DES-7200

Configuration Guide

D-Link®

Preface

Version Description

This manual matches the Firmware version v10.0.

Target Readers

This manual is intended for the following readers:

- Network engineers
- Technical salespersons
- Network administrators

Conventions in this document

1. General Format

Font Arial: Arial, size 10pt for body text

Regular script: All warnings, prompts, etc. use regular script and lines should be added to separate them from a text.

`Terminal displaying format: Courier New for English characters and Song for Chinese characters with size 8.5 to indicate the screen output information of the terminal. User's entries among the information shall be indicated with` **`bolded`** `characters.`

2. Command Lines

Format meaning

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:

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

 **Note**	Precaution, attention or reminder in the operation.

Description

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

Contents

1 Configuring DHCP

1.1 Overview

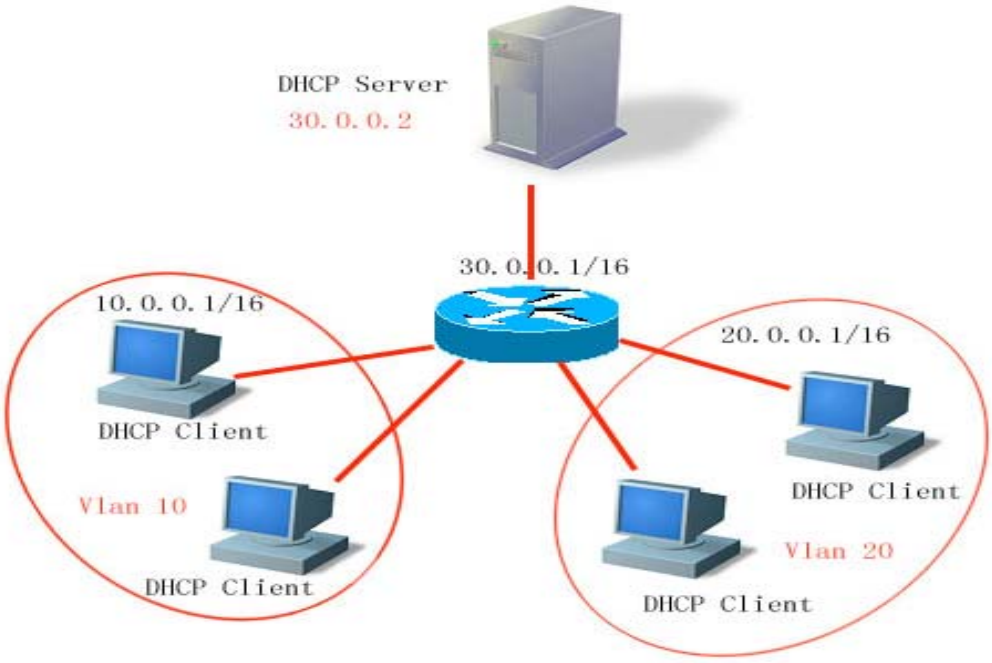
1.1.1 Understanding DHCP

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.

1.1.2 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 L3 network 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.



VLAN 10 and VLAN 20 correspond to the 10.0.0.1/16 and 20.0.0.1/16 networks, 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 switch that functions as the gateway, and specify the DHCP Server IP as 30.0.0.2.

1.2 Configuring DHCP

1.2.1 Configuring DHCP Relay Agent

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

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

1.2.2 Configuring the DHCP Server IP Address

After you have configured the IP address of the DHCP Server, the DHCP request packets received by the switch 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 be configured globally or on the L3 interface. In either mode, you can configure multiple server addresses. 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
D-Link(config)**#IP helper-address** *A.B.C.D*	Add a global DHCP server address
D-Link(config-if)**# IP helper-address** *A.B.C.D*	Add the DHCP server address of an interface
D-Link(config)**# no IP helper-address** *A.B.C.D*	Delete a global DHCP server address
D-Link(config-if)**#no IP helper-address** *A.B.C.D*	Delete the DHCP server address of an interface

1.2.3 DHCP Configuration Example

Below is the example for enabling the dhcp relay function and adding two server addresses:

```
Reg-Giant#configure  terminal
D-Link(config)#service dhcp           //Enable the dhcp relay function
D-Link(config)#ip helper-address192.18.100.1  //Add the global server address
D-Link(config)#ip helper-address192.18.100.2  //Add the global server address
D-Link(config)#interface FastEthernet 0/1
D-Link(config)#ip helper-address192.18.200.1  //Add the interface server address
D-Link(config-if)#ip helper-address192.18.200.2  //Add the interface server address
D-Link(config-if)#end
```

1.3 Showing DHCP Configuration

Please use the command of **show running-config** to show DHCP configuration in the privillged mode.

2 Port-based Flow Control

2.1 Storm Control

2.1.1 Overview

When there are numerous broadcast, multicast or unknown unicast packets in the LAN, the network performance will degrade. 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 an interface receives broadcast, multicast or unknown unicast packets at a rate higher than the set threshold, the switch will discard the excessive packets to avoid excessively flooding packets to the LAN, which may case storm.

2.1.2 Configuring Storm Control

By default, the storm control function for broadcast, multicast and unknown unicast packets is disabled.

When you set an interface in a unit, all other interfaces must be set in the same way. Otherwise, the setting will fail.

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

Command	Function
D-Link(config-if)#storm-control {broadcast | multicast | unicast} [{level *percent* | pps *packets* | *rate-bps*]	Enable the broadcast storm control function. Enable the unknown unicast storm control function. 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.

```
D-Link# configure terminal
D-Link(config)# interface GigabitEthernet0/1
D-Link(config-if)# storm-control multicast 4096
D-Link(config-if)# end
```


Note

The DES-7200 series switch does not support **storm-control action**.

2.1.3 Viewing the Enable Status of Storm Control

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

Command	Function
D-Link#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:

```
D-Link#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 storm control statuses of all interfaces at a time:

```
D-Link#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
```

2.2 Protected Port

2.2.1 Overview

Under certain application contexts, it is required that some ports on the same switch 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 switch 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.

2.2.2 Configuring the Protected Port

Set one port as the protection port:

Command	Function
D-Link(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.

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

2.2.3 Showing Protected Port Configuration

Command	Function
D-Link(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.

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

2.3 Port Security

2.3.1 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 switch. After you configure some secure addresses for the secure port (whose port security function is enabled), this port does not forward any other packets 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 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.

You can also manually configure some secure addresses and let the switch 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 number of secure addresses is full, the security port will discard all the packets of unknown addresses.

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.

2.3.2 Configuring Port Security

2.3.2.1 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


Note

If this series of switch is not bound with IP addresses, 1024 is supported for the maximum as a whole. Each port can be bound with up to 84 IP addresses.

2.3.2.2 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.

It is recommended that the secure addresses on a secure port should be in the same format. In other words, the addresses should be either bound or not bound with the secure addresses of the 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).

2.3.2.3 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
D-Link(config-if)#switchport port-security	Enable the port security function of this interface.
D-Link(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.
D-Link(config-if)#switchport port-security violation{protect | restrict | shutdown}	Set the violation handling mode: 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**.

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

2.3.2.4 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
D-Link(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 gigabitethernet 0/3: 00d0.f800.073c and bind it with an IP address:

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

2.3.2.5 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 switch 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
D-Link(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 on dynamically learned secure 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:

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

2.3.2.6 Configuring ARP Packet Check for Security Addresses

When you enable ARP packet check, you can effectively prevent the spoofing ARP packets and prevent invalid information sites from faking the IP addresses (for example, servers) of the key network devices, causing chaotic network communication.

ARP packet check restriction:

1. If you enable the ARP packet check for the secure addresses of the ports, the maximum number of the IP addresses bound with all the ports will be reduced by an half.
2. If you enable the ARP packet check for the secure addresses of the port, this is not effective for the existing secure addresses. If you want this also be effective to the old secure addresses set, you can first disable and then enable the security of the port. The port ARP packet check uses the policy management module, which shares the resources with other policy management modules. If the hardware resources are insufficient, the ARP packet check may not take effect for some secure addresses.
3. When there are many MAC+IP secure address entries, the CPU performance will be greatly affected, reducing its efficiency, if ARP check cpu is enabled.

By default, only IP packets are checked for secure addresses. Sometimes, the administrator needs to check the validity of the ARP packets. In this case, the following commands can be used in the interface configuration mode to enable ARP packet check.

Command	Function
D-Link(config-if)#port-security arp-check [cpu]	Enable ARP packet check for secure ports Where, cpu is the option of ARP Check for checking the packets sent to the CPU of the switch. When this option is enabled, the CPU load may increase. You must first enable arp-check before you enable the cpu option for it to take effect .

In the global configuration mode, you can disable the ARP packet check for secure addresses by using the no port-security arp-check[cpu] command.

Note The DES-7200 series switch does not support ARP packet check.

2.3.3 Viewing Port Security Information

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

Command	Function
D-Link#show port-security interface [interface-id]	View the port security configuration information of an interface.
D-Link#show port-secure address	View the secure address information.
D-Link#show port-secure address [*interface-id*]	Show the secure address information on an interface.
D-Link#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**:

```
D-Link# 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.

```
D-Link# show port-secure 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.

```
D-Link# show port-secure 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.

```
D-Link#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
```

3 Using File System

3.1 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.

3.2 Configuring File System

The following sections describe how to configure the file system.

- Show file contents
- Change directories
- Copy files
- Show directories
- Format the system
- Create directories
- Move files
- Show the current working paths
- Delete Files
- Delete empty directories

3.2.1 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.

3.2.2 Show 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
D-Link**#cat type bin file** *filename*	Show the contents of the specified binary file *filename*.

Command	Function
D-Link # 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:

```
Switch#cat type text log.txt
Switch# cat type bin sxx.bin
```

According to the above configuration, the contents of the text file and binary file are shown after the commands are executed.

3.2.3 Change 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
D-Link**#cd** *directroy*	Enter the specified directory.
D-Link**#cd** ../	Enter the higher-level directory
D-Link**#cd** ./	Enter the current-level directory

The following example enters the document directory in the mnt directory at the root:

```
Switch#cd mnt/document
```

After that, the operations will be performed in the mnt/document directory.

3.2.4 Copy 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
D-Link**# cp dest** *directoryname* **sour** *filename*	Copy the f ile to the specified directory
D-Link**#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:

```
Switch#cp dest ../bak sour config.text
Switch#cp dest con_bak.txt sour config.text
```

3.2.5 Show Directories

This shows the contents of the current working directory or specified directory:

Command	Function
D-Link**#ls**	Show the contents in the current directory
D-Link**#ls** *directory*	Show the contents in the specified directory

The following example shows the contents of the current directory and specified directory:

```
Switch#ls
Switch#ls ../bak
```

3.2.6 Format the System

In the privileged user mode, format the device managed and operated by the file system by using the following command:

Command	Function
D-Link**#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:

```
Switch#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.

3.2.7 Create Directories

In the privileged mode, create the needed directory at the specified location by performing the following steps:

Command	Function
D-Link**#mkdir** *directoryname*	Create directories

The following example creates a bak directory in the root directory:

```
Switch#mkdir bak
```

3.2.8 Move Files

In the privileged user mode, move the specified files to the specified directory:

Command	Function
D-Link**#mv dest** directoryname **sour** filename	Move the file named filename to the directory named directoryname.
D-Link**#mv dest** *filename1* **sour** *filename2*	Move the file named filename2 to the file named filename1 and remove the source file. When *filename1* and *filename2* are in the same directory, these operations are equivalent to renaming.

3.2.9 Show the Current Working Path

In the privileged user mode, show the current working path by performing the following steps:

Command	Function
D-Link**#pwd**	Show the current working paths

3.2.10 Delete Files

In the privileged user mode, delete a file permanently by performing the following step:

Command	Function
D-Link**#rm** *filename*	Delete the specified file.

The following example deletes the temporary file named large.c in the mnt directory:

```
Switch#rm mnt/large.c
```

3.2.11 Delete Empty Directories

In the privileged user mode, delete an empty directory permanently by performing the following step:

Command	Function
D-Link**#rmdir** *directoryname*	Remove an empty directory

The above example deletes an empty directory named mnt.

```
Switch#rmdir mnt
```

4 Configuring GVRP

4.1 Overview

GARP VLAN Registration Protocol(GVRP) is an application of Generic Attribute Registration Protocol (GARP) used to distribute and configure VLAN membership dynamically.

Through GVRP, the switch can:

- Switch listens to GVRP PDUs on each port, so as to learn VLAN information of the devices attached to the port from GVRP PDUs, then it uses this information to configure VLAN members on the ports that receives GVRP PDUs.
- Through transmitting GVRP PDUs, switch advertises VLAN information on each port. The information includes static local configuration and learned information of other devices by GVRP.

Through GVRP, switches on the switching network can create VLANs dynamically, and keep the consistence of VLAN configuration in real time. By advertising VLAN IDs automatically on the network, GVRP lowers the error probability resulted from configuration inconsistence. When VLAN configuration on one device changes, GVRP can change the configuration on connected device automatically, so as to reduce user's manual work on configurations.

GARP and GVRP are defined with following standard:

```
IEEE standard 802.1D
IEEE standard 802.1Q
```

4.2 Configuring GVRP

4.2.1 GVRP default configurations

This table shows default GVRP configurations.

Function	Default Configuation
GVRP global enable state	Disabled
GVRP dynamic creation of VLANs	Disabled
GVRP base vlan id	VLAN 1(only effective in MSTP)
GVRP registration mode	Enable
GVRP applicant state	Normal, (ports do not declare VLANs when in STP blocking state)
GVRP timers	Join time: 200 ms Leave time: 600 ms Leaveall time: 10,000 ms

4.2.2 GVRP Configuration Guide

- GVRP shall be enabled on the switches on sides of a link. The GVRP information propagates only on Trunk links. The information propagated includes all VLAN information of exist switches, no matter the VLAN information is learned or manually configured.
- If STP is used, only ports in forwarding states can participate in GVRP to receive and send GVRP PDUs, and only the information in forwarding port can be propagated by GVRP.
- All the VLAN ports added by GVRP are tagged ports.
- All the VLAN information learned by GVRP will be saved in the system, and will be lost after the switch is reset. It is acceptable if the user does not save this VLAN information.
- Dynamic VLAN parameters created by GVRP cannot be modified.
- The value of GVRP timer (join, leave, leaveall) to be exchanged shall be consistent.

4.2.3 Enabling GVRP

GVRP will not take effect if not globally enabled.

If GVRP is not globally enabled, the GVRP parameters can be configured, but they will not take effect until GVRP is enabled.

Global controlling GVRP:

Command	Function
D-Link(config)#**[no] gvrp enable**	Enable GVRP (if disabled)

Example:

```
D-Link # configure
Enter configuration commands, one per line. End with CNTL/Z.
D-Link(config)# gvrp enable
D-Link(config)# end
```

4.2.4 Controlling the creation of Dynamic VLANs

If the information (join, joinempty) received on one port indicates that VLAN not exist in the switch, GVRP will create this VLAN. User controls the creating of dynamic VLANs.

Controlling the creation of Dynamic VLAN:

Command	Function
D-Link(config)#[no] gvrp dymanic-vlan-creation enable	Allow creating VLAN dynamically (if disabled)

VLAN parameters created by GVRP cannot be modified.

Example:

```
D-Link # configure
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# gvrp dynamic-vlan-creation enable
D-Link(config)# end
```

4.2.5 Configuring the operation VLANs of GVRP

If STP is not enabled, all the ports can take part in running GVRP.

If SST is enabled, only the ports that are in forwarding state of SST context can take part in running GVRP.

If MST is enabled, GVRP can run in the spanning-tree context belongs to VLAN 1, and the user cannot specify other spanning-tree contexts.

4.2.6 Configuring the Registration Mode

There are two registration modes for the port:

```
GVRP Registration Normal
GVRP Registration Disabled
```

If one port is configured to the normal registration mode, it permits the dynamic creation (If dynamic VLAN creation Enabled), registration and logout of VLANs on the port.

If the port is configured with disabled registration mode, it forbids any actions of registration or logout of VLANs.

Configure GVRP Registration Mode:

Command	Function
D-Link(config-if)#**[no] gvrp registration mode {normal|disabled}**	Configure GVRP registration mode.

These two registration modes do not affect static VLANs on the port. Static VLANs created by users are Fixed Registrar.

This example shows how to enable Registration Mode on port 1:

```
D-Link # configure
Enter configuration commands, one per line. End with CNTL/Z.
D-Link(config)# interface gigabitethernet 1/1
D-Link(config-if)# gvrp registration mode enable normal
D-Link(config-if)# end
```

4.2.7 Configuring the advertising mode of the port

There are two advertising modes to control transmission of GVRP advertisement:

GVRP Normal Applicant

It allows advertising local VLANs including dynamic and static VLANs.

GVRP Non-Applicant

It do not allow advertising local VLANs.

Configuring the advertising mode of the port

Command	Function
D-Link(config-if)#**[no] gvrp applicant state {normal|non-applicant}**	Configuring the advertising mode of the port

This example shows how to configure the applicant state on port 1:

```
D-Link # configure
Enter configuration commands, one per line. End with CNTL/Z.
D-Link(config)# interface gigabitethernet 1/1
D-Link(config-if)# gvrp applicant state normal
D-Link(config-if)# end
```

4.2.8 Configuring GVRP Timers

There are three timers used in GVRP:

Join timer

Join timer_value controls the max-latency before sending advertisement, the actual interval is between 0 and max-latency. The default value is 200 ms.

Leave timer

Controls the period to remove the port from VLAN after receiving the leave messages, and the port will remain in VLAN members if it receives *join message* again in this period, and the timer will be disabled The default value is 600 ms.

LeaveAll timer

Controls the minimum interval to send LeaveAll Message on the port, if it receives LeaveAll Message before the timer timeout, the timer will be reset; If the timer timeouts, the port will send LeaveAll Message to other ports, including itself, and the leave timer starts. The default value is 10,000 ms. The actual interval for sending is between leaveall and leaveall + join.

When you configure timers, ensure that the value of leave >=join *3, and leaveall > leave. If this requirement is not meet, operations on timers will not succeed. For example, if leave time = 600 ms, and join timer = 320 ms, then switch will show you error cautions. If join time = 350 ms, leave time must not smaller than 1050 ms

Valid granularity for timer configuration is 10 ms.

Make sure that the values of GVRP timers in all GVRP devices are the same, otherwise GVRP might work abnormally.

Ajust the value of GVRP timer:

Command	Function
D-Link(config)#**[no] gvrp timer** {**join**|**leave**|**leaveall**} *timer_value*	Enter timer value of the port.

This example shows how to configure GVRP join timer:

```
D-Link #configure
Enter configuration commands, one per line. End with CNTL/Z.
D-Link(config)# gvrp timer join 1000
D-Link(config)# end
```

4.3 Showing the configuration and status of GVRP

4.3.1 Showing GVRP statistics value

GVRP statistics value is based on port. See the **show gvrp statistics** CLI command for more detail usages about the command to display statistics and their purpose.

Show the statistics value.

Command	Function
D-Link#**show gvrp statistics** { *interface-id* | **all**}	Show the statistics value.

This example shows the GVRP statistics value:

D-Link# show gvrp statistics gigabitethernet 1/1

```
Interface            GigabitEthernet 3/1
RecValidGvrpPdu      0
RecInvalidGvrpPdu    0
RecJoinEmpty         0
RecJoinIn            0
RecEmpty             0
RecLeaveEmpty        0
RecLeaveIn           0
RecLeaveAll          0
SentGvrpPdu          0
SentJoinEmpty        0
SentJoinIn           0
SentEmpty            0
SentLeaveEmpty       0
SentLeaveIn          0
SentLeaveAll         0
JoinIndicated        0
LeaveIndicated       0
JoinPropagated       0
LeavePropagated      0
```

Clear GVRP statistics statistics value, enable it re-count:

Command	Function
D-Link#**clear gvrp statistics** { *interface-id* | **all**}	Clear GVRP statistics value.

This example shows how to clear GVRP statistics value on the port:

```
D-Link# clear gvrp statistics gigabitethernet 1/1
```

4.3.2 Display GVRP running status

You can use the **show GVRP status** command to display GVRP running status. This command shows the current dynamic-created VLANs and the dynamic logical ports on static VLANs.

Command	Function
D-Link#show gvrp status	Display GVRP running status

Example:

```
D-Link# show gvrp status
VLAN 1
Dynamic Ports:
DVLAN 5
Dynamic Ports:
Port:GigabitEthernet 3/1
```

4.3.3 Display the current GVRP status

You can use the **show gvrp configuration** command to display the current GVRP running status. This command shows the current dynamic-created VLANs and the dynamic logical ports on static VLANs.

Command	Function
D-Link**#show gvrp configuration**	Display current GVRP configurations.

Example:

```
D-Link# show gvrp configuration
Global GVRP Configuration:
GVRP Feature:enabled
GVRP dynamic VLAN creation : enabled
Join Timers(ms) : 200
Join Timers(ms) : 600
Join Timers(ms) : 10000
Port based GVRP Configuration:
Port:GigabitEthernet 3/1 app mode:normal reg mode:normal
Port:GigabitEthernet 3/2 app mode:normal reg mode:normal
Port:GigabitEthernet 3/3 app mode:normal reg mode:normal
Port:GigabitEthernet 3/4 app mode:normal reg mode:normal
Port:GigabitEthernet 3/5 app mode:normal reg mode:normal
Port:GigabitEthernet 3/6 app mode:normal reg mode:normal
Port:GigabitEthernet 3/7 app mode:normal reg mode:normal
Port:GigabitEthernet 3/8 app mode:normal reg mode:normal
Port:GigabitEthernet 3/9 app mode:normal reg mode:normal
Port:GigabitEthernet 3/10 app mode:normal reg mode:normal
Port:GigabitEthernet 3/11 app mode:normal reg mode:normal
Port:GigabitEthernet 3/12 app mode:normal reg mode:normal
```

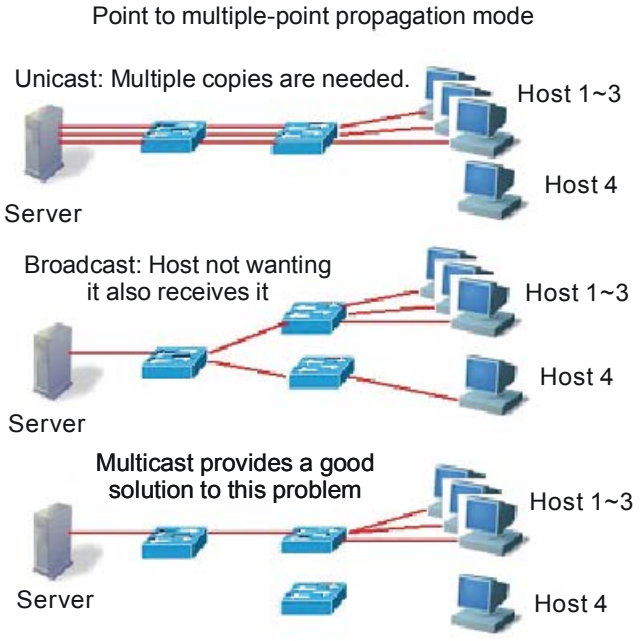
5 Configuring IGMP Snooping

5.1 Overview

5.1.1 Understanding IGMP

Let us first describe IP multicast and its function.

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 adapt to the transmission characteristics of this type of service, as the server has to provide each receiver with an IP message copy with the same content, at the same time, the network also repeatedly sends the messages with the same content, thus occupying much more resources, as shown in the following figure. The IP broadcast cannot satisfy this requirement either. The IP broadcast allows one host to send an IP message to all the hosts of the same network, but not all hosts need these messages, so the network resource is wasted. In this situation, the multicast emerges, providing a solution to the method for one host to send messages to designated multiple receivers.



Hosts 1~3 want to receive video flow, and Host 4 does not have this requirement.

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

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

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

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

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

IGMP(Internet Group management Protocol)

Through IGMP, the IP host applies for joining in (or leaving) the multicast group to the neighboring router. 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 message 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 continue to receive the message of this group, it shall respond the corresponding IGMP Report message. If a certain interface cannot receive the IGMP Report message of any host, it is believed that there is 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 message 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 message. If the router cannot receive the IGMP Report message 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. Upon receipt of the message, the router sends the IGMP Query message of this group. If other hosts need this multicast, they should return the IGMP Report response message. If the router cannot receive the response of any host, it will remove this 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:

It is used for querying the information of all multicast members under the interface;

It is used for querying the information of the designated group members under the interface;

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 downward compatible with IGMP Version1 and IGMP Version2.

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

5.1.2 Understanding IGMP Snooping

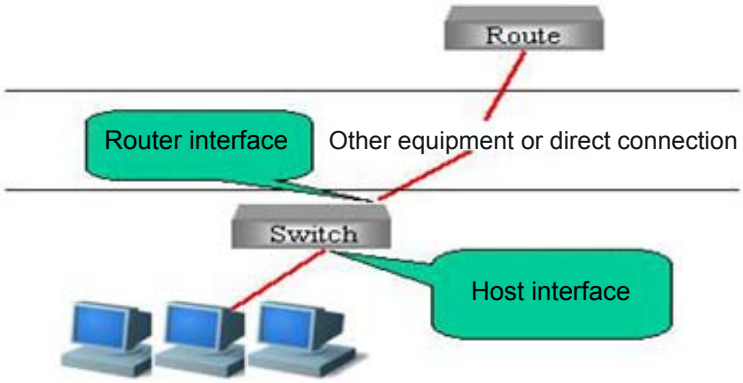
Under Layer 2 equipment, the multicast frame is forwarded as broadcast, which may easily lead to multicast flow storm, wasting the network bandwidth. The typical multicast frame on the network is video flow. In a VLAN, if a certain user registers the video flow of a certain group, then all members in 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.

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 message from the host within a certain period of time, the switch deletes this port from the table.

5.1.3 Understanding Router Interface

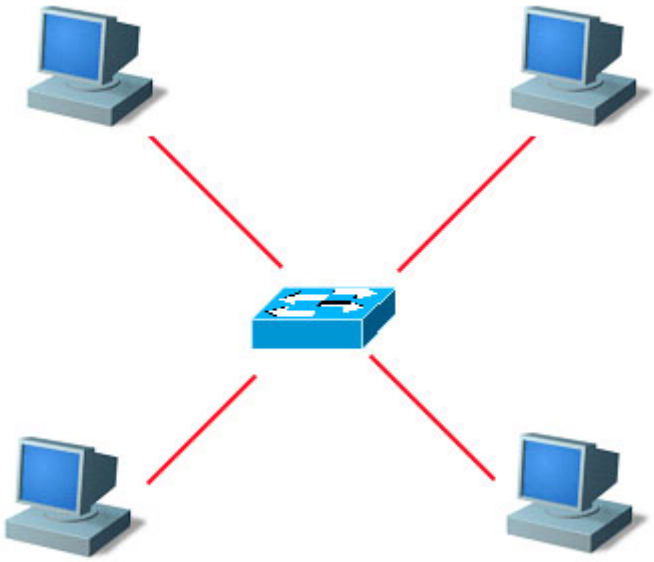
The router interface is the port connecting the multicast router, as shown below.



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. For information on how to configure and view the router interface, please see the chapter “Configuring IGMP Snooping”.

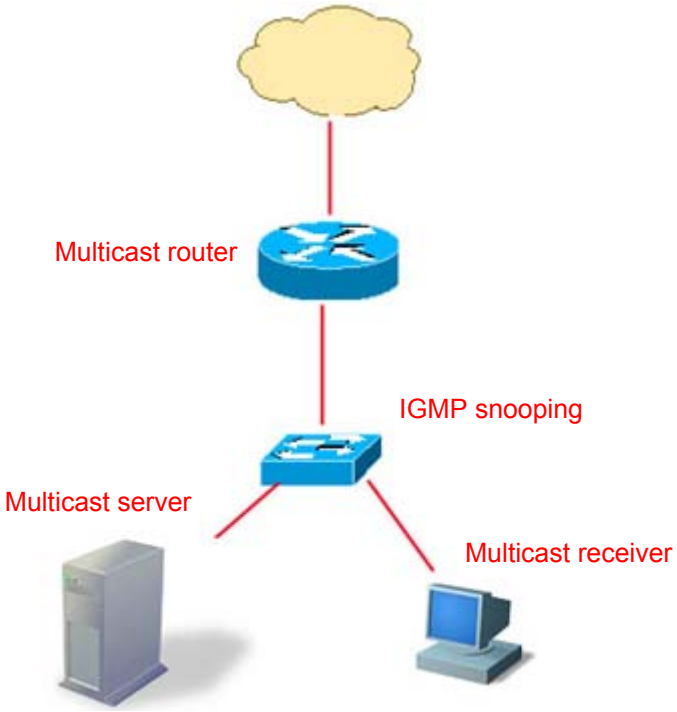
Note

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.



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.



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.

Note

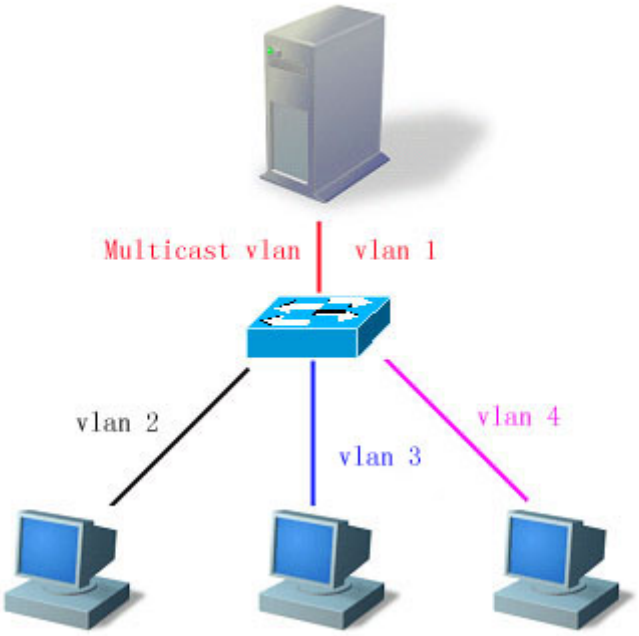
In the above network topology, if there is no "multicast traffic receiver", a multicast entry is still automatically created in the multicast router. However, such multicast entry generated by the "multicast data traffic" may be unstable. The administrator is recommended to directly configure one static multicast entry for the route connection interface (Please see Configuring Static Member of IGMP snooping) to ensure stable forwarding of the multicast traffic.

5.1.4 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.



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 D-Link Corporation strengthens the network application flexibility, enabling it to adapt to different network environment.

5.1.5 Understanding Source Port Check

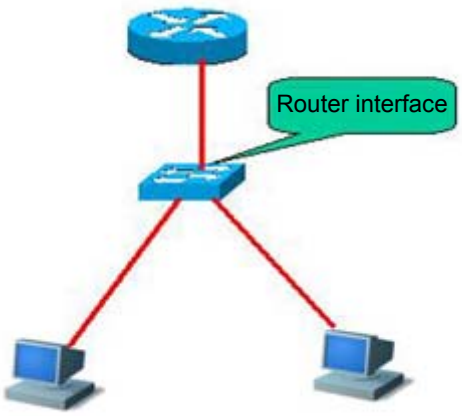
Some switches provided by D-Link support IGMP source port check function and improve the security of the network.

IGMP source port check refers to the entry port of strictly restricting the IGMP multicast flow. When IGMP source port check isdisabled, 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.

5.1.6 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.

Common network topology



Requirements for equipments:

1. Switch supporting IGMP Snooping

Required setup:

Enable IGMP Snooping function.

Set upper link as router interface.

Characteristics:

Simple configuration;

Effectively reducing broadcast storm, improving network bandwidth utilization rate.

5.2 Configuring IGMP Snooping

We will describe how to configure IGMP snooping in the following chapters

- IGMP Snooping Default
- Configuring IGMP Profiles
- Configuring Router Interface
- Configuring Range of Multicast Frame Forwarding by Router Interface
- Configuring IVGL Mode
- Configuring SVGL Mode
- Configuring Coexistence Mode of IVGL and SVGL
- Configuring ISABLE Mode
- Configuring Maximum Response Time of Query Message
- Configuring Source Port Check
- Configuring Source IP Check
- Configuring Static Members of IGMP Snooping
- Configuration IGMP Filtering

5.2.1 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

Precautions for Configuration:

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.

5.2.2 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 configuring mode, please set a profile by performing the following steps:

Command	Function
D-Link(config)# **ip igmp profile** *profile-number*	Enter IGMP Profile mode, and allocate a number for identification. The range is 1–65535.

Command	Function
D-Link (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**.**
D-Link(config-profile)**#range** *ip multicast-address*	Add one or more multicast address ranges.
D-Link**# end**	Return to the privileged EXEC mode.

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 indicates profile configuration process:

```
Switch(config)# ip igmp profile 1
Switch(config-igmp-profile)# permit
Switch(config-igmp-profile)# range 224.1.1.1 225.1.1.1
Switch(config-igmp-profile)# range 226.1.1.1
Switch(config-if)#end
Switch# 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**.**

5.2.3 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 configuring mode, you can set an router interface by performing the following steps:

Command	Function
ip igmp snooping vlan ***vlan-id*** mrouter {interface ***interface-id*****|** learn pim-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 commandcorresponding no command to close to disable the dynamic learning, and clear all router interfaces learned through dynamic learning. By default, dynamic learning is disabled.
D-Link(config)**#end**	Return to the privileged mode.

This example sets the Ethernet interface1/1 as the router interface, and configures the automatic learning router interface:

```
Switch#configure terminal
Switch(config)#ip igmp snooping vlan 1 mrouter interface fast 1/1
Switch(config)#ip igmp snooping vlan 1 mrouter learn pim-dvmrp
Switch(config)#end
Switch# show ip igmp snooping mrouter
```

```
Vlan    Interface     State    IGMP profile
----    ---------     ------   -------------
Fa0/1               static         1
Fa0/12              dynamic         0
Switch# show ip igmp snooping mrouter learn
Vlan    learn method
----    ------------------
pim-dvmrp
```

5.2.4 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 configuring mode, please configure the router interface to forward the range of multicast frame by performing the following steps:

Command	Function
D-Link(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.
D-Link(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:

```
Switch#configure terminal
Switch(config)#ip igmp snooping vlan 1 mrouter interface fast 1/1 profile 1
Switch(config)#end
Switch#show ip igmp snooping mrouter
Vlan    Interface    State    IGMP profile
----   ---------    ------   -------------
1      Fa0/1        static         1
Fa0/12              dynamic
```

5.2.5 Configuring IVGL Mode

In the configuring mode, please set IGMP Snooping to IVGL mode by performing the following steps:

Command	Function
D-Link(config)# ip igmp snooping ivgl	Enable IGMP Snooping and set it to the IVGL mode.
D-Link(config)# **end**	Return to the privileged mode.

This examples enables IGMP Snooping and sets it to the IVGL mode:

```
Switch#configure Terminal
Switch(config)#IP igmp snooping ivgl
Switch(config)#end
```

5.2.6 Configuring ISABLE Mode

In the configuring mode, please set IGMP Snooping to DISABLE mode by performing the following steps:

Command	Function
D-Link(config)# no ip igmp snooping	IGMP Snooping is disabled.
D-Link(config)# **end**	Return to the privileged mode.

5.2.7 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
D-Link(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.
D-Link(config)# **end**	Return to the privileged mode.

Use **no ip igmp snooping query-max-response-time** to restore its default value.

5.2.8 Configuring Source Port Check

In the configuring mode, please set the function of source port check by performing the following steps:

Command	Function
D-Link(config)# **ip igmp snooping source-check port**	Open source port check.
D-Link(config)**#end**	Return to the privileged mode.

You can disable source port check by using the **no ip igmp snooping source-check port** command.

5.2.9 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 configuring mode, please set the static members of IGMP Snooping by performing the following steps:

Command	Function
D-Link(config)# **ip igmp snooping ivgl**	Enable IGMP Snooping and set it to the IVGL mode.

Command	Function
D-Link(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* multicast flow vid • *ip-addr* multicast address • *interface-id* port number
D-Link(config)# **end**	Return to the privileged mode.

Use **no ip igmp snooping vlan** *vlan-id* **static** *ip-addr* **interface** *interface-id* to delete the static configuration of multicast member.

This example configures static member of IGMP snooping:

```
Switch#configure Terminal
Switch(config)#ip igmp snooping vlan 1 static 224.1.1.1 interface f 0/1
Switch(config)#end
Switch(config)#show ip igmp snooping gda
Abbr: M - mrouter
      D - dynamic
      S - static

VLAN  Address             Member ports
---- ----------------- ---------------------
1    224.1.1.1            Fa0/1(S)
```

5.2.10 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 a certain IGMP Profile on a port. If this port receives the IGMP Report message, our switch will search whether the multicast address that this port wants to add is within the range permitted by the IGMP Profile. Subsequent handling is conducted only after it is permitted.

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 message.

In the privileged mode, please follow the steps below to configure IGMP Filtering:

Command	Function
D-Link(config)# **interface** *interface-id*	Enter to the configuration interface.
D-Link(config-if)**#ip igmp snooping filter** *profile-number*	(Optional) apply the profile to this port. The profile number range is 1- 65535.
D-Link(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.
D-Link(config-if)**#end**	Return to the privileged mode.

5.3 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

5.3.1 Viewing Current Mode

In the privileged mode, use the following commands to view the current operation mode of IGMP Snooping and global configuration:

Command	Function
D-Link# show ip igmp snooping	View the current operation mode of IGMP Snooping and global configuration.

Following examples show how to use the command of show ip igmp snoopingto view the configuration information of IGMP Snooping:

```
Switch#show ip igmp snooping
Igmp-snooping mode      : svgl
SVGL vlan-id            : 1
SVGL profile number     : 0
Source check port       : Disabled
Query max response time : 10(Seconds)
```

5.3.2 View Router Interface Information.

In the privileged mode, use the following commands to view the router interface information of IGMP Snooping:

Command	Function
D-Link# show ip igmp snooping mrouter	Show the route connection port information of IGMP Snooping

Following examples use the command of show ip igmp snooping to view the router interface information of IGMP Snooping:

```
Switch#show ip igmp snooping mrouter
Vlan    Interface       State     IGMP profile number
----    --------       -------    -------------------
1      Fa0/2           static              1
2      Fa0/12          dynamic             0
3      Fa0/2           static              0
```

5.3.3 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
D-Link# 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:

```
show ip igmp snooping gda-table
–
Abbr: M - mrouter
```

```
      D - dynamic
      S - static
VLAN  Address           Member ports
---- ---------------- ---------------------------------------------------
2    229.1.1.2          Fa0/2(M), Fa0/11(D), Fa0/13(D)
```

5.3.4 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
D-Link# show ip igmp snooping	View the current operation mode of IGMP Snooping and global configuration.

5.3.5 Viewing IGMP Profile

In the privileged mode, view the IGMP Profile information by using the following command:

Command	Function
D-Link# **show ip igmp profile** *profile-number*	View the IGMP Profile information.

5.3.6 Viewing IGMP Filtering

In the privileged mode, view the IGMP Filtering configuring information by using the following command:

Command	Function
D-Link# show ip igmp snooping interface *interface-id*	View IGMP Filtering configuration information.

The following serves to view IGMP Filtering information.

```
Switch#show ip igmp snooping interface 0/1
Interface       Filter Profile number     max-groups
----------     ----------------------    -----------
Fa0/1
```

6 Configuring Interfaces

This chapter deals with the classification and configuration of interfaces used in D-Link switches. It is divided into three parts:

- Overview
- Configuring Interfaces
- Showing Interface Configuration and StatusL2 InterfacesL3 Interfaces

6.1 Overview

This chapter provides the classification of interfaces used in D-Link switches as well as a precise definition of each type. D-Link switch interfaces can be divided into two types:

- L2 Interfaces
- L3 Interfaces

6.1.1 L2 Interfaces

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

- Switch Ports
- L2 Aggregate Ports

6.1.1.1 Switch Ports

They consist of single physical ports on the switch and only have the L2 switching function. They fall into Access Port and Trunk Port. Access ports and trunk ports have to be configured manually. Switch ports are configured by executing switch port configuration commands. For details about the configuration of access ports and trunk ports, see the chapter “Configuring VLAN”.

An access port belongs to only one VLAN, transporting the frames belonging to the same VLAN only. It receives only three types of frames, untagged, tagged with vid=0, and those whose vid is the VLAN to which it belongs. An access port sends but untagged frames.

Trunk ports transfer frames belonging to multiple VLANs. By default, they transfer frames of all VLANs. You may limit the frames transported by a trunk port by setting the VLAN list. Each trunk port belongs to one native VLAN, which means UNTAG messages sent to or from the port are viewed as belonging to the VLAN. The trunk port receives tagged and untagged frames. When frames without an IEEE802.1Q tag arrive at a trunk port, they are transported on the native vlan of the port. The native vlan of each trunk port is configurable. If a frame has a VID of the native vlan of a trunk port, the port stripes the tag before sending the frame off. The frame of a non-native vlan sent by the Trunk Port has a tag.

