the forwarding of the multicast flow. With the information gained from IGMP, the device maintains a multicast member list that is specific to every interface. The multicast member list is activated only when at least one host of an interface is a member of the group.

Currently the IGMP is available in two versions - IGMPv2 is built on the basis of IGMPv1, and enables the host to proactively request leaving the multicast group by adding a Leave message. The behaviors of the IGMP can be divided into the host behaviors and the device behaviors.

35.1.1 Messages of Different Versions of IGMP

35.1.1.1 IGMP Version 1

There are two types of messages in version 1:

- Membership query
- Membership report

A host sends a report packet to join a group, and the device sends the query packet at a periodical interval to ensure that the group has at least one host. When a group contains no host, the device will delete that group.

35.1.1.2 IGMP Version 2

In Version 2, there are only four types of packets:

- Membership query
- Version 1 membership report
- Version 2 membership report
- Leave group

Similar to version 1 in terms of the processes, the quit mechanism of the host is improved. Version 2 support to send the Leave message to notify the device, and then the device sends the Query message to confirm whether the host still survives. Thus, the efficiency in joining and leaving is increased.

Meanwhile, version 2 deals with the situation of multiple devices in multi-access network. In the multicast network that runs the IGMP protocol, there is query-dedicated multicast device that is responsible for sending the IGMP query messages. This dedicated device is produced by the process of election. At the beginning all devices are in the status of querier. When the device receives the membership query from the device with a low IP address, the former becomes from the receiver status into the non-querier status. In this way, there is only one device in the query status finally. This device is the one with the lowest IP address among all of the multicast devices.

When the querier device fails, the IGMPv2 will handle that. The non-querier device maintains the current interval timer of the other queriers. Each time the device receives the membership query message, it will reset this timer. If the timer times out, that device starts to send the query message, and another round of device election begins.

The querier device must send the membership query requests at a regular basis to make sure that the other devices in the network knows the querier device is still working well. To function perfectly, the querier device maintains a query interval timer. When the membership query message is sent, this timer will be reset. When the interval timer is zero or not needed any more, the querier device 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 messages to see which multicast groups shall be forwarded on a specific interface. Those general query messages sent by the device are based on the startup query count value as configured on the device. The querying interval between the initial general query messages is defined through the startup query interval.

When the querier device receives the Leave message, it must send the membership query of a specific group to determine whether the host is the last one leaving the group. The device sends a series of this kind of messages before it stops forwarding packets for that group, and the number of messages is equal to the last number of membership queries. The device will send multiple specific group membership queries to ensure there is no member any more in that group. Such a query is sent every other the seconds of the last-member query interval to separate the queries. When no answer to the query is received, the device stops forwarding multicast communications for that group address on that specific interface.

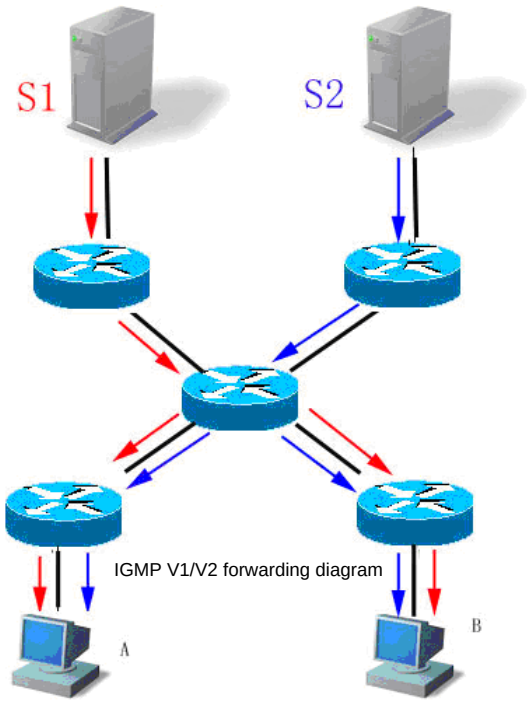
35.1.1.3 IGMP Version 3

The following defects exist in the IGMPV1 and V2 applications:

- 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.

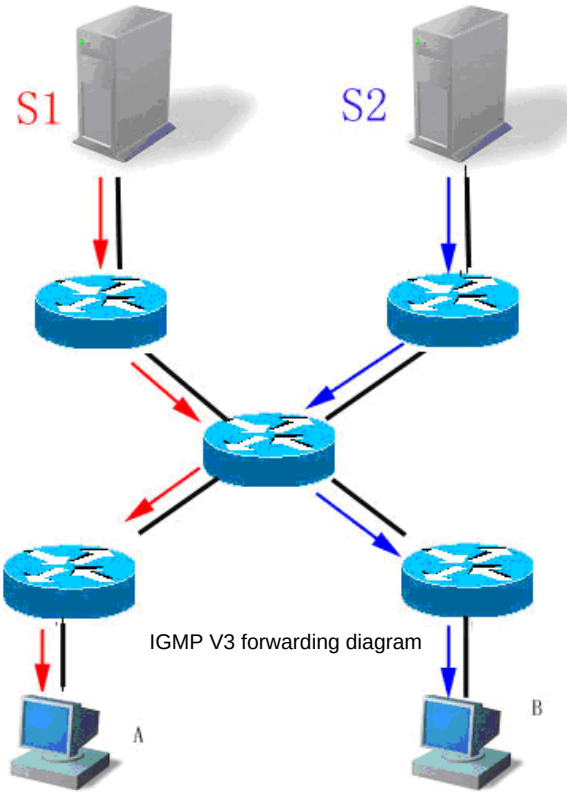
On the basis of the IGMPV1/V2, the IGMPV3 provides an additional source filtering multicast function. In the IGMP V1/V2, the host determines to join a group and receive the multicast traffic to the group address from any source only based on the group address. By contrast, the host running the IGMP V3 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.Both IGMPv1 and IGMPv2 implement certain “source address based filtering” but this is done on the receiving end of the multicast flow. See the figure below.There are multicast sources S1 and S2 that are sending the dataflow 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 35-1



If the device in the network supports IGMPv3, host A wants to receive the dataflow only from S1 by sending the “join G include S1” IGMPv3 message; host B wants to receive the dataflow only from S2 by sending the “join G include S2” IGMPv3 message. The dataflow forwarding is shown below, resulting in save of bandwidth.

Figure 35-2



In contrast to Version 2, Version 3 defines the following two kinds of messages:

- Membership Query
- Version 3 Membership Report

There are three types of Membership Query:

- General Query: Used to query the 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 if any member under the interface needs to receive the multicast traffic of the particular group from the sources in the specified source list.

Unlike the Membership Report in IGMP Version2, that sent in IGMP Version3 contains the fixed destination address 224.0.0.22, and can contain the information of multiple groups.

The IGMP Version3 also recognizes the Membership Report of both Versions 1 and 2 and the Leave Group message 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.

35.2 IGMP Configuration Task List

IGMP configuration tasks include the following items, but only the first one is required, and the others are optional depending on the actual network requirement.Note that the following commands must be configured under layer-3 interface:

- Configuring the IGMP service enablement (required)
- Configuring the IGMP version (required)
- Configuring the last-member query interval (optional)
- Configuring the last-member query count (optional)
- Configuring the general membership query interval (optional)
- Configuring the maximum response interval (optional)
- Configuring the timer interval of the other queriers (optional)
- Configuring the multicast group access control (optional)
- Configuring to leave group immediately (optional)
- Configuring the IGMP status quantity limit (optional)
- Clearing the dynamic group membership from response message in the IGMP cache (optional)
- Clearing all information of specific interface in the IGMP cache (optional)
- Showing the statuses of group members in the direct-connected subnet (optional)
- Showing the configuration information of the IGMP interface (optional)
- Showing the on/off status of the IGMP debug switch (optional)
- Turning on the IGMP debug switch (optional)

35.2.1 Default IGMP Configurations

IGMP version	**All interfaces support Version 3**
Query response period	10 seconds
Query interval	125 seconds
Multicast group access control	Allowing all groups
Interval of other query timers	255 seconds
Robustness variables	2
Last-member query interval	1000 milliseconds
Last-member query count	2
IGMP status	Off

35.2.2 Enabling IGMP

To enable the IGMP, run the following commands in the interface mode:

Command	Function
DES-7200(config-if) # **ip igmp**	Enable IGMP.
DES-7200(config-if) # **no ip igmp**	Disable IGMP.

35.2.3 Configuring IGMP Version

To configure the IGMP version, run the following commands in the interface mode:

Command	Function
DES-7200(config-if) # **ip igmp version {1|2|3}**	Configure the IGMP version.
DES-7200(config-if) # **no ip igmp version**	Restore the IGMP version to the default value V2.

35.2.4 Configuring Query Interval of the Last Member

When the message 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 period, 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 10 ms.

Run the following commands for configuration in the interface mode:

Command	Function
DES-7200(config-if) **# ip igmp last-member-query-interval** *interval*	Configure the query interval of the last member Interval range: <1-255> Unit:ms
DES-7200(config-if) **# no ip igmp last-member-query-interval**	Configure the last-member query interval as the default value.

35.2.5 Configuring Query Count of the Last Member

To prevent the loss of specific membership query message sent by the querier device, it will be sent for several times to ensure the reliability. That is why to configure the query count of the last member.

Run the following commands in the interface mode:

Command	Function
DES-7200(config-if) # **ip igmp last-member-query-count** *count*	Configure query count of the last member The default range is 2 - 7. The default value is 2.
DES-7200(config-if) # **no ip igmp last-member-query-count**	Configure the last-member query count as the default value.

35.2.6 Configuring the General Membership Query Interval

Whenever a group membership query interval period passes, the querier device sends the membership query message on regular basis to verify the current membership. The destination address to send the group membership query message 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
DES-7200(config-if) # **ip igmp query-interval** *seconds*	Configure the general membership query interval.
DES-7200(config-if) # **no ip igmp query-interval**	Configure the general member query interval as the default value.

35.2.7 Configuring the Maximum Response Interval

The membership query message sent by the querier device requires the maximum response interval. To decrease that interval can make the device know the change of the members earlier, 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 period.

Run the following commands for configuration in the privileged mode:

Command	Function
DES-7200(config-if)# **ip igmp query-max-response-time** *seconds*	Configure the maximum response interval. The range is 1-18,000, in seconds.
DES-7200(config-if)# **no ip igmp query-max-response-time**	Configure the maximum response interval as the default value, 125 s by default.

35.2.8 Configuring the Timer Interval of the Other Queriers

Configuring the timer interval of the other querier can adjust the time to elect the querier device. In case the querier device changes frequently, this value can be decreased to speed up responses.

Run the following commands in the interface mode:

Command	Function
DES-7200(config-if)# **ip igmp query-timeout** *seconds*	Configure the timer interval of the other queriers. The range is 60 – 300, 255 s by default.
DES-7200(config-if)# **no ip igmp query-timeout**	Restore the timer interval of the other queriers as the default.

35.2.9 Configuring Multicast Group Access Control

By default, the hosts on an interface can join any multicast group. If the administrator hopes to limit the range of the multicast group that the host can join, this feature prevails. By configuring a standard IP access list, it is possible to set the multicast group address range to allow or deny, and then apply it to a specific interface.

Run the following commands in the interface mode:

Command	Function
DES-7200# **config terminal**	Enter the global configuration mode.
DES-7200(config) # **access-list** *access-list-name* **permit** A.B.C.D 0.0.0.0	Define a access control list.
DES-7200(config)# **interface** *interface-id*	Enter the interface configuration mode.

DES-7200(config-if) # **ip igmp access-group** *access-list-name*	Configure the multicast group within the range controlled by the control access list access-list-name to be able to enter that interface.
DES-7200(config-if) # **no ip igmp access-group**	Delete the control access list to allow the entry of all groups.

35.2.10 Configuring to Leave Group Immediately

In the IGMP version2, this command can be used to reduce the delay in leaving group. When the host issues this message, it shall leave immediately without the necessity for the querier device to send the specific group query.This command is suitable only when the interface has one receiving host.

Command	**Function**
DES-7200# **config terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** *interface-id*	Enter the interface configuration mode.
DES-7200(config-if)# **ip igmp immediate-leave group-list** *access-list-name*	Configure the immediate-leave from the group with list access-list-name.
DES-7200(config-if) # **exit**	Enter the privileged mode.
DES-7200(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 limitation for any group.

35.2.11 Configuring the IGMP Status Quantity Limit

This command in the global configuration mode is used to limit the IGMP status quantity of the IGMP, IGMPv3lite and URD reports. The messages 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 messages 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
DES-7200(config) # **ip igmp limt** *number*	Configure the IGMP Status quantity limit globally. Range: 1-65536
DES-7200(config-if) **# ip igmp limit** *number*	Configure the IGMP status quantity limit on the interface. The range is 1-65536, 1024 by default.

35.3 Monitoring and Maintaining the IGMP Status and Membership Information

35.3.1 Clearing the dynamic group memebership from responding message, stored in IGMP cache

To clear up dynamic group member information acquired from response message which is stored in IGMP cache, run the following command in privileged mode:

Command	Function
DES-7200# **clear ip igmp group**	Clear up the dynamic group membership from responding message, which is stored in IGMP cache. * indicates clearing all IGMP groups

35.3.2 Clearing all information of specific interface in the IGMP cache

To clear all information of specific interface in the IGMP cache, run the following command in the privileged mode:

Command	Function
DES-7200# **clear ip igmp interface** *interface-type*	Clear the interface information in the IGMP cache

35.3.3 Display the Status of IGMP Group Member in Directly-connected Subnet

Use the following command in privileged mode to display the status of IGMP group member in directly-connected subnet:

Command	Function
DES-7200# **show ip igmp groups**	Display the status of IGMP group member in directly-connected subnet.
DES-7200# **show ip igmp groups detail**	Show the details of all members in the directly-connected subnets.
DES-7200# **show ip igmp groups** *A.B.C.D*	Display the status of specified group member in directly-connected subnet.
DES-7200# **show ip igmp groups** *A.B.C.D* **Detail**	Show the details of the specified member in the directly-connected subnets.
DES-7200# **show ip igmp interface** *interface-type*	Show the information of the specified interface in the directly-connected subnets.
DES-7200# **show ip igmp groups** *interface-type* **detail**	Show the details of the specified interface in the directly-connected subnets.
DES-7200# **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.
DES-7200# **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.

35.3.4 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
DES-7200# **show ip igmp interface** [*interface-type interface-number*]	Show the configuration information of the IGMP interface.
DES-7200# **show ip igmp interface**	Show the configuration information of all the IGMP interfaces.

35.3.5 Showing the on/off status of the IGMP debug switch

To show the on/off status of the IGMP debug switch, run the following command in the privileged mode:

Command	Function
DES-7200# **show debugging**	Show the on/off status of the IGMP debug switch.

35.3.6 Turning on IGMP debug switch to display IGMP behaviors

To turn on IGMP debug switch and display IGMP behavior, use the following command in the privileged mode:

Command	Function
DES-7200# **debug ip igmp all**	Turn on all IGMP debug switches
DES-7200# **debug ip igmp decode**	Turn on IGMP debug decode switch
DES-7200# **debug ip igmp encode**	Turn on IGMP debug encode switch
DES-7200# **debug ip igmp events**	Turn on IGMP debug event switch
DES-7200# **debug ip igmp fsm**	Turn on IGMP debug final-state-machine switch
DES-7200# **debug igmp tib**	Turn on IGMP debug tree switch.
DES-7200# **debug ip igmp warnning**	Turn on IGMP debug warning switch.

36 Configuring PIM-DM Protocol

36.1 About the PIM-DM Protocol

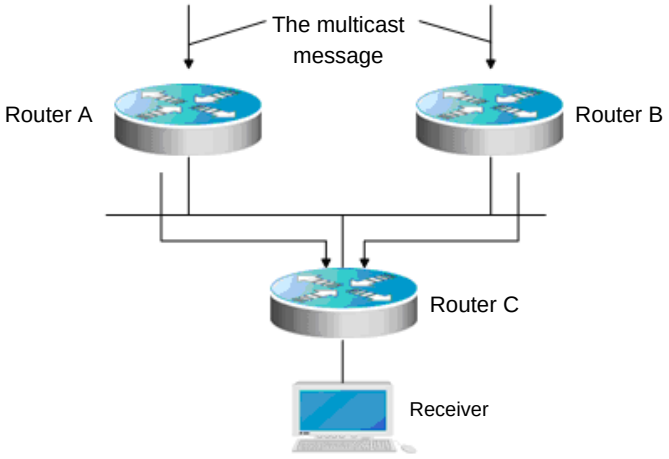
The Protocol Independent Multicast-Dense Mode (PIM-DM) is a dense mode multicast routing protocol that is suitable for small-scale network with relatively-concentrated multicast members. Because the PIM-DM is independent of any specific unicast routing protocol, it is considered a protocol independent multicast routing protocol. The PIM-DM is defined in the RFC 3973 documentation.

Neighbors are found between the PIM-DM device through the Hello message. Once the PIM-DM device is started, it sends the Hello message on regular basis on every interface with PIM-DM configured. The Hello message has a Hello Hold Time field, which defines the maximum duration for the neighbor to wait for the next message. If the neighbor does not receive the next Hello message from that device, it declares the death of the device.

The PIM-DM works with the “flood and prune” mechanism to set up the multicast tree. The PIM-DM assumes all systems need to receive the message when the multicast source starts to send the multicast message, and thus the message is forwarded to every system. Messages received from the upstream interface shall be RPF (Reverse Path Forwarding)-checked, where the messages that fail in the RPF check will be discarded. For the multicast messages that pass the RPF check, the device calculates the egress interface on the basis of the (S, G) pair, i.e. the source address and group address of the multicast message. If the calculated egress interface is not null, an outgoing entry is created for that (S, G) pair, and the multicast message is forwarded via the egress interface. Otherwise, it sends a prune message to the RPF to notify the upstream neighbor not to forward the multicast message from that (S, G) pair to this interface any more. When the upstream interface receives the prune message, it marks Pruned the interface that sends the prune message, and sets a prune status timer. In this way, a multicast forwarding tree is set up, with root of the multicast source.

The PIM-DM works with the Assert mechanism to eliminate redundant routes.

Figure 36-1 PIM-DM Assert mechanism



As shown in Figure 36-1 , the multicast message arrives at devices A and B at the same time, and both of them will forward it to device C. Now device C gets two copies of the same message, while this is not allowed. So, there must be a mechanism to select one between devices A and B to forward multicast messages to device and the other not. This is the Assert mechanism with PIM-DM.

The PIM-DM works with the State Refresh Message to update the network status information. The device with direct connection of the multicast source sends the status update messages on regular basis to notify the network topology changes. The devices that receive the status update message adds the topology status information of the local machine by modifying some fields in the message, and sends the message to the downstream device. When the message gets to the leaf device, the statuses of the whole network, from the top down, are refreshed.

The PIM-DM works with the Graft mechanism to rebuild the connection with upstream device. If the downstream device with the grafted status encounters network topology change, it needs to receive the multicast message from a (S, G) pair, and can send the graft message to the upstream device. When the upstream device receives the graft message, it responds with a Graft-Ack message and forwards again multicast messages to the device interface.

36.2 List of PIM-DM Configuration Tasks List

The PIM-DM configuration tasks involve the following items, where only the first and the second are required, and the remaining are optional depending on the actual network conditions.

- Enabling multicast routing (required)
- Enabling PIM-DM (required)
- Configuring the Hello message sent interval (optional)

- Configuring PIM neighbor filtering (optional)
- Configure PIM status refresh function (optional)
- Configure PIM status refresh message sent interval (optional)

36.2.1 Enabling multicast routing

Multicast messages cannot be forwarded unless the multicast routing is enabled, and to enable PIM-DM makes sense. For the command to enable multicast routing, see “Enable multicast routing”.

36.2.2 Enabling PIM-DM

The PIM-DM must be enabled on every interface separately. Only when PIM-DM is enabled on the device interfaces, it can have PIM-DM message interactions with other devices, maintain and update the multicast routing table, and forward multicast messages.

To configure PIM-DM on the interface, run the following command in the interface mode:

Command	Function
DES-7200(config-if)# ip pim dense-mode	Enable the PIM-DM protocol on the interface.
DES-7200(config-if)# no ip pim dense-mode	Disable the PIM-DM protocol on the interface.

In general cases, the PIM-DM protocol shall be enabled on all the interfaces of the device.

Caution

Enabling PIM-DM on the interface does not take effect until the multicast routing is enabled in the global configuration mode.

36.2.3 Configuring the Hello message sent interval

When the PIM-DM is enabled on the interface, it will send the Hello message on regular basis to the interfaces of the neighbor devices. The time interval at which an interface sends the Hello message to the interfaces of the neighbor device can be modified according to the actual conditions of the connected network.

To configure the Hello message sent interval, run the following commands in the interface mode:

Command	Function
DES-7200(config-if)# ip pim query-interval ***seconds***	Configure the Hello message sent interval of the interface as “seconds”, in seconds.

DES-7200(config-if)# no ip pim query-interval	Restore the Hello message sent interval of the interface to default.

By default, the Hello message sent interval of the interface is 30 seconds.

Note

Whenever the Hello message sent interval is updated, the Hello hold time automatically changes into 3.5 times the Hello message sent interval.

36.2.4 Configuring PIM neighbor filtering

Neighbor filtering function can be configured on the interface to enhance network security. With neighbor filtering enabled, as long as a neighbor is denies buy the filter access list, the PIM-DM will either not establish the neighborhood with that neighbor or stop the currently established neighborhood with that neighbor.

To configure the PIM neighbor filtering function, run the following command in the interface mode:

Command	Function
ip pim neighbor-filter *access-list*	Enable the PIM neighbor filtering function on the current interface.
no ip pim neighbor-filter *access-list*	Disable the PIM neighbor filtering function on the current interface.

The PIM neighbor filtering function is disabled by default on an interface.

Note

Notes on the **ip pim neighbor-filter** commands:

When the associated ACL rule is “permit”, only the neighbor address in the ACL can act as the PIM neighbor of the current interface. When the associated ACL rule is “deny”, the neighbor address in the ACL cannot act as the PIM neighbor of the current interface.

36.2.5 Configure PIM status refresh function

When the PIM-DM is enabled on the device, if the RPF interface of the multicast entry is directly connected with the multicast source (that is, there are some PIM interfaces in the same subnet of the multicast source), the status refresh messages will be sent to the downstream device on regular basis, so as to refresh the statuses of the whole network. It is possible to stop processing or forwarding the PIM-DM status refresh messages in the global mode.

To configure the PIM-DM status refresh function, run the following command in the global mode:

Command	Function
ip pim state-refresh disable	Disable processing or forwarding PIM-DM status refresh messages.
no ip pim state-refresh disable	Enable processing or forwarding PIM-DM status refresh messages.

By default, the status refresh function is enabled.

Caution

Disabling the status refresh function may cause the converged PIM-DM multicast forwarding tree to converge again, resulting in unwanted bandwidth waste and fluctuation of multicast routing table. Therefore, it is better not to disable the status refresh function in general cases.

36.2.6 Configure PIM status refresh message sent interval

When the PIM-DM is enabled on the device, if some interface is directly connected with the multicast source, the status refresh messages will be sent to the downstream device on regular basis, so as to refresh the statuses of the whole network.The PIM status refresh message sent interval of the interface can be modified according to the actual conditions of the network with the device.

To configure the PIM status message sent interval on the interface, run the following command in the interface mode:

Command	Function
ip pim state-refresh origination-interval *seconds*	Configure the PIM status refresh message sent interval of the current interface as “seconds”, where “seconds” is an integer within 1-100, in seconds.
no ip pim state-refresh origination-interval	Cancel the configuration of the PIM flood delay on the current interface.

By default, the PIM status refresh message sent interval of the interface is 60 seconds.

Note

Only the devices directly connected to multicast source can periodically send the PIM status updated message to the downward interfaces. Thus, if the devices are not directly connected to the multicast source, the forwarding interval of PIM status update message configured on the downforward interface is invalid.

36.3 Monitor and maintain PIM-DM

The PIM-DM provides a **show** command to monitor and maintain the PIM-DM. The **show** command can be used to view the PIM-DM interface, multicast group and multicast routing table.

36.3.1 Viewing PIM-DM Status Information

The RGONS10.1 provides the following command to check the PIM-DM status information on the local machine:

Command	Function
show ip pim dense-mode interface [*interface-type interface-number]* *[detail]*	Show the PIM-DM information on the interface.
show ip pim dense-mode neighbor [*interface-type interface-number*]	Show the PIM-DM neighbor information.

For details on the use of the above command, see *PIM-DM Command References*.

Here are some examples of the commands:

1. **show ip pim dense-mode interface detail:**

```
DES-7200# 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 example above, the wm0 has IP address 193.168.1.53, subnet 255.255.255.0, Hello message sent interval 30 seconds, next Hello message to be sent in 30 seconds, and two neighbors with addresses 192.168.1.152 and 192.168.1.149. The wm1 interface has similar information of the wm0 but has no neighbors.

2. **show ip pim dense-mode neighbor:**

```
DES-7200# 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
```

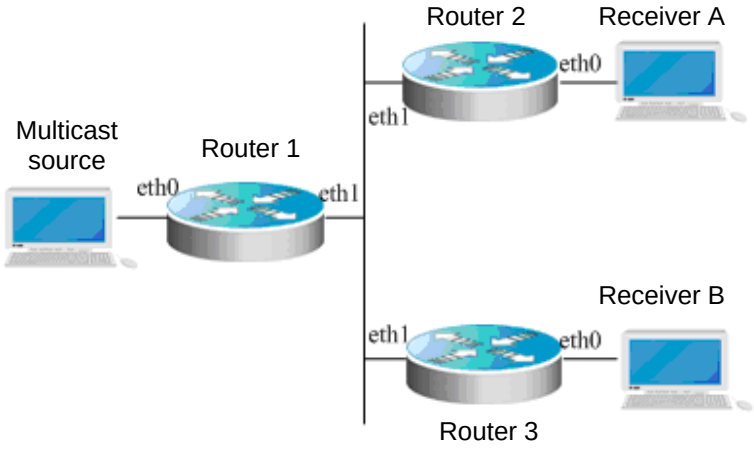
In the example above, the device has two neighbors, where neighbor 192.168.1.152 is connected with wm0 and has survived for 17 hours 16 minutes and 20 seconds, with neighbor survival period to expire in one minute and 20 seconds. Neighbors 192.168.1.149 and 192.168.1.149 are similar.

36.4 PIM-DM Configuration Examples

36.4.1 Configuration requirements

The network topology is shown in Figure 36-2 . Device 1 is in the same network of the multicast source, device 2 is in the same network of receiver A, and device 3 is in the same network of receiver B. It is assumed that the devices and hosts are connected properly and configured with IP addresses.

Figure 36-2 Topology of the PIM-DM configuration example



36.4.2 Device Configuration

With device 1 as the example, the procedure shows how to configure PIM-DM, similar configurations for devices 2 and 3.

Step 1: Enable multicast routing.

```
DES-7200# configure terminal
DES-7200(config)# ip multicast-routing
```

Step 2: Enable the PIM-DM on interface eth0.

```
DES-7200(config)# interface eth 0
DES-7200(config-if)# ip pim dense-mode
DES-7200(config-if)# exit
```

Step 3: Enable PIM-DM on interface eth 1 and return to the privileged user mode.

```
DES-7200(config)# interface eth 1
DES-7200(config-if)# ip pim dense-mode
DES-7200(config-if)# end
```

Similar configurations for devices 2 and 3, the multicast routing is enabled first and then the PIM-DM is enabled on every interface.

Note

Once the PIM-DM is enabled, the IGMP is automatically enabled on every interface without the necessity of manual configuration.

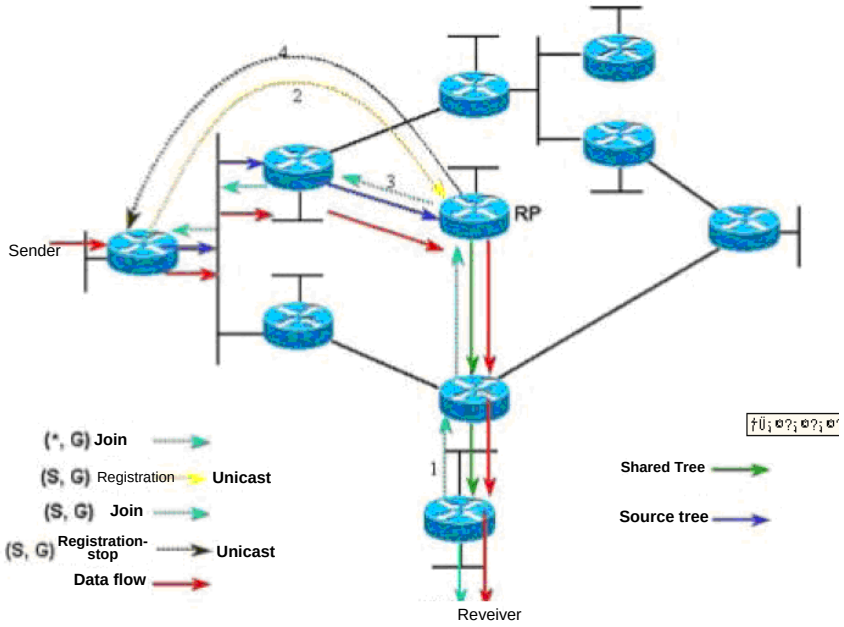
37 Configuring PIM-SM Protocol

37.1 About the PIM-SM Protocol

PIM, shortened form of the Protocol Independent Multicast, is designed by Inter-Domain Multicast Routing (IDMR) workgroup. Just as its name implies, PIM does not depend on any specific unicast routing protocol. Instead of maintaining a separate multicast routing table, the protocol takes advantage of the routing table established by various unicast routing to verify RPF.As the PIM does not receive or send the multicast route updating information, it requires much less overhead in comparison with other multicast protocols.The design idea of the PIM is to support both the SPT and the shared tree within the Internet and to enable flexible conversion so as to improve the multicast efficiency by integrating the advantages.PIM defines two modes: Dense-Mode and Sparse-Mode.

The PIM-SM (Protocol Independent Multicast Sparse Mode) is a spare multicast routing protocol. In the PIM-SM domain, the device running the PIM-SM protocol sends the Hello message on regular basis to find the neighboring PIM-SM device. It is also responsible for the election of the designated router (DR) in the multi-access network. Here, the DR is responsible for sending the “join/prune” message in the direction towards the root node of the multicast distribution tree, or sending the data of directly-connected multicast source to the multicast distribution tree.

Figure 37-1 PIM-SM explicit join mechanism



The PIM-SM forwards multicast packets by setting up multicast distribution tree. There are two kinds of multicast distribution trees: Shared Tree with the RP of group G as the root, and the Shortest Path Tree with the multicast source as the root. The PIM-SM works with explicit join/prune mechanism to set up and maintain the multicast distribution tree. As shown above, when the DR receives a Join from the receiving end, it sends a hop-by-hop multicast (*.G) join message towards the RP of group G, so as to join the shared tree. When the source host sends multicast data, the source data is encapsulated in the registration message and unicast to RP by its DR. The RP forwards the source decapsulation packets to every member along the shared tree. The RP sends the (S, G) join information to the first-hop device towards the source direction, so as to join the shortest path tree of this source. In this way, the source packets are sent to the RP without encapsulation along its shortest path tree. When the first multicast data arrives along that tree, the RP sends the registration-stop message to the source DR, so that the DR stop the registration encapsulation process. Later, the multicast data of that source will not be processed with registration encapsulation, but sent to the RP first along the shortest path tree of the source and then forwarded to the members along the shared tree by the RP. When multicast data is not needed any more, the DR multicasts the prune message hop by hop towards the RP of group G, so as to prune the shared tree.

The root node election mechanism is also involved in the PIM-SM. The PIM-SM domain is configured with one or more Candidate-BSRs, and choose the BSR through certain rules. The PIM-SM domain is also configured with Candidate-RPs), which unicast the packets to the BSR device, included with their IP addresses, multicast groups that can be served, and more information. On regular basis, the BSR generates a series of candidate RP and “bootstrap” message of the corresponding group address. The “bootstrap” message is sent hop by hop in the whole domain. The device receives and stores those “bootstrap”

messages. If the DR receives the membership report of a group from the directly-connected host, but has no routing entry of that group, it maps the group address through a hash algorithm to a candidate RP that can serve the group. Then, the DR multicasts the “join/prune” message hop by hop towards the RP. If the DR receives the multicast packets from the directly-connected host, but has no routing entry of that group, it maps the group address through a hash algorithm to a candidate RP that can serve the group. Then, the DR encapsulates the multicast data in the registration message and unicasts to the RP.

In contrast to the flood/prune-model-based PIM-DM, the IM-SM is based on the explicit join model. In other words, the receiver sends the join message to RP, while the device forwards only the packet of that multicast group on the multicast group output interface. The PIM-SM works with the shared tree to forward multicast packets. Every group has a Rendezvous Point (RP). The multicast source sends data to the RP along the shortest path, and then the RP sends the data to every receiving end along the shortest path. This is similar to the CBT but the PIM-SM does not use the concept of core. One of the benefits of the PIM-SM is that it not only receives multicast information via shared tree but also provides a mechanism of conversion from shared tree to SPT. Despite of the reduced network delay in the conversion from shared tree to SPT and the possible blocking on the RP, this kind of conversion consumes considerable device resources. So, it is suitable in the case there are multiple pairs of data sources and a small amount of network groups.

The PIM-SM works with the shared tree and SPT to distribute multicast frames. At this time, it is assumed that no other device wants to receive those multicast data unless there is clear join declaration. When a host joins a group, the device that is connected with that host will notify the root (the RP) by using the PIM join message, That join message is transferred one by one through the device, creating a structure of shared tree. Then, the RP records this transfer path as well as the registration message from the first-hop device (DR) of the sending multicast source. These two messages are used to consummate the shared tree. The leaf information is refreshed through periodical query information. When the shared tree is used, the multicast source first sends multicast messages to the RP, to ensure all receivers can receive them. A *.G is used to indicate a tree. “*” indicates all sources, and “G” indicates that the multicast address prune information of specific multicast address is also used in the shared tree. In other words, it is sent when the leaf does not want to receive the multicast frames.

The PIMv2 BSR is a method to distribute the group-to-RP messages to all devices. It eliminates the needs to configure RP for every device. The BSR uses the hop-by-hop flood BSR message to distribute the mapping information. First, the BSR is elected from the devices. The election method is similar to the election of root-bridge in layer-2 bridge, where a priority value is used, every BSR checks the BSR messages and forwards only the BSR message that has a priority higher than or equal to its priority (higher IP address). The elected BSR sends the BSR message to all-PIM-routers multicast group (224.0.0.13), with TTL as 1. When the neighbor PIMv2 device receives it, it muticasts it again outwards and sets again TTL as 1. In this way, the BSR message is received by all devices hop by hop. Since the message contains the IP address of the BSR, the candidate BSRs knows which

device is the current RP, through that message. The candidate RP sends the candidate RP advertisement to declare they can become RP in which address range. The BSR keeps them in its candidate RP buffer. The BSP notifies the local candidate RP to all PIM devices on regular basis. Similarly, these messages reach to every device hop by hop.

37.2 List of PIM-SM Configuration Tasks

The PIM-SM configuration tasks involve the following items, where only the first and the second are required, and the remaining are optional depending on the actual network conditions.

- Enable multicast routing (required)
- Enabling PIM-SM (required)
- Configuring the Hello message sent interval (optional)
- Configure PIM neighbor filtering (optional)
- Configuring RP filtering (optional)
- Configure the priority of DR (optional)
- Configure candidate BSR status (optional)
- Configure static RP (optional)
- Configure candidate RP (optional)
- Configure the duration of flood/prune timer (optional)
- Configure the speed limit to send registration message (optional)
- RP registration message reachability check (optional)
- Configure the source address of registration packet (optional)
- Configure the suppressed duration of the registration message (optional)
- Configure the duration of the KAT timer (optional)
- Last-hop device switches from shared tree to the shortest path tree (optional)
- Allow last-hop device switching from shared tree to the shortest path tree for multiple multicast groups (optional)
- Viewing PIM-SM Status Information (optional)

37.2.1 Enable multicast routing

Multicast messages cannot be forwarded unless the multicast routing is enabled, and to enable PIM-SM makes sense.

37.2.2 Enabling PIM-SM

The PIM-SM must be enabled on every interface separately. Only when PIM-SM is enabled on the device interfaces, it can have PIM-SM message interactions with other devices, maintain and update the multicast routing table, and forward multicast messages.

To configure PIM-SM on the interface, run the following command in the interface mode:

Command	Function
DES-7200(config-if)# **ip pim sparse-mode**	Enable the PIM-SM protocol on the interface.
DES-7200(config-if)# **no ip pim sparse-mode**	Disable the PIM-SM protocol on the interface.

Caution

Enabling PIM-SM on the interface does not take effect until the multicast routing is enabled in the global configuration mode.

37.2.3 Configuring the Hello message sent interval

As mentioned above, when the PIM-DM is enabled on the interface, it will send the Hello message on regular basis to the interfaces of the neighbor devices. The time interval at which an interface sends the Hello message to the interfaces of the neighbor device can be modified according to the actual conditions of the connected network.

To configure the Hello message sent interval, run the following commands in the interface mode:

Command	Function
DES-7200(config-if)# **ip pim query-interval** *seconds*	Configure the Hello message sent interval of the interface as “seconds”, in seconds.
DES-7200(config-if)# **no ip pim query-interval**	Restore the Hello message sent interval of the interface to default.

By default, the Hello message sent interval of the interface is 30 seconds.

Note

Once the Hello message sent interval is updated, the Hello hold time automatically updates by the following rule: If the Hello hold time is not configured or the configured value is less than the current Hello message sent interval, it is updated to 3.5 times the Hello message sent interval; otherwise, it remains unchanged.

37.2.4 Configure PIM neighbor filtering

Neighbor filtering function can be configured on the interface to enhance network security. With neighbor filtering enabled, as long as a neighbor is denies buy the filter access list, the PIM-SM will either not establish the neighborhood with that neighbor or stop the currently established neighborhood with that neighbor.

To configure the PIM neighbor filtering function, run the following command in the interface mode:

Command	Function
ip pim neighbor-filter *access-list*	Enable the PIM neighbor filtering function on the current interface.
no ip pim neighbor-filter *access-list*	Disable the PIM neighbor filtering function on the current interface.

The PIM neighbor filtering function is disabled by default on an interface.

Note

Notes on the **ip pim neighbor-filter** commands:

When the associated ACL rule is “permit”, only the neighbor address in the ACL can act as the PIM neighbor of the current interface. When the associated ACL rule is “deny”, the neighbor address in the ACL cannot act as the PIM neighbor of the current interface.

37.2.5 Configuring RP filtering

When filtering multicast sources is configured on the RP interface, the RP interface can decide to receive or deny the registration mechanism for the multicast packets of specific sources.

Execute the following commands in the global configuration mode:

Command	Function
ip access-list *access_name* **permit** *add-range*	Define the control list.
ip pim accept-register list *access_name*	Configure the RP interface to filter the access-name multicast source.

By default no filtering function is configured.

37.2.6 Configure the priority of DR

This command is used to configure the priority of the designated router (DR), higher weight value for higher priority.

Run the following commands in the interface mode:

Command	Function
ip pim dr-priority *priority*	Configure the priority value in range 1-4294967294.
no ip pim dr-priority *priority*	Restore the default value 1.

37.2.7 Configure candidate BSR status

Configure the device on an interface to make it enter the candidate BSR status. The configuration of candidate RP produces the globally-unique BSR in the PIM-SM domain, which will collect and distribute RPs in the domain, so as to ensure the uniqueness of the RP mapping in the domain.

Execute the following commands in the global configuration mode:

Command	Function
ip pim bsr-candidate *IFNAME (HASH) (PRIORITY)*	Configure the local machine as the candidate BSR, to learn and contest the global BSR role through BSM messages.
no ip pim bsr-candidate *IFNAME (HASH) (PRIORITY)*	Cancel the configuration of the current candidate BSR.

37.2.8 Configure static RP

In case of small-scale network, configuring static RP to use PIM-SM and require the consistent static RP configurations on all device within the PIM-SM domain ensures no ambiguity of the PIM-SM multicast routes.

If some device in the PIM-SM domain runs the BSR, the RP find order is as follows: If “override” is configured, the static RP takes precedence of the RP in the RP mapping table as distributed by the BSR; otherwise, the latter prevails.

Run the following commands in the global configuration mode:

Command	Function
ip pim rp-address *A.B.C.D ((SIMPLERANGE | EXPRANGE | ACCESSLIST)*	Configure static RP on the local machine.
no ip pim rp-address *A.B.C.D ((SIMPLERANGE | EXPRANGE | ACCESSLIST)*	Cancel the static RP configuration.

37.2.9 Configure candidate RP

Configuring candidate RP to send it to the BSR at an interval and then flood to all PIM-SIM devices within the domain ensure the uniqueness of RP mapping.

Run the following commands in the global configuration mode:

Command	Function
ip pim rp-candidate *IFNAME* (*PRIORITY*) (*INTERVAL*) (*GROUPLIST*)	Configure candidate RP on the local machine.
no ip pim rp-candidate	Cancel the candidate RP configuration.

The "acl" option with the command can specify the interface as the candidate RP of the specific group range. Note that the calculation of group range is based on only the ace with “permit” status, not “deny” status.

37.2.10 Configure the duration of flood/prune timer

A prune waiting timer controls the duration from the time when the PIM receives the prune message to the time when the interface is pruned and notified the downstream devices. The duration of the timer is 3 seconds by default. If the duration is too long, to prune messages may take too long while the downstream interfaces are still receiving multicast messages, causing waste of bandwidth. Too shorter duration of this timer may aggravate the burden of the device. So, it shall be set according to the actual requirements. When all neighbors support this option, the device will take the maximum of the “override interval” of all neighbors as the duration value of the prune waiting timer.

Run the following commands in the global configuration mode:

Command	Function
ip pim rp-candidate *IFNAME* (*PRIORITY*) (*INTERVAL*) (*GROUPLIST*)	Configure candidate RP on the local machine.
no ip pim rp-candidate	Cancel the candidate RP configuration.

37.2.11 Configure the speed limit to send registration message

This command is used to configure the speed for the DR to send the registration packets, no format of it for no speed limit. It is configured for each (S, G) pair, not for the bandwidth of the system.

Run the following commands in the global configuration mode:

Command	Function
ip pim register-rate-limit *<1-65535>*	Define the maximum registration message packets that can be sent very seconds, within the range 1-65535.
no ip pim rp-candidate	Cancel the configuration and apply no speed limit.

37.2.12 RP registration message reachability check

This command is used to detect whether the RP registration message sent from the DR can reach the destination device or not.

Run the following commands in the global configuration mode:

Command	Function
ip pim register-rp-reachability	Detect whether the registration message can reach the destination device or not.
no ip pim register-rp-reachability	Do not detect the reachability.

37.2.13 Configure the source address of registration packet

This command is used to configure the source address of the registration message sent from the DR. The no format of this command is used to send from the DR to the source host, with the reply address of the default source address of the RPF interface. The address configured must be reachable, and must respond when the RP sends correct Register-Stop information. Generally it is the loop-back address of the interface but can also be another physical address that has been advertised by unicast routes on the DR interface.

Run the following commands in the global configuration mode:

Command	Function
ip pim register-source [*SOURCEADDRESS* | *IFNAME*]	Configure the source address used in the registration message.
no ip pim register-source	Use the interface address of the RPF as the source address in the registration message.

37.2.14 Configure the suppressed duration of the registration message

This command is used to configure the suppressed duration of the registration message. This value can be modified on the DR to define the registration message suppression duration on the DR. If there is no configuration of the **ip pim rp-register-kat** command, to define this value on the RP will modify the RPkeepalive period.

Run the following commands in the global configuration mode:

Command	Function
ip pim register-suppression <*1-65535*>	Configure the suppressed duration of the registration message
no ip pim register-suppression	The suppressed duration is 60 seconds.

37.2.15 Configure the duration of the KAT timer

The KAT timer is configured to monitor the PIM registration message.

Run the following commands in the global configuration mode:

Command	Function
ip pim rp-register-kat <*1-65535*>	Configure the duration of the KAT timer.
no ip pim rp-register-kat	Use the KAT default value.

37.2.16 Last-hop device switches from shared tree to the shortest path tree

The command allows the last-hop device switching from shared tree to the shortest path tree.

If a source sent speed is greater than or equal to the transmission speed, the join message of a PIM is triggered and a source tree is built. If the final keyword is defined, all sources of this specific group will use the shared tree. If the transmission speed is less than the threshold transmission speed, the leaf device will turn to the shared tree again and send a prune message to the source.

Run the following commands in the global configuration mode:

Command	Function
ip pim spt-threshold	Allow the last-hop device switching from shared tree to the shortest path tree.
no ip pim spt-threshold	Disable this function.

37.2.17 Allow last-hop device switching from shared tree to the shortest path tree for multiple multicast groups

This command allows last-hop device switching from shared tree to the shortest path tree for multiple multicast groups.

Run the following commands in the global configuration mode:

Command	Function
ip pim spt-threshold group-list (*SIMPLERANGE* | *EXPRANGE* | *ACCESSLIST*)	Allow the last-hop device switching from shared tree to the shortest path tree.
no ip pim spt-threshold group-list (*SIMPLERANGE* | *EXPRANGE* | *ACCESSLIST*)	Disable this function.

37.3 Monitor and maintain PIM-SM

The PIM-SM provides a **show** command to monitor and maintain the PIM-DM. The **show** command can be used to view the PIM-SM interface, multicast group and multicast routing table.

37.3.1 Viewing PIM-SM Status Information

The RGONS10.1 provides the following command to check the PIM-SM status information on the local machine:

Command	Function
show debugging pim sparse-mode	Show the on/off status of the debug switch.
show ip pim interface [i*nterface-type interface-number*] [**detail**]	Show the PIM-SM information on the interface.

show ip pim neighbor [*interface-type interface-number*]	Show the PIM-SM neighbor information.
Show ip sparse-mode mroute	Show the PIM-SM multicast routing table.
show ip pim sparse-mode bsr-router	Show the details of the BSR.
show ip pim sparse-mode rp-hash *A.B.C.D*	Show the information of the elected RP.
show ip pim sparse-mode rp mapping	Show the group RP mapping information and RP setting information.
show ip sparse-mode nexthop	Show the PIM-SM next-hop information from NSM.
show memory pim sparse-mode	Show the memory statistics of the PIM-SM daemon.

For details on the use of the above command, see *PIM-SM Command References*.

37.4 PIM-SM Configuration Examples

37.4.1 Device Configuration

Here are the configurations 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

Once the PIM-SM is enabled, the IGMP is automatically enabled on every interface without the necessity of manual configuration.

37.5 BSR Configuration Examples

The example below illustrates the BSR configuration on 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
!
```

38 CPU Protection Configuration Guide

38.1 Overview

38.1.1 Function of CPU Protect

Malicious attacks often occur in the network environment, and such attacks will create too much a load for our switches.Sometimes when the messages in the network overload the switches, this may cause too high CPU utilization on the switch and abnormal operation of it.

For this reason, our L3 switches provide the CPP feature to reduce the load of the CPU of the switch and protect the normal processing capability of the switch. When a switching card is under attack, the CLI management interface for the card can still allow normal management operations, without too high CPU utilization. The management packets from other switching cards can be timely processed by the switch.

Our switches allow you to configure the CPP on the switching card or management card to adjust the appropriate thresholds for the most detailed management on the part of the administrators.

Caution

The CPP (CPU Protect Policy) is a means used to enhance the security of the switch. With the CPP, the processor and channel bandwidth resource of the switch are protected to ensure the normal forwarding of the packets and normal running of the protocols.

38.1.2 Operating 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 by using the strict priority algorithm. With this algorithm, each queue has a different priority, where queue 7 has the highest priority, queue 6 a lower priority, and queue 0 the lowest priority. The packets of the high priority queue are

always transmitted earlier than those in the low priority queue. This way, you can map each type of packet to a different priority queue according to its importance to ensure the most important packets are transmitted first.

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).

38.2 Configuring CPU Protect

The following sections describe how to configure CPU Protect.

- CPU Protect Default value
- Configuring the Bandwidth for Each Type of Packet
- Configuring the Priority for Each Type of Packet

38.2.1 CPU Protect Default value

Each type of packet has the default bandwidth of 1000pps, with the priority of 0.

38.2.2 Configuring the Bandwidth for Each Type of Packet

In the configuration mode, configure the queue of each type of packet by performing the following steps:

Command	Function
DES-7200(config)# **cpu-protec 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.
DES-7200# **end**	Return to the privileged mode.

This example shows the profile configuration process:

```
DES-7200(config)#cpu-protect type bpdu pps 200
Set packet type bpdu pps 100.
```

38.2.3 Configuring the Priority for Each Type of Packet

In the configuration mode, configure the queue of each type of packet by performing the following steps:

Command	Function
DES-7200(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.
DES-7200# **end**	Return to the privileged mode.

This example shows the profile configuration process:

```
DES-7200(config)# cpu-protect type bpdu pri 7
Set packet type bpdu priority 7.
```

38.3 Viewing CPU Protect Information

On the switch, it is possible to view the following information about the CPU Protect:

- Show the statistics of the packets received by the CPU of the management board
- Showing the Statistics of the Packets Received by the CPU of the Line Card
- Showing the Statistics of the Packets received of a specific type

38.3.1 Show the statistics of the packets received by the CPU of the management board

In the privileged mode, show the CPP information of the management board by using the following commands:

Command	Function
DES-7200# **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:

```
DES-7200#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
```

38.3.2 Showing the Statistics of the 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 by using the following commands:

Command	Function
DES-7200# **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.

```
DES-7200(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
```

38.3.3 Showing the Statistics of the Packets received of a specific type

In the privileged mode, show the priority and bandwidth of each type of packet by using the following commands:

Command	Function
DES-7200# **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 by using the **show cpu-protec type arp** command:

```
DES-7200(config)# show cpu-protect type arp
 Slot        Type          Pps       Total      Drop
 ---------   ------------ --------- ---------  ---------
 MainBoard   arp          200       15         0
 Slot-2      arp          200       15         0
```

38.4 Precuations for CPU Protect

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.

39 Anti-attack System Guard Configuration

39.1 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 message consumes network bandwidth significantly and causes abnormal operation of the network communication.