6.1.1.2 L2 Aggregate Ports

They are logical switch ports consisting of multiple physical switch ports. For L2 switching, an L2 Aggregate port is like a high bandwidth switch port that balances traffic among its member ports. When the link of a member port fails, the L2 Aggregate port automatically shifts the traffic on it to another port. Likewise, an L2 Aggregate port can serve as an access port or trunk port if its member ports are of the same type. You may create an L2 Aggregate port by using the **Interface Aggregateport** command.

6.1.2 L3 Interfaces

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

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

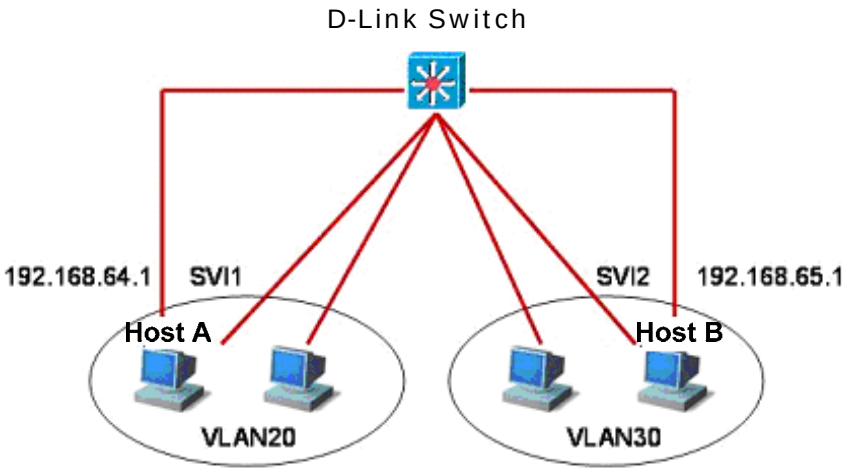
6.1.2.1 SVI (Switch virtual interface)

The SVI is an IP interface associated with some VLAN. Each SVI can be associated to but one VLAN in the following two ways.

- The SVI is the management interface of the switch, through which the administrator manages the switch.
- The SVI is a gateway interface used for routing among VLANs in L3 switches.

You may establish routes among VLANS by first creating an SVI by using the **interface vlan** command and then assigning an IP address to it. For more information about SVI, please refer to *Configuring IP Single Address Route*.

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



6.1.2.2 Routed Ports

On L3 switches, a Routed port is a single physical port used as the gateway interface for L3 switching. 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.

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

6.1.2.3 L3 Aggregate Ports

An L3 Aggregate port serves as the gateway interface for L3 switching. 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.

6.2 Configuring Interfaces

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

6.2.1 Numbering Rules for Interfaces

The number of a switch port consists of a slot number and 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 panels: For panels facing the switch, 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 switches 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 supportable number of Aggregate Ports by the switch.

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

Note

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

6.2.2 Using Interface Configuration Commands

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

Command	Function
D-Link(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 is to show the accessing the gigabitethernet2/1 interface:

```
D-Link(config)# interface gigabitethernet 2/1
```

```
D-Link(config-if)#
```

You may set interface attributes in interface configuration mode.

6.2.3 Using the interface range Command

6.2.3.1 Setting Interface Range

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

Command	Function
D-Link(config)#**interface range** {*port-range*|**macro** *macro_name*}	Key in 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, please note the format of the parameters:

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*};

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

fastethernet *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:

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

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

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

6.2.3.2 Configuring and Using Macro Definition for Interface Range

You may define some macros instead of inputting port ranges. However, it is worth pointing out that you have to define macros using the **define interface-range** command before you can use the **macro** in the **interface range** command.

Command	Function
D-Link(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.
D-Link(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:

```
D-Link#configure terminal
D-Link (config)#define interface-range resource fastethernet1/1-4
D-Link(config)#end
```

This example defines a macro for multiple ranges:

```
D-Link#configure terminal
D-Link (config)#define interface-range ports1to2N5to7 fastethernet1/1-2, 1/5-7
D-Link(config)#end
```

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

```
D-Link#configure terminal
D-Link(config)#interface range macro ports1to2N5to7
D-Link(config-if-range)#
```

This example deletes macro ports1to2N5to7:

```
D-Link#configure terminal
D-Link(config)#no define interface-range ports1to2N5to7
D-Link#end
```

6.2.4 Selecting Interface Medium Type

Some interfaces have multiple medium types and allow users to choose. You can choose one of the mediums for use. Once you have selected a medium, the attributes like connection status, speed, duplexing, 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 physical 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
D-Link(config-if)**#medium-type** { **fiber** | **copper** }	Set medium type of the port.

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

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

6.2.5 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
D-Link(config-if)**#description** *string*	Describe the interface in no more than 32 characters

This example sets the description of gigabitethernet 1/1:

```
D-Link#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
D-Link(config)#interface gigabitethernet 1/1
D-Link(config-if)#description PortForUser A
D-Link(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
D-Link(config-if)**#shutdown**	Shut down an interface.

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

```
D-Link#configure terminal
D-Link(config)#interface gigabitethernet 1/2
```

```
D-Link(config-if)#shutdown
D-Link(config-if)#end
```

6.2.6 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
D-Link(config-if)#**speed** {10 | 100 | 1000 | auto }	Select a speed or set it to auto. **Note** 1000 applies only to gigabit interfaces.
D-Link(config-if)#**duplex** {*auto* | *full* | *half*}	Set duplex mode
D-Link(config-if)#**flowcontrol** {*auto* | *on* | *off*}	Set flow control mode. **Note** The interface shutdown the procedure of auto-negotiation when **speed**, **duplex**, and **flow control** are set as **auto-off**

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**.

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

6.2.7 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 transceive 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 prot 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 a physical port. The SVI interface currently does not support the mtu setting.

Command	Function
D-Link(config-if)#**Mtu** *num*	Set the MTU.

This example sets mtu for gigabitethernet 1/1:

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

6.2.8 Configuring L2 Interfaces

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

Default settings of L2 interfaces

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	Auto-negotiation
Flow control	Auto-negotiation
Aggregate port	None
Storm control	Disabled
Port protection	Disabled
Port security	Disabled

6.2.8.1 Configuring Switch Ports

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
D-Link(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 to access port.

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

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

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

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

Configuring the native VLAN of the trunk port:

Command	Function
D-Link(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.

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

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

Command	Function
D-Link(config-if)#**switchport port-security**	Set the port-security.

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

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

For setting of speed, duplexing, and flow control, 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.

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

6.2.8.2 Configuring L2 Aggregate Ports

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

You may create an L2 Aggregate Port by using **aggregateport** in interface configuration mode. For details, see chapter 15 of *Setting Aggregate Port.*

6.2.8.3 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
D-Link**#clear counters** [*interface-id*]	Clear interface statistics.
D-Link**#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.

```
D-Link#clear counters gigabitethernet 1/1
D-Link#
```

6.2.9 Configuring L3 Interfaces

Configuring L3 Interfaces

Command	Function
D-Link(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.
D-Link(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.

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

6.2.9.1 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.

SVI configuration:

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

Then, you can configurate the properties related to SVI. For detailded information, please refer to *Configurating IP Single Address Route*.

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

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

6.2.9.2 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
D-Link(config-if)**#no switchport**	Shut down the interface and then change it to L3 mode.
D-Link(config-if)**#ip address** *ip_address subnet_mask*	Configure the IP address and subnet mask.

Note

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.

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

6.2.9.3 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
D-Link(config-if)**#no switchport**	Shut down the interface and change it to L3 mode.
D-Link(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.

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

6.3 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
D-Link**#show interfaces** [*interface-id*]	Show all the statuses of a specified interface and its configuration information.
D-Link**#show interfaces** *interface-id* **status**	Show the status of an interface.
D-Link**#show interfaces** [*interface-id*] **switchport**	Show the administrative and operational status information of an switch interface (non-routing interface).
D-Link**#show interfaces** [*interface-id*] **description**	Show the description and status of a specified interface.
D-Link**#show interface**s [*interface-id*] **counters**	Show the statistics of a specified port.

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

```
D-Link#show interfaces gigabitethernet 1/1
GigabitEthernet     : Gi 1/1
Description         : user A
AdminStatus         : up
OperStatus          : down
Hardware            : 1000BASE-TX
Mtu                 : 1500
PhysAddress         :
LastChange          : 0d: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 SVI 5.

```
D-Link#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 aggregateport 3.

```
D-Link#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 gigabitEthernet 1/1:

```
D-Link#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 description of gigabitethernet 2/1.
D-Link#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.
D-Link#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 0
packets received of length (in octets):
  64:46264, 65-127: 47427, 128-255: 3478,
  256-511: 658, 512-1023: 18016, 1024-1518: 125
```

7 Configuring IP Multicast Routing

7.1 Overview

This chapter describes how to configure multicast routing protocol. For a complete description of the IP multicast routing commands in this chapter, please refer to other chapters about "IP Multicast Routing Commands".

Traditional IP communication allows a host to send packets to a single host (*unicast transmission*) or to all hosts (*broadcast transmission*). IP multicast provides a third scheme, allowing a host to send packets to a subset of all hosts. These hosts are known as group members.

The destination address is a Class D IP addresses which can be in the range 224.0.0.0 to 239.255.255.255. Transmission of multicast packets is similar to UDP, which is a best effort service. It does not provide reliable transmission and error control as well as TCP.

The multicast environment consists of senders and receivers. The sender, regardless of whether it is a member of a group, can send the multicast message. However, only the members of a group can receive the message of this group.

Membership in a multicast group is dynamic; hosts can join and leave at any time. There is no restriction on the location or number of members in a multicast group. If necessary, a host can be a member of more than one multicast group at a time. Therefore, how active a multicast group is and what members it has can vary from time to time.

Routers executes a multicast routing protocol (such as PIM-DM, PIM-SM, etc.) to maintain routing tables to forward multicast datagrams, and use the IGMP to learn the status of the members within a group on their directly attached subnets. A host can join a certain IGMP group by sending IGMP Report message.

These characteristics of IP multicast above is suitable to “1 to N” based multimedia applications.

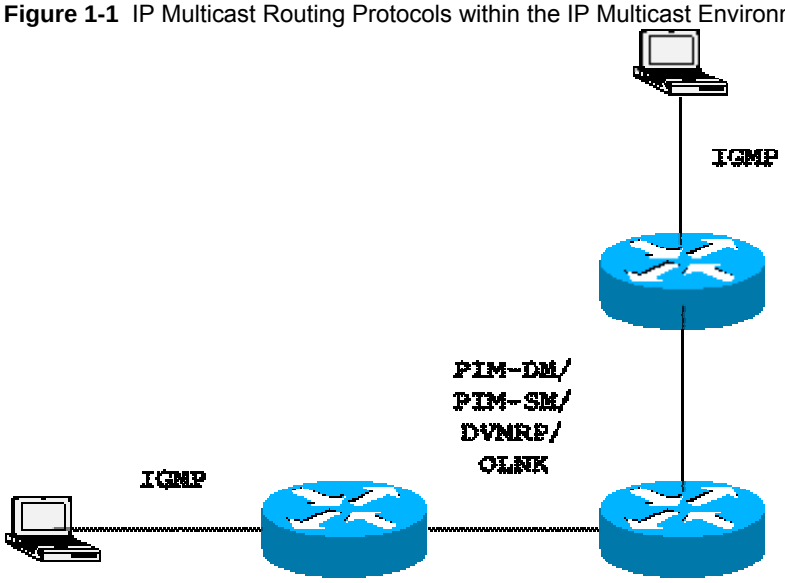
7.1.1 IP Multicast Routing Implementation

Multicast routing is composed of the following protocols in router software:

- IGMP is used between hosts on a LAN and the routers on that LAN to track the multicast groups of which hosts are members.
- PIM-DM is a dynamic multicast routing protocol, which is used between routers to implement multicast forwarding based on multicast routing table.

It shows where these protocols operate within the IP multicast environment in the following figure:

Figure 1-1 IP Multicast Routing Protocols within the IP Multicast Environment



7.1.2 IGMP Overview

To participate in IP multicast, the multicast host, router, and multi-layer switch must support IGMP. This protocol is used by the host to notify the router or multi-layer switch the multicast membership of the network they connect, to determine how to forward the multicast traffic.

By using the information obtained from the IGMP, the router or multi-layer switch can maintain one multicast member list, which is based on each interface. The multicast member list is activated only when one interface has at least one host in a group. It supports IGMP v1-v3 in our switch.

7.1.2.1 IGMPV1

There are only two types of messages defined in IGMP Version 1: Membership query and Membership report.

A host sends a report packet to join a group, and the router sends the query packet at periodical intervals to ensure that a group has at least one host. When a group contains no host, the router will delete that group.

7.1.2.2 IGMPV2

In Version 2, there are only four types of packets:

- Membership query
- Version 1 membership report
- Version 2 membership report
- Leave group.

The process is basically the same as that of version 1, except that the leave mechanism of the host has been improved. The host can send a leave packet to notify the router, which then sends a query to verify the existence of the host. This makes more efficient joining and leaving.

In addition, version 2 handles multiple routes of multiple access networks. At the beginning, all the routers are queriers. When a router receives the query from a router with lower IP address for membership, it changes from the receiver to the non-querier. Therefore,

ultimately only one router is at the query status. This router is the one with the lowest IP address in all multicast routers.

When the querier router fails, the IGMPv2 also handles the fault. The non-query router maintains the interval timers of other queriers. Every time when a router receives a membership query packet, it resets the timer. If the timer expires, the router starts to send query packets, and the querier router election starts again.

The querier router must send membership query requests at periodical intervals to ensure that other routers on the network know that the querier router still works. For this purpose, the querier router maintains one query interval timer. When the membership query packet is sent, this timer is reset. When the interval timer is zero or not necessary, the querier router sends another membership query.

At first time a router appears, it sends a series of common query packets to see what multicast groups should be forwarded at the particular interface. The number of common query packets sent by a router is based on the start query count configured of the router. Initially, the interval of common query packets is defined by the start query interval.

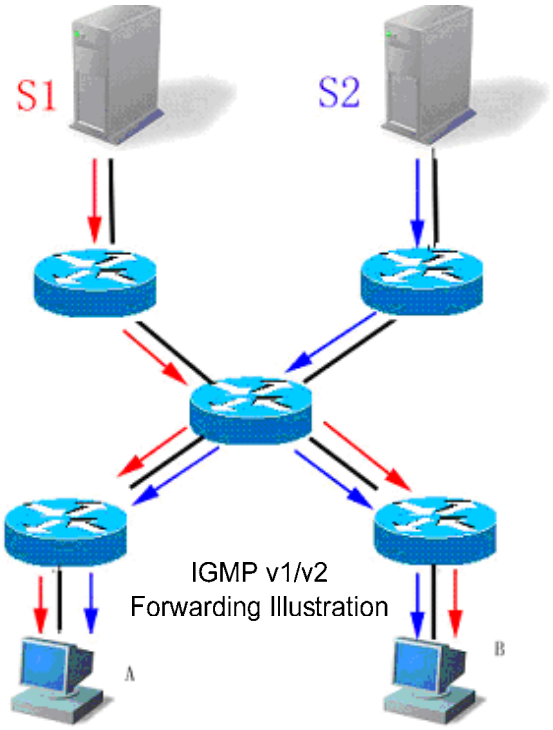
When a querier router receives a leave packet, it must send a particular group membership query to see if the host is the last that leaves the group. Before the router stops forwarding packets to the group, it sends a series of such packets, the number of which is equal to the last member query number. The router sends multiple particular membership queries to ensure that there is no member in the group. It sends such a query at the interval of the last membership query interval second. When no response is received, the router stops forwarding multicast packets to the group at the particular interface.

7.1.2.3 IGMPV3

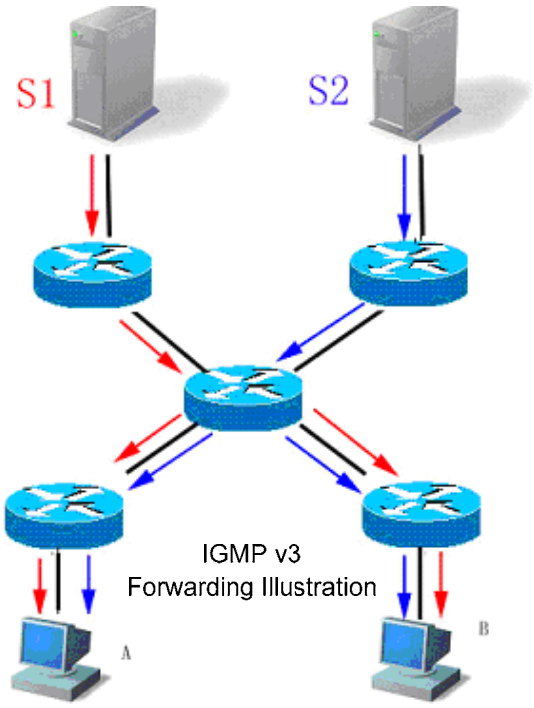
In the applications of the IGMPV1 and V2, there are the following defects:

- There is effective means for controlling multicast sources.
- It is difficult to establish multicast paths since the locations of multicast sources are not known.
- It is difficult to find a unique multicast address, since multicast groups may share one multicast address.

On the basis of the IGMPV1/V2, the IGMPV3 provides an additional source filtering multicast function. In the IGMP V1/V2, the host determines to join a group and receive the multicast traffic to the group address from any source only based on the group address. On the other hand, the host running the IGMP V3 notifies this host the desired multicast group to join, and also the addresses of the multicast sources to receive. The host can indicate that it wants to receive multicast traffic from which sources through a list or an exclusion list. At the same time, another benefit of the IGMP v3 is that it saves bandwidth to avoid unnecessary, invalid multicast data traffics from occupying network bandwidth. It is particularly useful in the case where multiple multicast sources share one multicast address. The IGMPv1 and IGMPv2 can also implement “source address filtering” in some sense, which, however, is performed on the reception end of the multicast traffic. As shown in the following diagram, there are two multicast sources (S1 and S2), which send the data traffic of the same multicast address (G). The multicast traffics from S1 and S2 are sent to all the hosts that receive G. On the other hand, if host A wants to receive the traffic from S1 only, you can only use the appropriate client software to filter on the terminal, to avoid the interference from the traffic from S2.



If the equipment in the network supports IGMP v3, host A wants to receive the traffic from S1 only, it can send the IGMPv3 packet of join G include S1. If host B wants to receive the traffic from S2 only, it can send the IGMPv3 packet of join G include S2. Therefore, the traffics are forwarded as shown in the following diagram. This saves some bandwidths.



Compared with Version 2, Version 3 specifies the following two types of packets:

- 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.

Different from the Membership Report in IGMP Version2, that in IGMP Version3 has the constant destination address of 224.0.0.22. In addition, the Membership Report packets in IGMP Version3 can include the information of multiple groups.

IGMP Version3 can also identify the Membership Report packets in Version 1 and Version 2 and the Leave Group packets in Version 2.

The process of IGMP Version3 is similar to that of IGMP Version2. IGMP Version3 is backward compatible with IGMP Version1 and IGMP Version2.

7.1.3 PIM-DM Overview

PIM-DM (Protocol Independent Multicast Dense Mode) is a multicast routing protocol with dense mode. All network nodes are considered to receive the data when multicast source begins to forward multicast data by default. Therefore, PIM-DM forwards multicast packets by "flood and prune" principle. When multicast source begins transmitting data, switches which are traversed forward multicast packets towards all PIM enabled interfaces except the source RPF interface. Thus all network nodes will receive these multicast packets in PIM-DM area. To transmit multicast, switches which are traversed create the corresponding multicast routing entry (S,G). (S,G) contains multicast source address, multicast group address, ingoing interface, outgoing interface list, timer and identifier, etc.

If there are no group members in a certain area, PIM-DM will send a pruning message to prune the forwarding interfaces which are connected to this area and create pruning state. Pruning state is corresponding to timeout timer. When timer expires, Pruning is transmitted into forwarding, which enables multicast data to flow down along these branches. Besides, pruning state contains multicast source and multicast group information of multicast. When multicast group members appear in pruning area, to reduce reaction period, PIM-DM will be active to send a prune message to upstream without waiting for timeout of upstream pruning state so as to enable pruning to forwarding state.

As long as Source S can still send message to Group G, the first hop switch will periodically send (S,G) state refresh message to initial broadcast tree to finish the refreshing. With PIM-DM state refresh mechanism, you can refresh the state of downstream so that pruning of broadcast tree branches will not timeout.