For this reason, DES-7200 provides the anti-scanning function to prevent the 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 referred to as the scan dest ip attack. This scanning is the most serious threaten to the network for it consumes the network bandwidth and adds the load of the switches, so it becomes the primary means of most hacker attacks.
2. The destination IP address doesn't exist, while a large number of message is 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 message will be forwarded directly by the switching chip and doesn't occupy the resource of the CPU for the switches. If the destination IP address doesn't exist, the CPU of the switches 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 DES-7200, 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, administrators can set a batch of ports by the **interface range** function.

39.2 Anti-attack System Guard Configuration

The anti-attack system guard is completed in the global mode of the router. It is required to enter into the global configuration mode first to make anti-attack system guard configuration.

39.2.1 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

39.2.2 Enable 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, use the **no system-guard** to set in the interface mode.

39.2.3 Set the isolation period for illegal attacking IP

The isolated time of unauthorized attack IP is port-based. You may configure the isolated time of unauthorized attack user in the interface mode. This IP will restore the communication 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 Isolated 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 isolated time, use the **no system-guard isolation-time** to set in the interface mode.

In addition, when the unauthorized user is isolated, we will send a LOG record to the log system for the query of administrators. Furthermore, it will send another LOG notification when the unauthorized isolation is released.

39.2.4 Set 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 segment.
2. The attack to some IP that doesn't exist by sending the IP message continuously.

Our switches carry out above limits. Among a batch of messages sent by the users, once any one of above limits exceeds the message limit controlled by the administrator, this 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*	The maximum threshold of the attack that some IP which doesn't exist sends the IP message continuously. The value range is 1 – 2000 messages 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 of the attack for scanning a batch of IP network segment. The value range is 1 – 1000 messages per second, 10 by default. Setting to 0 indicates this attack is not monitored.

end	Return to the privileged mode.
show system-guard	Check the configuration entities.
copy running-config startup-config	Save the configuration.

Caution

The less the threshold is set, the poorer 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 to configure corresponding threshold according to the security degree of the actual network environment.

If you want to restore the default value of corresponding parameters, use the **no system-guard same-dest-ip-attack-packets** and **no system-guard scan-dest-ip-attack-packets** to set in the interface mode.

39.2.5 Set the maximum monitored IPs

You can set the maximum quantity of the attacked hosts monitored by the devices. In general, this quantity should be maintained as the quantity of the actual operated hosts divided by 20. 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 requirement for better system guard.

You can set the maximum quantity of the attacked host by 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. Its value range is 1-500, 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 original quantity, it will cause the data of current monitored host is cleared. It may display the "chip resource full" in the isolate reason for the switch has isolated many users, which causes the hardware chip resource of the switch is full (This quantity is about 100-120 IP addresses is isolated 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 process these attackers.

If you want to restore the default value of the maximum quantity for the monitored hosts, use the "**no system-guard detect-maxnum"** in the global configuration mode.

39.2.6 Set exceptional IPs free from monitoring

You may set the exceptional IPs that is out of the monitoring. Messages 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, the **no** option of this command deletes an exceptional IP entry. The **no** and **all-eip** options of this command will delete all exceptional IP entries.

For example, to delete all exceptional IPs:

```
DES-7200(config)# no system-guard all-eip
```

To delete a single exceptional IP:

```
DES-7200(config)# no system-guard 192.168.5.145  255.255.255.0
```

Caution

For the IP isolated, it will be isolated before they are aged even if it is configured as an exceptional IP. To allow the IP messages to be sent to the CPU, you may execute the **clear system-guard** command to cancel the isolation of the IP.

39.2.7 Clear the isolation status of isolated IPs

The user isolated will automatically recover after a period of isolation. To clear the user 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.

39.2.8 View Related Information of System Guard

39.2.8.1 View Related Information of System Guard

Use the show system-guard to view the configuration parameters of the system guard:

Command	Meaning
show system-guard [interface *interface-id***]**	View the configuration parameter of the system guard.

Let's consider an example:

```
DES-7200# 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
……

DES-7200# 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
```

39.2.8.2 Check 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 system guard

```
DES-7200# 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
```

Above column indicates respectively the port on which the isolated IP address displays, the isolated IP address, the isolated reason and the remaining isolated time.

39.2.8.3 View User that being Monitored

Command	Meaning
show system-guard detect-ip [interface *interface-id***]**	View the IP that is being Monitored.

```
DES-7200# 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
```

39.2.8.4 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.

```
DES-7200# 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
```

40 Configuring Radius

40.1 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 the DES-7200, 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.

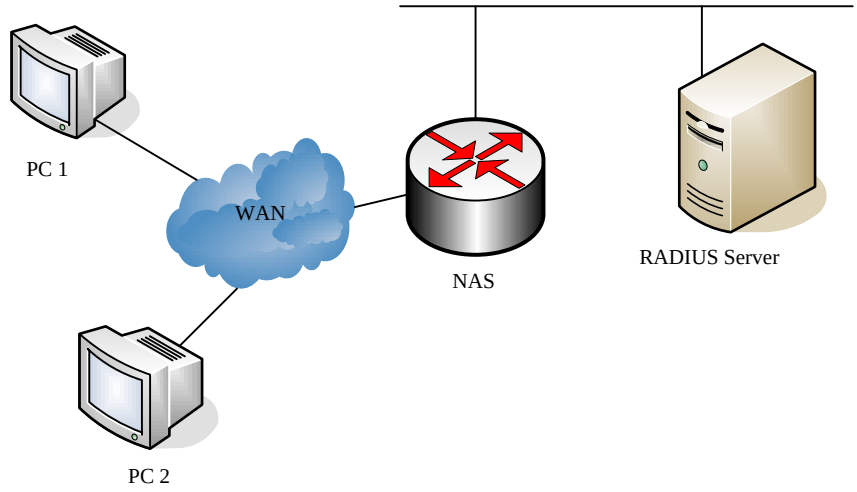
Since the RADIUS is a completely-open protocol, it has become a component and been installed in such systems as UNIX and WINDOWS 2000, so it is the security server most widely used for the time being.

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 40-1 Typical RADIUS network configuration



40.2 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 by using 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.

40.2.1 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.
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 s 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 the RADIUS Key. The sharing password on the network device and the sharing password on the Radius server must be the same.

40.2.2 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.

40.2.3 Specify Radius Private Attribute Type

The contents in this section enable configuring freely the type of private attributes. The default configurations are as follows:

Default configurations of DES-7200 private attribute recognition:

ID	Function	TYPE
1	**max down-rate**	**1**
2	**qos**	**2**
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**	**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 privilige**	**22**
23	**login privilige**	**42**
24	**limit to user number**	**50**

Extended manufacturer ID default configuration:

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-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 privilige**	**42**
24	**limit to user number**	**50**

Note

Two functions cannot be configured with the same type number.

Here is an example on 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 privilige      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 privilige      42
24   limit to user number 50
RedGiant(config)#
RedGiant(config)#
```

40.3 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

40.4 Radius Configuration Example

In a typical Radius network configuration diagram, the RADIUS server performs authentication for the visiting users, enables the accounting function for the visiting users and records the network usage of the users.

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 on how to configure the Radius for network device:

```
DES-7200# configure terminal
DES-7200(config)# aaa new-model
DES-7200(config)# radius-server host 192.168.12.219
auth-port 1645 acct-port 1646
DES-7200(config)# radius-server key aaa
DES-7200(config)# aaa authentication login test group radius
DES-7200(config)# end
DES-7200# show radius server
Server IP:       192.168.12.219
Accounting Port: 1646
Authen  Port:    1645
Server State:    Ready
DES-7200#configure terminal
DES-7200(config)#line vty 0
DES-7200(config-line)#login authentication test
DES-7200(config-line)#end
DES-7200#show running-config
!
aaa new-model
!
!
aaa authentication login test group radius
!
username dlink 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
!
```

41 About AAA

The access control is used to control which people can access the network server and which services can be accessed by the users on the network. The authentication, authorization and accounting (AAA) is a key security mechanism for access control.

41.1 Basic AAA Principles

Authentication, Authorization and Accounting (shortened as AAA) provide a consistence framework for configuring the authentication, authorization and accounting functions, which are supported by DES-7200.

The AAA provides the following services in a modular manner:

- Authentication:It verifies whether a user can access, 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 application of it 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 series attributes 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 DES-7200.

Although the AAA is the primary access control method, DES-7200 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

41.1.1 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.

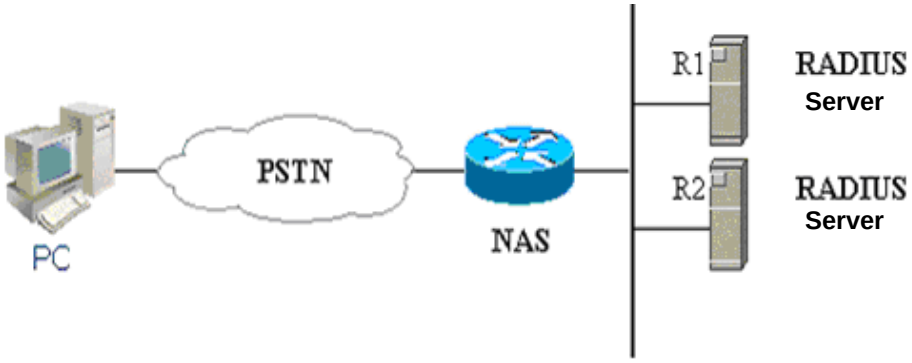
41.1.2 Method List

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 method 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. DES-7200 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

Only when there is no reply from a method, DES-7200 will attempt the next 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 41-1 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.

Supposed 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 dialup, 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, 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 an ERROR is detected, the AAA selects the next authentication method in the method list to continue the authentication process.

41.2 Basic AAA Configuration Steps

First you shall decide to choose which 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 the network security.

41.2.1 Overview of AAA Configuration Steps

The AAA configuration may become simple when the basic operation process of AAA is understood.On DES-7200, the AAA is configured through the following steps:

1. Enable AAA by using 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, if no named method list is clearly specified, the default authentication method list will apply.

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*.

41.2.2 Enable AAA

It is required to enable AAA first to be able to use the AAA security features.

To enable AAA, execute the following command in the global configuration mode:

Command	Function
DES-7200(config)# **aaa new-model**	Enable AAA

41.2.3 Disable AAA

To disable AAA, execute the following command in the global configuration mode:

Command	Function
DES-7200(config)# **no aaa new-model**	Disable AAA

41.2.4 Sequential Configuration Steps

After the AAA is enabled, it is time to configure the other parts related with the selected security solutions. 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 not using AAA for authentication, see Configuring Authentication.

41.3 Configuring Authentication

The authentication allows the user's identity verification before the user of network resources. In most cases, the authentication is implemented with the AAA security features. We recommend the use of AAA as much as possible.

41.3.1 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 the failure of the first method. DES-7200 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

Only when there is no reply from a method, DES-7200 will attempt the next method. During the authentication, if the user access is refused by a method, the authentication process ends and no other methods will be attempted.

41.3.2 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 the user authentication. In case of no reply, R2 will be used. In case 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.
DES-7200(config)# **line vty** *2*	Enter the configuration layer of line 2
DES-7200(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 Telnet the network (NAS), the NAS first queries the authentication information from R1. If the user passes the authentication on R1, R1 sends a ACCEPT reply to the NAS, and thus the user's access to the network is allowed. If R1 returns the REJECT reply, the user's access is refused and then disconnected.If R1 does not respond, NAS considers TIMEOUT and queries the authentication information to R2. This process continues for the remaining methods till the user passes the authentication, is refused or the session is terminated.If all servers (R1 and R2) returns TIMEOUT, the authentication will be performed by the NAS local database.

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 an TIMEOUT is detected, the AAA selects the next authentication method in the method list to continue the authentication process.

41.3.3 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.

41.3.4 Configuring the AAA Line Authentication

This section deals with how to configure the AAA authentication methods supported by the DES-7200:

Caution

Only after the AAA is enabled through the command **aaa new-model** in the global configuration mode, the AAA security features are available for your configuration. For the details, see AAA Overview.

In many cases, the user needs to Telnet the network access server (NAS). 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 list 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. The keyword "method" means the actual algorithm for authentication. Only when the current method returns ERROR (no reply), the next authentication method will be

attempted. 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 specific "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 dialup user can 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 dialup 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 DES-7200.

41.3.4.1 Use the local username database for PPP authentication

To configure the line authentication with local database, it is required to configure the local database first. DES-7200 supports authentication based on the local database. To establish the username 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.
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.

41.3.4.2 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. DES-7200 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.
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.

41.3.5 Example of Authentication Configuration

The example below illustrates show to configure the network device to use “Radius + local” for authentication.

```
DES-7200(config)# aaa new-model
DES-7200(config)# username dlink password starnet
DES-7200(config)# radius-server host 192.168.217.64
DES-7200(config)# aaa authentication login test group radius local
DES-7200(config)# line vty 0
DES-7200(config-line)# login authentication test
DES-7200(config-line)# end
DES-7200# show running-config
!
aaa new-model
!
!
aaa authentication login test group radius local
username dlink 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 the identity authentication.

41.4 Configuring Authorization

The AAA authorization enables the administrator to control the user's use of the services. After the AAA authorization service is enabled, the network device configures the user sessions by using the user configuration file stored locally or in the server. After the authorization is completed, the user can only use the services allowed in the profile.

DES-7200 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 (as defined with the username) and then grants the user with specific rights. In the local database, only limited functions can be defined for the users, which is applicable for simple authorization for the users.

Caution

Now the configuration does support the 802.1X AAA authorization, while the 802.1X is implemented by using other commands.

41.4.1 Preparations for Authorization

The following tasks must be completed before the AAA authorization is configured:

- Enable the AAA server. For the 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. DES-7200 supports RADIUS. For details of the RADIUS, see Configuring RADIUS.
- (Optional) if the local authorization is required, it is required to use the **username** command to define the user rights.

41.4.2 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.
aaa authorization network{**default** | *list-name} method1 [method2*|…]	Enable the AAA authorization and define the authorization method.

41.4.3 RADIUS Authorization

To use the Radius security server to authorize the users, the **aaa authorization** command with the keyword "Radius" can be used. See 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.

41.4.4 Local Authorization

To use the local authorization, the **aaa authorization** command with keyword "local" can be used. 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.

41.4.5 None Authorization

To enable no authorization for the user, the **aaa authorization** command with keyword "none" can be used.

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.

41.4.6 Example of Configuring Network Authorization

The example below illustrates how to perform network authorization.

```
DES-7200# configure terminal
DES-7200(config)# aaa new-model
DES-7200(config)# radius-server host 192.168.217.64
DES-7200(config)# username dlink privilege 6
DES-7200(config)# aaa authorization network test group radius local none
DES-7200(config)# end
DES-7200# show running-config
aaa new-model
!
aaa authorization network test group radius local  none
!
username dlink password 0 starnet
username dlink privilege 6
!
radius-server host 192.168.217.64
```

41.5 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.

41.5.1 Accounting Types

DES-7200 currently supports the following accounting types:

- Network Accounting

41.5.2 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 the firmwareversion.

41.5.3 Preparations for Accounting

The following tasks must be completed before the AAA accounting is configured:

- Enable the AAA security server. For the details, see AAA Overview.
- Define the security protocol parameters. DES-7200 supports the Radius security protocol. For details of the RADIUS, see Configuring RADIUS.

41.5.4 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.

41.5.5 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.

41.5.6 Example of Configuring Accounting

Below is an example to use the Radius for accounting:

```
DES-7200# config
DES-7200(config)# aaa new-model
DES-7200(config)# radius-server host 192.168.217.64
DES-7200(config)# aaa accounting network acct start-stop group radius
DES-7200(config)# end
DES-7200# show running-config
!
aaa new-model
!
aaa accounting network acct start-stop group radius
!
username dlink password 0 starnet
username dlink privilege 6
!
radius-server host 192.168.217.64
```

Note

For the information on how to configure the accounting method list command, see the related command reference manual.

42 Configuring 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 CLI command set.

42.1 Overview

In an IEEE 802 LAN, users can access the network device without needing authorization and authorization as long as they are connected to the network device. Therefore, an unauthorized user can access the network unobstructed by connecting the LAN. As the LAN technology finds wide application, and particularly the appearance of the operating network, it is necessary to address the safety authentication needs of the network.It has become the focus of concerns in the industry that how to provide user 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 access point-to-point security access. Specially designed by the IEEE Standardization Commission to tackle the safety 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 authentication of the authentication server.

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 streams can be transmitted over the network.

By using 802.1x, our switches provide Authentication, Authorization, and Accounting (AAA).

- Authentication: It is used to determine whether a user has the access, 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.

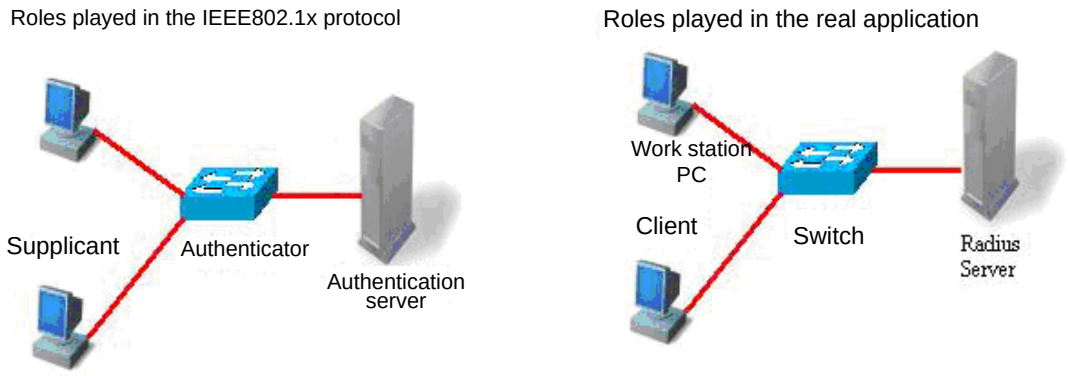
The 802.1x is described in the following aspects as below:

- Device Roles
- Authentication Initiation and Packet Interaction During Authentication
- States of Authorized Users and Unauthorized Users
- Topologies of Typical Applications

42.1.1 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 42-1



- Supplicant:

The **supplicant** is a role played by the end user, usually a PC. It requests for the access to network services and acknowledges 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 a uncontrolled port can directly access network resources without needing authentication. We can control users by simply connecting them to an controlled port. On the other hand, the uncontrolled port is used to connect the authentication server, for ensuring normal communication between the server and switch.

- Authentication server:

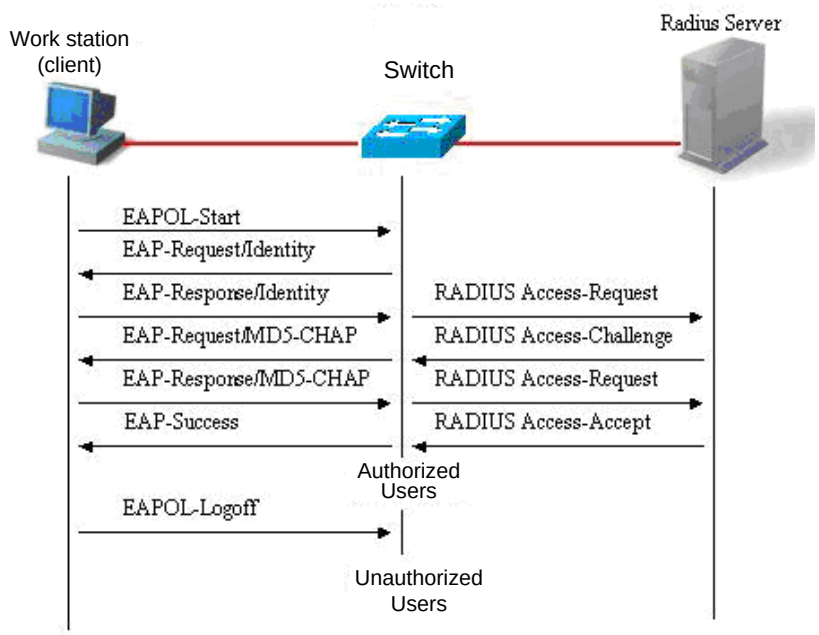
The **authentication server** is usually an **RADIUS** server, which works with the authenticator to provide users with authentication services. The authentication server saves the user name and password and related authentication information. One server can provide authentication services for multiple 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.

42.1.2 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 42-2



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).

42.1.3 States of Authorized Users and Unauthorized Users

The 802.1x determines 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 determine 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 user 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 changes 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, when the equipment requests the username of the user, the workstation will not respond to the request due to no support. This means that the user is still unauthorized and cannot access the network resources.

On the contrary, if the client supports 802.1x, while the connected switch does not: The EAPOL-START frames from the user are not responded, and the user deems it 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 a 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 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 changes from authorized to unauthorized.

When a port of the switch changes to the LINK-DOWN status, all the users on the port change to the unauthorized status.

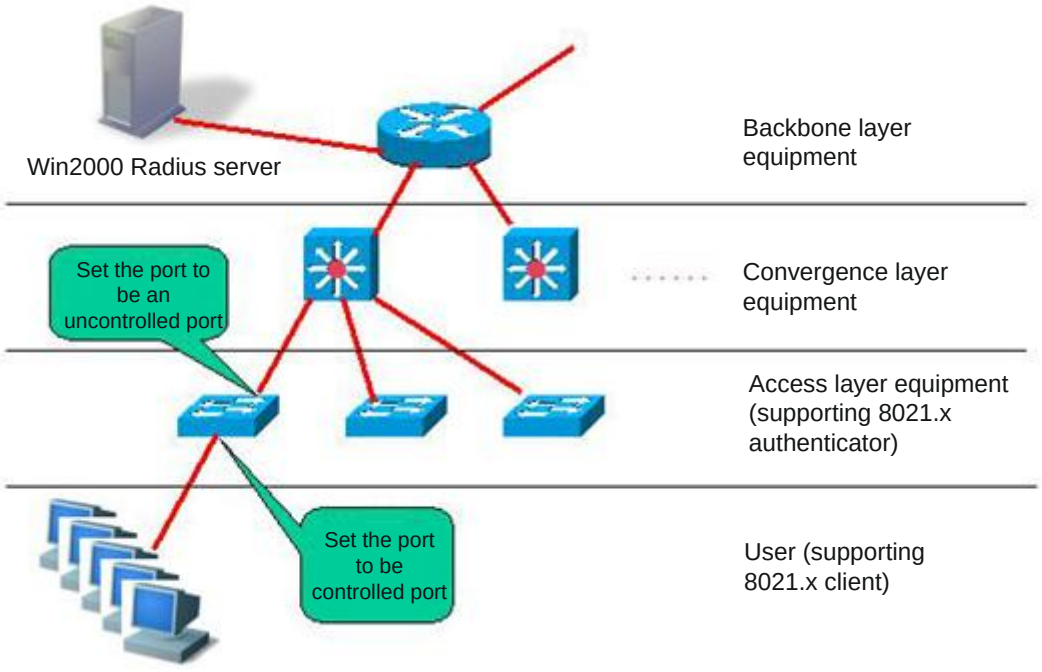
When the device restarts, all users on the device turn into the unauthorized status.

To force a user to pass the authentication, you can add a static MAC address.

42.1.4 Topologies of Typical Applications

A. The 802.1x-enabled device is used as the access layer device

Figure 42-3

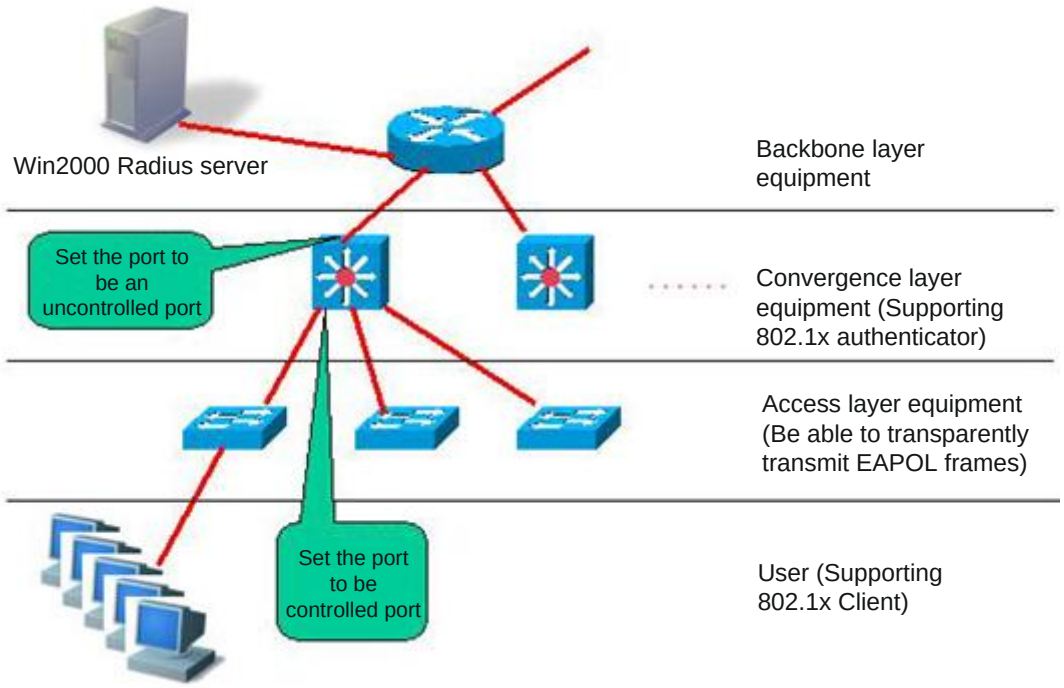


This solution is described as below:

- 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 switch 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 as 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. Each 802.1x-enabled switch 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 switch 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 42-4



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 switch 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 switches must be set as 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 many users to normally access the network.
  2. User management is performed on the Radius Server in a centralized manner. The administrator does not have to know which switch a user is connected to, making management much easier.
  3. The access layer device can be the less expensive non-NM switches (as long as they support transparent transmission of EAPOL frames).
  4. The administrator cannot manage the device on the access layer through the network.

42.2 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 proactively
- 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

42.2.1 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

42.2.2 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.

42.2.3 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 switches, 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. At registration, you must supply the Radius Server switch's IP address, authentication UDP port (add the accounting UDP port, if needed), and the agreed key for communication between the switch 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 appropriate 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 switch 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 use 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 use 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:

```
DES-7200# configure terminal
DES-7200(config)# radius-server host 192.168.4.12
DES-7200(config)# radius-server host 192.168.4.12 auth-port 600
DES-7200(config)# radius-server key MsdadShaAdasdj878dajL6g6ga
DES-7200(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.

42.2.4 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 by performing 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:

```
DES-7200# configure terminal
DES-7200(config)# aaa new-model
DES-7200(config)# radius-server host 192.168.217.64
DES-7200(config)# radius-server key starnet
DES-7200(config)# aaa authentication dot1x authen group radius
```

```
DES-7200(config)# dot1x authentication authen
DES-7200(config)# end
DES-7200# show running-config
!
aaa new-model
!
aaa authentication dot1x authen group radius
!
username dlink 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 switch cannot perform authentication. For how to set the communication between the Radius Server and the switch, please see the previous section.

42.2.5 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 by performing 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.

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:

```
DES-7200# configure terminal
DES-7200(config)# interface f 1/1
DES-7200(config-if)# dot1x port-control auto
DES-7200(config)# end
```

42.2.6 Enabling Timed Re-authentication

The 802.1x can ask users for re-authentication at periodical intervals, to prevent authorized users from being used by other 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 while as accurate as possible.

In the privileged mode, you can enable/disable re-authentication and set the re-authentication interval by performing the following steps.

Command	Function
configure terminal	Enter the global configuration mode.
dot1x re-authentication	Enable timed 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 timed 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.

```
DES-7200# configure terminal
```

```
DES-7200(config)# dot1x re-authentication
DES-7200(config)# dot1x timeout re-authperiod 1000
DES-7200(config)# end
DES-7200# 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.

42.2.7 Changing the QUIET Time

When a user fails authentication, the switch does not allow that user to re-authenticate until a specified period, which is referred to as Quiet Period.This value functions to protect the device from malicious attacks. The default interval for Quiet Period is 5 seconds.

A shorter Quiet Period may speed up re-authentication for the users.

In the privileged mode, you can set the Quiet Period by performing 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 as 500 seconds:

```
DES-7200# configure terminal
DES-7200(config)# dot1x timeout quiet-period 500
DES-7200(config)# end
```

42.2.8 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 30 seconds. You should modify this value to suit the specific network size.

In the privileged mode, you can set the packet retransmission interval by performing 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:

```
DES-7200# configure terminal
DES-7200(config)# dot1x timeout tx-period 100
DES-7200(config)# end
```

42.2.9 Setting the Maximum Number of Requests

If the switch does not receive response within the ServerTimeout after it sends an authentication request to the RadiusServer, it will retransmit the packets.The maximum number of requests are the maximum retransmission requests of the device, and the authentication fails if this number is exceeded. By default, this value is 2. You should modify this value to suit the specific network size.

In the privileged mode, you can set the maximum number of retransmissions by performing 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.

```
DES-7200#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:
DES-7200# configure terminal
DES-7200(config)# dot1x max-req 5
DES-7200(config)# end
```

42.2.10 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 switch believes that this user is already disconnected, and ends the authentication process accordingly. By default, the number is 2. However, you can modify this value.

In the privileged mode, you can set the maximum number of re-authentications by performing the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
dot1x reauth-req 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:

```
DES-7200# configure terminal
DES-7200(config)# dot1x reauth-max 3
DES-7200(config)# end
DES-7200#
```

42.2.11 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 by performing the following steps:

Command	Function
configure terminal	Enter the global configuration mode.

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.

42.2.12 Configuring the device to initiate the 802.1x authentication proactively

The 802.1x is secure access authentication based on port. Users must first undergo authentication before they can access the network. In most cases, authentication is initiated by 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 switch in some cases. Fro example, when the switch is reset and the status of the authentication port changes from linkdown to linkup, the switch needs to automatically initiate authentication to ensure that the authenticated users can continue to use the network. In addition, if you use a 802.1x client that does not actively initiate authentication requests (for example, the Windows XP 802.1x client), the switch should be able to actively initiate authentication. The switch 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 the switch to actively initiate 802.1x authentication and how you should configure appropriately in different application environments.

Turn on/off the switch for the proactive authentication initiation of the device

When this function is disabled, the switch 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 switch 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 by performing the following steps:

Command	**Function**
configure terminal	Enter the global configuration mode.

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. Only when the function is enabled, the following settings take effect. The user can set the number of proactive 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 by performing the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
dot1x auto-req packet-num *num*	The device proactively initiates num 802.1x authentication request messages. If num is equal to 0, the device will continually send that message. 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 message sent interval.

In the privileged mode, you can set the packet sending interval by performing 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 message 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 whether to stop sending the request messages 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 by performing the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
dot1x auto-req user-detect	Stop sending the messages 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**

42.2.13 Configuring 802.1x Accounting

Our 802.1x has implemented the accounting function. Accounting is based on interval. 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 switch detects user disconnection.

After the first successful authentication of the user, the switch sends an accounting start request to the server. When the user gets off-line or the switch finds that the user has got off line or when the physical connection of the user is broken, the switch 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 switch 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 switch 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 switch 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 by performing 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:

```
DES-7200# configure terminal
DES-7200(config)# aaa new-model
DES-7200(config)# aaa group server radius acct-use
DES-7200(config-gs-radius)# server 192.168.4.12 acct-port 1200
DES-7200(config-gs-radius)# server 192.168.4.13 acct-port 1200
DES-7200(config-gs-radius)# exit
DES-7200(config)# aaa accounting network acct-list start-stop group acct-use
DES-7200(config)# dot1x accounting acct-list
DES-7200(config)# end
DES-7200# write memory
DES-7200# show running-config
```

Caution

1. The accounting key must be agreed with the Radius Server, same as that case 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 at periodical intervals. 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 by performing 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 using the **no aaa accounting update** command.

```
DES-7200# configure terminal
DES-7200(config)# aaa accounting update
DES-7200(config)# end
DES-7200# write memory
DES-7200# show running-config
```

The following chapters introduce the propriety features of DES-7200:

To make it easy for broadband operators and to accommodate use in special environments, our 802.1x has been expanded on the basis of the account (such expansion is completely based on the standard, and has not any incompatibility with IEEE 802.1x).

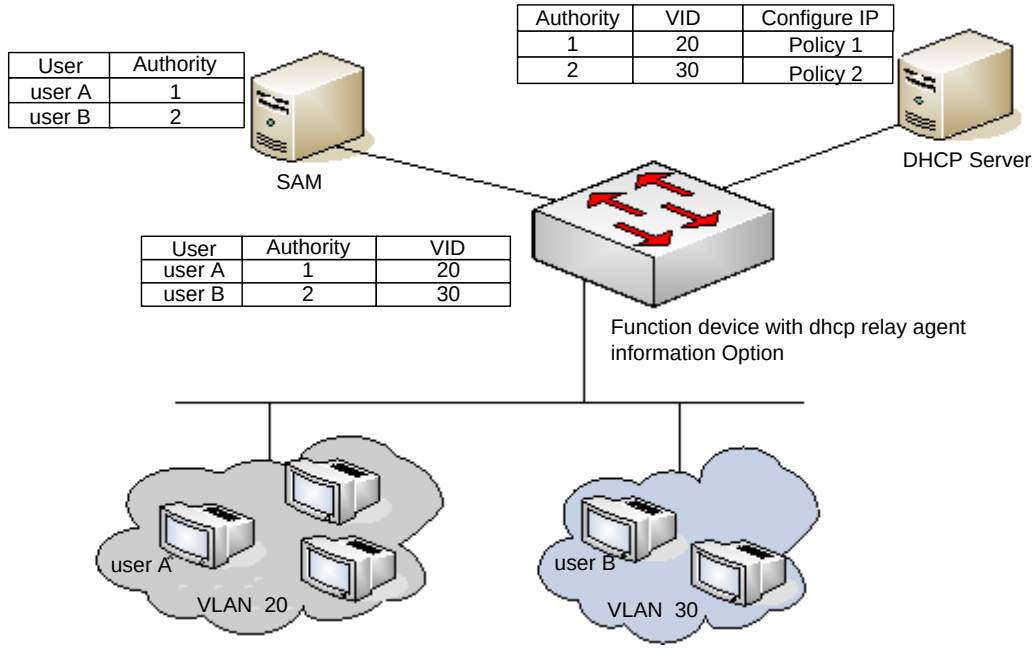
42.2.14 Configuring the IP authorization mode

The 802.1x implemented by DES-7200 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 42-5



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 message. 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 information to the device. The user has to use the IP at authentication to be able to access the network.

Caution When the user switches modes, it will cause all authenticated users to get offline. So, it is recommended to configure the authentication mode before the uses of the users.

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:

```
DES-7200# configure terminal
DES-7200(config)# aaa authorization ip-auth-mode radius-server
DES-7200(config)# end
DES-7200# show running-config
!
aaa new-model
!
aaa authorization ip-auth-mode radius-server
!
DES-7200# write memory
```

42.2.15 Releasing Advertisement

Our 802.1x allows you to configure the Reply-Message 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 at the first authorization of the user, but not at 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 message into links capable of direct switching, for easier browsing.

Releasing of the advertising information:

1. The operator configures the Reply Message 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.

42.2.16 List of Authenticable Hosts under a Port

For enhanced 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.
show running-config	Show the configuration.

Caution

If the list of the host is empty, the port allows any host to be authenticated.

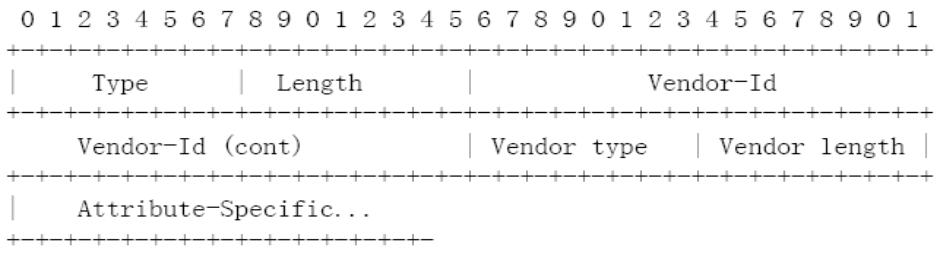
42.2.17 Authorization

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 switch.

Since the Radius has no standard attribute to represent the maximum data rate, we can only transfer the authorization information by the manufacturer customized attribute.

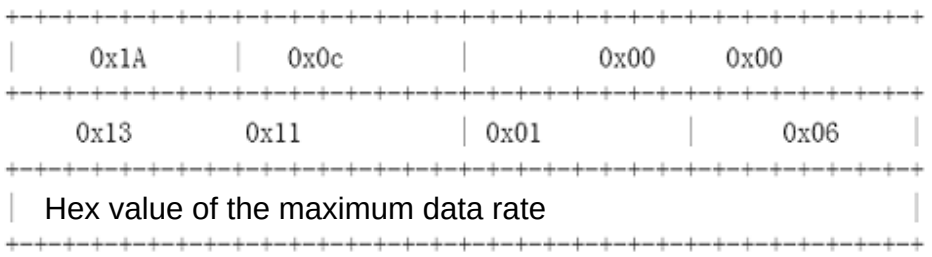
The general format of the definition is as follows:

Figure 42-6



For the maximum data rate, you need to fill in the following values:

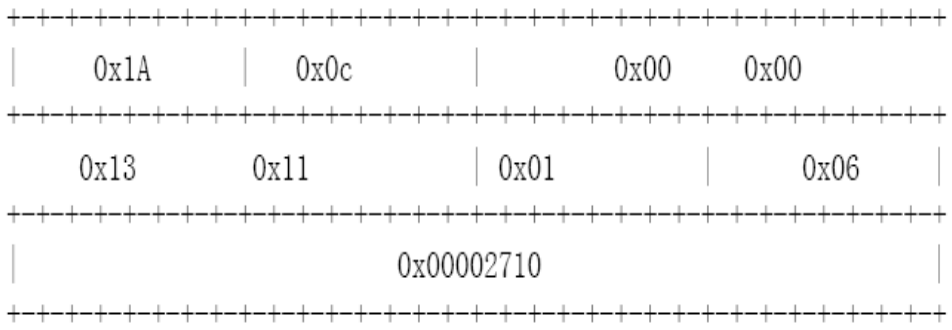
Figure 42-7



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 42-8



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 appropriate field.

This function calls for no settings on the device end, and works as long as the device end supports authorization.

42.2.18 Configuring the Authentication Mode

In the standard, the 802.1x implements authentication through the EAP-MD5. The 802.1X of DES-7200 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 switch 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 used 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 by performing 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:

```
DES-7200# configure terminal
DES-7200(config)# dot1x auth-mode CHAP
DES-7200(config)# end
DES-7200# 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
```

42.2.19 Configure 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 by performing 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:

```
DES-7200# configure terminal
DES-7200# aaa new-model
DES-7200(config)# aaa group server radius auth-ll
DES-7200(config-gs-radius)# server 192.168.4.1
DES-7200(config-gs-radius)# server 192.168.4.12
DES-7200(config-gs-radius)# end
DES-7200#
```

42.2.20 Configuring and Managing Online Users

DES-7200 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.

42.2.21 Implementing User-IP Binding

With our clients and by correctly configuring the 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 switch. The user needs to use our client and the administrator needs to configure the Radius Server.

42.2.22 Port-based Traffic Charging

In addition to the duration-based billing, DES-7200 provide the traffic-based billing function in case 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.

42.2.23 Implementing Automatic Switching and Control of VLAN

If the user's "down VLAN" is set on the Radius server, the Radius server will notify the device via the manufacturer customized attribution of DES-7200. DES-7200 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 by using the **show dot1x summary** command.

Follow these steps to configure a port to allow dynamic VLAN jump or not:

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.
show dot1x	Show the configuration.

42.2.24 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. Star switches provide the function to shield proxy servers and dial-up connections.

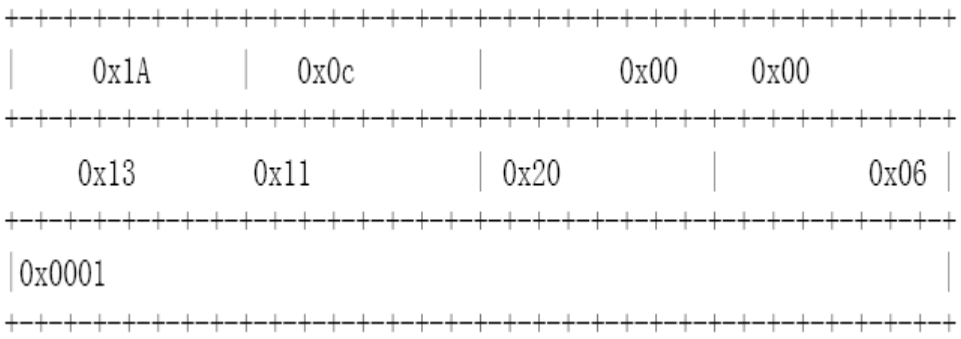
To implement this function needs no settings on the device end and needs only the corresponding attributes configured on the Radius server end. Since the Radius has no standard attributes to indicate the maximum data rate, we can transfer the authorization information only through the manufacturer custom 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.

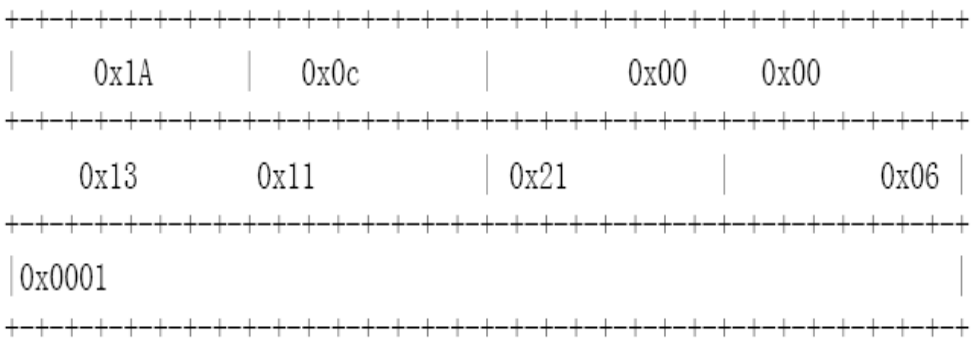
To shield the access via the proxy server, you should fill in the following information:

Figure 42-9



To shield the access via the dial-up connection, you should fill in the following information:

Figure 42-10



42.2.25 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 switch and RADIUS server. To meet the need to implement accurate charging with few resources occupied, we use a new client on-line probe mechanism. Such mechanism only needs interaction between the switch 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 announcement.
- 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 by performing 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.
show dot1x	Show the configuration.

42.2.26 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 outputted 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 by performing 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 using the **no dot1x eapol-tag** command.

42.3 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

42.3.1 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.

```
DES-7200# sh radius server
Server IP:       192.168.5.11
Accounting Port: 1813
Authen  Port:    1812
Server State:    Ready
```

42.3.2 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:

```
DES-7200# 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
```

42.3.3 Viewing the List of the Addresses Authenticable

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 by performing 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.

```
DES-7200# show dot1x auth-address-table
interface:g3/1
-----------------------------------
mac addr: 00D0.F800.0001
```

42.3.4 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 by performing the following steps:

Command	Function
show dot1x summary	Viewing the User Authentication Status Information

The following example shows the user authentication status information.

```
DES-7200# show dot1x summary
 ID   MAC       Interface  VLAN  Auth-State  Backend-State Port-Status
---- ----------- --------- ----  ----------  ------------  -----------
1   00d0f8000001 Gi3/1     1   Authenticated  IDLE       Authed
```

42.3.5 Showing the 1x Client Probe Time Configuration

In the privileged mode, you can view the 1x timer setting by performing the following steps:

Command	Function
show dot1x probe-timer	Show the 1X timer setting

The following example shows the 1.1x timer setting:

```
DES-7200# show dot1x probe-timer
Hello Interval: 20 Seconds
Hello Alive: 250 Seconds
DES-7200#
```

42.3.6 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 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. At 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 messages. 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, but the users cannot communicate. For the filtering domain templates in particular, at least one should be available for user authentication in the IP authentication mode.

43 Configuring LINE Mode

43.1 Overview

This chapter describes some operations on LINE:

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

43.2 Configuring LINE Mode

43.2.1 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
Red-Giant(config)# **line** [**aux** | **console** | **tty** | **vty**] **first-line** [**last-line**]	Enter the specified LINE mode.

43.2.2 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
Red-Giant(config)# **line vty** *line-number*	Increase the number of LINE VTY to a value.
Red-Giant(config)# **no line vty** *line-number*	Decrease the number of LINE VTY to a value.

43.2.3 Configure the allowed communication protocol in LINE

To restrain 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

43.2.4 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 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

44 SSH Terminal Service

44.1 About SSH

SSH is the shortened form of Secure Shell. The SSH connection functions like a Telnet connection, except that all transmissions based on the connection are encrypted. When the user logs onto the device via a network environment where security cannot be guaranteed, the SSH feature provides safe information guarantee and powerful authentication function to protect the devices from IP address fraud, plain password interception and other kinds of attacks.

44.2 DES-7200's 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
Message authentication algorithm	Not supported	MD5, SHA1, SHA1-96, MD5-96
Compression algorithm	NONE (uncompressed)	NONE (uncompressed)

44.3 DES-7200's SSH Supports

Caution

DES-7200 supports only the SSH server (compatible with the SSHv1 and SSHv2) but do not support the SSH client.

44.4 SSH Configuration

44.4.1 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

44.4.2 User authentication configuration

1. For the consideration of the SSH connection security, the login without authentication is forbidden. Therefore, in the login authentication of the users, 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, the username can be entered randomly but the entry length must be greater than zero.

44.4.3 Enable 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
Crypto key generate {**rsa**|**dsa**}	Generate the key.

Caution

The command **crypto key zeroize** instead of [**no**] **crypto key generate** is used to delete the key.

44.4.4 Disable SSH SERVER

After the SSH Server is enabled, deleting the public key of the server end will automatically disable the SSH Server. Enter the global configuration mode, delete the public key and make the SSH Server status become DISABLE.

Command	Description
configure terminal	Enter the configuration mode
Crypto key Zeroize {**rsa|dsa**}	Delete the key.

44.4.5 Configure SSH server support versions

By default, the SSH SERVER is compatible with versions 1 and 2. Run the following command to configure the SSH version.

Command	Description
configure terminal	Enter the configuration mode
ip ssh version {**1	2**}	Configure SSH support versions
no ip ssh version	Restore the SSH default configurations, supporting SSHv1 and SSHv2.

44.4.6 Configure SSH user authentication timeout period

By default, the user authentication timeout period of the SSH SERVER is 120 seconds. Run the following commands to configure the SSH user authentication timeout period.

Command	Description
configure terminal	Enter the configuration mode
ip ssh time-out *time*	Configure the SSH timeout period (1-120sec)
no ip ssh time-out	Restore the SSH default user authentication timeout period 120 seconds.

44.4.7 Configure 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 3 for the SSH Server by default. In other words, it allows the user to enter the username and password for three times to attempt the authentication. Run the following commands to configure the SSH re-authentication times:

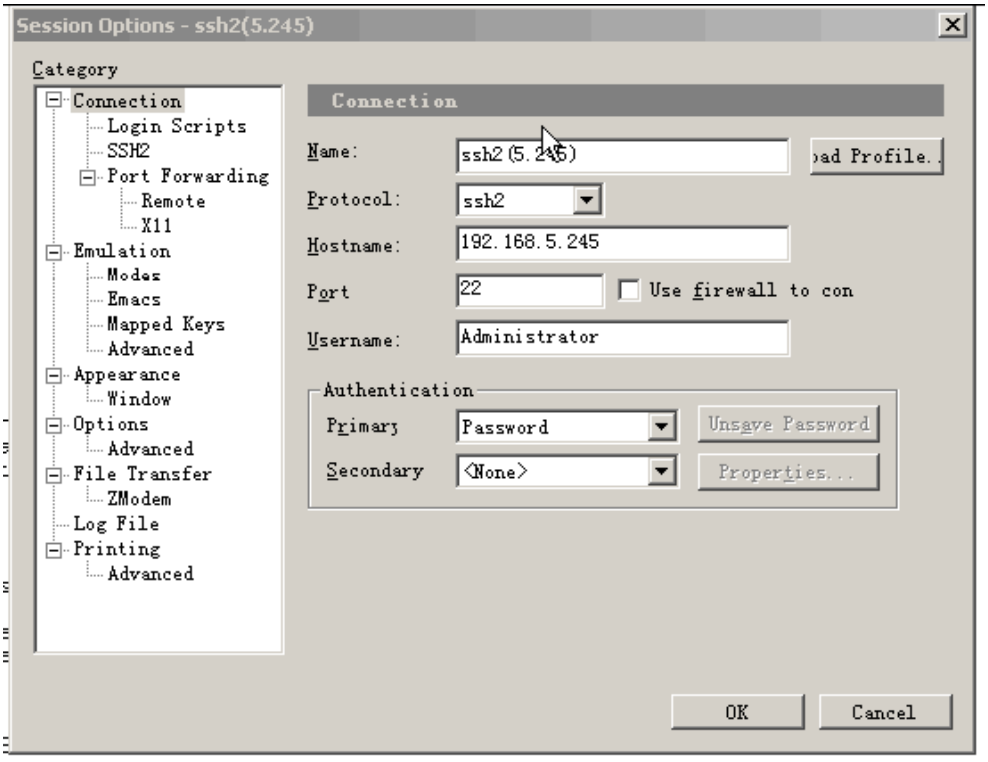
Command	Description
configure terminal	Enter the configuration mode
ip ssh authentication-retries *retry times*	Configure SSH re-authentication times (range 0-5)
no ip ssh authentication-retries	Restore the default SSH re-authentication times as 3.

Note: For details of the above commands, see SSH Command Reference Manual.

44.5 Use SSH for device management

You may use the SSH for device management by first enabling the SSH Server function that is disabled by default. Since the Telnet that comes with the Windows does not support SSH, third-party client software has to 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):

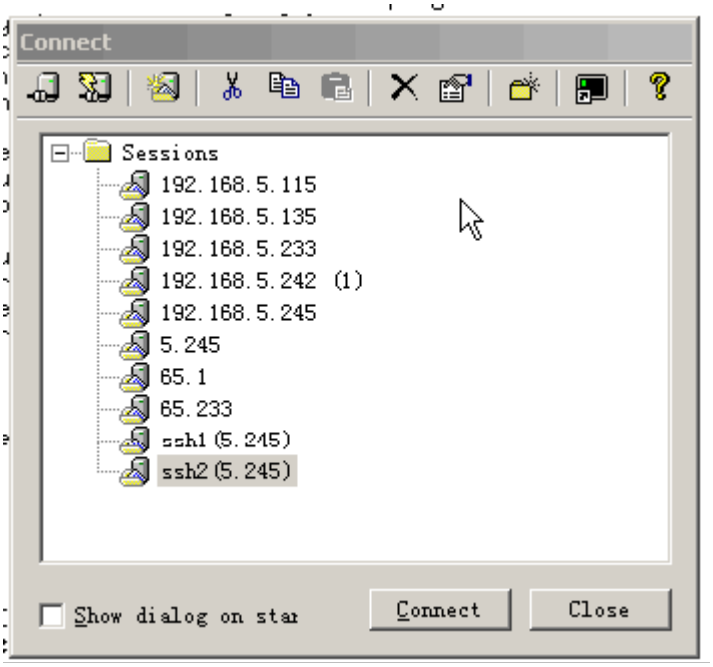
Figure 44-1



As shown in Figure 44-1 , protocol 2 is used for login, so SSH2 is chosen in “Protocol”. “Hostname” indicates the IP address of the host that will log in, 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.

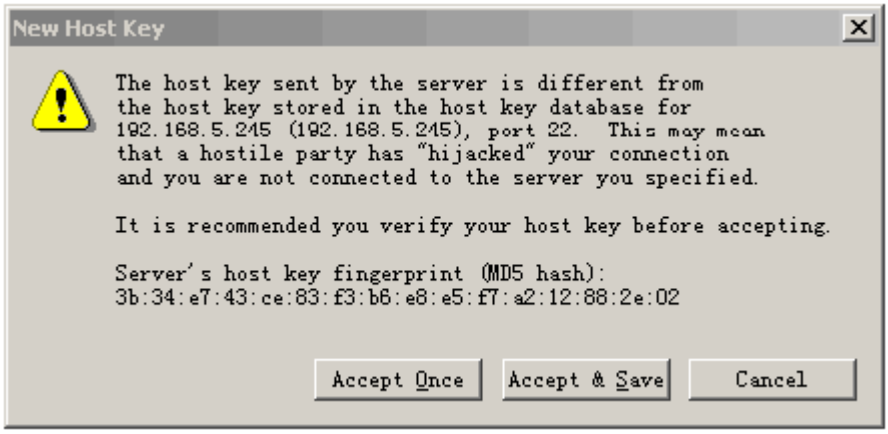
Click “OK” to pop up the following dialog:

Figure 44-2



Click “Connect” to log into the host just configured, as shown below:

Figure 44-3

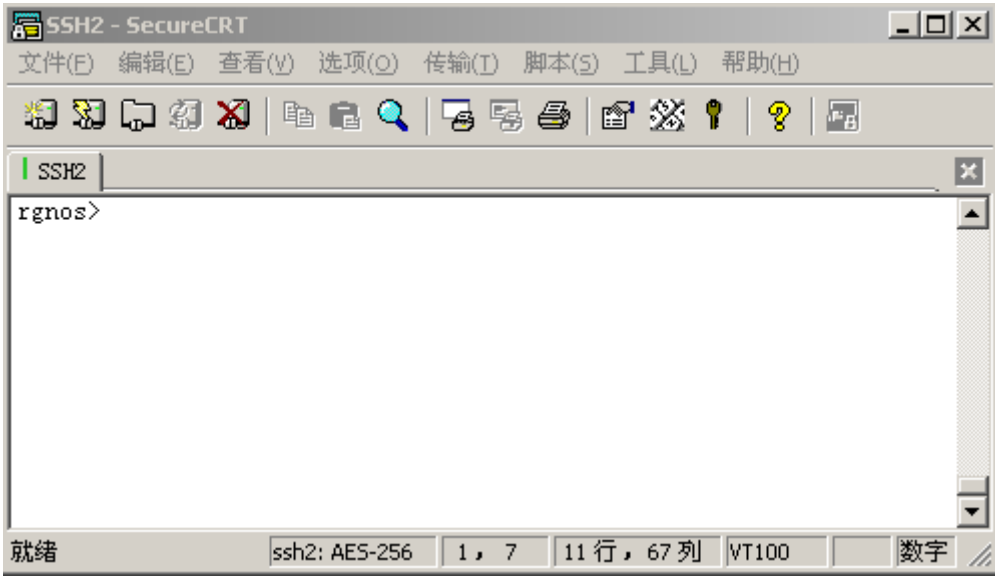


Ask the machine that is logging into the host 192.168.5.245 to see whether the key from the server end is received or not. Select “Accept & Save” or “Accept Once” to enter the password confirmation dialog box, as shown below:

Figure 44-4

Enter the Telnet login password to enter the UI that is the same as the Telnet. See the diagram below:

Figure 44-5



45 Access Control List

45.1 Overview

As part of DES-7200 security solution, DES-7200 uses access control lists to provide a power data flow filtering function.At present, DES-7200 supports 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.

45.1.1 Access Control List Introduction

ACLs is the shortened form of Access Control Lists, or Access Lists. It is also popularly called firewall, or packet filtering in some documentation. ACLs controls the messages on the 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 streams, 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 streams pass the switch, ACLs classify and filter them, that is, check the data streams inputted from the specified interface and determine whether to permit or deny them according to the matching conditions.

Generally, the security ACLs is used to control which dataflow is 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.

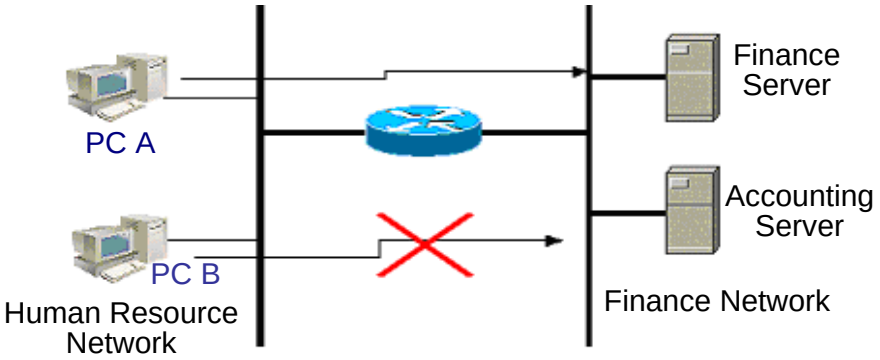
Access list rules can be about the source addresses, destination addresses, upper layer protocols, time-ranges or other information of data flows.

45.1.2 Why to Configure Access Lists

There are many reasons why we need configure access lists. Some of them are as follows:

- Restrict route updating: Control where to send and receive the route updating information.
- Restrict network access: To ensure network security, by defining rules, make users unable to access some services. (When a user only need access the WWW and E-mail services, then other services like TELNET are disabled). Or, allow users to access services only during a given period or only allow some hosts to access networks. Figure 45-1 is a case. In the case, only host A is allowed to access Finance Network, while Host B is disallowed to do so.See Figure 45-1 .

Figure 45-1 Using Access List to Control Network Access



45.1.3 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 requirement.However, experienced hackers may use some software spoof source address and cheat the devices so as to gain accesses. 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 to provide spoof source addresses to deceive switches is called spoofing and it is a inherent problem of all access lists. Even you use the dynamic list, a spoofing problem occurs. 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 resolve the problem. One method is to Set free time for a user to access the network as little as possible, making a hacker feel it hard to attack the network. Another method is to use the IPSEC encryption protocol to encrypt network data, ensuring that all the data entering switches are encrypted.

Access lists are usually configured in the following locations of network devices:

- Devices between the inside network and outside 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 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.

45.1.4 Input/Output ACL, Filtering Domain Template and Rule

When a device interface receives a message, the input ACL checks whether the message matches an ACE of the ACL input on the interface. When a device interface is ready to output a message, the output ACL checks whether the message matches an ACE of the ACL output on the interface.

When detailed filtering rules are formulated, all or some of the above eight items may be used. As long as the message matches one ACE, the ACL processes the message as the ACE defined (permit or deny). The ACE of an ACL identifies Ethernet messages according to some fields of Ethernet messages. 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 32 bits of the IP address, or specify a type of streams of the defined subnet)
- Destination IP address field (you can specify all the 32 bits of the IP address, or specify a type of streams of the defined subnet)
- Protocol type fields

Layer-4 fields:

- You can specify one UDP source port, destination port, or both
- You can specify one UDP source port, destination port, or both

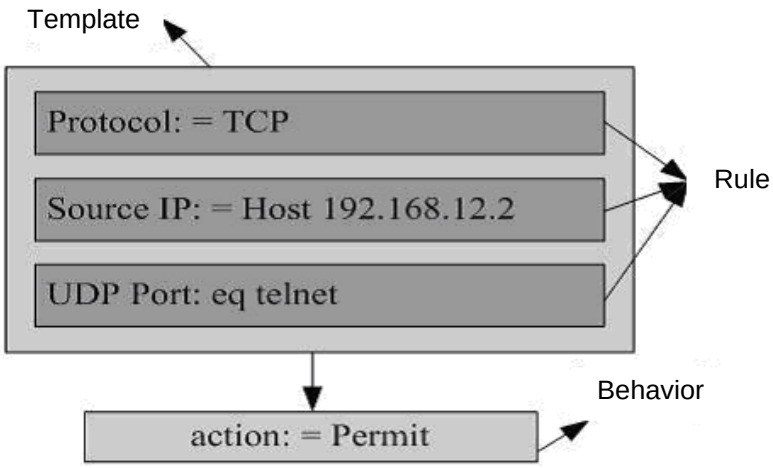
The filtering domain consists of the fields in the packets based on which the packets are identified and classified when you create an ACE. A filtering domain template is the definition formed by these field. For example, when one ACE is generated, you want to identify and classify messages according to the destination IP field of a message. When another ACE is generated, you want to identify and classify messages according to the source IP address field of a message 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 mask. 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 45-2 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 user the combination of L2, L3 and L4 fields, it is possible to apply the Expert ACLs.

45.2 Configuring IP Access List

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

45.2.1 Guide to configure IP access list

When you create an access list, defined rules will be applied to all packet messages on a switch. The switch decides whether to forward or block a packet messages 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 the following:

- Source address
- Destination address
- Upper layer protocol
- Time range

Standard IP access lists (1 – 99, 1300 – 1999) forward or block packets according to source 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 sentences to define multiple rules. Where, all sentences use a same number or name to bind these sentences to a same access list. However, the more the used sentences, the more difficult to read and understand an access list.

45.2.1.1 Implicating "Deny Any Data Flow" Rule Sentence

The ending part of each access list implicates a "Deny any data flow" rule sentence. Therefore, if a packet matches no rule, then it is denied.

as shown in the following example:

```
access-list 1 permit host 192.168.4.12
```

This list allows only the message 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 messages from any host will be denied on the port.

Caution

It is required to consider the routing update message when defining the access list. Since the end of the access list "denies all dataflow", this may cause all routing update messages blocked.

45.2.1.2 Order to Input Rule Sentences

Each added rule is appended to the access list. If a sentence is created, then you cannot delete it separately and can only delete the whole access list. Therefore, the order of access list sentences is very important. When deciding whether to forward or block packets, a switch compares packets and sentences in the order of sentence creation. After finding a matching sentence, it will not check other rule sentences.

If you have created a sentence and it allows all data flows to pass, then the following sentences 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 sentence denies all IP messages, the host telnet message of the 192.168.12.0/24 network will be denied. Because the switch discover that the messages match the first rule sentence, it will not check other rule sentences.

45.2.2 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
DES-7200(config)# **access-list** id {**deny** | **permit**} {**src** *src-wildcard* | **host** src | **any** | **interface** idx} [**time-range** *tm-rng-name*]	Define an access list
DES-7200(config)# **interface** *interface*	Select the interface to which the access list is to be applied.
DES-7200(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
DES-7200(config)# **ip access-list** { **standard** | **extended** } { *id* | *name* }	Enter the access list configuration mode

DES-7200(config-xxx-nacl)# [sn] { **permit** | **deny** } {**src** *src-wildcard* | **host** src | **any** | **interface** *idx*} [**time-range** *tm-rng-name*]	Add table entries for ACL. For details, please see command reference.
DES-7200(config-xxx-nacl)# **exit** DES-7200(config)# **interface** *interface*	Exit from the access control list mode and select the interface to which the access list is to be applied.
DES-7200(config-if)# **ip access-group** id { **in** | **out** }	Apply the access list to the specific interface

45.2.3 Show the configuration of IP access list

To monitor access lists, please run the following command the in privileged user mode:

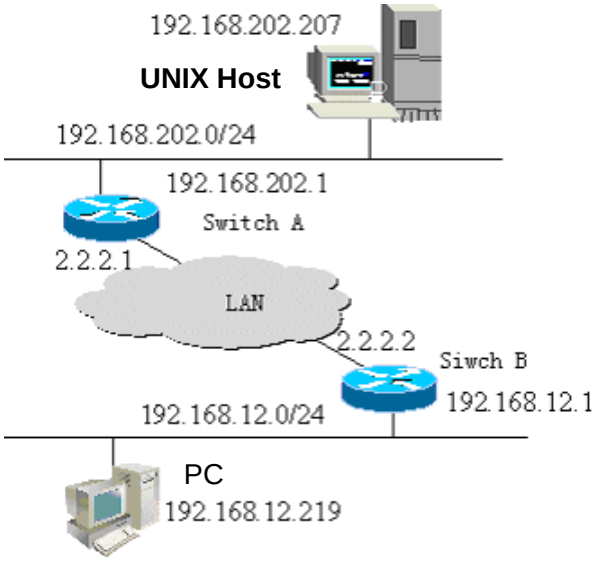
```
DES-7200# show access-lists [ id | name ]
```

This command can be used to view the basic access list.

45.2.4 IP Access List Example

Configuration requirements: There are two devices Switch A and Switch B, as shown in Figure 45-3 :

Figure 45-3 Basic Access List Example



It is required to implement the following security functions by configuring access lists on Switch B:

Hosts at the 192.168.12.0/24 network section can only access the remote UNIX host TELNET service during the normal working time period and deny the PING service.

On the Switch B console, access to any of the services of hosts at the 192.168.202.0/24 network section is denied.

Note

The above case simplifies the application in the bank system. Namely, it only allows the hosts on the Local Area Network of branches or savings agencies to access the central host and disallows accessing the central host on the device.

- Equipment Configuration

Switch B configuration:

```
DES-7200(config)# interface GigabitEthernet 0/1
DES-7200(config-if)# ip address 192.168.12.1 255.255.255.0
DES-7200(config-if)# exit
DES-7200(config)# interface GigabitEthernet 0/2
DES-7200(config-if)# ip address 2.2.2.2 255.255.255.0
DES-7200(config-if)# ip access-group 101 in
DES-7200(config-if)# ip access-group 101 out
```

According to requirements, configure an extended access list numbered 101

```
access-list 101 permit tcp 192.168.12.0 0.0.0.255 any eq telnet time-range check
DES-7200(config)# access-list 101 deny icmp 192.168.12.0 0.0.0.255 any
DES-7200(config)# access-list 101 deny ip 2.2.2.0 0.0.0.255 any
DES-7200(config)# access-list 101 deny ip any any
```

Configure the time-range time range

```
DES-7200(config)# time-range check
DES-7200(config-time-range)# periodic weekdays 8:30 to 17:30
```

Note

For access list 101. the lat rule sentence ”access-list 101 deny ip any any” is not needed, for the ending part of the access list implicates a “deny any” rule sentence.

Switch A configuration:

```
DES-7200(config)# hostname dlink
DES-7200(config)# interface GigabitEthernet 0/1
DES-7200(config-if)# ip address 192.168.202.1 255.255.255.0
DES-7200(config)# interface GigabitEthernet 0/2
DES-7200(config-if)# ip address 2.2.2.1 255.255.255.0
```

45.3 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

45.3.1 MAC Extended Access List Configuration Guide

When you create an expert access list, defined rules will be applied to all packet messages on a switch. The switch decides whether to forward or block a packet messages by judging whether the packet matches a rule.

The typical rules defined in MAC access lists are the following:

- 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 sentences to define multiple rules. Where, all sentences use a same number or name to bind these sentences to a same access list.

45.3.2 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
DES-7200(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.
DES-7200(config)# **interface** *interface*	Select the interface to which the access list is to be applied.
DES-7200(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
DES-7200(config)# **mac access-list extended** {*id* | *name*}	Enter the access list configuration mode
DES-7200(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.
DES-7200(config-mac-nacl)# **exit** DES-7200(config)# **interface** *interface*	Exit from the access control list mode and select the interface to which the access list is to be applied.
DES-7200(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 (they support priority ACE products and are supported on DES-7200 switches).

45.3.3 Showing Configuration of MAC Extended Access List

To monitor access lists, please run the following command the in privileged mode:

```
DES-7200# show access-lists [ id | name]
```

You can view basic access lists

45.3.4 MAC Extended Access List Example

It is required to 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 messages passing in and out on the port.

```
DES-7200> enable
DES-7200# configure terminal
DES-7200(config)# mac access-list extended mac-list
DES-7200(config-mac-nacl)# deny host 0013.2049.8272 any ipx
DES-7200(config-mac-nacl)# permit any any
DES-7200(config-mac-nacl)# exit
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# mac access-group mac-list in
DES-7200(config-if)# end
DES-7200# show access-lists
mac access-list extended mac-list
deny host 0013.2049.8272 any ipx
permit any any
DES-7200#
```

Note

For access lists, ”permit any any” cannot be discarded, for the ending part of an access list implicates a “deny any” rule sentence.

45.4 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

45.4.1 Expert Extended Access List Configuration Guide

When you create an expert access list, defined rules will be applied to all packet messages on a switch. The switch decides whether to forward or block a packet messages by judging whether the packet matches a rule.

The typical rules defined in expert access lists are the following:

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 sentences to define multiple rules. Where, all sentences use a same number or name to bind these sentences to a same access list.

45.4.2 Configuring Expert Extended Access List

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 (application particular case)

There are two methods to configure an expert access list.

Method 1: Run the following command in the global configuration mode:

Command	Function
DES-7200(config)# **access-list** *id* {**deny** | **permit**} [*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*] [**fragment**] [**time-range** *tm-rng-name*]	Define an access list. For details about commands, please see command reference.
DES-7200(config)# **interface** *interface*	Select the interface to which the access list is to be applied.
DES-7200(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
DES-7200(config)# **expert access-list extended** {id|name}	Enter the access list configuration mode

DES-7200(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*] [**fragment**] [**time-range** *tm-rng-name*]	Add table entries for ACL. For details about commands, please see command reference.
DES-7200(config-exp-nacl)# **exit** DES-7200(config)# **interface** *interface*	Exit from the access control list mode and select the interface to which the access list is to be applied.
DES-7200(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).

45.4.3 Showing Configuration of ExpertExtended Access List

To monitor access lists, please run the following command the in privileged user mode:

```
DES-7200# show access-lists [id | name]
```

You can view expert access lists

45.4.4 Expert Extended Access List Example

It is required to 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.

```
DES-7200> enable
DES-7200# config terminal
DES-7200(config)# expert access-list extended expert-list
DES-7200(config-exp-nacl)# permit ip vid 20 any host 0013.2049.8272 any any
DES-7200(config-exp-nacl)# deny any any any any
DES-7200(config-exp-nacl)# exit
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# expert access-group expert-list in
DES-7200(config-if)# end
```

```
DES-7200# show access-lists
expert access-list extended expert-list
petmit ip vid 20 any host 0013.2049.8272 any any
deny any any
```

45.5 Configuring IPv6 extended access list

45.5.1 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
DES-7200(config)# **ipv6 access-list** *name*	Enter the access list configuration mode
DES-7200(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*] [**fragments**] [**time-range** *tm-rng-name*]	Add table entries for ACL. For details about commands, please see command reference.
DES-7200(config-exp-nacl)# **exit** DES-7200(config)# **interface** *interface*	Exit from the access control list mode and select the interface to which the access list is to be applied.
DES-7200(config-if)# **ipv6 traffic-filter** *name* {**in** | **out**}	Apply the access list to the specific interface

45.5.2 Showing Configuration of IPv6Extended Access List

To monitor access lists, please run the following command the in privileged user mode:

```
DES-7200# show access-lists [name]
```

This command can be used to view the basic access list.

45.5.3 IPv6 Extended Access List Example

It is required to 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.

```
DES-7200> enable
DES-7200# config terminal
DES-7200(config)# ipv6 access-list v6-list
DES-7200(config-ipv6-nacl)# permit ipv6 ::192:68:4:12/24 any
DES-7200(config-ipv6-nacl)# deny ipv6 any any
DES-7200(config-ipv6-nacl)# exit
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# ipv6 traffic-filter v6-list in
DES-7200(config-if)# end
DES-7200# show access-lists
ipv6 access-list extended v6-list
petmit ipv6 ::192.168.4.12 any
deny any any
DES-7200#
```

45.6 Configuring access list ACL80

The ACL80 is also call the custom access list, which means matching the first 80 bytes of the message to filter the messages. A message consists of a series of byte flows. The ACL80 enables the user to perform match filtering by bits in the specified 64 bytes of the first 80 bytes in the message.

For nay 16-byte field, it is possible to compare or not the configured value by bits. In other words, it allows setting any bit of those 16 bytes as 0 or 1. There are two factors in filtering any byte: filtering rule and filter domain template. The bits of the both are one-to-one corresponding. 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 as 0, no match will be done no matter what the corresponding bit is in the filtering rule.

For example,

```
DES-7200(config)# expert access-list advanced name
DES-7200(config-exp-dacl)# permit 00d0f8123456 ffffffffffff 0
DES-7200(config-exp-dacl)# deny 00d0f8654321 ffffffffffff 6
```

The user custom 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 messages. To use the user custom 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
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 it offset in the SNAP+tag 802.3 data frame. In the user custom 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 messages 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 messages.

45.7 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. Namely, when the TCP flags in a received message exactly match those defined in the ACL table entry, the message will be checked by the ACL rule. A user can define any combination of TCP flags to filter some messages with specific TCP flags.

For example,

```
permit tcp any any match-all rst
```

Allow the messages 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
DES-7200(config)# **ip access-list extended** { id | *name* }	Enter the access list configuration mode
DES-7200(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.
DES-7200(config-exp-nacl)# **exit** DES-7200(config)# **interface** *interface*	Exit from the access control list mode and select the interface to which the access list is to be applied.
DES-7200(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 permission and password

```
DES-7200> enable
DES-7200#
```

2. Enter the global configuration mode.

```
DES-7200# configure terminal
```

3. Enter the ACL configuration mode.

```
DES-7200(config)# ip access-list extended test-tcp-flag
```

4. Add an ACL entry

```
DES-7200(config-ext-nacl)# permit tcp any any match-all rst
```

5. Add a deny entry

```
DES-7200(config-ext-nacl)# deny tcp any any match-all fin
```

6. Adding/delete entries repeatedly.

7. end

```
DES-7200(config-ext-nacl)# end
```

8. Show

```
DES-7200# 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
```

45.8 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:

```
DES-7200(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:

```
DES-7200(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:

```
DES-7200(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

```
DES-7200(config-std-nacl)# no 106
ace1: 100
ace2: 103
ace5: 105
ace4: 109
The above numbers can also facilitate deleting ACE.
```

45.9 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 by performing the following steps:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **time-range** time-range-name	Identify a time-range by using a meaningful display character string as its name
DES-7200(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.

DES-7200(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.
DES-7200# **show time-range**	Verify the configurations.
DES-7200# **copy running-config startup-config**	Save the configuration.
DES-7200(config)# **ip access-list extended** *101*	Enter the ACL configuration mode.
DES-7200(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, which should not include any 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 streams during the working hours in a week by using the ACLs as example:

```
DES-7200(config)# time-range no-http
DES-7200(config-time-range)# periodic weekdays 8:00 to 18:00
DES-7200(config)# end
DES-7200(config)# ip access-list extended limit-udp
DES-7200(config-ext-nacl)# deny tcp any any eq www time-range no-http
DES-7200(config-ext-nacl)# exit
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# ip access-group no-http in
DES-7200(config)# end
```

Example of displaying time range:

```
DES-7200# 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
```

45.10 Configure bound source interface address ACL

The IP standard, IP extended and Expert ACLs can be used to configure matching source interface address.

Starting from the privileged mode, you can use the following steps to set an ACL to match the source interface addresses:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **ip access-list standard** *1*	Enter the configuration mode.
DES-7200(config-std-nacl)# **permit ip interface** *idx*	Configure the match source interface address ACL entry.

Note

1. The entry does not take effect if the interface has no address.
2. Whenever the interface is deleted, the corresponding entry is also deleted.
3. Match only the master address of the interface to use a the host address.

Here are the ACL application examples:

```
DES-7200(config)# ip access-list extended ifaddr
DES-7200(config-ext-nacl)# permit tcp interface vlan 1 any eq www
DES-7200(config-ext-nacl)# exit
DES-7200(config)# interface vlan 1
DES-7200(config)# ip address 1.1.1.1 255.255.255.0
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# ip access-group ifaddr in
```

46 Configuring QOS

46.1 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.