Except for DR related selection in multi-path access network, PIM-DM also introduces the following mechanism: use assertion to select a single transmission in case that multicast packets are forwarded repeatedly to the same segment; use join/prune suppression to reduce redundant join/prune message; use pruning deny to deny these illegal pruning.

In PIM-DM domain, PIM-DM switches periodically send Hello message to find adjoining PIM switches and make judgment of leaf network and leaf switches. and is also responsible for DR selection in multi-path access network.

To be suitable for IGMP v1, PIM-DM is responsible for DR selection. Choose the highest Priority to be DR when all the PIM neighbors support DR Priority on the port. If the priority is identical, choose the switch with the largest port IP to be DR. If many switches do not announce their priorities in hello messages, switches with the highest port IP value is selected to be DR.

PIM-DM v2 of our switches supports neighbor filtering list, CIDR, VLSM and IGMP v1, v2, v3.

7.1.4 DVMRP Interoperability Overview

DVMRP (Distance Vector Multicast Routing Protocol) is a dense-mode multicast routing protocol, which is widely used within Internet applications.

DVMRP devices use probe message to advertise their own addresses, to learn neighbors' address and create adjoined connection. IP address of DVMRP devices are contained in probe message sent from neighbors, which means adjoined connection has been created successfully.

DVMRP neighbors exchange source network routing information, which includes mask and hops of source network by periodically sending report message. The routing information stored in the DVMRP routing table is separate from the unicast routing table and is used to build a source distribution tree and to perform multicast forward using RPF.

DVMRP is a dense-mode protocol and builds a multicast forwarding tree for each multicast source. Multicast data stream is initially forwarded along this tree except redundant paths. For specified multicast forwarding tree, devices will send prune message to upstream once it knows that no more multicast data stream is required. Once a device is notified that there is no downward neighbor and other multicast members, it is necessary for this device to decide whether it starts to receive the specified multicast data stream again. Since DVMRP is also a dense-mode based multicasting routing protocol, multicast data stream will re-diffused once pruning is overtime.

Furthermore, in order to add multicast receiver to the forwarding tree fast, DVMRP also provides graft and graft acknowledgement mechanism to re-add these pruned path back to forwarding tree quickly. Graft acknowledgement mechanism is used to prevent graft message from being lost for the reason that network is busy.

The complete DVMRP routing protocol function is not provided on our software at present. By implementing DVMRP neighbors discovery and DVMRP source routes exchange features, information is provided to other multicast routing protocols(such as PIM-DM) to launch RPF checking.

7.2 Basic Multicast Routing Configurating

Basic multicast configuration includes:

- Enabling multicast routing forwarding (required)
- Enabling IP multicast routing protocol (required)
- Configuring TTL threshold (optional)

7.2.1 Enabling Multicast Routing Forwarding

Enabling multicast routing to allow switch software forwarding multicast packets.

Enter the following commands in global configuration mode to enable multicast packets transmission:

Command	Purpose
ip multicast-routing	Enable IP multicast routing

7.2.2 Enabling IP Multicast Routing Protocol

So far it supports PIM-DM multicast routing protocol in our products.

Enable PIM-DM on the port to activate multicast with dense mode, use the following steps:

Command	Purpose
ip pim dense-mode	Enter the port that needs to run PIM-DM and enable PIM-DM multicast routing process in port configuration mode.

The following example demonstrates how to configure PIM-DM on the interface FastEthernet0/1.

```
ip multicast-routing
interface FastEthernet0/1
 ip address 172.16.8.1 255.255.255.0
 ip pim dense-mode
```

Tip

Running multicast routing protocol on an interface will activate inter-operation of IGMP and DVMRP at the same time.

7.2.3 Enabling IGMP

When multicast routing protocol enabled, IGMP is enabled as well.

Tip

Hosts and routers of IGMP are activated simultaneously.

7.2.4 Enabling DVMRP Interoperability

It mainly provides two DVMRP interpretabilities as follow:

- Non-DVMRP multicast routing area, such as inter-connection between PIM-DM multicast routing area and DVRMP multicast routing area. By enabling DVMRP interoperability, these multicast data stream of different routing area can be inter-forwarded.
- So far this kind of interoperability is not provided on our product.
- The DVMRP can establish its own routing topology, independent of the unicast routing protocol. If you want the multicast routing uses different paths from unicast routing, the use of the DVMRP unicast routing may be a good solution. So far it is provided on our product to create multicast topology based routing forwarding within multicast routing area.

To enable DVMRP interoperability on an interface, these requirements as follow should be satisfied:

- Enabling multicast routing protocol on the interface.
- Receiving DVMRP probe message, or enabling DVMRP unicast-routing.

To enable DVMRP unicast-routing on an interface, use the following command in interface configuration mode:

Command	Purpose
ip dvmrp unicast-routing	Enable DVMRP unicast-routing to send and receive report message.

7.3 Advanced Multicast Routing Configuration

Advanced multicast routing configuration includes:

- Configuring multicast routing characteristics (optional)
- Configuring IGMP tasks list(optional)
- Configuring PIM-DM tasks list(optional)
- Configuring DVMRP interoperability tasks list(optional)

7.3.1 Configuring Multicast Routing Characteristics

7.3.1.1 Configuring TTL Threshold

Use ip multicast ttl-threshold to configure TTL threshold of multicast packet which is allowed to transmit through the port, and use no ip multicast ttl-threshold to deploy the default value. The default value is 1.

Command	Purpose
ip multicast ttl-threshold *ttl-value*	Configure ttl threshold on the port.

7.3.1.2 Configuring IP Multicast Boundary

Use **ip multicast boundary** to configure multicast boundary of a port and use **no ip multicast boundary** to disable the configured boundary. The second configuration command will cover the first one.

Execute the command in interface configuration mode:

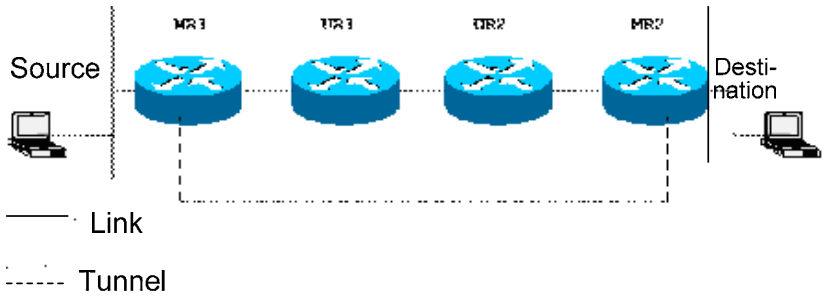
Command	Purpose
ip multicast boundary *access-list*	Configuring IP Multicast Boundary

7.3.1.3 Configuring IP Multicast Static Route

Multicast static route allows multicast forwarded path to differ from unicast path. RPF inspection will be processed when forwarding multicast packets. The actual receiving port is the port expected to receive packets (the port is the next hop of unicast reaching the sender). The inspection is reasonable if the topologies of unicast and multicast are the same. But in some cases, unicast path is expected to differ from that of multicast.

The most common cases adopt tunneling technology. GRE tunnel is configured between two switches to solve the problem that multicast protocol is not supported by the switches on one path. Each unicast switch (UR) only supports the unicast packets while each multicast switch (MR) supports multicast packets in the figure below. Source sends multicast packets to destination by MR1 and MR2. MR2 forwards multicast packets only when they are received from tunnel. If so, unicast packets will also pass the tunnel when forwarded from destination to source. As we know, it is slower to forward packets through tunnel than direct sending.

Figure 1-2 Configuring Static Multicast Route Diagrame



Switch can implement RPF inspection by configured information instead of unicast routing list through multicast static route configuration. Therefore, multicast packets use tunnel while unicast packets does not. Multicast static routes only exist locally. They will not declare outgoing or implement routing transmission.

In global configuration mode, use the following command to configure multicast static route.

Command	Purpose
ip mroute *source-address mask* {*interface-type interface-number*} [*distance*]	Configure multicast static route

It demonstrates how the system administrator configures management boundary of an interface in the following example.

```
interface FastEthernet 5/2
 ip multicast boundary acl
ip access-list standard acl
permit 192.168.20.97 255.255.255.0
```

7.3.1.4 Monitoring and Maintaining Multicast Routing

You can remove the content of a particular cache or a routing table if they are suspected to be invalid. Input commands below in administration mode:

Command	Purpose
clear ip mroute [* | group-address | source-address]	Clear entries from multicast routing table.

You can determine the resource utilization and solve network problems by displaying IP multicast route table, associated cache and database. Use the following command in administration mode:

Command	Purpose
show ip rpf {*source-address*}	Show RP information.

7.3.2 Configuring IGMP

7.3.2.1 Configuring IGMP Version

Use the following command in interface configuration mode to configure the IGMP version.

Command	Purpose
ip igmp version*{1 | 2 | 3}*	Configure the running IGMP version.

Use **no ip igmp version** to set the current IGMP version a default value Version2.

7.3.2.2 Adding Membership Information on Routers Statically

Sometimes the subnet connected to an interface has no host that can send IGMP member reports, but you still want the switch to forward the multicast packets of one group to the subnet. In this case, you can configure the interface to be a static connection multicast group, to forward the multicast frames to the interface.

In the privileged mode, make configuration by performing the following steps:

Command	Purpose
ip igmp static-group *group-address*	Configure the static multicast group of the switch. For *group-address*, indicates static multicast address of the switch.

You can use the **no ip igmp static-group** *group-address* command to cancel the configured static connection group.

7.3.2.3 Configuring a Router to Be a Member of a Group

The switch can be configured as the member of a multicast group. You can use this feature to determine the reachability of multicast on the network. In this case, the switch can send the IGMP group member report, while responding to the ICMP ECHO packets whose destination address is the group address.

In the privileged mode, make configuration by performing the following steps:

Command	Purpose
ip igmp join-group *group-address*	Configure a router as the member of a group. For *group-address*, indicates the multicast group address;

You can use the **no ip igmp join-group** *group-address* command to remove the switch from the group.

The following command shows how to add the **gigabitethernet**0/1 interface to the multicast group of 224.1.1.1:

```
interface gigabitethernet0/1
ip igmp join-group
```

7.3.2.4 Configuring Query Count of the Last Member

When a group leave packet is received, the inquire router sends the particular group member query to determine if there is still any member in the group. The default value is 2.

In the privileged mode, make configuration by performing the following steps:

Command	Purpose
ip igmp last-member-query-interval *lmqc*	Configure query interval of the last member in range of 1~7.

Use **no ip igmp last-member-query-count** to restore the default value.

7.3.2.5 Configuring Query Interval of the Last Member

When a group leave packet is received, the inquire router sends the particular group member query to determine if there is still any member in the group. Within the last member query interval, if not any response is received, the router believes that the router leaving is the last member in the group and deletes the group accordingly. By default, the interval is 1 second.

In the privileged mode, make configuration by performing the following steps:

Command	Purpose
ip igmp last-member-query-interval *lmqi*	Configure the query interval in the range of 1~255 in 0.1 seconds.

Use **no ip igmp last-member-query-interval** to restore the default value.

7.3.2.6 Configuring Common Query Interval

The querier router sends the group member query packets at the query interval to determine the current group membership. The group member query packets are sent to the all-hosts multicast address of 224.0.0.1, with the TTL being 1. By default, the interval is 125 second.

In the privileged mode, make configuration by performing the following steps:

Command	Purpose
ip igmp query-interval	Set the query interval, within the range of 1~18000. in second.

Use **no ip igmp query-interval** to restore the default value.

7.3.2.7 Configuring the Maximum Response Interval of the Query Message

It is the maximum response time required in the membership query packets sent from the querier router. When you lower this time, the router can quickly know the change of the group members, but the number of group member reports will increase accordingly. The network administrator can consider the tradeoff between these two factors to determine the final value. By default, the time is 10 seconds. In addition, please note that this time should be shorter than the query interval.

In the privileged mode, make configuration by performing the following steps:

Command	Purpose
ip igmp query-max-response-time *seconds*	Set the query response time, within the range of 10~250. In 0.1 second.

Use **no ip igmp query-max-response-time** to restore the default value.

7.3.2.8 Configuring the Keep-living Interval of Other Queriers

By configuring the keep-living interval of other queriers at interface layer, you can control how long it takes to act as non-queriers. Note that state of non-querier can be updated by the query message from other queriers.

In the privileged mode, make configuration by performing the following steps:

Command	Purpose
ip igmp querier-timeout *seconds*	Set the query response time, within the range of 60~300. In second.

Use **no ip igmp query-timeout** to restore to the default value.

7.3.2.9 Configuring the Maximum Count of Source Information Globally

Configure globally to limit the count of group sources.

In the privileged mode, make configuration by performing the following steps:

Command	Purpose
ip igmp limit *number*	Configure globally to limit the number of multicast groups to which group member is added dynamically. For number, indicates the number of (s, g, ifindex) or (g, ifindex), the range is from 1 to 65535 and default is 10240.

Use **no ip igmp limit** to cancel restriction of configured group sources on global layer.

7.3.2.10 Configuiring IGMP Limit

Configure the IGMP limit at the interface layer.

In the privileged mode, make configuration by performing the following steps:

Command	Purpose
ip igmp limit *number*	Configure to limit the number of multicast groups to which group member is added dynamically at interface layer. For number, indicates the number of (s,g,ifindex) or (g,ifindex), the range is from 1 to 1024 and default is 1024.

Use **no ip igmp limit** to cancel restriction of configured group sources on interface layer.

7.3.2.11 Configuring Filtering the Information of Group Members

By default, the interface on one interface can join any multicast group. When the administrator wants to control the range of the multicast groups that a host can join, he can use this feature. By configuring a standard IP access list, you can set the range of the allowed/prohibited range of multicast group addresses, and apply them to a particular interface.

In the privileged mode, make configuration by performing the following steps:

Command	Purpose
ip igmp access-group *access-list-num*	Control the ACL number of multicast groups; 1-199.

You can use the **no ip igmp access-group** command to restore the access control to its default, that is, not restricting any group.

The following command shows how to restrict the hosts at the **gigabitethernet**0/1 interface so that they can only join the group of 224.1.1.1:

```
access-list 1 permit 225.2.2.2 0.0.0.0
interface ethernet 0
ip igmp access-group 1
```

Tip

When ACL is located in the range of 1 to 99, igmpv1/v2/v3 will only match group (g).

When ACL is located in the range of 100 to 199, igmpv1/v2 will match (source ip is 0.0.0.0,group ip).

When ACL is located in the range of 100 to 199, igmpv3 will match (source ip, group ip), For source ip, indicates the source ip of igmpv3 report message. IF the corresponding source ip does not exist, such as exclude{}/is_ exclude{}/to_ exclude{}/include{}/is_include{}/to_include{}, the source ip is 0.0.0.0.

7.3.2.12 Clearing Dynamic IGMP Group Information

To clear up dynamic group member information acquired from response message which is stored in IGMP cache, use the following command in privileged mode:

Command	Purpose
clear ip igmp group [*group-address* | *interface-type interface-number*]	Clear up the dynamic group memebership from responding message, which is stored in IGMP cache.

7.3.2.13 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	Purpose
show ip igmp groups [*group-address* | *interface type numbe*r [*group-address*]][**details**]	Display the status of IGMP group member in directly-connected subnet.

```
Switch#sh ip igmp groups
Group Address    Interface            Uptime    Expires   Last Reporter
239.255.255.250  Vlan1                00:00:40  00:02:19  192.168.65.43
```

```
224.0.1.40      FastEthernet0/1     00:01:24  00:02:17  202.113.2.2
230.0.0.2       FastEthernet0/1     04:02:10  00:02:25  202.113.2.2
230.0.0.3       FastEthernet0/1     04:02:10  00:02:17  202.113.2.2
230.0.0.0       Vlan2               04:02:09  00:02:21  202.113.1.1
```

7.3.2.14 Display Interface Information About IGMP

To display interface information about IGMP, use the following command at privileged mode:

Command	Purpose
show ip igmp interface [*interface type*]	Display interface information about IGMP.

```
Switch# show ip interface
FastEthernet 0/0
mtu is 1500
IP interface state is: DOWN
Internet address is 192.11.11.11 mask is 255.255.255.0
igmp config general query interval is 18000
igmp config robustness is 2
igmp current general query interval is 18000
igmp group member interval is 36010
igmp host robustness is 2
igmp join group unsolicited report counter is 2
igmp join group unsolicited report interval is 1
igmp last member query counter is 7
igmp last member query interval is 255  1/10seconds
igmp has 5 different config in this interface
igmp nif learnt mem num is 0
igmp nif limit num is 1024
igmp other querier interval is 255
igmp querier ip is 192.11.11.11
igmp query response interval is 100 1/10seconds
igmp router robustness is 2
igmp special query num is 0
igmp version is 3
IGMP is enabled on interface
```

7.3.2.15 IGMP Debug Switch

To open IGMP debug switch and display IGMP behavior, use the following command at privileged mode:

Command	Purpose
debug ip igmp	Open IGMP debug switch to display IGMP behavior.

Use **no debug ip igmp** to close IGMP debug switch.

7.3.3 Configuring PIM-DM

7.3.3.1 Adjusting the PIM Hello Message Interval

PIM-DM uses timers to detect the frequency of sending Hello message. The interval length of sending Hello message will influence whether neighbor relationship can be created successfully.

To adjust timers, use the following command at interface configuration mode:

Command	Purpose
ip pim query-interval *interval* [**msec**]	Configure how long it takes in seconds to send hello message to neighbor from an interface.

7.3.3.2 Configuring PIM-DM State Refresh

At administration mode, it is permitted to forward PIM-DM state refresh control message by default. At interface configuration mode, configure the interval of sending state refresh message periodically on the first hop directly connected to source, which is valid only to upstream interfaces. For the following routers, it is the interval of sending state refresh message which is permitted to receive and process on the interface.

Command	Purpose
no ip pim state-refresh disable	Allow to process and forward state-refresh message.
ip pim state-refresh origination-interval [*interval*]	Configure the interval of sending state refresh message periodically on the first hop directly connected to source, which is valid only to upstream interfaces. For the following routers, it is the interval of sending state refresh message which is permitted to receive and process on the interface.

The following example demonstrates how to set state refreshing interval 60 seconds on FastEthernet0/1.

```
ip multicast-routing
!
interface FastEthernet0/1
 ip address 172.16.8.1 255.255.255.0
 ip pim state-refresh origination-interval 60
 ip pim dense-mode
```

7.3.3.3 Configuring PIM-DM Filtering List

PIM-DM is not configured filtering list by default, including neighbors filtering list and multicast boundary filtering list, which will be configured at interface configuration mode.

If you expect to prohibit a router or a segment from being added into the PIM-DM negotiation, you have to configure neighbors filtering list. To disable or enable some groups go through this region, you have to configure boundary groups filtering list.

Command	Purpose
ip pim neighbor-filter *access-list*	Configure neighbors filtering list.
ip multicast boundary *access-list-name*	Use this command to configure multicast boundary.

7.3.4 Configuring DVMRP Interoperability

7.3.4.1 Configuring Metric of DVMRP Routes

By default, once a DVMRP route received, the metric will be increased by 1,which means hops is increased by 1. When sending DVMRP route message, shortcut routes will be increased by 1, others keep unchanged.

If you expect to adjust metric of routes, use the following command at interface configuration mode:

Command	Purpose
ip dvmrp metric-offset [**in** | **out**] *metric-offset*	Adjust the metric of sending and receiving routes. **in**: indicates input. **out**: indicates output. *metric-offset*: indicates the increased metric, the range is [1,31]. For **in**, default is 1, for **out**, it is not configured on default.

You can also set metric for each routes to be sent by using the following command at interface configuration mode:

Command	Purpose
ip dvmrp metric *metric* [**list** *access-list*] [**connected** | **dvmrp**]	Modify the metric of forwarded routes *metric*: Set the metric value, the range is [0,32]. **list** access-list-number: it is used to match route metric which will be modified. **connected**|**dvmrp**: it is used to match protocol type by which metric is modified.

Tip

ip dvmrp metric-offset explanation:

This command is only valid to DVMRP routes, which will be matched before **ip dvmrp metric**.

Tip

ip dvmrp metric explanation:

1. It can be configured repeatedly on the same interface, which will be matched in the configuration sequence. Any of two configuration is considered the same only when "[**list** *access-list-number*]" and "[**connected** | **dvmrp**]" are same configured.
2. When associated ACL does not exist or ACL permit is used, please modify the metric

7.3.4.2 Configuring Management Distance of DVMRP Routes

By default, when mulicast routing protocol using RPF lookup function, the management distance of DVMRP unicast route is considered 0, so as to be selected prior to other unicast routes

You can adjust the management distance of DVMRP unicast routes received from the specified interface, so as to launch RPF check on unicast routes first. Use the following command at global configuration mode:

Command	Purpose
ip dvmrp distance *distance*	Modify the management distance of received routes. *distance*: Set distance value. The range is [0,255], default is 0.