46.1.1 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 bandwidth is abundant, 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 message is classified into a category in the network, and the classification information is included in the IP message header. The first 6 bits in the TOS (Type Of Service) field for IPv4 message header or the Traffic Class field for Ipv6 message header carry the classification information of the message. 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 message header or Traffic Class field for IPv6 message header, called IPprecedence value; or carried by the first 6 bits of the TOS field for IPv4 message header or Traffic Class field for IPv6 message header, called Differentiated Services Code Point (DSCP) value.

In a DiffServ-compliant network, every device has the same transmission service policy for the messages 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 as appropriate. This behavior of these independent devices is call 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.

46.1.2 QOS processing flow

46.1.2.1 Classifying

The process of classifying involves putting the messages to the dataflow indicated with CoS value according to the trust policy or the analysis of the message contents. As a result, the core task of classifying is to determine the CoS value of a message. It happens when the port is receiving the inbound messages. 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 messages input through that port.

For general non-IP messages, the switch classifies the messages according to the following criteria:

- If the message itself does not contain any QoS information, which means the layer-2 message header has no User Priority bits, it gets the QoS information of the message by using the default CoS value of the message input port. Like the User Priority bits of the message, the default CoS value of the port ranges 0~7.
- If the message itself contains QoS information, which means the layer-2 message header has User Priority bits, it gets the CoS information directly from the message.

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 message or the input port of the message without analyzing the message 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 message on that port, to determine the DSCP value of the message. Note that, if a port is associated with a policy-map but has no DSCP value set for it, the switch will assign the priority for the messages of this classification by performing the default behavior: following the priority information contained in the layer-2 message header of the message 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 message or the port; otherwise, default DSCP value 0 will be assigned for the messages failing the classifying operation.

For IP messages, the switch classifies the messages 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 message and fills the CoS field (3 bits) of the output message.
- If the port trust mode is Trust cos, it extracts directly the CoS field (3 bits) of the message and overwrite the ip precedence field (3 bits) of the message. There are the following two cases. Case 1 is that the layer-2 message header does not contain User Priority bits, and now the CoS value is got from the default CoS value of the message input port. Case 2 is that the layer-2 message header contains User Priority bits, and now the CoS is got directly from the message 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 message, to determine the DSCP value of the message, 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 message 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 the details of the CoS-to-DSCP map and IP-precedence-to-DSCP map, see the descriptions below.

46.1.2.2 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 message in the classified dataflow. If the message is occupying more bandwidth as allowed by the police that applies on that dataflow, the message 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 messages in the classified dataflow will remain unchanged, and no message will be discarded before the message is sent for the Marking action.

46.1.2.3 Marking

After the Classifying and Policing actions, the Marking action will write the QoS information for the message to ensure the DSCP value of the classified message 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 message, 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 message header.

46.1.2.4 Queueing

The Queuing action is responsible for transferring the messages in the dataflow to an output queue of the port. The messages 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 switch convert the DSCP value of the message into output queue number so as to determine which output queue to transfer the messages into.

46.1.2.5 Scheduling

The Scheduling action is the last cycle in the QoS process. After the messages are transferring into different output queues of the port, the switch works with WRR or another algorithm to transmit the messages in those 8 queues.

It is possible to set the weight in the WRR algorithm to configure the amount of messages to be transmitted in every cycle of message output, thus affecting the transmission bandwidth. Alternatively, it is possible to set the weight in the DRR algorithm to configure the amount of message bytes to be transmitted in every cycle of message output, thus affecting the transmission bandwidth.

46.2 QOS Configuration

46.2.1 Default QOS configuration

Make clear the following points of QoS before starting the 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 amount 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 messages 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 as 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

46.2.2 Configure 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:

```
DES-7200(config)# interface gigabitEthernet 0/4
DES-7200(config-if)# mls qos trust dscp
DES-7200(config-if)# end
DES-7200# show mls qos interface g0/4
Interface GigabitEthernet 0/4
Attached input  policy-map:
Default COS: trust dscp
Default COS: 0
DES-7200#
```

46.2.3 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 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 set the default CoS value of interface g0/4 to 6:

```
DES-7200# configure terminal
```

```
DES-7200(config)# interface g 0/4
DES-7200(config-if)# mls qos cos 6
DES-7200(config-if)# end
DES-7200# show mls qos interface g 0/4
Interface GigabitEthernet 0/4
Attached input  policy-map:
Default COS: trust dscp
Default COS: 6
DES-7200#
```

46.2.4 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**[…]	Creat 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 a ACL:acl_1. This class-map will classify all TCP messages with port 80.

```
DES-7200(config)# ip access-list extended acl_1
DES-7200(config-ext-nacl)# permit tcp any any eq 80
DES-7200(config-ext-nacl)# exit
DES-7200(config)# class-map class1
DES-7200(config-cmap)# match access-group acl_1
```

```
DES-7200(config-cmap)# end
```

46.2.5 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 messages in the dataflow; it does not take effect for non-IP messages. *new-dscp* is the new DSCP value to be set, whose range varies with the specific product.

For example, the following steps create a policy-map named policy1 and associate it with interface gigabitethernet 1/1.

```
DES-7200(config)# policy-map policy1
DES-7200(config-pmap)# class class1
DES-7200(config-pmap-c)# set ip dscp 48
DES-7200(config-pmap-c)# exit
Router(config-pmap)# exit
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# switchport mode trunk
DES-7200(config-if)# mls qos trust cos
DES-7200(config-if)# service-policy input policy1
```

46.2.6 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.

[**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.

46.2.7 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 method, 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

For example, the following steps set the port output algorithm to SP:

```
DES-7200# configure terminal
DES-7200(config)# mls qos scheduler sp
DES-7200(config)# end
DES-7200# show mls qos scheduler
Global Multi-Layer Switching scheduling
Strict Priority
DES-7200#
```

46.2.8 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 as 1:2:3:4:5:6:7:8

```
DES-7200# configure terminal
DES-7200(config)# wrr-queue bandwidth 1 2 3 4 5 6 7 8
DES-7200(config)# end
DES-7200# show mls qos queueing
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
DES-7200(config)#
```

46.2.9 Configuring Cos-Map

You may set cos-map to change which queue to select for the messages in output. 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

```
DES-7200# configure terminal
```

```
DES-7200(config)# priority-queue Cos-Map 1 2 4 6 7 5
DES-7200(config)# end
DES-7200# show mls qos queueing
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
```

46.2.10 Configuring CoS-to-DSCP Map

CoS-to-DSCP Map is used to map the CoS value 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:

```
DES-7200# configure terminal
DES-7200(config)# mls qos map cos-dscp 56 48 46 40 34 32 26 24
DES-7200(config)# end
DES-7200# show mls qos maps cos-dscp
cos dscp
--- ----
0   56
1   48
```

```
2   46
3   40
4   34
5   32
6   26
7   24
```

46.2.11 Configuring DSCP-to-CoS Map

DSCP-to-CoS is used to map internal DSCP value to CoS value so that it is possible to select output queue for messages.

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 delimited 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 default

For example, the following steps set the DSCP values 0, 32 and 56 to map 6:

```
DES-7200# configure terminal
DES-7200(config)# mls qos map dscp-cos 0 32 56 to 6
DES-7200(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
```

46.2.12 Configuring IPpre to DSCP Map

IPpre-to-Dscp is used to map the IPpre values of message 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:

```
DES-7200# configure terminal
DES-7200(config)# mls qos map ip-precedence-dscp 56 48 46 40 34 32 26 24
DES-7200(config)# end
DES-7200# 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
```

46.3 QOS Displaying

46.3.1 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,

```
DES-7200# show class-map
Class Map cc
Match access-group 1
DES-7200#
```

46.3.2 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-name* 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,

```
DES-7200# show policy-map
Policy Map pp
Class cc
DES-7200#
```

46.3.3 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,

```
DES-7200# show mls qos interface gigabitEthernet 0/4
Interface GigabitEthernet 0/4
Attached input  policy-map: pp
Default COS: trust dscp
Default COS: 6
DES-7200#show mls qos interface policers
Interface: GigabitEthernet 0/4
Attached input  policy-map: pp
DES-7200#
```

46.3.4 Showing mls qos queueing

You may show the QoS queue information through the following steps:

Command	Description
show mls qos queueing	Show the QoS queue information, CoS-to-queue map, wrr weight and drr weight;

For example:

```
DES-7200# show mls qos queueing
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
```

46.3.5 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:

```
DES-7200# show mls qos scheduler
Global Multi-Layer Switching scheduling
Strict Priority
DES-7200#
```

46.3.6 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:

```
DES-7200# show mls qos maps cos-dscp
cos dscp
--- ----
0   0
1   8
2   16
3   24
4   32
5   40
6   48
7   56
DES-7200# 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
DES-7200# 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
```

46.3.7 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]

```
DES-7200# show mls qos rate-limit
Interface GigabitEthernet 0/4
rate limit input bps = 100 burst = 100
```

47 Configuring VRRP

47.1 Overview

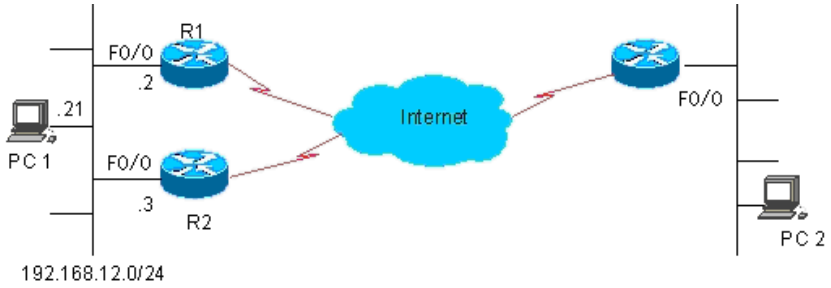
The Virtual Router Redundancy Protocol (VRRP) is designed to work in the active/standby mode to ensure the function switching can be implemented without affecting internal and external data communication, and the internal network parameters need no modification. when the active device is faulty Multiple 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 messages 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 messages mean a kind of multicast message with specified destination address, which are sent by the master router by schedule to indicate its operation and are also used to elect the master router. The VRRP allows another router automatically takes over the operations when the router that undertaking route forwarding function in the IP LAN fails, 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 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 message sent by the master device. In normal operation, the master device sends a VRRP message at an interval, called advertised message, to notify the backup devices. The master device is in the normal working status. If the backup device within the group doesn’t receive the message from the master device for a long time, the status itself will be switched to the Master.If there

is 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 47-1 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 device s R1 and R2 in the VRRP group. Once the master device fails, the other device automatically becomes the master.

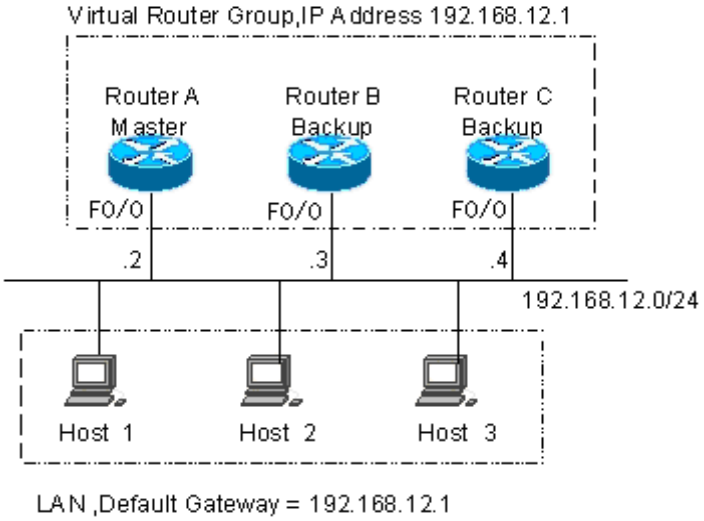
47.2 VRRP Applications

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.

47.2.1 Route redundancy

The basic VRRP applications are illustrated in Figure 47-2 .

Figure 47-2 Basic VRRP applications

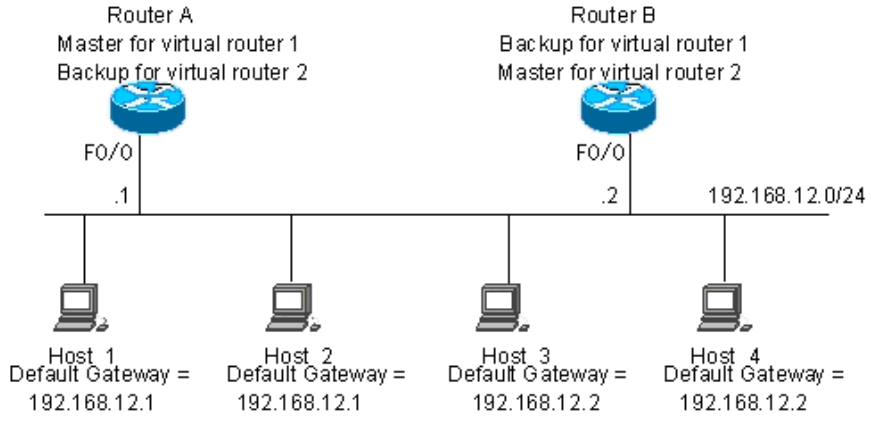


As shown in Figure 47-2 , devices A, B and C are connected with the LAN through Ethernet interfaces, on which the VRRP is configured. They are in the same VRRP group with virtual IP address 192.168.12.1. Device A is elected as the master device of the VRRP, and devices B and C are standby. Hosts 1, 2 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 a simply route redundancy.

47.2.2 Load balancing

The advanced VRRP applications are illustrated in Figure 47-3 .

Figure 47-3 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.

47.3 VRRP configuration

47.3.1 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:

- VRRP configuration task list (required)
- Enable VRRP backup function (optional)
- 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 the interface to be monitored by the VRRP backup group (optional)
- Set the host address to be monitored by the VRRP backup group (optional)
- 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 the user demands.

47.3.2 Enable 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
DES-7200(config-if)# **vrrp** *group* **ip** *ipaddress* [**secondary**]	Enable VRRP
DES-7200(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.

47.3.3 Set 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 be able 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
DES-7200(config-if)# **vrrp** *group* **authentication** *string*	Set the authentication string of the VRRP.
DES-7200(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.

47.3.4 Set the broadcast interval of the VRRP backup group

Command	Purpose
DES-7200(config-if)# **vrrp** *group* **timers advertise** *interval*	Set the master device VRRP advertisement interval

DES-7200(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.

47.3.5 Set the preemption mode of device in the VRRP backup group

If the VRRP group is working in the preemption mode, once a device finds its priority is higher than the Master priority, it will preempt to become the master of the VRRP group. If the VRRP group is not working in the preemption mode, even if a device finds its priority is higher than the Master priority, it will not preempt to become the master of the VRRP group. 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**
DES-7200(config-if)# **vrrp** *group* **preempt** [**delay** *seconds*]	Set the preemptive mode for the VRRP group
DES-7200(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.

47.3.6 Set the device priority in the VRRP backup group

The VRRP stipulates 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**
DES-7200(config-if)# **vrrp** *group* **priority** *level*	Set the priority of the VRRP backup group.

DES-7200(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).

47.3.7 Set the interface to be monitored by the VRRP backup group

After the interface to be monitored by the VRRP backup group is configured, the system will dynamically adjust the priority of the router according to the monitored interface. Once the status of the monitored interface becomes unavailable, the priority of the router in the VRRP backup group will be decreased according to the preset value. At the same time, another router in the backup group which has a more stable interface status or higher priority will become the active (master) router of the VRRP backup group.

Command	**Purpose**
DES-7200(config-if)# **vrrp** group **track** interface-type number [interface –priority]	Set the interface to be monitored by the VRRP backup group
DES-7200(config-if)# **no vrrp** group **track** interface-type number	Cancel setting of the interface to be monitored by the VRRP backup group

By default, there is no interface configured to be monitored by the VRRP backup group. The parameter *interface –priority* ranges 1~255. If the parameter *interface –priority* is default, the system will use the default value 10.

Note

The monitored interface only allows layer-3 routable logical interfaces (such as Routed Port, SVI, Loopback and Tunnel).

47.3.8 Set the host address to be monitored by the VRRP backup group

After the host address to be monitored by the VRRP backup group, the system dynamically adjusts the priority of the local machine according to whether the monitored host is reachable or not. Once the status of the monitored host becomes unavailable, the priority of the device in the VRRP backup group will be decreased according to the preset value. At the same time, another device in the backup group which has a more stable interface status or higher priority will become the active (master) device of the VRRP backup group.

Command	Purpose
DES-7200(config-if)# **vrrp** *group* **track** *a.b.c.d* [**interval** *interval_value*] [**timeout** *timeout_value]* *[priority-decrement]*	Set the host address to be monitored by the VRRP backup group. "**interval** interval_value" is used to specify the interval to send detection messages. "**timeout**timeout_value" is used to specify the timeout for the response of the monitored host.
DES-7200(config-if)# **no vrrp** *group* **track** *a.b.c.d*	Delete the host address to be monitored by the VRRP backup group

By default, there is no interface configured to be monitored by the VRRP backup group.The default detection interval is 3 seconds, and the default timeout period is 1 second. The parameter "*priority-decrement*" has a value range 1~255, 10 by default.

Note

The detection interval must be greater than or equal to the timeout period.

47.3.9 Set 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
DES-7200(config-if)# **vrrp** *group* **timers learn**	Set the timer learning function
DES-7200(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, if the timer learning function is not configured on the VRRP backup device, the VRRP backup device will drop the VRRP advertisement; otherwise, the VRRP backup device receives the VRRP advertisement and use the advertisement interval to calculate the failure judgment interval of the VRRP Master device.

47.3.10 Set the description string of device in the VRRP backup group

This command will set the descriptor for the VRRP group to facilitate identifying the VRRP group.

Command	Purpose
DES-7200(config-if)# **vrrp** *group* **description** *text*	Set the description string of the VRRP group
DES-7200(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 blanks are contained in the VRRP backup group description string, quotation marks (") must be used to identify the description string.

47.4 VRRP Monitoring and Maintenance

DES-7200 has commands **show vrrp** and **debug vrrp** to monitor and maintain 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.

47.4.1 show vrrp

DES-7200 has the following **show vrrp** commands to check the VRRP status of the local router.

Command	Purpose
DES-7200# **show vrrp** [**brief** | *group*]	Check the current VRRP status
DES-7200# **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

```
DES-7200# 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 messages 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 monitoring interface function is enabled.

2. **show vrrp brief** command

```
DES-7200# 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

```
DES-7200# 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
DES-7200#
```

The displayed messages 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.

47.4.2 debug vrrp

DES-7200 has the following **debug vrrp** commands to provide the VRRP status debugging information of the local router.

Command	Purpose
DES-7200# **debug vrrp error**	Turn on VRRP error prompt debugging switch
DES-7200# **no debug vrrp error**	Turn off VRRP error prompt debugging switch
DES-7200# **debug vrrp events**	Turn on the VRRP event debugging switch
DES-7200# **no debug vrrp events**	Turn off the VRRP event debugging switch
DES-7200# **debug vrrp packets**	Turn on the VRRP message debugging switch
DES-7200# **no debug vrrp packets**	Turning off the VRRP message debugging switch
DES-7200# **debug vrrp state**	Turn on the VRRP state debugging switch
DES-7200# **no debug vrrp state**	Turn off the VRRP status debugging switch
DES-7200# **debug vrrp**	Enable the IP debug switch
DES-7200# **no debug vrrp**	Turn off the VRRP debugging switch

Here are some examples of the command:

1. **debug vrrp** command

```
DES-7200# debug vrrp
DES-7200#
VRRP: Grp 1 Advertisement priority 120, ipaddr 192.168.201.213
VRRP: Grp 1 Event - Advert higher or equal priority
%VRRP-6-STATECHANGE: GigabitEthernet 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: GigabitEthernet 0/0 Grp 1 state Backup -> Master
DES-7200#
```

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

```
DES-7200# debug vrrp error
DES-7200#
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

```
DES-7200# debug vrrp events
DES-7200#
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
DES-7200#
```

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

```
DES-7200#debug vrrp packets
DES-7200#
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.

```
DES-7200# debug vrrp packets
DES-7200#
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

```
DES-7200# debug vrrp state
VRRP State debugging is on
DES-7200#
```

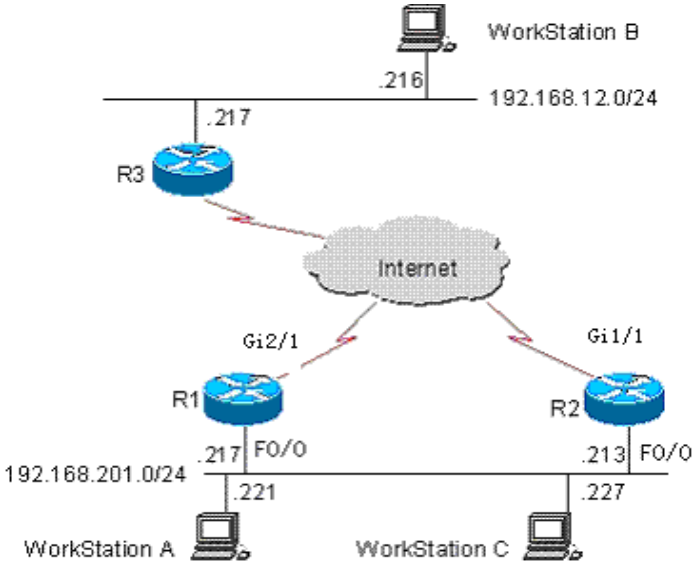
```
%VRRP-6-STATECHANGE: GigabitEthernet 0/0 Grp 2 state Master -> Backup
%VRRP-6-STATECHANGE: GigabitEthernet 0/0 Grp 2 state Backup -> Master
DES-7200# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)# interface GigabitEthernet 0/0
DES-7200(config-if)# no shutdown
DES-7200(config-if)# end
DES-7200#
%VRRP-6-STATECHANGE: GigabitEthernet 0/0 Grp 2 state Master -> Init
DES-7200#
```

The above displayed information indicates the VRRP group status on GigabitEthernet 0/0 is shifting among Master, Backup and Init.

47.5 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 47-4 Network connection with VRRP



In the configuration example below, the configurations of device R3 remain unchanged,The configuration on device R3 is shown below:

```
DES-7200# configure terminal
DES-7200(config)# interface gigabitEthernet 0/0
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 192.168.12.217 255.255.255.0
DES-7200(config-if)# exit
DES-7200(config)# interface GigabitEthernet 1/1
DES-7200(config-if)# no switchport
```

```
DES-7200(config-if)# ip address 60.154.101.5 255.255.255.0
DES-7200(config-if)# exit
DES-7200(config)# interface GigabitEthernet 2/1
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 202.101.90.61 255.255.255.0
DES-7200(config-if)# exit
DES-7200(config)# router ospf 1
DES-7200(config-router)# network 202.101.90.0 0.0.0.255 area 10
DES-7200(config-router)# network 192.168.12.0 0.0.0.255 area 10
DES-7200(config-router)# network 60.154.101.0 0.0.0.255 area 10
DES-7200(config-router)# end
```

47.5.2 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:

```
DES-7200# configure terminal
DES-7200(config)# interface gigabitEthernet 0/0
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 192.168.201.217 255.255.255.0
DES-7200(config-if)# vrrp 1 priority 120
DES-7200(config-if)# vrrp 1 timers advertise 3
DES-7200(config-if)# vrrp 1 ip 192.168.201.1
DES-7200(config-if)# exit
DES-7200(config)# interface GigabitEthernet 2/1
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 202.101.90.63 255.255.255.0
DES-7200(config-if)# exit
DES-7200(config)# router ospf 1
DES-7200(config-router)# network 202.101.90.0 0.0.0.255 area 10
DES-7200(config-router)# network 192.168.201.0 0.0.0.255 area 10
```

Configurations on device R2:

```
DES-7200# configure terminal
DES-7200(config)# interface GigabitEthernet 0/0
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 192.168.201.213 255.255.255.0
DES-7200(config-if)# vrrp 1 ip 192.168.201.1
DES-7200(config-if)# vrrp 1 timers advertise 3
```

```
DES-7200(config-if)# exit
DES-7200(config)# interface GigabitEthernet 1/1
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 60.154.101.3 255.255.255.0
DES-7200(config-if)# exit
DES-7200(config)# router ospf 1
DES-7200(config-router)# network 60.154.101.0 0.0.0.255 area 10
DES-7200(config-router)# network 192.168.201.0 0.0.0.255 area 10
DES-7200(config-router)# 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.

47.5.3 Example of configuration to monitor interface with 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 function 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:

```
DES-7200# configure terminal
DES-7200(config)# interface gigabitEthernet 0/0
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 192.168.201.217 255.255.255.0
DES-7200(config-if)# vrrp 1 priority 120
DES-7200(config-if)# vrrp 1 timers advertise 3
DES-7200(config-if)# vrrp 1 ip 192.168.201.1
DES-7200(config-if)# vrrp 1 track GigabitEthernet 2/1 30
DES-7200(config-if)# exit
DES-7200(config)# interface GigabitEthernet 2/1
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 202.101.90.63 255.255.255.0
```

```
DES-7200(config-if)# exit
DES-7200(config)# router ospf 1
DES-7200(config-router)# network 202.101.90.0 0.0.0.255 area 10
DES-7200(config-router)# network 192.168.201.0 0.0.0.255 area 10
DES-7200(config-router)# end
```

Configurations on device R2:

```
DES-7200# configure terminal
DES-7200(config)# interface gigabitEthernet 0/0
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 192.168.201.213 255.255.255.0
DES-7200(config-if)# vrrp 1 ip 192.168.201.1
DES-7200(config-if)# vrrp 1 timers advertise 3
DES-7200(config-if)# exit
DES-7200(config)# interface GigabitEthernet 1/1
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 60.154.101.3 255.255.255.0
DES-7200(config-if)# exit
DES-7200(config)# router ospf 1
DES-7200(config-router)# network 60.154.101.0 0.0.0.255 area 10
DES-7200(config-router)# network 192.168.201.0 0.0.0.255 area 10
DES-7200(config-router)# 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.

47.5.4 Example of Multiple VRRP Backup Groups

In addition to the single backup group, DES-7200 also allows multiple VRRP backup groups configured on the same Ethernet interface. There are obvious benefits for the use of multiple backup groups. It is possible to implement load balancing yet 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 1The configurations for devices R1 and R2 are described as follows.

Configurations on device R1:

```
DES-7200# configure terminal
DES-7200(config)# interface gigabitEthernet 0/0
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 192.168.201.217 255.255.255.0
DES-7200(config-if)# vrrp 1 timers advertise 3
DES-7200(config-if)# vrrp 1 ip 192.168.201.1
DES-7200(config-if)# vrrp 2 priority 120
DES-7200(config-if)# vrrp 2 timers advertise 3
DES-7200(config-if)# vrrp 2 ip 192.168.201.2
DES-7200(config-if)# vrrp 2 track GigabitEthernet 2/1 30
DES-7200(config-if)# exit
DES-7200(config)# interface GigabitEthernet 2/1
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 202.101.90.63 255.255.255.0
DES-7200(config-if)# exit
DES-7200(config-router)# router ospf
DES-7200(config-router)# network 202.101.90.0 0.0.0.255 area 10
DES-7200(config-router)# network 192.168.201.0 0.0.0.255 area 10
DES-7200(config-router)# end
```

Configurations on device R2:

```
DES-7200# configure terminal
DES-7200(config)# interface Loopback 0
DES-7200(config-if)# ip address 20.20.20.5 255.255.255.0
DES-7200(config-if)# exit
DES-7200(config)# interface GigabitEthernet 0/0
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 192.168.201.213 255.255.255.0
DES-7200(config-if)# vrrp 1 ip 192.168.201.1
DES-7200(config-if)# vrrp 1 timers advertise 3
DES-7200(config-if)# vrrp 1 priority 120
DES-7200(config-if)# vrrp 2 ip 192.168.201.2
DES-7200(config-if)# vrrp 2 timers advertise 3
DES-7200(config-if)# exit
DES-7200(config)# interface GigabitEthernet 1/1
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 60.154.101.3 255.255.255.0
DES-7200(config-if)# exit
DES-7200(config)# router ospf
DES-7200(config-router)# network 60.154.101.0 0.0.0.255 area 10
DES-7200(config-router)# network 192.168.201.0 0.0.0.255 area 10
DES-7200(config-router)# 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.

47.6 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 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.

48 Configuring RERP

48.1 About RERP

48.1.1 Understanding RERP

For the loop blocking and link recovery in core ring network, currently the OSPF and BGP4 are mostly used for the implementation. For complex network, the link recovery may take tens of seconds. If MSTP is used for loop blocking in the link layer, the STP needs to advertise level by level by the spanning tree, the network convergence may take rather long time in case of complicated network.

The Rapid Ethernet Ring Protection Protocol (RERP) is a special layer-2 link redundancy backup protocol designed for core Ethernet. The loop blocking and link recovery for the RERP are centrally implemented on the master device and the non-master devices directly report their link conditions to the master device without additional processing on the non-master devices; however the STP works with the spanning tree to advertise level by level by the spanning tree and determine the final link statuses through level-by-level calculations. So, the loop block and recovery with the RERP are faster than those with the STP. Based on the above difference, the link recovery of RERP in ideal environment may be completed in several microseconds.

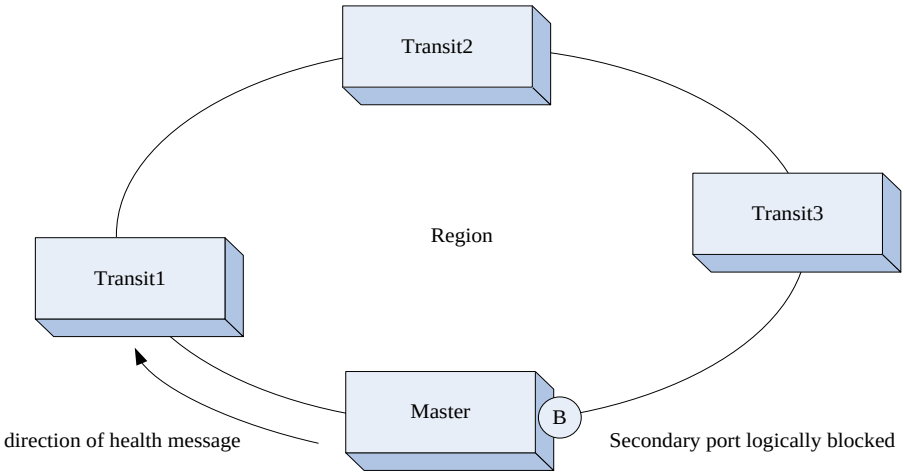
The RERP involves the following key concepts: ring, Region, Master, Backup, Transit, Primary Port, Secondary Port, and control vlan. They are explained through the following typical applications.

Note

As an alternative of STP in the core ring network, the RERP cannot be turned on at the same time with the STP in the actual configurations. Otherwise, unexpected results may produce.

48.1.2 Typical Applications

Figure 48-1



As shown above, the four devices are all core Ethernet devices and form a ring core network. In such a topology, each device has two and only two interface to be connected with the ring. This type of ring is called a RERP region, identified uniquely with an integer. Each RERP region can have only one Master and one Backup specified. The others are all Transit. Each device must be specified with the region and configured with the master/backup port.

Master:

The link is a TRUNK connection. The ring has an independent VLAN as the control VLAN, which is specially used to transmit various control messages defined by the RERP. The other VLANs are the data VLANs and used for the transmission of dataflow.

The two ports of the master connected to the ring are called the primary port and secondary port respectively, whether the primary port sends the Hello message outside on regular basis.

Loop blocking:

In normal cases, the master device prevents the generation of layer-2 loop in the whole ring by blocking the secondary port.

Link interruption:

When a link fails in the Ethernet ring (the link between Transit1 and Transit2 is broken, for example), both Transit1 and Transit2 may recognize this condition in the link, and advertise a LINK DOWN message via the control VLAN to the master. When the master receives it, it clears the layer-2 forwarding table information related with its data VLAN, and sends the FLUSH NOW message to notify all control devices to clear all data VLAN related layer-2 forwarding information. At the same time, the BLOCK status turns into the FORWARDING status.

Link recovery:

When the interrupted link recovers in the Ethernet (the one between Transit1 and Transit2 recovers normal, for example), Transit1 and Transit2 recognize the link recovery information, and make the ports of the recovery link ends in the BLOCK status, to forbid forwarding any messages. Then, they send the LINK UP advertisement to the master. The master receives it and turns the secondary interface in the BLOCK status, and then sends FLUSH NOW message to notify all controlled device to clear all data VLAN related layer-2 address table information. When Transit1 and Transit2 find the link recovery devices receive the FLUSH NOW message, they clear the layer-2 address table information in all data VLAN and then change the ports in BLOCK status into the FORWARDING status.

Device abnormity detection:

When the primary port of the master sends the HELLO message on regular basis (at an adjustable time interval, in 100 ms), if the secondary interface of the master does not receive the HELLP message from the primary port of the master, it considers the devices on the ring abnormal. Now, the master clears the data VLAN related layer-2 forwarding table information and sends the FLUSH NOW message to notify all controlled device to clear the DATA VLAN layer-2 forwarding table information, and then changes the BLOCK status of the secondary port into the FORWARDING status.

When the secondary port of the master receives the HELLO message from the primary interface, it immediately turns the secondary port to the BLOCK status, and then sends the FLUSH NOW message to notify the controlled devices to clear the layer-2 address table information in all data VLANs.

Master failure detection:

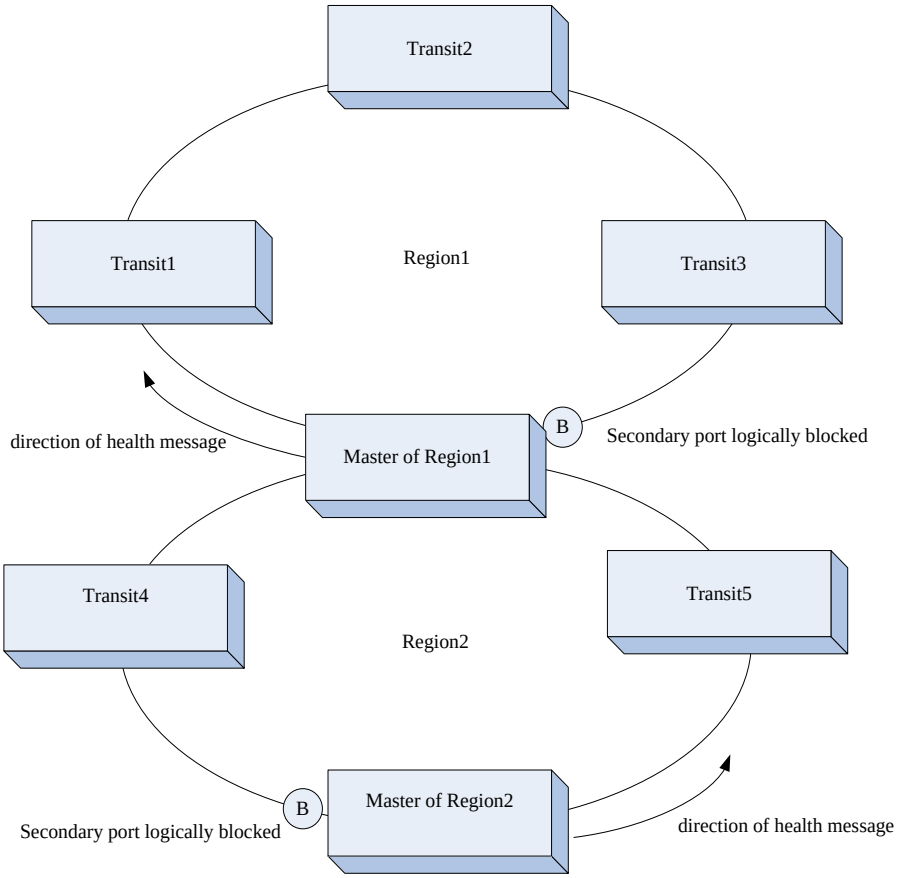
The user can specify a secondary device as the backup master. When the backup master does not detect the HELLO message sent from the master, it considers failure of the master and escalates itself to the master.

After the backup master switches to the master device, if it receives the message from the original master, it transfers the control to the original master and degrades again to the backup master.

The RERP supports tangent multiple rings. In other words, it allows multiple rings to share one device but does not support intersection of multiple rings.

Because the intersection of multiple rings may cause rings among adjacent devices, the user shall pay attention to the topology planning in deploying the RERP.

Figure 48-2



Configuring RERP

The following sections describe how to configure CPU Protect.

- RERP defaults
- Configure global RERP
- Configure RERP detection interval
- Configure RERP detection failure period
- Configure RERP region
- Configure RERP region role
- Configure RERP region control VLAN
- Configure RERP primary/secondary port

48.1.3 RERP defaults

Global RERP status	**DISABLE**
RERP detection interval	1S
RERP failure time	3S

Precautions before Configuration:

- The RERP and STP are exclusive. In other words, if the RERP is configured, the STP shall be turned off.
- The refresh failure waiting time and the detection failure time are always the same and equal to the failure time.
- If the Transit and Backup do not receive the HELLO message from the Master, they will use the detection interval and detection failure interval that are configured on the local machine. If the HELLO message is received from the master, the master configurations will be used to keep consistent protocol operations on the ring network.
- The RERP control VLAN does not include vlan 1 and vlan 4094.
- Each RERP region must have one and only one master and at the same time at most one backup.

48.1.4 Configure global RERP

The related parameter configurations do not take effect unless the global RERP is enabled.

In the global configuration mode, follow these steps to enable RERP:

Command	Function
DES-7200(config)# **rerp enable**	Turn on the global RERP function switch.
DES-7200(config)# **end**	Return to the privileged mode.

The **no** option of the command turns off the global RERP.

48.1.5 Configure RERP detection interval

The Master needs to send the RERP detection message on regular basis to check the health conditions of the loop. In the configuration mode, follows these steps to set the RERP detection interval:

Command	Function
DES-7200(config)# **rerp hello-interval** *interval*	Configure the detection interval within the range 1-6s, 1s by default.
DES-7200(config)# **end**	Return to the privileged mode.

The **no** option of the command restores default.

48.1.6 Configure the RERP failure time

If the secondary port of the master does not receive the detection message from the primary port in a certain period, it considers the fault of the loop, and then the master forces the secondary port to enter the learning forwarding status. In addition, the address refresh waiting time of the Transit and Backup is also that value.

In the global configuration mode, follow these steps to configure the RERP failure time:

Command	Function
DES-7200(config)# **rerp fail-interval** *num*	Configure the failure interval within the range 3-18s, 3 s by default.
DES-7200(config)# **end**	Return to the privileged mode.

The **no** option of the command restores default.

Note

The failure interval must be greater than the detection interval.

48.1.7 Configure RERP region

An RERP region is uniquely identified with an integer, and up to 64 regions can be configured on a machine. While the RERP region is configured, it also specifies the device to support the region and enter the RERP region configuration mode.

In the privileged mode, follow these steps to configure the RERP region:

Command	Function
DES-7200(config)# **RERP region** *num*	Create an RERP region and enter the RERP region configuration mode. The range for "num" is 1-64.

48.1.8 Configure RERP region role

Each device can play only one role in an RERP region, and each RERP region allows the configuration of only one master.

In the global configuration mode, follow these steps to configure the RERP region role:

Command	Function
DES-7200(config)# **RERP region** *num*	Create an RERP region and enter the RERP domain configuration mode at the same time.
DES-7200(config-rerp)# **role** [**master** | **backup** | **transit**]	Configure the role of the device in the RERP domain.

48.1.9 Configure RERP region control VLAN

Each RERP can have one and only one control VLAN specified. This VLAN can be used to transmit the RERP messages only, and is not used too transmit data messages.

In the global configuration mode, follow these steps to configure the RERP region control VLAN:

Command	Function
DES-7200(config)# **RERP region** *num*	Create an RERP region and enter the RERP domain configuration mode at the same time.
DES-7200(config-rerp)# **ctrl-vlan** *vid*	Configure the control VLAN with VID range 2-4,093.

Note

Since the RERP blocks only the Ethernet frame of data VLAN, please do not configure SVI for the control VLAN; otherwise, broadcast storm of the control VLAN may be caused.

In addition, the VLAN that has been created cannot be configured as the control VLAN, and the VLAN that is configured as the control VLAN cannot be created.

48.1.10 Configure RERP primary/secondary port

Each device must have one and only one primary port and secondary port in an RERP region. Ports cannot be shared between different RERP regions on the same device.

In the global configuration mode, follow these steps to configure the RERP primary/secondary port:

Command	Function
DES-7200(config)# **rerp region** *num*	Create an RERP region and enter the RERP domain configuration mode at the same time.
DES-7200(config-rerp)# **port primary-port interface** *interface-id* **secondary-port interface** *interface-id*	Specify the primary/secondary port of the device in the RERP domain.

Note

The RERP primary/secondary port does not support layer-3 interface or the member interface of the aggregate port. In addition, if the user configures the primary/secondary port and then configure it as the routing interface or aggregate member port, this may cause the primary/secondary member port deleted.

48.2 View RERP information

The following RERP-related information can be viewed:

- View the RERP configuration and status of the device

48.2.1 View the RERP configuration and status of the device

In the privileged mode, run the following command to view the RERP configuration and status of the device:

Command	Function
DES-7200# **show rerp**	View the RERP configuration and status of the device

In the example below, the **show rerp** command is used to view the RERP configuration and status of the device.

```
DES-7200# show rerp
rerp state            : disable
rerp hello interval   : 1
rerp fail interval    : 18
rerp local bridge     : 00d0.f822.89b2
----------------------------------------
region 64
region master         : none
ctrl-vlan             : 4001
role                  : transit
primary-port          : GigabitEthernet 3/12(down)
secondary-port        : GigabitEthernet 3/8(down)
```

49 Configuring RLDP

49.1 About RLDP

49.1.1 Understanding RLDP

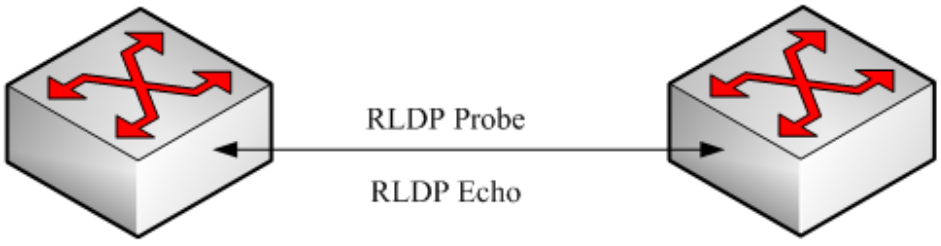
The Rapid Link Detection Protocol (RLDP) is one of DES-7200 link protocol designed to detect Ethernet link fault quickly.

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 the user. For example, if the optical fiber receiving line pair on the optical interface is misconnected, due to the existence of the optical converter, the related port of the device is "linkup" physically but actually the corresponding layer-2 link cannot work for communications. 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 messages at the two ends of the link, as shown below:

Figure 49-1



The RLDP defines two protocol messages: Probe message and Echo message. The RLDP sends the Probe message of this port to the port with RLDP configured and in linkup status on regular basis, and waits for the Echo message from the neighbor port and waits for the Probe message sent by the neighbor ports. If a link is correct both physically and logically, a

port shall be able to receive the Echo message of the neighbor port as well as the Probe message of the neighbor port. Otherwise, the link is considered abnormal.

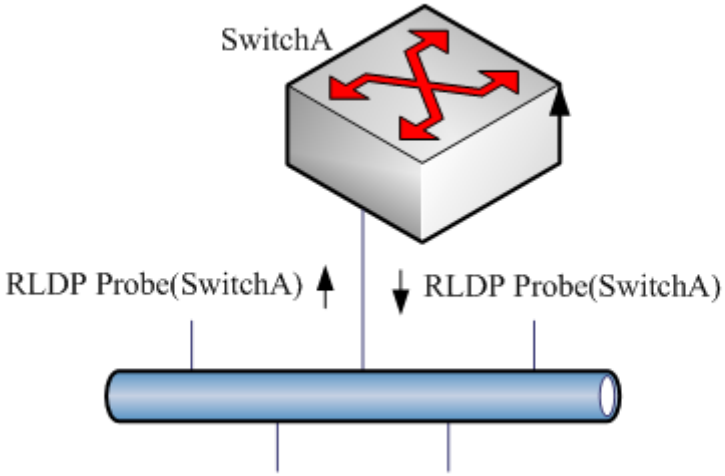
Note

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.

49.1.2 Typical Application

Loop detection:

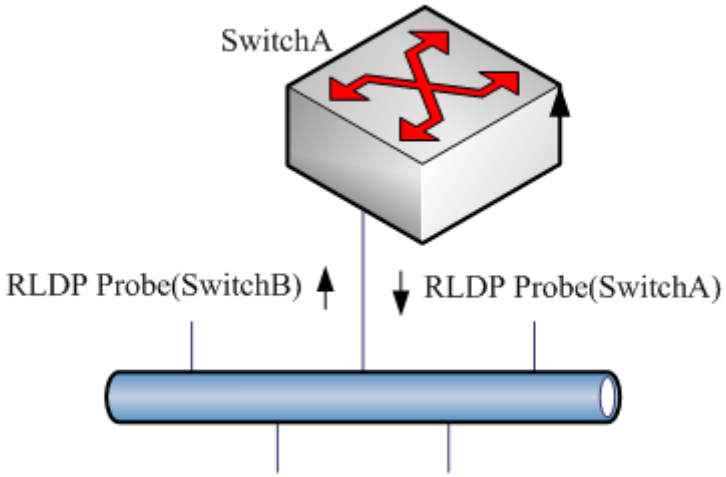
Figure 49-2 Loop detection



The so-called loop fault means that a loop appears on the links connected with the port. A shown above, on a port the RLDP receives the RLDP message sent from its machine, so the port is considered as loop fault. So, the RLDP deals with the fault according to the user configurations, including alarming, setting port violation, turning off the SVI with that port, turning off the port learning forwarding, and more.

One-way link detection:

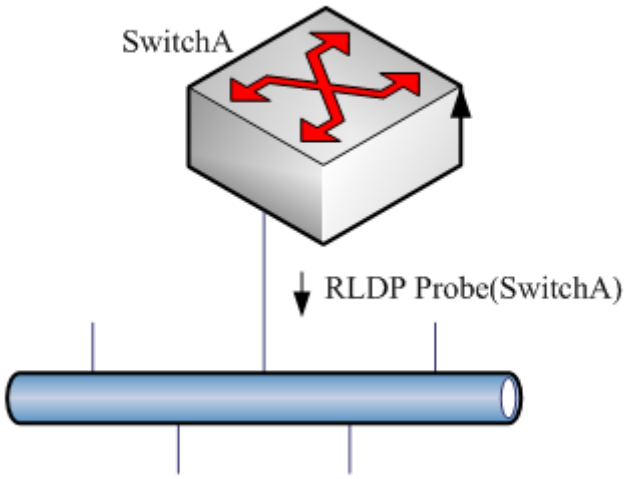
Figure 49-3 One-way link detection



The so-called one-way link detection means the link connected with the port can receive message only or send messages only (due to misconnection of the optical receiving line pair, for example). As shown above, the RLDP only receives the detection message from the neighbor port on a port, so it is considered one-way link fault. So, the RLDP deals with the fault accordingly according to the user configurations. In addition, if the port cannot receive any RLDP detection message, it is also considered one-way link fault.

Two-way link detection:

Figure 49-4 Two-way link detection



This means that 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 message but has never received the Echo message or the Probe message 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 shall make sure that the RLDP is enabled at both ends to avoid the incorrect diagnosis information.

49.2 Configuring RLDP

The following sections describe how to configure CPU Protect.

- RLDP defaults
- Configure global RLDP
- Configure port RLDP
- Configure RLDP detection interval
- Configure the RLDP maximum detection times
- Restore the RLDP status of the port

49.2.1 RLDP defaults

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 itnerface (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.

49.2.2 Configure global RLDP

The RLDP works on the port only when the global RLDP is enabled.

In the global configuration mode, follow these steps to enable RLDP:

Command	Function
DES-7200(config)# **rldp enable**	Turn on the global RLDP function switch.
DES-7200(config)# **end**	Return to the privileged mode.

The **no** option of the command turns off the global *RLDP*.

49.2.3 Configure port RLDP

The RLDP operation is port-based, so the user needs to explicitly configure which ports shall run RLDP. In configuring the port RLDP, it is required 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 the RLDP on the port:

Command	Function
DES-7200(config)# **interface** *interface-id*	Enter the interface mode.
DES-7200(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.
DES-7200(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:

```
DES-7200# configure terminal
DES-7200(config)# interface gigabitEthernet 0/5
DES-7200(config-if)# rldp port unidirection-detect
shutdown-svi
DES-7200(config-if)# rldp port bidirection-detect warning
DES-7200(config-if)# rldp port loop-detect block
DES-7200(config-if)# end
DES-7200# 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 in case of the occurring of detection error.
- 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 the link detection error happens, 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, alarm information will be given. 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.

49.2.4 Configure RLDP detection interval

The port with the RLDP function enabled will send the RLDP Probe messages on a regular basis.

In the global configuration mode, follow these steps to configure the RERP detection interval:

Command	Function
DES-7200(config)# **rldp** **detect-interval** interval	Configure the detection interval within the range 2-15s, 3s by default.
DES-7200(config)# **end**	Return to the privileged mode.

The **no** option of the command restores default.

49.2.5 Configure the RLDP maximum detection times

If the port with RLDP enabled cannot receive messages 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 RERP maximum detection times:

Command	Function
DES-7200(config)# **rldp detect-max** Num	Configure the maximum detection times, num range 2-10, 2 by default.
DES-7200(config)# **end**	Return to the privileged mode.

The **no** option of the command restores default.

Note The maximum detection times only take effect in undirection link detection and bidirection link detection, and will not take effect if only loop detection is enabled on a port.

49.2.6 Restore 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 removed, run the recovery command to restart the RLDP on the shutdown port. This command sometimes may make the other ports with detection errors resume.

In the privileged mode, follow these steps to resume the RLDP detection of the port:

Command	Function
DES-7200# **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 violation by RLP.

49.3 View 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

49.3.1 View 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
DES-7200# **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:

```
DES-7200# 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.