7.3.4.3 Configuring DVMRP Routes Information Filter

By default, receivers will not filter the received DVMRP routes. If you expect to filter these routes, use the following command at interface configuration mode:

Command	Purpose
ip dvmrp **accept-filter** *access-list* [**neighbor-list** *access-list*] [**distance** *distance*]	Modify management distance of received routes **accept-filter** access-list-number: filter routes information **neighbor-list** *access-list-number*: filter neighbor addresses. **distance** *distance*: Set the management distance. The range is from 0 to 255.

Tip

ip dvmrp accept-filter explanation:

1. It can be configured repeatedly on the same interface and will be matched in the sequence of configuration.
   Any of two configurations are considered the same only when "**accept-filter** *access-list-number*" is same matched.
2. By defaulting, all routing entries are received. After this command is configured, only entries with "ACL permit" can be received.

7.3.4.4 Configuring Distribution of DVMRP Default Routes

You can configure software to advertise network 0.0.0.0 (default route) to DVMRP neighbors. The DVMRP default route calculates the RPF information for any multicast source that does not match a more explicit route.

Use the following command in interface configuration mode:

Command	Purpose
ip dvmrp default-information {**originate** | **only**} [**metric** *metric*]	Configure to advertise default route to neighbors. **Originate**: Other routes are also advertised besides default route. **only**: Only default route will be advertised. **metric** *metric*: indicates the metric value of default route. Range is from 1 to 31 and default is 1.

7.3.4.5 Controlling the Number of DVMRP Routes Entries

There are two ways to limit DVMRP routes entries provided on our device.

- Limit the number of routes information

Set the number of DVMRP routes advertised on each interface.

- Routes threshold

If there are too many DVMRP routes within a period, it may indicate a fault of the network. By means of this characteristic, it will be alarmed when the number of routes entries exceeds the threshold.

Use the following command in global configuration mode:

Command	Purpose
ip dvmrp route-limit	Limit the number of DVMRP routes advertised on each interface. The range is [0, 65535], and default is 16000.
ip dvmrp routehog-notification *route-count*	Change the threshold number of routes that trigger the warning within 1 minute interval The range is [1, 65535], and default is 8000.

7.3.4.6 Rejecting a DVMRP Nonpruning Neighbor

When forwarding multicast message to DVMRP area on non-DVMRP devices which support DVMRP interoperability, it may arise wasting bandwidth for these forwarded multicast data stream within DVMRP area since some devices run old versions of DVMRP that cannot prune.

You can configure to reject nonpruning DVMRP messages and prevent creating DVMRP neighbors, so as to prevent multicast data stream from being forwarded to DVMRP area.

Command	Purpose
ip dvmrp reject-non-pruners	Configure rejecting nonpruning neighbors

Tip

Our products can not support forwarding multicast data stream to DVMRP area at present. It will be implemented later.

7.3.4.7 Monitoring and Maintaining DVMRP Interoperability

If you found that DVMRP route is invalid, or you expect to clear invalid DVMRP route information, use the following command in privilege mode:

Command	Purpose
clear ip dvmrp route [* | *ip-address*]	Clear the DVMRP route information.

If you expect to display DVMRP route information, use the following command at privilege mode:

Command	Purpose
show ip dvmrp route [*ip-address*]	Show the DVMRP route information.

7.3.5 Multicast Routing Configuration Examples

7.3.5.1 PIM-DM Configuration Example

It demonstrates how to configure PIM-DM on FastEthernet0/1 in the following example.

```
ip multicast-routing
interface FastEthernet0/1
 ip address 172.16.8.1 255.255.255.0
 ip pim dense-mode
```

7.3.5.2 PIM-DM State Refresh Configuration Example

It demostrates how to provide state refresh message on FastEthernet0/1 in the following example. The refresh interval is 60s.

```
ip multicast-routing

interface FastEthernet0/1
 ip address 172.16.8.1 255.255.255.0
 ip pim state-refresh origination-interval 60
 ip pim dense-mode
```

7.3.5.3 Boundary Management Configuration Example

The following example shows how the administrator configures the boundray management of a port.

```
interface FastEthernet 5/2
ip multicast boundary acl
ip access-list standard acl
permit 192.168.20.97 255.255.255.0
```

8 IPv4 Express Forwarding Configuration

8.1 Overview

To meet the requirements of higher end devices, we currently use Express Forwarding models formed by combining Prefix Trees with Adjacencies to implement express forwarding.An Express Forwarding model structures the mirroring of a whole kernel route table, not only caches part of information about the kernel route table. Therefore, there is no such situation that a cahce fails and .CPU need add another cache. In this way, it reduces impact to CPU and also ensures the stability of route performance

The Express Forwarding model structures the mirroring of the route table by use of the following parts:

- Prefix Tree

Prefix Tree. This is an IP prefix tree organized according to the longest match principle and it is used to search adjacencies. In implementation, the data structure used to organized a Prefix Tree usually differs from a Radix Tree of the kernel route table. Instead, it uses a data structure called M-Tries Tree to implement faster multistep lookup.When we construct a Prefix Tree by using M-Tries Trees instead of Radix Trees, it consumes more memory space and the time spent on updating Prefix and Adjacency information is also relatively longer. However, it can provide a very high search performance.

- Adjacency

Adjacency.An adjacency contains the output interface information of a routed message, i.e., nexthop list, next processing part and link layer output encapsulation information. When a message matches the adjancency, the system directly encapsulates the message and then invokes the send function held by the node to implement forwading. For easy search and updating, talbes made up of adjacencies are usually in the form of hash tables. For route load balance support, the next piece of list information of adjacencies is orgnized in the form of load balance tables. An adjancency may contain no nexthop information and it also may contain the index of a next processing part,such as any other cable-routing clip and Multi-Serial Card (Any port, Any service).

Express Forwarding routing includes the following three steps:

1. Express Forwarding decapsulates a message.
2. Use Prefix Tree to search its message route for the adjacency to be outputed.
3. After matching the outputed adjancency, determine the final output interface for the message according to the information about the adjacency, and then encapsulate the message according to the output interface type.

For the present DES-7200 switch, IP message forwarding is implemented mainly through switching chips. Therefore, it is necessary to put this kind of forwarding information to chips through the API provided by SSP to implement hardware express forwarding.IP Express Forwarding modules are responsible for maintaining route forwarding information and doing corresponding settings for the lower layer. However, they are not responsible for data forwarding.

8.2 Express Forwarding Load Balance Policy Configuration

Express forwarding supports the load balance processing of messages. At present, it implements two types of load balance policies based on IP addresses.In the EF model, when the rote prefix IP/MASK is associated to multiple nexthops, i.e., a Multipath route, the route will be associated to a load balance table and it implements load balance according to route weight.When an IP message matches the load balance table according to the longest prefix, express forwarding hashs IP addresses based on messages and selects one of the paths to forward the message.The two policies to seclect paths are as follows:

1. Balance according to the destination IPs of IP messages and hash the destination addresses of messages. The possibility of a path with a bigger weight being selected is higher.By default, express forwarding uses this policy.
2. Balance according to the destination IPs and source IPs of IP messages and hash the destination IPs and originating IPs of messages. The possibility of a path with a bigger weight being selected is higher.

To configure the load balance policy, run the following commands in the global configuration mode:

Command	Function
D-Link(config)# **ip ref load-sharing algorithm original**	Configure the load balance algorithm to obey the policy based on the pair of source and destination IP addresses
D-Link(config)# **no ip ref load-sharing algorithm original**	Cancel the load balance algorithm based on source and destination IPs,and restore the default balance algorithm based on message destination IPs

Note

This command is a router-specific command.

8.3 Express Forwarding Table Maintence and Monitoring

The Eexpress Forwarding module only passively accepts and maintains outer route informatio.The module itself does not positively add or delete any route information. Therefore, the Express Forwarding module internally provides current route statistics.

For express forwarding table monitoring and maintence, there are the following commands at present:

- Global statistics
- Adjacency table information
- Message forwarding path information
- Express forwarding route information

8.3.1 Global Statistics

Global statistics is the information related to those types of data structures in the current express forwarding table, including the counts of current routes, adjacency nodes, load balance tables and weight nodes.

Command	Function
D-Link# **show ip ref**	Show the statistics in the current express forwarding

8.3.2 Adjacency Table Information

Among express forwarding tables, one type of important data sets is the adjacent talbe.We can run the following command to view current adjacency information:

Command	Function
D-Link**#show ip ref adjacency [glean | local | *ip* | (interface** *interface_type interface_number***)]**	Show the information related to collection adjacency, local adjacency, adjacency corresponding to specifed IPs, adjacency associated with specified interfaces and all adjacency nodes.

8.3.3 Message Forwarding Path Information

The route forwarding of a message is performed based on the IP address of the message. Therefore, if you have specified the source and destination IP addresses of a message, then the forwarding path of the message will be certain.If you invoke the following command and specify the source and destination IPs of a message,then the system will show the actual forward path of the message, such as message discard, commit to CPU or forwarding. Further, you can also know the interface where the message is forwarded.

Command	Function
D-Link**#show ip ref exact-route** *source-ipaddress dest_ipaddress*	Show the actual forwarding path of a specific message.

Note

This command is a router-specific command.

8.3.4 Express Forwarding Table Route Information

Express Forwarding receives external route notifications, and maitains its own express forwarding table and a mirroring of the express forwarding table and the kernel route table.The route information in the two tables are same. You can use the following command to show the route information related to the express forwarding talbe:

Command	Function
D-Link# **show ip ref route [default | (***ip mask***)]**	Show the default route information in the current express forwarding table. If no default route information is specified, then the system shows all route information in the express forwarding talbe, including 0 route, the default route and normal gateway routes.

8.4 Switch Express Forwarding ECMP/WCMP Policy Configuration

In a switch, for hardware forwarding, when there is an ECMP/WCMP route, .there is also a load balance policy.When the route has multiple nexthops, the hardward can select one of these nexthops according to the policy we have set.

The policy can be expressed as follows: **HASH**(**KEY**(sip,[dip] [tcp/udp port] [udf]))

The explanation of the expression is as follows: We perform the hash operation on a keyword and use the value we get from the operation to select a nexthop.Where, the policy that we can set includes the following two aspects: For the selection of HASH algorithms, the hardware can provide two choices: crc32_upper and crc32_lower. Another aspect: KEY. We can select to use some fields of a message to form a KEY. By default, we only select source IP address(sip). At the same time, we can additionally select the value of the corresponding port for a TCP/UDP message, the destination IP (dip) of the message and a user defiend value to compose the KEY.

Command	Function
D-Link(config)# **ip ref ecmp load-balance {[crc32_lower | crc32_upper] [dip] [port] [udf** *number***]}**	Use any combineation of dip, port and udf to compose a key.Moreover, select crc32_lower or crc32_upper as your hash algorithm.
D-Link(config)# **no ip ref ecmp load-balance {[crc32_lower | crc32_upper] [dip] [port] [udf** *number***]}**	The no command removes the keywords in the no command from the setting saved by the system and uses the rest as a component of the key. For example, the setting saved by the system is sip + dip + port. After the no ip ref ecmp route dip port command runs, only sip is a component of the key. If the members following the no command do not exist in the setting saved by the system, then no error occurs when you run the command.

9 Configuring IPv4 Unicast Routing

9.1 IP Routing Protocol Overview

9.1.1 IP Routing and Routing Table

The basic function of a router is routing. For a specific router, routing is the process to forward the packets from an interface to another. This process is similar to the switching process performed by a switch, except that it is referred to as switching on the link layer, and as routing on the IP layer. For a network, routing is the process to transmit packets from one end (host) to another end (host).

The routing process involves two essential steps: The first one is route selection, where the router selects a route according to the destination addresses of the packets and the contents in the routing table. The second step is packet forwarding, where the router forwards the packets from a port according to the selected route.

The routing table is the basis for the router to select routes. The contents (that is, route entries) in the routing table come from two sources: static configuration and dynamic learning by the routing protocols. The contents of a routing table are shown as below:

```
D-Link#show ip route

Codes:  C - connected, S - static, R - RIP, D - EIGRP,
EX - EIGRP external, O- OSPF, IA - OSPF inter area
E1 - OSPF external type 1, E2 - OSPF external type 2,
* - candidate default


Gateway of last resort is 10.5.5.5 to network 0.0.0.0

C   172.16.11.0 is directly connected, serial1/2
O  E2 172.22.0.0/16 [110/20] via 10.3.3.3, 01:03:01, Serial1/2
S* 0.0.0.0/0 [1/0] via 10.5.5.5
```

At the very beginning of the routing table are the explanations of the abbreviations, for clarity in describing the sources of the routes. The “Gateway of last resort” shows that a default route is available and also where it comes from and which network segment it resides.

One route is shown usually on one line, and occasionally on multiple lines if it is too long. From the left to the right, each field of a route entry is described as below:

- Route source

The first field of a route entry shows the source of the route entry. For example, “C” means a direct-connected route, “S” means a static route, and “*” means a default route.

- Destination network segment

It includes the network prefix and mask description, for example, 172.22.0.0/16.

- Management distance/metric

The management distance represents the creditability of the source of the route. Different route sources may have different values for this parameter, while the metric represents the cost of the route. The routing table all contains the optimal routes, which, in other works, have the minimum management distances and metrics. If two routes to the same destination network segment but from different sources are to be added to the beginning of the routing table, a comparison should be performed. First, their management distances are compared, and that with a smaller one is choosen. If they happen to have the same management distances, their metrics are further compared. If the metrics are still the same, then both of them are added.

- Next-hop IP address

This describes the next-hop router of the route.

- Alive time

This describes the time for how long this route is alive, as shown in “HH:MM:SS”. Only dynamic routes and learnt routes have this field.

- Next-hop interface

This describes the IP packets that match this router will be sent to that interface.

9.1.2 IP Routing Protocol Selection

To select the routing protocol, you must consider the two factors: network scale and complexity.

- Whether it is necessary to support VLSMs (variable length subnet mask);
- Network traffic volume;
- Security consideration;
- Reliability consideration;
- Interworking delay feature;
- Routing policies of the organization.

This configuration guide only describes the details of the configuration of various routing protocols, without elaborating how to select routing protocols. You need to select the appropriate routing protocols according to your specific needs.

9.1.3 Interior and Exterior Gateway Protocols

There are two types of IP routing protocols: IGPs (Interior Gateway Protocols) and EGPs (Exterior Gateway Protocols).

Tip

In the definition of many routing protocols, routers are referred to as gateways, so gateways are often used as part of the names of the routing protocols. However, routers are often defined in the L3 interworking equipment, while the protocol conversion gateway is re-defined in the L7 equipment. Please note that routing protocols always work on L3 in the Open System Interconnection reference model no matter whether the routing protocol names include the wording of gateways.

9.1.3.1 Interior Gateway Protocols

Interior gateway protocols are used in the routing networks managed by the same network management organization to exchange routing information. All IGPs must be defined with their interested networks. A routing process listens to the route update packets from other routers in these networks, while sending their own routing information update packets to these network ports. DES-7200 currently supports the following IGPs:

- RIP routing protocol Version 1 and Version 2;
- OSPF routing protocol

DES-7200 will support more IGPs in future versions.

9.1.3.2 Exterior Gateway Protocols

Exterior gateway protocols are used between the routing networks managed by different network management organizations to exchange routing information. Currently, the Border Gateway Protocol (BGP) is a widely-used EGP. DES-7200 will support the BGP in future versions.

9.1.4 Running Multiple Routing Protocol Processes

One router can be configured to run multiple routing protocol processes for connection with the networks that run different routing protocols. For example, a subnet is configured with the RIP, while another subnet is configured with the OSPF, and these routing processes need to exchange routing information between each other.

However, interoperability is not implemented between different routing protocols, with each routing protocol collecting its routing information and responding to the network topology change according to its own unique way. For example, the RIP routing information is measured in hops, while the OSPF routing information is measured in a compound way. Therefore, in order for different routing protocol processes to exchange routing information, the configuration option must be used for appropriate control.

DES-7200 can concurrently handle multiple dynamic IP routing processes. Among them, there can be only one RIP routing process and also one OSPF process.

9.1.5 About the Contents

There are the following chapters:

- Configuring static routes
- Configuring RIP routing protocol
- Configuring OSPF routing protocol
- Configuring protocol-independent features
- Configuring policy-based routing

9.2 Configuring Static Routes

9.2.1 Configuring Static Routes

Static routes are manually configured so that the packets to the specified destination network go through the specified route. When 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
D-Link(config)**#ip route** *network mask* {ip-address | *interface-type interface-number* } [*distance*] [**tag** *tag*] [**permanent**] [**weight** *number*]	Configure static routes
D-Link(config)**#no ip route** *network mask*	Delete 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, DES-7200 software 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 DES-7200 firmware:

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, if there is a recursive static route, when DES-7200 firmware fails to find the forwarding route to the next-hop address, the static route will also disappear from the routing table.

9.2.2 Configuring Default Routes

Not all routers have a complete network-wide routing table. To allow every router to route all packets, it is a common practice that the powerful core network is provided with a complete routing table, while the other routers 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 router 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
D-Link(config)**#ip default-network** *network*	Configure the default network
D-Link(config)**#no ip default-network** *network*	Delete the default network

Tip

To generate the default routes by using the default-network command, only the following two conditions must be met: 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”.

9.3 Configuring RIP Routing Protocol

9.3.1 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, DES-7200 firmware will generate the default route and advertise it to the neighbor router:

- The 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 features of the RIP, see Protocol-Independent Configuration.

9.3.2 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.

Creating the RIP routing process (required)

Configuring packet unicast for the RIP (required)

- Configuring Split Horizon (optional)
- Defining the RIP version (optional)
- Disabling the automatic route summary (optional)
- Adjusting the RIP timer (optional)
- Configuring the RIP route source address validation (optional)

For other topics, see Protocol-Independent Configuration.

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

9.3.2.1 Creating 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:

Step 1	Switch(config)**#router rip**	Create the RIP routing process
Step 2	D-Link (config-router)**#network** *network-number*	Define the associated network

Tip

The associated network defined by the Network command has two meanings:

1. The RIP only advertises the routing information of the associated network to the outside;
2. The RIP only advertises the route information to the port of the associated network.

9.3.2.2 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
D-Link (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 Protocol-Independent Configuration.

Tip

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.

9.3.2.3 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
D-Link (config-if)**#no ip split-horizon**	Disable split horizon
D-Link (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.

9.3.2.4 Defining the RIP Version

DES-7200 firmware supports RIP version 1 and version 2, where RIPv2 supports authentication, key management, route summary, CIDR and VLSMs.

By default, 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
D-Link (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
D-Link (config-if)**#ip rip send version 1**	Specify to send the packets of only RIPv1
D-Link (config-if)**#ip rip send version 2**	Specify to send the packets of only RIPv2
D-Link (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
D-Link (config-if)**#ip rip receive version 1**	Specify to receive the packets of only RIPv1
D-Link (config-if)**#ip rip receive version 2**	Specify to receive the packets of only RIPv2
D-Link (config-if)**#ip rip receive version 1 2**	Specify to receive the packets of RIPv1 and RIPv2

9.3.2.5 Disabling the 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
D-Link (config-router)**#no auto-summary**	Disable automatic route summary
D-Link (config-router)**#auto-summary**	Enable automatic route summary

9.3.2.6 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:

Step 1	D-Link (config-if)**#ip rip authentication key-chain** *key-chain-name*	Apply the key chain and enable RIP authentication
Step 2	D-Link (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.

9.3.2.7 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
D-Link (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.

Tip

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

9.3.2.8 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
D-Link (config-router)#no validate-update-source	Disable source address validation

Command	Function
D-Link (config-router)#validate-update-source	Enable source address validation

9.3.3 RIP Configuration Examples

This section provides three RIP configuration examples:

- Example of configuring split horizon
- Example of configuring RIP authentication

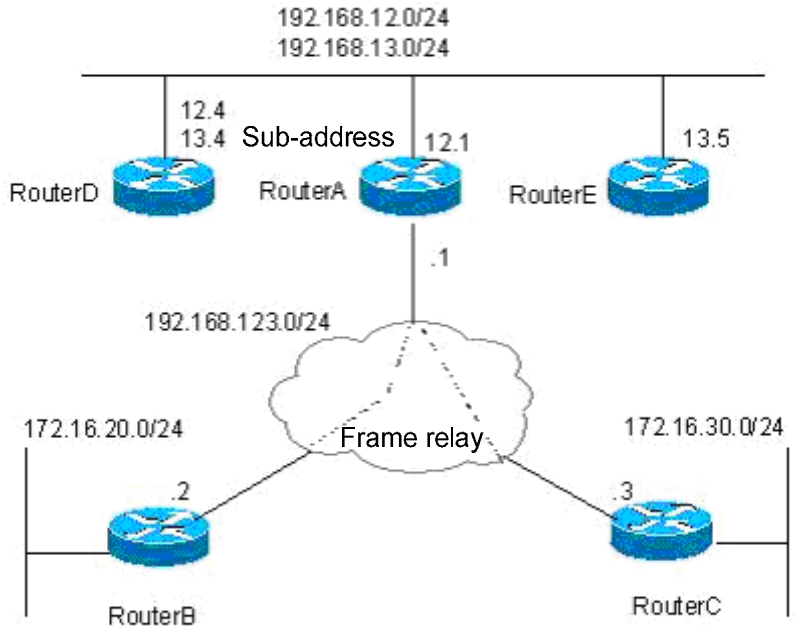
Example of configuring RIP unicast update packets

9.3.3.1 Example of Configuring Split Horizon

- **Configuration requirements:**

There are five routers. RouterA, RouterD, and RouterE are connected via Ethernets. RouterA, RouterB, and RouterC are connected via frame relay. Figure 1-1 shows IP address distribution and equipment connection, where RouterD is configured with a sub-address.

Figure 1-3 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.

- **Specific configuration**

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. The following is the specific configuration of each router.

Configuration of Router A:

```
!Configure the Ethernet port
interface FastEthernet0/0
 ip address 192.168.12.1 255.255.255.0

!Configure the WAN port
interface Serial1/0
 ip address 192.168.123.1 255.255.255.0
 encapsulation frame-relay
 no ip split-horizon

!Configure the RIP routing protocol
router rip
 version 2
 network 192.168.12.0
 network 192.168.123.0
```

Configuration of Router B:

```
!Configure the Ethernet port
interface FastEthernet0/0
 ip address 172.16.20.1 255.255.255.0

!Configure the WAN port
interface Serial1/0
 ip address 192.168.123.2 255.255.255.0
 encapsulation frame-relay

!Configure the RIP routing protocol
router rip
 version 2
 network 172.16.0.0
 network 192.168.123.0
 no auto-summary
```

Configuration of Router C:

```
!Configure the Ethernet port
interface FastEthernet0/0
 ip address 172.16.30.1 255.255.255.0

!Configure the WAN port
interface Serial1/0
 ip address 192.168.123.3 255.255.255.0
 encapsulation frame-relay

!Configure the RIP routing protocol
router rip
 version 2
 network 172.16.0.0
 network 192.168.123.0
 no auto-summary
```

Configuration of Router D:

```
!Configure the Ethernet port
```

```
interface FastEthernet0/0
 ip address 192.168.12.4 255.255.255.0
 ip address 192.168.13.4 255.255.255.0 secondary
 no ip split-horizon

!Configure the RIP routing protocol
router rip
 version 2
 network 192.168.12.0
 network 192.168.13.0
```

Configuration of Router E:

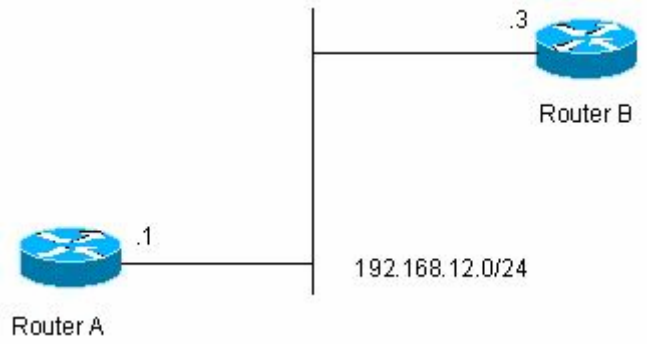
```
!Configure the Ethernet port
interface FastEthernet0/0
 ip address 192.168.13.5 255.255.255.0

!Configure the RIP routing protocol
router rip
 version 2
 network 192.168.13.0
```

9.3.3.2 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. Figure 1-2 shows the connection between the routers and the IP address allocation.

Figure 1-4 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.

- **Specific configuration**

Configuration of Router 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

  !Configure the Ethernet port
  interface FastEthernet0/0
   ip address 192.168.12.1 255.255.255.0
   ip rip authentication mode md5
   ip rip authentication key-chain ripkey

  !Configure the RIP routing protocol
  router rip
   version 2
   network 192.168.12.0
```

Configuration of Router B:

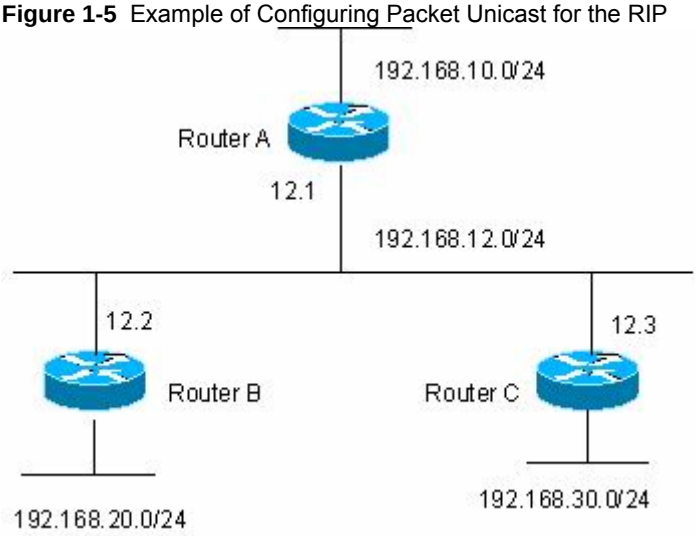
```
  !Configure the key chain
  key chain ripkey
   key 1
    key-string keya
    accept-lifetime infinite
    send-lifetime 00:00:00 Dec 4 2000 00:00:00 Dec 5 2000
   key 2
    key-string keyb
    accept-lifetime infinite
    send-lifetime 00:00:00 Dec 4 2000 infinite

  !Configure the Ethernet port
  interface FastEthernet0/0
   ip address 192.168.12.2 255.255.255.0
   ip rip authentication mode md5
   ip rip authentication key-chain ripkey

  !Configure the RIP routing protocol
  router rip
   version 2
   network 192.168.12.0
```

9.3.3.3 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 1-3 shows the IP address allocation and connection of the equipment.

Figure 1-5 Example of Configuring Packet Unicast for the RIP



By configuring the RIP packet unicast, you must achieve the following purposes:

1. Router A can learn the routes advertised by Router C;
2. Router C cannot learn the routers advertised by Router A.

■ **Specific configuration**

To achieve the above purposes, RIP packet unicast must be configured at router A.

Configuration of Router A:

```
!Configure the Ethernet port
interface FastEthernet0/0
 ip address 192.168.12.1 255.255.255.0

!Configure the loopback port
interface Loopback0
 ip address 192.168.10.1 255.255.255.0

!Configure the RIP routing 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 Router B:

```
!Configure the Ethernet port
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

!Configure the RIP routing protocol
router rip
```

```
 version 2
 network 192.168.12.0
 network 192.168.20.0
```

Configuration of Router C:

```
!Configure the Ethernet port
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

!Configure the RIP routing protocol
router rip
 version 2
 network 192.168.12.0
 network 192.168.30.0
```

9.4 Configuring OSPF Routing Protocol

9.4.1 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 number is 89 and it performs OSPF packet switching through multicast, with the multicast address to be 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:

- At the initialization stage, the router will create the link status advertisement, which includes all the link statuses of the router;
- All the routers exchange the link status information via multicast. When each router receives the link status update packets, it will send a copy to the local database before distributing them to other routers;
- When every router has a complete link status database, the router uses the Dijkstra algorithm to calculates 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.

In the OSPF router domain, there are three router roles depending on where the routers are deployed:

- Intra-area router: All the interfaced networks of the router belong to the same area;
- ABR (Area Border Router): The interfaced networks of this router belong at least to two areas, one of which must be the backbone area;
- ASBR (Autonomous System Boundary Routers): It is the router between which the OSPF route domain exchanges the external route domain.

DES-7200 firmware implements the OSPF by fully complying with the OSPF v2 defined in RFC 2328. The main features of the OSPF implemented by DES-7200 firmware 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

9.4.2 OSPF Configuration Task List

The configuration of the OSPF needs mutual coordination between various routers (including the internal routers, ABRs and ASBRs). 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) Dead interval:4 times the hello interval. Priority: Authentication type : No authentication. Authentication password: No password specified.
Area	Authentication type : No authentication. Default metric: 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. Dead interval: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 LSA.
Neighbor change log	Enable
Neighbor	None
Neighbor database filter Disabled.	All outgoing LSAs are sent to the neighbor.
Network area	None
Router 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 seconds5 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

9.4.2.1 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:

Step 1	D-Link**# configure terminal**	Enter the global configuration mode.
Step 2	D-Link(config)**# ip routing**	Enable the IP routing (if disabled)
Step 3	D-Link(config)**# router ospf**	Enable OSPF and enter OSPF route configuration mode.
Step 4	Router(config-router)# **network** *address wildcard-mask* **area** *area-id*	Define an IP address range for an area.
Step 5	Router(config-router)# **End**	Return to the privileged EXEC mode.
Step 6	D-Link**# show ip protocol**	Display the routing protocol that is running currently.
Step 7	D-Link**# write**	Save the configuration.

Tip

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, 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** command. The example shows how to start the OSPF protocol:

```
D-Link(config)# router ospf
D-Link (config-router)# network 192.168.0.0 255.255.255.0 area 0
D-Link (config-router)# end
```

9.4.2.2 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:

Step 1	D-Link**# configure terminal**	Enter the global configuration mode.
Step 2	D-Link(config)**# Ip routing**	Enable the IP routing (if disabled)
Step 3	D-Link(config)**# interface** *interface-id*	Enter the interface configuration mode.
Step 4	Router(config-if)**# Ip ospf cost** *cost-value*	(Optional) Define the interface cost
Step 5	Router(config-if)**# Ip ospf retransmit-interval** *seconds*	(Optional) Set the link status retransmission interval;
Step 6	Router(config-if)**# ip ospf transmit-delay** *seconds*	(Optional) Set the transmit delay for the link status update packets;
Step 7	Router(config-if)**# ip ospf hello-interval** *seconds*	(Optional) Set the hello packet send interval, which must be the same for all the nodes of the entire network;
Step 8	Router(config-if)**# ip ospf 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;
Step 9	Router(config-if)**# ip ospf priority** *number*	(Optional) Set the priority, used to elect the Designated Router (DR) and Backup Designated Router (BDR)
Step 10	Router(config-if)**# Ip ospf authentication [message-digest | null]**	(Optional) Set the authentication type on the network interface.
Step 11	Router(config-if)**# ip ospf authentication-key** *key*	(Optional) Configure the key for text authentication of the interface
Step 12	Router(config-if)**# ip ospf message-digest-key** *keyid* **md5** *key*	(Optional) Configure the key for MD5 authentication of the interface
Step 13	Router(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.
Step 14	Router(config-if)**#End**	Return to the privileged EXEC mode.

Step 15	D-Link# **show ip ospf interface** [*interface-id*]	Display the routing protocol that is running currently.
Step 16	D-Link# **write**	(Optional) Save the configuration.

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

9.4.2.3 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:

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.

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
D-Link(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-multipoint 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

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:

Step 1	D-Link(config-if)# **ip ospf network point-to-multipoint**	Configure the point-to-multipoint network type for an interface
Step 2	D-Link(config-if)# **exit**	Exit to the global configuration mode
Step 3	D-Link(config)# **router ospf**	Enter the routing process configuration mode
Step 4	D-Link(config-router)# **neighbor** *ip-address* **cost** *cost*	Specify the cost of the neighbor (optional)

Tip

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.

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. When you configure it to the NBMA network, you must specify neighbors. Since the election of the designated router is involved, you may have to specify the designated router by configuring the priorities. The higher the priority a router has, the more likely it becomes the designated router.

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

Step 1	D-Link (config-if)**#ip ospf network non-broadcast**	Specify the network type of the interface to be the NBMA type
Step 2	D-Link (config-if)**#exit**	Exit to the global configuration mode
Step 3	D-Link (config)**#router ospf**	Enter the routing process configuration mode
Step 4	D-Link(config-router)**#neighbor** *ip-address* [**priority** number] [**poll-interval** seconds]	Specify the neighbor and specify its priority and hello polling interval

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:

Step 1	D-Link (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
Step 2	D-Link (config-if)**#exit**	Exit to the global configuration mode
Step 3	D-Link (config)**#router ospf**	Enter the routing process configuration mode
Step 4	D-Link(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.

Configuring Broadcast Network Type

For the OSPF broadcast network, the Designated Router (DR)and Backup Designated Router (BDR) need to be specified, and the DR will advertise the link status of the network to the outside. All routers are in neighborhood relationship, but they only maintain this relationship between the designated router and backup router. In other words, each router only exchanges link status packets with the designated router or backup router and then the designated router will advertise it to all the routers, so that every router can maintain 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 only condition for the new round of election is: The OSPF neighbor does not receive the HELLO packets from the designated router within the specified period, and believes that the designated router is down.

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

Step 1	D-Link (config-if)**#ip ospf network broadcast**	Specify the type of the interface to be the broadcast network type

Step 2	D-Link (config-if)**#ip ospf priority** *priority*	(Optional) Specify the priority of the interface

9.4.2.4 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 an stub area. The routers in a stub area can learn only three types of routes:

1. Routes in the stub area;
2. Routes in other areas;
3. Default route advertised by the border router in the stub area.

Since there are not many external routes, the routers in a stub area have a much smaller routing table, saving the resources of the routers. For this reason, the routers in the stub area can medium or low-end devices. 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
D-Link (config-router)**#area** *area-id* **authentication**	Set plain-text authentication as the authentication mode for the area
D-Link (config-router)**#area** *area-id* **authentication message-digest**	Set MD5 authentication as the authentication mode for the area

Command	Function
D-Link (config-router)**#area** *area-id* **stub [no-summary]**	Set the area as a stub area **no-summary:**Set the area as a stub area to prevent the ABR between areas from sending summary-LSAs to the stub area
D-Link (config-router)**#area** *area-id* **default-cost** *cost*	Configure the cost of the default route sent to the stub area

Tip

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.

9.4.2.5 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
D-Link (config-router)**# area** *area-id* **nssa** [**no-redistribution**] [**default-information-originate**] [**no-summary**]	(Optional) Define a NSSA
D-Link (config-router)**# area** *area-id* **default-cost** *cost*	Configure the cost of the default route sent to the NSSA

The default-information-originate parameter is used to generate the default Type-7 LSA. This option varies slightly between the ARR and ASBR of the NSSA. On the ABR, whether there is a default route or not in the routing table, the Type-7 LSA default route will be created. On the other hand, this is only created when there is a default route in the routing table on ASBR.

The no-redistribution parameter allows other external routes introduced by using the redistribute commands via the OSPF on the ASBR not to be distributed to the NSSA. This option is usually used when the router in the NSSA is both an ASBR and an ABR to prevent external routes from entering the NSSA.

To further reduce the LSAs sent to the NSSA, you can configure the no-summary attribute on the ABR to prevent the ABR from sending the summary LSAs (Type-3 LSA) to the NSSA.

In addition, the area default-cost is used on the ABR connected to the NSSA. This command configures the cost of the default route sent by the border router to the NSSA. By default, the cost of the default route sent to the NSSA is 1.

9.4.2.6 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
D-Link (config-router)**# area** area-id **range** ip-address mask [**advertise** | **not-advertise**]	Configure the summary route of the area


Tip

If route summary is configured, the detailed routes in this area will not be advertised by the ABR to other areas.

9.4.2.7 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
D-Link (config-router)**# summary-address** *ip-address mask*[**advertise**|**not-advertise**]	Configure the external summary route

9.4.2.8 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. Virtual connections are identified by the router-id of the router on the other end. 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
Router(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 areas, 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.

Tip

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. For how to manually configure the router-id, see the "Using the Loopback Address as the Route ID" in this chapter.

9.4.2.9 Creating the Default Routes

An ASBR can be forced to generate a default route, which is injected to the OSPF routing area. If a router is forced to generate the default route, the route automatically becomes an ASBR. 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
D-Link (config-router)# **default-information originate [always] [metric** *metric-value***] [metric-type** *type-value***] [route-map** *map-name***]**	Configure to generate the default route


Tip

When you configure a stub area, the ABR will automatically generate the default route and then advertise it to all the routers in the stub area.

9.4.2.10 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:

Step 1	D-Link (config)# **interface loopback 1**	Create the loopback interface
Step 2	D-Link (config-if)# **ip address** *ip-address mask*	Configure the Loopback IP address

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

9.4.2.12 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
Router(config-router)**#timers spf** *spf-delay spf-holdtime*	Configure the route calculation timer

9.4.2.13 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:

Step 1	D-Link**# configure terminal**	Enter the global configuration mode.
Step 2	D-Link(config)**# router ospf**	Enable OSPF and enter OSPF route configuration mode.
Step 3	Router(config-router)**# timers lsa-group-pacing** *seconds*	(Optional) Change the LSAs group pacing.
Step 4	Router(config-router)**# End**	Return to the privileged EXEC mode.
Step 5	D-Link**# show running-config**	Show the configuration
Step 6	D-Link**# write**	(Optional) Save the configuration.

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

9.4.2.14 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, and an Ethernet interface has the bandwidth of 10Mbps, that is, the bandwidth is 100, the 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:

Step 1	D-Link**# configure terminal**	Enter the global configuration mode.
Step 2	D-Link(config)**# router ospf**	Enable OSPF and enter OSPF route configuration mode.
Step 3	Router(config-router)**# auto-cost [reference-bandwidth** *ref-bw***]**	(Optional) Set the default cost based on the bandwidth on an interface.
Step 4	Router(config-router)**# End**	Return to the privileged EXEC mode.

Step 5	D-Link# **show ip protocol**	Display the routing protocol that is running currently.
Step 6	D-Link# **write**	(Optional) Save the configuration.

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

9.4.2.15 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	Function
Router(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.

9.4.2.16 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:

Step 1	D-Link# **Configure terminal**	Enter the global configuration mode.
Step 2	D-Link(config)# **router ospf**	Enter the routing protocol configuration mode (currently RIP and OSPF are supported)
Step 3	Router(config-router)# **passive-interface** *interface-id*	(Optional) Set the specified interface as passive interface.
Step 4	Router(config-router)# **passive-interface default**	(Optional) Set all the network interfaces as passive
Step 5	Router(config-router)# **end**	Return to the privileged EXEC mode.
Step 6	Router(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 routing information, you can use the **no passive-interface** *interface-id* command. To re-enable tall network interfaces, use the keyword **default.**

9.4.3 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	Function
D-Link# **show ip ospf**	Show the general OSPF information.