49.3.2 View the RLDP status of the specified port

In the privileged mode, run the following command to view the RLDP detection information of the specified port:

Command	Function
DES-7200# **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:

```
DES-7200# 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.

50 Configuring TPP

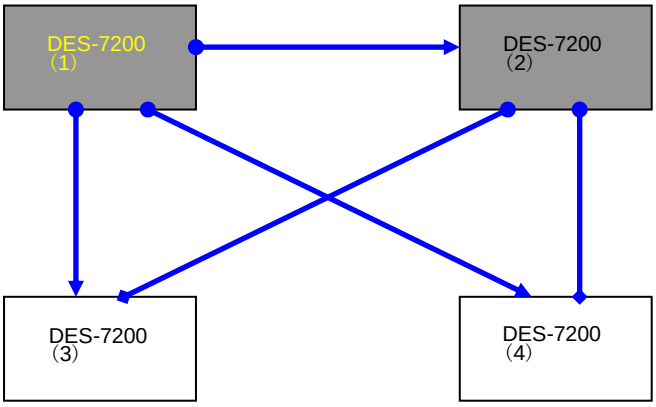
50.1 About TPP

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, etc. These are apt to cause network topology turbulence. The topology protection aims to stabilize the network topology by detecting the abnormalities (high CPU utilization, frame buffer abnormal, etc.) and detecting the abnormalities of neighbor devices. The interaction with neighbor devices is implemented by sending specific abnormity advertisement. This function has rather high priority and can effectively prevent network topology turbulence.

50.2 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 (MSTP, VRRP, etc.) to make the network more stable and reliable.

Figure 50-1



As shown above, the dual core topology has the DES-7200(1) as the root bridge. The topology protection function is enabled on every network device.

The DES-7200(1) encounters extreme CPU busy due to network attacks, which causes the BPDU messages cannot be sent normally. When the topology protection function detects the abnormity, it sends the abnormity notification messages to the neighbor devices. In the diagram above, both DES-7200(3,4) and DES-7200(2) receive the notification, and they will perform related anti-fluctuation treatment based on the abnormity notification information.

Due the attacks of a numerous messages, the DES-7200(2) encounters extreme CPU busy, resulting in abnormal packet receiving/transmitting. When the abnormity is detected, it sends abnormity notification to all neighbor devices. When DES-7200(1) receives the abnormity message, it finds there is no effect on itself so it does not perform further treatment. The downstream DES-7200(3,4) receives the abnormity message and finds its topology calculation will be affected by the abnormity, it performs further guard treatment to maintain stable network topology.

50.3 Configuring TPP

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 abnormities 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.

50.3.1 Configure 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
DES-7200> **enable**	Enter the privileged mode.
DES-7200# **config terminal**	Enter the global configuration mode.

DES-7200(config)# **topology guard**	Enable the global topology protection
DES-7200(config)# **end**	Exit to the privileged mode.
DES-7200# **copy running-config startup-config**	Save the configuration.

The **no topology guard** command diables the global topology protection function on the device.

50.3.2 Configure the topology protection on port

The configuration commands are as follows:

Command	**Function**
DES-7200> **enable**	Enter the privileged mode.
DES-7200# **config terminal**	Enter the global configuration mode.
DES-7200(config)# **interface gi** *0/1*	Enter the interface configuration mode.
DES-7200(config-if)# **tp-guard port enable**	Enable the port topology protection function.
DES-7200(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.

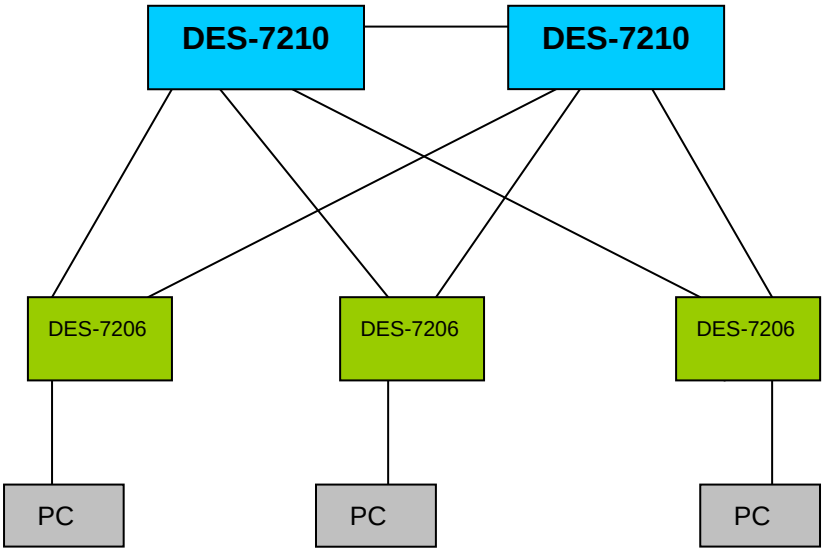
Note

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 abnormity appears locally, it sends abnormity notification messages to the neighbor devices. When the port topology protection function is enabled, if abnormity occurs locally, it sends abnormity notification message to neighbor devices.

50.4 Typical TPP Configuration Examples

The figure below shows a dual-core networking topology:

Figure 50-2



Both DES-7210 and DES-7206 have enabled MSTP and the two DES-7210 have enabled the VRRP. The topology protection function may make the operation of MSTP and VRRP more stable and prevent unnecessary fluctuation in the network topology.

Enable the topology protection function on the two DES-7210, and enable the topology protection functions on all the ports.

Enable the global topology protection function on every DES-7206.

50.5 View TPP information

The following TPP-related information can be viewed:

View the TPP configuration and status of the device

50.5.1 View the TPP configuration and status of the device

In the privileged mode, run the following command to view the TPP configuration and status of the device:

Command	Function
DES-7200# **show tpp**	View the TPP configuration and status of the device

51 Configuring Redundancy Management

51.1 Overview

DES-7200 supports dual management boards (i.e. dual engines), which offers management redundancy while increasing switching capacity, enhancing the stability of the switch. If the master management board cannot work normally during the operation of the switch, the switch will automatically switch over to the slave management board without loss of the user configuration, thus ensuring the normal operation of the network.

51.2 Configuring Redundant Management

This chapter includes:

- Automatic selection of master management board
- Manual selection of master management board

51.2.1 Automatic selection of master management board

DES-7200 supports dual management boards. You can plug or unplug the management boards while the switch is working. Based on the current conditions, the switch automatically selects an engine for its operation without normal data switching. In case of any conditions below during you use, the master management board will be selected accordingly:

- If only one management board is plugged when the switch is started up, the switch will select it as the master management board no matter whether it is in slot M1 or M2.
- If both management boards are plugged when the switch is started up, by default, the one in slot M1 will be selected as the master and the one in slot M2 as the slave for purpose of redundancy. Related prompt message will be provided.
- If only one management board is plugged when the switch is started up, and the other management board is plugged while the switch is in normal operation, the latter will be regarded as the slave management board for purpose of redundancy, no matter whether it is slot M1 or M2. Related prompt message will be provided.

- If both management boards are plugged when the switch is started up, and one of them is unplugged while the switch is in normal operation (or one becomes abnormal): if the unplugged management board is the slave before it is unplugged (or abnormal), the switch only prompts that the slave management board is unplugged (or becomes abnormal); if the unplugged management board is the master before it is unplugged (or abnormal), the other management board will turn from slave to master, and related prompt will be provided.

Caution During the normal operation of the switch, the parameters must be saved when the configurations are done; otherwise, the configuration will be lost in case of master/salve switchover.

51.2.2 Manual selection of master management board

DES-7200 supports dual management boards. You may select the master and slave management boards by using the commands available in CLI.

In the privileged user mode, execute the following commands to forcibly switch over the master management board:

Command	***Meaning***
redundancy force-switchover	This command is executed immediately without the necessity for global configuration mode.

For example, the current master management board is the one in slot M1. When the following commands are executed, the management board will be switched over to the slave management board, and the one in slot M2 becomes the master.

```
DES-7200#
DES-7200# redundancy  force-switchover
DES-7200#
```

In the global configuration mode, execute the following commands to configure the priority of the management board:

Command	**Meaning**
configure terminal	This command is executed immediately without the necessity for global configuration mode.
main-cpu prefer [**M1 | M2**]	Specify the management board in which slot shall be started preferentially
end	Return to the privileged mode.
write memory	Save the configuration.
show main-cpu preference	Check the preferential selection of the master management board

For example, you may execute the following commands and save them. After the switch is restarted, the master management board will be selected as your settings.

```
DES-7200#
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# main-cpu  prefer  m2
2006-04-22 09:26:00  @5-CONFIG:Configured from outband
DES-7200# show main-cpu  preference
main-cpu preference : M2
DES-7200#
```

51.3 Reliability Configuration

This chapter includes:

- Configure the synchronization mode
- Configure the heart-beat check time
- Reset the management board

51.3.1 Configure the synchronization mode

Run the following commands to configure the configuration files to be synchronized:

Command	Function
DES-7200(config)# **redundancy**	Enter the redundancy configuration mode
DES-7200(config-rdnd)# **auto-sync** {**standard** | **running-config** | **startup-config**}	Configure the configuration files to be synchronized.
DES-7200#**show running-config**	Confirm the hot-backup started.
DES-7200#**show redundancy states**	Show the current redundancy operation mode.

51.3.2 Configure the heart-beat check time

Run the following command to configure the heart-beat check time between the master and slave management boards.

Command	Function
DES-7200(config)# **redundancy**	Enter the redundancy configuration mode
DES-7200(config-rdnd)# **switchover timeout** *timerout-period*	Control the heart-beat check time between the master and slave boards
DES-7200#**show running-config**	Confirm the hot-backup started.
DES-7200#**show redundancy states**	Show the current redundancy operation mode.

51.3.3 Reset the management board

Run the following command to reset the specified management board or both the master and salve ones.

Command	Function
DES-7200(config)#**redundancy reload {peer | shelf}**	"peer" indicates resetting the slave management board only. "shelf" indicates resetting both.

52 Module Hot-Plugging/ Unplugging

52.1 Overview

DES-7200 support hot-plugging/unplugging of modules. You may plug and unplug modules while the device is powered on, without affecting the normal system operation or other modules.

52.2 Module Hot-Plugging/Unplugging Configuration

This chapter includes:

- Plugging or Unplugging Modules
- Installing or Uninstalling Modules
- View module information

52.2.1 Plugging or Unplugging Modules

You may plug modules while the device is operating (hot-plugging/unplugging). The operation of the other modules will not be affected.After the module is plugged in the slot, the management software of the device attempts to install its driver.

Caution

If the slot has been installed with another module driver, it is required to delete the original driver before installing the new module. You may execute the **show version module** command to get the related information.

You may plug modules while the switch is operating (hot-plugging/unplugging), which will not affect the operation of the other modules. The related configuration will be reserved when the module is unplugged, and it is possible to continue the setting of the module. When the module is re-plugged, the module will be automatically activated. All the configurations take effect automatically.

52.2.2 Installing or Uninstalling Modules

In addition to automatic installation of module driver after the module is plugged, you may also install the module driver manually. After the installation, all configurations for the slot will be done for the type of the installed module. Even if the module is unplugged, you can still configure it without loss of the configuration.

In the global configuration mode, execute the following commands to install a module manually:

Command	Meaning
configure terminal	Enter the global configuration mode.
install *slot-num moduletype*	Install the module of a specified type in a slot
end	Return to the privileged mode.

Caution

The installation of driver does not need physical presence of the module. This means that you may "pre-configure" the device. You may use the **Install** command to virtualize the module of a specified type and then configure it. When the module is plugged, all configurations take effect automatically.

You can uninstall an operating module. Once uninstalled, all configurations for it will be lost, and the module is disabled. To restore that module, you may "install" its driver manually, or unplug and then plug it again.

In the global configuration mode, execute the following commands to uninstall a module manually:

Command	Meaning
configure terminal	Enter the global configuration mode.
no install *slot-num*	Uninstall the module in a slot
end	Return to the privileged mode.

52.2.3 View module information

In the privileged user mode, execute the following commands to check the details of a module so as to uninstall it manually:

Command	Meaning
show version module detail	View module information

```
DES-7200# show version module detail
Device  : 1
Slot    : 1
User Status:      installed
Software Status: ok
Online Module :
         Type    : 7200-24G
       Ports   : 24
       Version : 01-01-05-02
Configured Module :
    Type    : 7200-24G
    Ports   : 24
    Version : 01-01-05-02

Device  : 1
Slot    : 2
User Status:      installed
Software Status: ok
Online Module :
   Type    : 7200-2XG
    Ports   : 2
    Version : 01-01-05-02
Configured Module :
    Type    : 7200-2XG
    Ports   : 2
    Version : 01-01-05-02

Device  : 1
Slot    : 3
User Status:      installed
Software Status: ok
Online Module :
    Type    : 7200-24
    Ports   : 24
    Version : 01-01-05-02
Configured Module :
    Type    : 7200-24
    Ports   : 24
    Version : 01-01-05-02

Device  : 1
Slot    : 4
User Status:      installed
    Software Status: none
    Online Module :
    Type    :
    Ports   : 0
    Version :
    Configured Module :
    Type    : 7200-24
    Ports   : 24
    Version :
```

```
Device  : 1
Slot    : M1
Status  : master
Online Module :
Type    : 7200-CM1
Ports   : 0
Version : 01-01-05-02
```

53 Configuring LCD

53.1 Overview

The LCD display is a visual display that features simple and easy operation with buttons. The user can know the running status of the device at a glance even if the user has no knowledge about the CLI commands. When abnormity occurs with the device operation, the displaying immediately notifies the abnormity to the users.

The state information shown by the LCD includes the switch name, duration of work, CPU utilization ratio (Management Board), memory utilization ratio (Management Board), temperature (Management Board and Line Card), fan and the working state of power supplies.

Generally, the device prints out the information circularly.

A user can use keys to show desired state information. The LCD provides the following four key:

- Menu key (Menu): Show a menu.
- Selection key (Enter): Select an item.
- Page Up key (Pgup): Page up.
- Page Down key (Pgdn): Page down,

When there is an unexpected condition in a module, for example, the CPU utilization ratio is too high, then the LCD keeps showing the warning information. The information will not disappear from the display until the user push the selection key (enter).

53.1.1 LCD Key Introduction

When the switch prints state information circularly, each page displays for a fixed period. If a user pushes one of the four keys, then the following condition occurs.

1. Menu: Stop the current displaying and show the main menu. Stops showing the menu and shows the state beginning at this page.
2. Selection key (enter): The key does not work.
3. Page Up key (Pgup): Shows the content of the previous screen. If the information of a state is not fully shown in one screen, then it can be shown in multiple screens. If the first screen is not currently shown, then push the key Pgup to show the previous screen

of the current content. If the first screen is shown, then push the key Pgup to show the last screen of the state information.

4. Page Down key(Pgdn): Shows the content of next screen. If the information of a state is not fully shown in one screen, then it can be shown in multiple screens. If the last screen is not currently shown, then push the key Pgdn to show the next screen of the current content. If the last screen is shown, then push the key Pgdn to show the first screen of the state information.

Press Menu to show the main menu, and the selected line will be highlighted. If there is no button pressing operation, it returns to the circular displaying again and display the next screen since the previous displaying. If a key is pressed, the following condition may occur:

1. Menu: Stop the current displaying and show the main menu.
2. Selection key (enter): Select the currently selected menu item. If there is a submenu in the menu item, then the submenu is shown. If a menu item indicates the information of a state, then the state information is shown.
3. Page Up key (Pgup): Shows the content of the previous screen.

All the menu items of a menu page are circularly organized. The previous item of the first menu item is the last item. The next item of the last item is the first item. If a menu is currently shown and the selected menu is not in the first line of the screen, when you push the Pgup key, the content of the screen will not change, the selected menu item will move up a line and the selected line is still the first line.

The state information that menu items point to are also circularly organized. The previous screen of the first screen is the last screen and the next screen of the last screen is the first screen. If the content of a menu item is currently shown, then Pgup shows the content of the previous screen. When the content of a menu item is shown, push the key enter to return to the menu page.

4. Page Down key(Pgdn): Shows the content of next screen.

If a menu is currently shown and the selected menu is not in the last line of the screen, when you push the Pgdn key, the content of the screen will not change, the selected menu item will move down a line and the selected line is still the last line.

If the content of a menu item is currently shown, then Pgdn shows the content of the next screen. When the content of a menu item is shown, push the key enter to return to the menu page.

If warning messages need be shown in the LCD, then the display shows generated warning messages. If a warning message need be shown in multiple screens, then the display shows the content of the warning message in screens circularly. If multiple warning messages are generated at the same time, then various warning messages are shown in turn and then the content of the newest warning message is shown circularly. The condition will not end until the user types the selection key (enter) to stop showing the warning message. If you push one of the four keys when a warning is shown, the following condition will occur:

1. Menu key (Menu): Stops showing the warning message and begins to show the main mp
2. Selection key (enter): Stops showing the current warning message. If there is no updated warning message, then returns to the circular display mode. If there is a updated warning message, the new warning message is shown.
3. Page Up key (Pgup): All the warning messages are circularly organized. The previous screen of the first screen is the last screen of the previous warning message. The next screen of the last screen is the first item of the next warning message. Pgup shows the content of the previous screen. If the first screen of the first warning message is currently shown, the shown content will not change.
4. Page Down key (Pgdn): Warning messages are circularly organized. Pgdn shows the content of the next screen. If the last screen of the last warning message is currently shown, the shown content will not change.

53.2 LCD Configuration Task List

53.2.1 Configuring Warning Information Queue Length

After a warning message is generated, the LCD keeps showing the new warning message unless a user pushes the key Enter. The user can browse history warning messages through menu items after pushing the key Enter. The command can be used to configure the length of a warning message.

The current version of DES-7200 saves 100 history warning messages by default. To configure the length of a history warning message, run the following command in the global configuration mode:

Command	Function
DES-7200(config)# **lcd trap-number** *num*	Set a new length of a warning message
DES-7200(config)# **no lcd trap-number**	Restore to the default setting

53.3 LCD Configuration Instance

Use the following command to configure the length of a history warning message:

```
lcd trap-number 200  //Configure the length of a warning message to 200
```

54 Using the USB

54.1 Overview

This chapter introduces the use of the USB storage (mostly the USB disk). The system can recognize the FAT-partitioned USB disk only and cannot recognize the other file systems.

When a USB disk is inserted, the system automatically loads the recognized partitions to the system. The operation on the USB disk is the same as normal directories.

54.2 Inserting the device

Just insert the USB device into the USB slot without additional operations. If the system finds the device and loads its driver, the following prompts are printed:

0:1:18:57 DES-7200: %5:USB Device Found ..... <USB Mass Storage Device>!

0:1:18:57 DES-7200: %5: Auto Mount Disk Partitions:

0:1:18:57DES-7200: %5: * /dev/uba/disc0/part1 --> /mnt/uba size : 131072000B(125MB)

<USB Mass Storage Device> is the name of the found device. The /dev/uba/disc0/part1 is the device file of the partition. The /mnt/uba is the directory for the partition. The "size" means the partition size. In the example above, the USB disk has free space 125MB.

54.2.1 Using the device

When the partition of the USB disk is loaded to the system, the commands of the file system (dir, copy, del, etc.) can be used to operate the USB disk. The operation below copies the files in the USB disk to the flash.

DES-7200# cd /mnt/uba # Enter the USB disk partition

DES-7200# copy flash: a.txt flash: /b.txt # Copy the file a.txt from the USB disk to the root directory of the device.

Now, run " dir /" to see the file b.txt added into the flash.

Similar to other file operations, the partition of the USB disk is like a directory on the file system.

54.2.2 Format the partition

The system may format the partition by using the **makefs** command.

Command	Function
DES-7200#**makefs dev** *dev_file* **fs** *fs_name*	Format the partition of device file dev_file into a file system named fs_name.

For the above USB disk found, run the following command:

```
DES-7200#makefs dev /dev/uba/disc0/part1 fs vfat
```

Then the partition of the USB disk is reformatting into a FAT32 partition.

Caution

A USB disk supports only to be formatted into vfat.

54.2.3 Show USB device information

Command	Function
DES-7200# **show usb**	Show the USB device information of the system

In the CLI command mode, use the **show usb** command to view the USB device information of the system. The displayed information is as follows:

```
DES-7200#sh usb
Device: USB Mass Storage Device :
        ID: 778
        Lun 0:
            ID: 0
            Disk Partitions:
            1: /dev/uba/disc0/part1 --> /mnt/uba
            size : 131072000B(125MB)
```

As shown above, "USB Mass Storage Device" is the device name.

"778" is the ID assigned by the system to the device, which is used when the device is to be uninstalled.

"Lun" is the logical unit number of the storage. Some devices have multiple logical units. The following ID is the one assigned by the system for the logical unit.

"Disk Partitions" shows the partition information of the logical unit. In the example above, there is one partition with device name /dev/uba/disc0/part1, loaded directory /mnt/uba, and size 125MB.

54.2.4 Unplugging USB device

Before unplugging the USB device, run the CLI command to unload it first to prevent the occurring of errors when the device is in use.

Command	Function
DES-7200# **usb remove** *Device_ID*	Unload the USB device with ID Device_ID

After the unloading command is executed, the system prints:

OK, now you can poll out the device 778.

0:1:1:38 DES-7200: %5:USB Device <USB Mass Storage Device> Removed!

Now it is ready to unplug the USB device.

Sometimes the device cannot be unloaded temporarily since it is in use, wait for a while, execute the command and unplug the device.

Caution

Be sure to unload the device first and then unplug the device to prevent the occurring of system error.

55 Using File System

55.1 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 are 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 will automatically de-fragment the storage device and recycle the trash. This is for providing the 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.

55.2 Configuring File System

The following sections describe how to configure the file system.

- Showing File Contents
- Changing Directories
- Copying Files
- Showing Directories
- Formatting the System
- Create directories
- Moving Files
- Showing the Current Working Path
- Removing Files
- Deleting Empty Directories

55.2.1 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 the all the file names and paths support the wildcard.

55.2.2 Showing File Contents

This command shows the contents of a text file or binary file.

In the privileged mode, use this command by performing the following steps:

Command	Function
DES-7200# **cat type bin file** *filename*	Show the contents of the specified binary file filename.
DES-7200# **cat type text file** *filename*	Show the contents of the specified text file filename.

The following example indicates the cat configuration process, showing the contents of a text file and a binary file:

```
DES-7200# cat type text log.txt
DES-7200# cat type bin sxx.bin
```

According to the above configuration, the contents of the text file and binary file are shown are the commands are executed.

55.2.3 Changing Directories

This shifts from the current director to the specified directory.

In the privileged mode, use this command by performing the following steps:

Command	Function
DES-7200# **cd** *directroy*	Enter the specified directory.
DES-7200# **cd** ../	Enter the higher-level directory
DES-7200# **cd** ./	Enter the current-level directory

The following example enters the document directory in the mnt directory at the root:

```
DES-7200# cd mnt/document
```

After that, the operations will be performed in the mnt/document directory.

55.2.4 Copying Files

This copies the files to a directory or a file.

In the privileged user mode, copy files to a directory or files by using the cp command:

Command	Function
DES-7200# **cp dest** *directoryname* **sour** *filename*	Copy the file to the specified directory
DES-7200# **cp dest** *filename* **sour** *directoryname*	Copy the file to the specified file

The following example shows how to copy a file to a directory and another file:

```
DES-7200# cp dest ../bak sour config.text
DES-7200# cp dest con_bak.txt sour config.text
```

55.2.5 Showing Directories

This shows the contents of the current working directory or specified directory:

Command	Function
DES-7200# **ls**	Show the contents in the current directory
DES-7200# **ls** *directory*	Show the contents in the specified directory

The following example shows the contents of the current directory and specified directory:

```
DES-7200# ls
DES-7200# ls ../bak
```

55.2.6 Formating the System

In the privileged user mode, format the device managed and operated by the file system by using the following command:

Command	Function
DES-7200# **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 use by the jffs2 file system:

```
DES-7200# 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.

55.2.7 Create directories

In the privileged mode, create the needed directory at the specified location by performing the following steps:

Command	Function
DES-7200# **mkdir** *directoryname*	Create directories

The following example creates a bak directory in the root directory:

```
DES-7200# mkdir bak
```

55.2.8 Moving Files

In the privileged user mode, move the specified files to the specified directory:

Command	Function
DES-7200# **mv dest** *directoryname* **sour** *filename*	Move the file named filename to the directory named directoryname.
DES-7200# **mv dest** *filename1* **sour** *filename2*	Move the file named filename2 to the file named file2name and remove the source file. When filename1 and filename2 are in the same directory, these operations are equivalent to renaming.

55.2.9 Showing the Current Working Path

In the privileged user mode, show the current working path by performing the following steps:

Command	Function
DES-7200# **pwd**	Show the current working paths

55.2.10 Removing Files

In the privileged user mode, delete a file permanently by performing the following step:

Command	Function
DES-7200# **rm** *filename*	Delete the specified file.

The following example deletes the temporary file named large.c in the mnt directory:

```
DES-7200# rm mnt/large.c
```

55.2.11 Deleting Empty Directories

In the privileged user mode, delete an empty directory permanently by performing the following step:

Command	Function
DES-7200# **rmdir** *directoryname*	Remove an empty directory

The above example deletes an empty directory named mnt.

```
DES-7200# rmdir mnt
```