Command	Function
D-Link# **show ip ospf** [*area-id*] **database**	OSPF database information Show the information of each type. area-id:It specifies the area on which the LSA is to show. For a class 5 LSA, the area filtering does not work.
D-Link# **show ip ospf** [*area-id*] **database** [**adv-router** *ip-address*]	
D-Link# **show ip ospf** [*area-id*] **database** [**self-originate**]	
D-Link# **show ip ospf** [*area-id*] **database** [**database-summary**]	
D-Link# **show ip ospf** [*area-id*] **database** [**router**] [*link-state-id*]	
D-Link# **show ip ospf** [*area-id*] **database** [**router**] [**adv-router** ip address	
D-Link# **show ip ospf** [*area-id*] **database** [**router**] [**self-originate**]	
D-Link# **show ip ospf** [*area-id*] **database** [**network**][*link-state-id*]	
D-Link# **show ip ospf** [*area-id*] **database** [**network**] [*link-state-id*] [**adv-router** *ip-address*]	
D-Link# **show ip ospf** [*area-id*] **database** [**network**] [*link-state-id*] [**self-originate**]	
D-Link# **show ip ospf** [*area-id*] **database** [**summary**] [*link-state-id*]	
D-Link# **show ip ospf** [*area-id*] **database** [**summary**] [*link-state-id*] [**adv-router** *ip-address*]	
D-Link# **show ip ospf** [*area-id*] **database** [**summary**] [*link-state-id*] [**self-originate**]	
D-Link# **show ip ospf** [*area-id*] **database** [**asbr-summary**] [*link-state-id*]	
D-Link# **show ip ospf** [*area-id*] **database** [**asbr-summary**] [*link-state-id*] [**adv-router** *ip-address*]	
D-Link# **show ip ospf** [*area-id*] **database** [**asbr-summary**] [*link-state-id*] [**self-originate**]	
D-Link# **show ip ospf** [*area-id*] **database** [**external**] [*link-state-id*]	
D-Link# **show ip ospf** [*area-id*] **database** [**external**] [*link-state-id*] [**adv-router** *ip-address*]	
D-Link# **show ip ospf** [*area-id*] **database** [**external**] [*link-state-id*] [**self-originate**]	
D-Link# **show ip ospf** [*area-id*] **database** [**nssa-external**] [*link-state-id*]	

Command	Function
D-Link# **show ip ospf** [*area-id*] **database** [**nssa-external**] [*link-state-id*] [**adv-router** *ip-address*]	
D-Link# **show ip ospf** [*area-id*] **database** [**nssa-external**] [*link-state-id*] [**self-originate**]	
D-Link# **show ip ospf border-routers**	Show the routes to the ABR and ASBR
D-Link# **show ip ospf interface** [*interface-name*]	Show the information on the OSPF interface
D-Link# **show ip ospf neighbor** [*interface-name*] [*neighbor-id*] **[detail]**	Show the routing information of the neighbor on the specified interface interface-name: The local interface ID connected to the neighbor neighbor-id:the router ID of the neighbor.
D-Link# **show ip ospf virtual-links**	Show the virtual connection information
D-Link# **show ip ospf retransmission-list** *[neighbor-id] [interface-name]*	Show the LSA information of the retransmission list of the specified neighbor on the interface
D-Link# **show ip ospf request-list** *[neighbor-id] [interface-name]*	Show the LSA information of the request list of the specified neighbor on the interface

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

The following command shows that there are currently three neighbors. The neighbor of the Fa0/0 port is the specified router and itself is a backup router. The neighbor of the F0/1 port is a backup router and itself is the designated router. “FULL” means that the two neighbors have already synchronized the link status library, forming the adjacent neighbor. The neighbor on the Fa1/1 port is neither the designated router nor the backup router. Also, it has no adjacency with itself, only retaining the bidirectional communication status.

```
D-Link #show ip ospf neighbor
Neighbor ID   Pri  State        DeadTime    Address         Interface
-----------   ---  ------      -------     ----------      ----------
1.1.1.7    1   full/DR         00:00:36    192.168.65.100   Fa0/0
1.1.1.10   1   full/BDR        00:00:36    192.168.65.110   Fa0/1
1.1.1.1    1   2Way/DROTHER    00:00:35    192.168.65.114   Fa1/1
```

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.

```
D-Link # sh ip ospf interface fastEthernet 0/0
 FastEthernet 0/0 State: Up
  Internet address : 192.168.123.1/24
  Area : 0.0.0.0
  Router ID : 192.168.124.1
  Network Type : Broadcast
  Cost : 100
  Transmit Delay : 1
  State : BDR
```

```
 Priority : 1
 Designated Router(ID) : 100.1.1.1
 DR's Interface address : 192.168.123.33
 Backup designated router(ID) : 192.168.124.1
 BDR's Interface address : 192.168.123.1
 Authentication : none
 Hello : 10
 Dead : 40
 Retransmit : 5
 Hello Due in : 00:00:00
 Neighbor Count is : 1
 Adjacent Neighbor Count is : 1
 Adjacent with neighbor : 192.168.123.33
 Passive status : Disabled
 Database-filter all out : Disabled
```

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.

```
D-Link#show ip ospf
Router ID : 192.168.124.1
Router Type : Normal Router
Support Tos : Single Tos(Tos0)
Number of external LSA : 0
External LSA Checksum Sum : 0x0
Number of areas in this router : 1
Number of normal area : 1
Number of stub area : 0
Number of nssa area : 0
Minimum LSA Interval : 5
Minimum LSA Arrival : 1
SPF Delay : 5
SPF-holdtime : 10
LsaGroupPacing : 240
RFC1583Compatibility flag : Enabled
Default-information originate : Disabled
Log Neighbor Adjency Changes : Disabled
Auto-Cost Status : Enabled  (reference-bandwidth is 100 Mbps)
Redistribute Default Metric : 20

Area : 0(BackBone Area)
       Area type : normal
       Number of interfaces in this area : 5
       Area authentication : none
       SPF algorithm executed times : 8
       Number of LSA : 3
       Checksum Sum : 0x71E4
       Number of Area Border Routers : 0
       Number of AS Border Routers : 0

Area            Range             Advertising   Status   Aggregate
--------------- ----------------- ------------- -------- ---------
```

4. Show the related information of the routing protocol

```
D-Link#show ip protocols

Routing Protocol is "ospf"
 Outgoing update filter list for all protocols is not set
 Incoming update filter list for all interfaces is not set
 Router ID 192.168.124.1
 It is a normal router(*)
 Redistributing External Routes from:
 Number of areas in this router is 1. 1 normal  0 stub  0 nssa
 Routing for Networks:
   0.0.0.0 255.255.255.255 area 0
 Routing Information Sources:
   Gateway        Distance     Last Update
   100.1.1.1      110          00:04:00
 Distance: (default is 110)
```

9.4.4 OSPF Configuration Example

This section provides seven OSPF configuration examples:

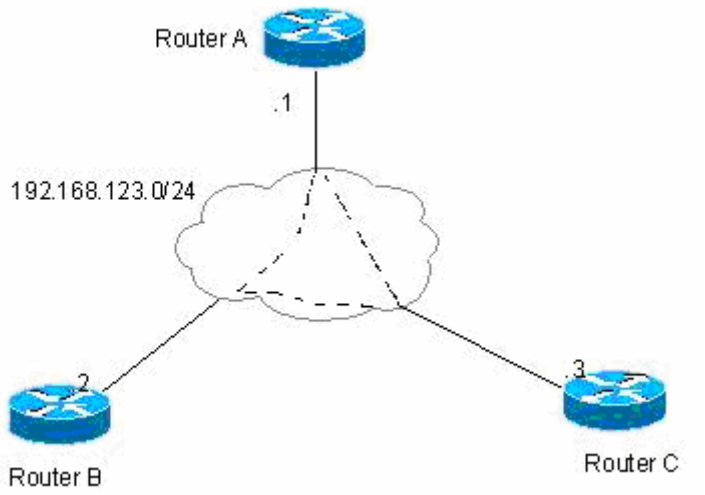
- Example of configuring the OSPF NBMA network type
- Example of configuring the OSPF point-to-multipoint network type
- Example of configuring OSPF authentication
- Example of configuring route summary
- Example of configuring OSPF ABR and ASBR
- Example of configuring OSPF stub area
- Example of configuring OSPF virtual connection

9.4.4.1 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 1-4 shows the IP address allocation and connection of the equipment.

Figure 1-6 Example of configuring the OSPF NBMA network type



Requirements:

1. The NBMA network type is configured among routers A, B, and C;
2. Router A is the designated router, while router B is the backup router;
3. All the networks are in one area.

■ **Configuration of the 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 Router A:

```
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 for a smaller cost to router B
router ospf
 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 Router 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

!Configure the OSPF routing protocol
router ospf
 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 Router C:

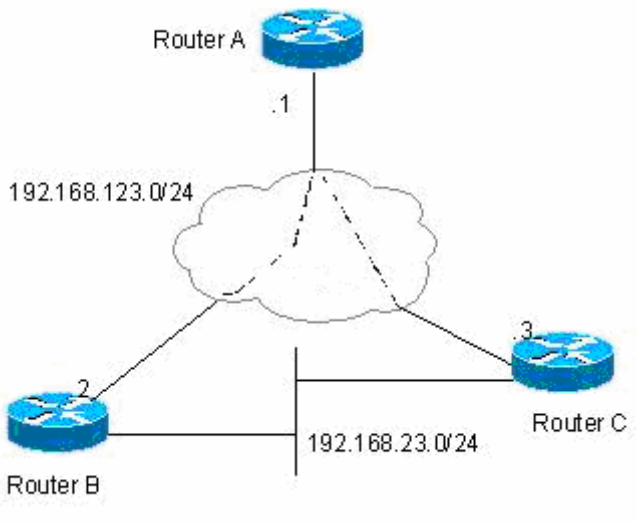
```
!Configure the WAN port
interface Serial 1/0
 ip address 192.168.123.3 255.255.255.0
 encapsulation frame-relay
 ip ospf network non-broadcast

!Configure the OSPF routing protocol
router ospf
 network 192.168.123.0 0.0.0.255 area 0
 neighbor 192.168.123.1 10
 neighbor 192.168.123.2 5
```

9.4.4.2 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 1-5 shows the IP address allocation and connection of the equipment.

Figure 1-7 Example of Configuring the OSPF Point-to-Multipoint Network Type



Requirements: The point-to-multipoint network should be configured among routers A, B, and C.

- **Configuration of the 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 Router A:

```
!Configure the Ethernet port
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
network 192.168.23.0 0.0.0.255 area 0
 network 192.168.123.0 0.0.0.255 area 0
```

Configuration of Router B:

```
!Configure the Ethernet port
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

!Configure the OSPF routing protocol
router ospf
network 192.168.23.0 0.0.0.255 area 0
 network 192.168.123.0 0.0.0.255 area 0
```

Configuration of Router C:

```
!Configure the Ethernet port
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

!Configure the OSPF routing protocol
router ospf
```

```
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.

You can configure the following commands at router A:

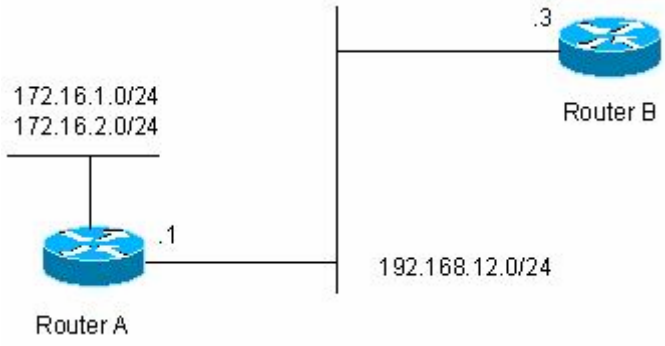
```
router os
 neighbor 192.168.123.2 cost 100
 neighbor 192.168.123.3 cost 200
```

9.4.4.3 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. Figure 1-6 shows the connection between the routers and the IP address allocation.

Figure 1-8 Example of configuring OSPF authentication



- **Configuration of the 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 the authentication methods of both the area and interface have been configured, that of the interface shall apply.

Configuration of Router A:

```
!Configure the Ethernet port
interface FastEthernet0/0
 ip address 192.168.12.1 255.255.255.0
 ip ospf message-digest-key 1 md5 hello

!Configure the OSPF routing protocol
router ospf
```

```
 network 192.168.12.0 0.0.0.255 area 0
 area 0 authentication message-digest
```

Configuration of Router B:

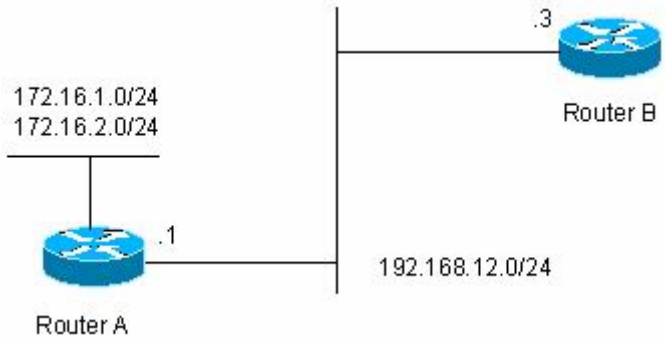
```
!Configure the Ethernet port
interface FastEthernet0/0
 ip address 192.168.12.2 255.255.255.0
 ip ospf message-digest-key 1 md5 hello

!Configure the OSPF routing protocol
router ospf
 network 192.168.12.0 0.0.0.255 area 0
 area 0 authentication message-digest
```

9.4.4.4 Example of configuring route summary

- **Configuration requirements:**

The two routers are connected via Ethernet. Figure 1-7 shows the IP address allocation and connection of the equipment.

Figure 1-9 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.

- **Configuration of the 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 Router A:

```
!Configure the Ethernet port
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

!Configure the OSPF routing protocol
router ospf
 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 Router A:

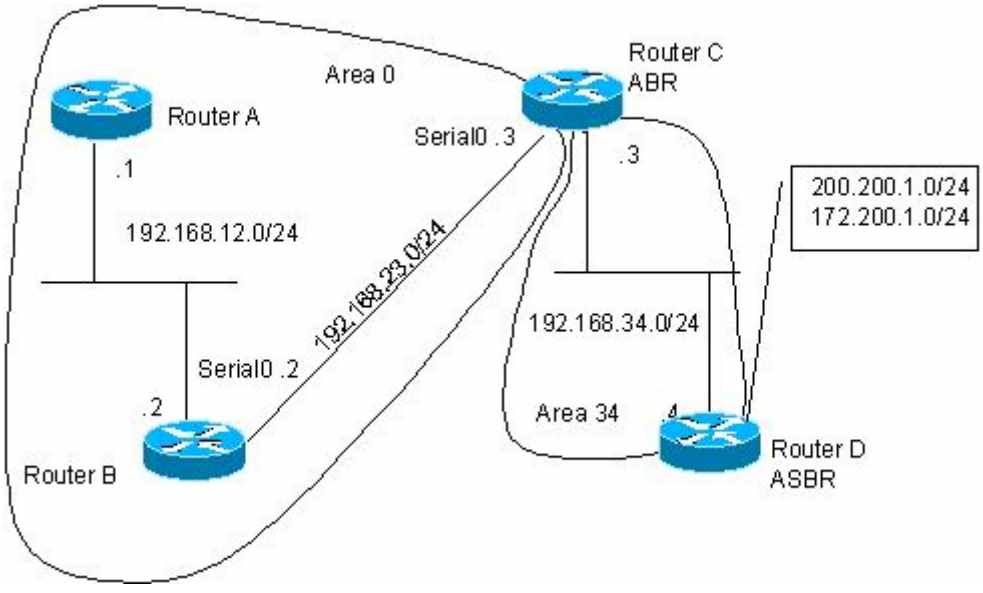
```
!Configure the Ethernet port
interface FastEthernet0/0
 ip address 192.168.12.2 255.255.255.0

!Configure the OSPF routing protocol
router ospf
 network 192.168.12.0 0.0.0.255 area 0
```

9.4.4.5 Example of configuring OSPF ABR and ASBR

- **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 1-8 shows the IP address allocation and connection of the equipment.

Figure 1-10 Example of configuring OSPF ABR and ASBR



As shown in the diagram, routers A and B are within the area, while router C is an ABR, and router D is an ASBR. 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.

■ **Configuration of the 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 Router A:

```
!Configure the Ethernet port
interface FastEthernet0/0
 ip address 192.168.12.1 255.255.255.0

!!Configure the OSPF routing protocol
router ospf
 network 192.168.12.0 0.0.0.255 area 0
```

Configuration of Router B:

```
!Configure the Ethernet port
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

!Configure the OSPF routing protocol
router ospf
 network 192.168.12.0 0.0.0.255 area 0
 network 192.168.23.0 0.0.0.255 area 0
```

Configuration of Router C:

```
!Configure the Ethernet port
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

!Configure the OSPF routing protocol
router ospf
 network 192.168.23.0 0.0.0.255 area 0
 network 192.168.34.0 0.0.0.255 area 34
```

Configuration of Router D:

```
!Configure the Ethernet port
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
 network 192.168.34.0 0.0.0.255 area 34
 redistribute rip metric-type 1 subnets tag 34

!Configure the 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”.

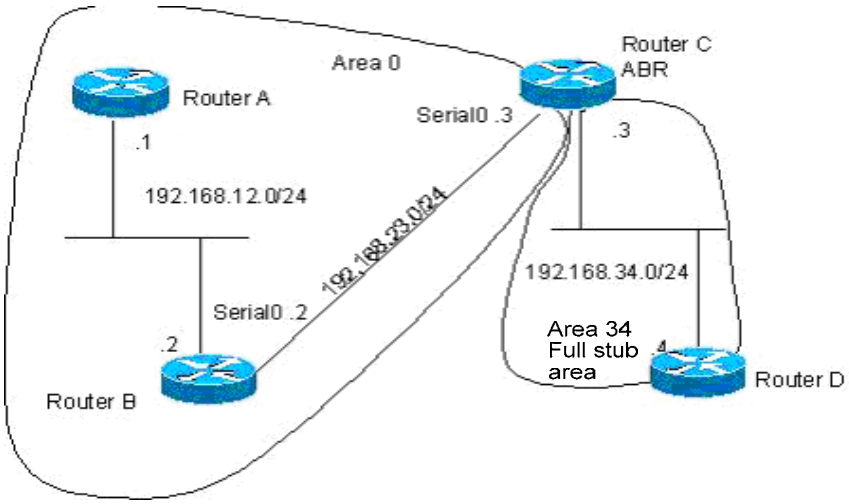
```
RouterB#show ip ospf database

     OSPF Router 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#
```

9.4.4.6 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 1-9 shows the IP address allocation and connection of the equipment.

Figure 1-11 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.

■ **Configuration of the 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. To see the inter-area routes on router D, router C advertises a 192.168.30.0/24 network.

Configuration of Router A:

```
!Configure the Ethernet port
interface FastEthernet0/0
 ip address 192.168.12.1 255.255.255.0

!Configure the OSPF routing protocol
router ospf
 network 192.168.12.0 0.0.0.255 area 0
```

Configuration of Router B:

```
!Configure the Ethernet port
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
```

```
!Configure the OSPF routing protocol
router ospf
 network 192.168.12.0 0.0.0.255 area 0
 network 192.168.23.0 0.0.0.255 area 0
```

Configuration of Router C:

```
!Configure the Ethernet port
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

!Configure the OSPF routing protocol
router ospf
 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 Router D:

```
!Configure the Ethernet port
interface FastEthernet0/0
 ip address 192.168.34.4 255.255.255.0

!Configure the OSPF routing protocol
router ospf
 network 192.168.34.0 0.0.0.255 area 34
 area 34 stub
```

On Router D, you can see the routes generated by the OSPF:

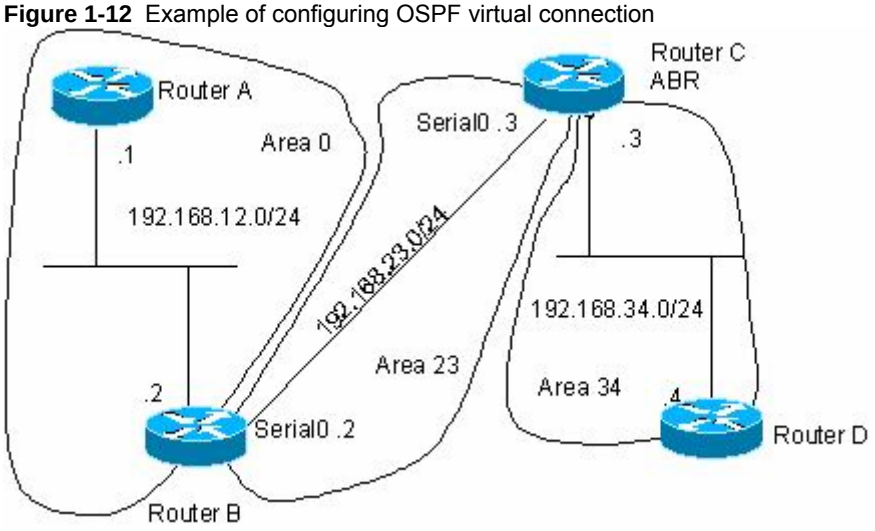
```
O 192.168.30.0/24 [110/1786] via 192.168.34.3, 00:00:03, FastEthernet0/0
O*IA 0.0.0.0/0 [110/2] via 192.168.34.3, 00:00:03, FastEthernet0/0
```

9.4.4.7 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 1-10 shows the IP address allocation and connection of the equipment.

Figure 1-12 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.

- **Configuration of the 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.

Configuration of Router A:

```
!Configure the Ethernet port
interface FastEthernet0/0
 ip address 192.168.12.1 255.255.255.0

!Configure the OSPF routing protocol
router ospf
 network 192.168.12.0 0.0.0.255 area 0
```

Configuration of Router B:

```
!Configure the Ethernet port
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 as the OSPF router ID
interface Loopback2
 ip address 2.2.2.2 255.255.255.0

!Configure the OSPF routing protocol
router ospf
 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 Router C:

```
!Configure the Ethernet port
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 as the OSPF router ID
interface Loopback2
 ip address 3.3.3.3 255.255.255.0

!Configure the OSPF routing protocol
router ospf
 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 Router D:

```
!Configure the Ethernet port
interface FastEthernet0/0
 ip address 192.168.34.4 255.255.255.0

!Configure the OSPF routing protocol
router ospf
 network 192.168.34.0 0.0.0.255 area 34
```

On Router D, you can see the routes generated by the OSPF:

```
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
```

9.5 Protocol-Independent Configuration

This chapter describes how to configure the “protocol-independent” features for IP routing.

9.5.1 Use of VLSMs

The RIPv2, EIGRP, OSPF, and static routing all support the Variable Length Subnet Mask (VLSM). The VLSM can be used to allocate different natural networks for different interfaces on a router, and the interfaces can have diversified subnet masks. The use of the VLSM will undoubtedly save the network address resources, but this also poses some difficulty and challenges for the network administrator to allocate IP addresses.

For the details about the VLSM and how to allocate the addresses, see RFC 1219.

Tip

You must be carefully in determining whether to use the VLSM, since the use of the VLSM increases the possibility of making errors when you allocate addresses and such errors are difficult to detect. If the VLSM is used in the existing network, you should preferably retain the network address as far as possible, and then allocate the IP address so saved to another network.

9.5.2 Configuring Route Redistribution

To support the routers to run multiple routing protocol processes, DES-7200 firmware 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 show the tasks for configuring the route redistribution. The configuration tasks are divided into four parts:

1. Define the redistribution route maps, one of which may consist of many policies. The serial numbers of the policies are in descending order. Once a policy is matched, the execution of the route maps is stopped;
2. Define the matching rules or conditions of each policy of the route map;
3. Define the operation of the router when the policy is matched;
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	Funtion
D-Link(config)**#route-map** *route-map-name* [**permit** | **deny**] *sequence*	Define the route map
D-Link (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
D-Link (config-route-map)**#match interface** *interface-type interface-number*	Match the next-hop interface of the route
D-Link (config-route-map)**#match ip address** *access-list-number […access-list-number]*	Match the address in the access list
D-Link (config-route-map)**#match ip next-hop** *access-list-number […access-list-number]*	Match the next-hop address in the access list
D-Link (config-route-map)**#match ip route-source** *access-list-number […access-list-number]*	Match the route source address in the access list
D-Link (config-route-map)**#match metric** *metric*	Match the metric of the route
D-Link (config-route-map)**#match route-type** {**local** | internal | external [type-1 | type-2]}	Match the type of the route
Route(config-route-map)**#match tag** *tag*	Match the tag of the route

To define the operation after matching, execute the following commands in the route map configuration mode:

Command	Function
D-Link (config-route-map)**#set level** {**stub-area** **| backbone**}	Specify the area of route inputted
D-Link (config-route-map)**#set metric** *metric*	Set the metric for route redistribution
D-Link (config-route-map)**#set metric-type** {**type-1** | **type-2**}	Set the type for route redistribution
D-Link (config-route-map)**#set tag** *tag*	Set the tag for route redistribution
D-Link (config-route-map)**#set next-hop** next-hop	Set the next hop for route redistribution

To redistribute routes from one routing area to another and control route redistribution, execute the following commands in the routing process configuration mode:

Step 1	D-Link (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
Step 2	D-Link (config-router)**#default-metric** *metric*	Set the default metric for all redistributed routes (OSPF RIP)

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.

Tip

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.

If no subnets key words are defined when you configure route redistribution in the OSPF routing process, only the redistribution of the classful routes is supported.

Route redistribution may easily cause loops, so you must be very careful in using them.

9.5.3 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.

9.5.3.1 Preventing Route Update of the Specified Interface

To prevent the routers on the local network from dynamically learn the routing protocol, you can set such that the route update packets cannot be sent from the network interface. Since no route update packets are sent from the router interface, the router connected to the interface cannot learn the route information. This feature can be used on all IGP.

In the OSPF routing area, if the router interface is configured with the route update prevention, the interface becomes a residual network in the OSPF routing area and the interface will neither send nor receive the LSAs. In fact, if the route update prevention is configured for an interface, the interface will not send OSPF and HELLO packets, so the interface does not have neighbors, and it naturally does not exchange routes.

The RIP performs in a way different from the OSPF. After the RIP router interface is configured with the route update prevention, it does not send the route update packets, but can still receive the route update packets. Also, the RIP can only send the update packets to the specified neighbor as defined.

Step 1	Router(config-router)**#passive-interface** *interface-type interface-number*	Prevent the interface from sending update packets
Step 2	Router(config-router)**#neighbor** *ip-address*	Define the neighbor only to which the RIP update packets are sent. This applies to the RIP.

Tip

The residual network is the border network of an interconnected network. If an interconnected network is compared to a tree, the residual network is its top. Every interconnected network has its residual network.

9.5.3.2 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
D-Link (config-router)**#distribute-list** {[*access-list-number* **	** *name]*	**prefix** *prefix-list-name}* **out** [*interface*	*protocol*]	Allow or not allow some LSAs to be sent according to the access list rule.
D-Link (config-router)**#no distribute-list** {[*access-list-number*	*name]*|**prefix** *prefix-list-name}* **out** [*interface*	*protocol*	*process-id*]	Cancel the prevention of the LSA

Tip

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.

9.5.3.3 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
D-Link (config-router)**#distribute-list** {[*access-list-number* | *name]* | **prefix** *prefix-list-name* | **gateway** *prefix-list-name}* **in** [*interface-type interface-number*]	Allow or not allow the reception of the routes specified by route update according to the access list rule.
D-Link (config-router)**#no distribute-list** {[*access-list-number* | *name]* | **prefix** *prefix-list-name* | **gateway** *prefix-list-name}* **in** [*interface-type interface-number*]	Cancel the control over route update processing

9.5.4 Route Authentication Key Management

Key management is a method for controlling the authentication key of the routing protocol. No all protocols need key management. Currently, the key management is only for the authentication key of the RIPv2 routing protocols of DES-7200 firmware.

The key management is actually the process to define the keys in three steps:

1. Define the key chain in the key chain configuration mode;
2. Define the key number in the key configuration mode. One key chain may contain multiple keys, each of which has a key number;
3. Define the key in the key configuration mode to configure the attributes of the key.

You can configure multiple keys in their lifetimes, but only one authentication key sends the authentication packets despite the number of the valid keys. When authentication packets are sent, if there are multiple keys available, DES-7200 will search them in the ascending order. The first valid key will act as the transmission authentication key. When packets are received, if there are multiple keys, DES-7200 searches the key chain in the ascending order and receives the packets if the authentication key is found, or discards them if not found. If multiple keys are configured and different of them must be used in different times, the timers of the routers must be unified by using the time configuration command and Network Timer Protocol (NTP).

To configure key management, execute the following commands in the global configuration mode:

Step 1	D-Link(config)**#key chain** *key-chain-name*	Define the key chain in the key chain configuration mode
Step 2	Router(config-keychain)**#key** *key-id*	Define the key ID in the key configuration mode
Step 3	Router(config-keychain-key)**#key-string** *key-string*	Define the key contents
Step 4	Router(config-keychain-key)**#accept-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*}	Define the accept lifetime of the key
Step 5	Router(config-keychain-key)**#send-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*}	Define the send lifetime of the key


Tip

DES-7200 firmware allows the reception of the packets with different accept key IDs but the same key contents. The implementation of the software of some manufacturers may do not allow the reception of the authentication packets of this type. You must pay attention to this problem when the equipment is interconnected with the equipment of other manufacturers.

9.5.5 Monitoring and Maintaining IP Networks

You can delete all the contents of some particular buffers, tables, and databases and show the specified network status. The monitoring and maintenance of the IP network include two parts:

1. Clear the IP routing table;
2. Show the system and network statistics.

9.5.5.2 Clearing IP Routing Table

The update of the routing table is automatically maintained by the routing protocol. However, you may feel that the routing table contains invalid routes or some special configuration requires the execution of this action to reflect the latest changes. In this case, you need to manually clear the routing table to refresh it.

To clear the routing table, execute the following commands in the command execution mode:

Command	Function
D-Link**#clear ip route** {*network* [*mask*] | *}	Clear the routing table


Note

You must be very careful when you clear the IP routing table, since this may cause temporary network interruption. Do not clear all the routes if you can achieve the same purpose by clearing some of the routes.

9.5.5.3 Showing System and Network Statistics

You can show the contents of the IP routing table, buffer, and database. Such information is very helpful in troubleshooting the network. By showing the reachability of the local equipment network, you can know the path to which the packets are sent after they leave the equipment.

To show the system and network statistics, execute the following commands in the command execution mode:

Command	Function
D-Link**#show ip route** [*network* [*mask*]]	Show the current status of the IP routing table
D-Link**#show key chain** *key-chain-name*	Show the key chain
D-Link**#show route-map** *route-map-name*	Show all or the specified route maps

9.5.6 Configuration Examples

This section provides three protocol-independent configuration examples:

- Example of configuring route redistribution
- Example of configuring RIP&OSPF redistribution
- Example of configuring the route map

9.5.6.1 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.

- **Specific configuration**

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.

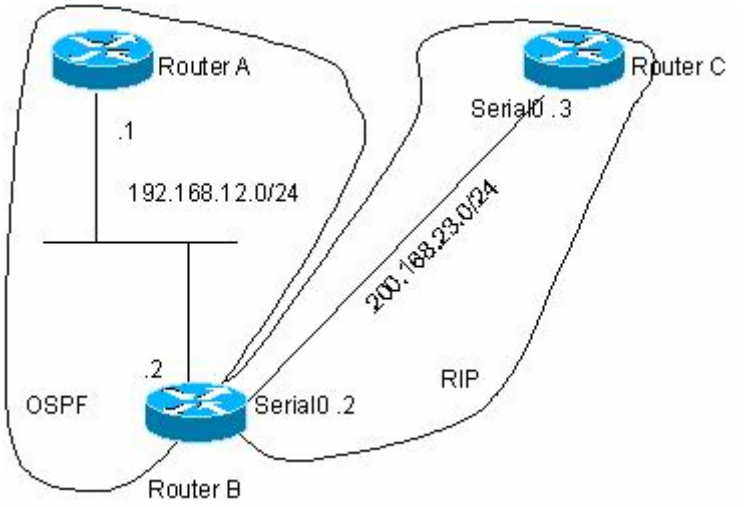
```
ip route 172.16.1.0 255.255.255.0 172.200.1.2
ip route 192.168.1.0 255.255.255.0 172.200.1.2
ip route 192.168.2.0 255.255.255.0 172.200.1.4
!
 router rip
 version 2
 redistribute static
 network 192.168.34.0
 distribute-list 10 out static
 no auto-summary
!
access-list 10 permit 192.168.1.0
access-list 10 permit 172.16.1.0
```

9.5.6.2 Example of configuring RIP&OSPF redistribution

- **Configuration requirements:**

There are three routers. Figure 1-11 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 1-13 Example of configuring 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.

■ Specific configuration

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:

```
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 no ip directed-broadcast
!
interface loopback 1
ip address 192.168.100.1 255.255.255.0
no ip directed-broadcast
!
interface FastEthernet0/1
ip address 192.168.12.55 255.255.255.0
!
router ospf
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.12.0 0.0.0.255 area 0
 network 192.168.100.0 0.0.0.255 area 0
```

Configuration of Router B:

```
interface FastEthernet0/0
 mac-address aaaa.aaaa.aabb
 ip address 192.168.12.5 255.255.255.0
!
interface Serial1/0
ip address 200.168.23.2 255.255.255.0
```

```
encapsulation ppp
!Configure OSPF and set the redistribution route type
router ospf
  redistribute rip metric 100 metric-type 1 subnets
  network 192.168.12.0 0.0.0.255 area 0
!Configure the RIP and use the distribute list to filter the redistributed routes
router rip
 redistribute ospf metric 2
 network 200.168.23.0
 distribute-list 10 out ospf
 no auto-summary
!Define the access list
access-list 10 permit 192.168.10.0
```

Configuration of Router C:

```
interface 0/0
 ip address 200.168.30.1 255.255.255.0
!
interface FastEthernet 0/1
 ip address 200.168.3.1 255.255.255.0
!
interface Serial1/0
 ip address 200.168.23.3 255.255.255.0
 encapsulation ppp
 timer rate 64000
!
router rip
 network 200.168.23.0
 network 200.168.3.0
 network 200.168.30.0
```

OSPF routes seen 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 seen by Router C:

```
R    192.168.10.0/24 [120/2] via 200.168.23.2, 00:00:00, Serial1/0
```

9.5.6.3 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.

```
router ospf
 redistribute rip subnets route-map redrip
 network 192.168.12.0 0.0.0.255 area 0
!
access-list 10 permit 200.168.23.0
```

```
!
route-map redrip permit 10
 match metric 4
 set metric 40
 set metric-type type-1
 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.

```
router rip
 version 2
 redistribute ospf route-map redospf
 network 200.168.23.0
!
route-map redospf permit 10
 match tag 10
 set metric 10
!
```

9.5.6.4 Example of Configuring Key Management

Authentication key management is to configure and maintain the key chain, for which multiple keys can be configured. The keys are arranged in the sequence of their serial numbers in the key chain. When the routing protocols send packets by using the key chain, they will search the key chain in the ascending order of the serial numbers until a valid key is found. When the packets received need authentication, the key will be compared and the authentication is successful as long as the key is found in the key chain.

By defining the key lifetime, you can allow different keys to be at different alive status at different times. This greatly improves the authentication security. A key has two lifetimes: 1) Send lifetime: Only the keys alive in this lifetime can be used as the send keys; 2) Accept lifetime: Only the keys alive in this lifetime can be used to authenticate the received packets.

In the following configuration example, the key chain ripkey defines three keys. The send lifetime of the first key is from 8:00, January 1, 2003 to 12:00, January 1, 2004. The accept lifetime of the second key is from 11:00, January 1, 2004 to 12:00, January 1, 2005. The third key is always in the accept and send alive status.

```
key chain ripkey
 key 1
  key-string morning
  accept-lifetime 08:00:00 Jan 1 2003 12:00:00 Jan 1 2004
  send-lifetime   08:00:00 Jan 1 2003 12:00:00 Jan 1 2004
 key 2
  key-string afternoon
  accept-lifetime 11:00:00 Jan 1 2004 12:00:00 Jan 1 2005
  send-lifetime   11:00:00 Jan 1 2004 12:00:00 Jan 1 2005
 key 3
  key-string othertime
```

The following is the example for using the key chain ripkey:

```
interface Serial1/0
 ip address 200.168.23.3 255.255.255.0
 ip rip authentication mode md5
 ip rip authentication key-chain ripkey
 encapsulation ppp
```

```
!
router rip
 network 200.168.23.0
!
```

After the above configuration, the RIP routing protocol can authenticate the RIP packets by using different send and accept keys at different times. When DES-7200 firmware authenticates the accept keys, their serial numbers are ignored, only verifying their contents.

9.6 Configuring Policy-Based Routing

9.6.1 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 the policy-based routing for the packets reaching a router interface, execute the following commands in the interface configuration mode:

Command	Function
Router(config-if)**#ip policy route-map** *route-map*	Apply the policy-based routing at the interface


Note

- On DES-7200 10.0, 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 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.
- 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 switch 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.

To configure load-balance or redundancy backup in the policy-based routing, execute the following command in the global configuration mode:

Command	Function
D-Link(config)**#ip policy** [**load-balance|redundance**]	Set the load-balance or redundancy for the policy-based routing

When the policy-based routing executes load-balance, the WCMP supports up to four next hops and the ECMP supports up to 32 next hops.

To configure the default policy-based routing in the policy-based routing, execute the following command in the route-map mode.

Command	Function
set ip default next-hop *ip-address* [*…ip-address*]	Configure the default policy-based routing

When the default policy-based routing is configured, the WCMP supports up to four next hops and the ECMP supports up to 32 next hops.

The related commands in the protocol-independent module:

Command	Function
route-map route-map-name [*permit* | *deny*] [*sequence-number*]	Configure the route map
set ip next-hop ip-address [*...ip-address*]	Set the next hop

Command	Function
match ip address *access-list-name* [*...access-list-number*]	Set the matched nexthop rule
match length	Set the match length rule
set interface *interface-type interface-numbe*r [*...interface-type interface-number*]	Set the egress rule
set default interface *interface-type interface-number* [*...interface-type interface-number*]	Set the default egress rule

9.6.2 Configuration Examples

The policy-based routing does not affect the restriction of the routing table. The policy-based routing can distribute the data in conjunction with the routing table so that different service data are transmitted separately in the WAN lines, for balanced load and higher network resource utilization. As long as policy-based routing is configured properly, the packets can be routed even without the routing table.

In the following configuration, when the Fast Ethernet interface FE0 receives the packets: it sends them to the next-hop gateway for telnet traffic; it sends them to the Fa 0/1 interface for the www traffic if the target network has no matched item in the routing table; it discards them for other traffics, if the target network has not matched item in the routing table.

```
interface FastEthernet 0/0
 ip address 192.168.12.6 255.255.255.0
 ip policy route-map pmap
!
access-list 100 permit tcp any eq telnet any gt 1024
access-list 100 permit tcp any gt 1024 any eq telnet
access-list 101 permit tcp any eq www any gt 1024
access-list 101 permit tcp any gt 1024 any eq www
!
route-map pmap permit 10
 match ip address 100
 set ip next-hop 192.168.34.2
!
route-map pmap permit 20
 match ip address 101
 set default interface FastEthernet 0/1
!
route-map pmap permit 30
 set default interface Null0
```

10 IP Addressing and Services Configuration

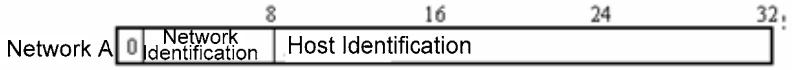
10.1 IP Addressing Configuration

10.1.1 IP Address Overview

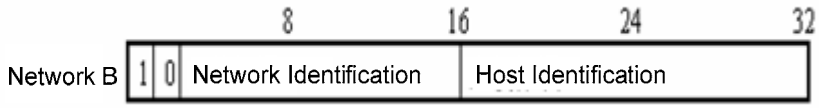
IP address is made up of 32 binary bits and expressed in dotted decimal format for the convenience of writing and describing. When expressed in decimal format, the 32 binary bits are broken into four octets (1 octet = 8 bits). Each octet is separated by a period (dot) in range from 0 to 255(for example, 192.168.1.1).

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.

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.

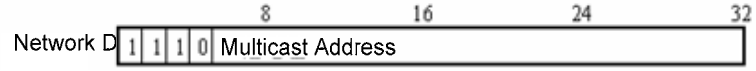


Cass B, has a 14-bit network number and a 16-bit local address. The two highest-order bits are set to 1-0. This allows 16,384 class B networks.



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.



Tip

No addresses are allowed with the four highest-order bits set to 1-1-1-1. 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	0.0.0.0	Reserved
	1.0.0.0~126.0.0.0	Available
	127.0.0.0	Reserved
Class B	128.0.0.0~191.254.0.0	Available
	191.255.0.0	Reserved
Class C	192.0.0.0	Reserved
	192.0.1.0~223.255.254.0	Available
	223.255.255.0	Reserved
Class D	224.0.0.0~239.255.255.255	Available
Class E	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	10.0.0.0~10.255.255.255	1 Class A network
Class B	172.16.0.0~172.31.255.255	16 Class B networks
Class C	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.

10.1.2 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 (Optional)
- Configuring IP address mapping to WAN Address (Optional)
- Disabling IP routing (Optional)
- Configuring Broadcast Packet Handling (Optional)

10.1.2.1 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
D-Link(config-if)# **ip address** *ip-address mask* D-Link(config-if)# **ip address** *ip-address mask*	Set an IP address for an interface.
D-Link(config-if)# **no ip address** D-Link(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.

Tip

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

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. When hosts are more than 254 on a LAN, it is necessary to assign one more Class C network address to the subnet. By this way, the router will be connected to two subnet and you need to configure multiple IP addresses on the router.
- 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.
- 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.

Tip

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 other routers has not been configured 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
D-Link(config-if)# **ip address** *ip-address mask* **secondary** D-Link(config-if)# **ip address** *ip-address mask* **secondary**	Set secondary IP addresses to a network interface.
D-Link(config-if)# **no ip address** *ip-address mask* **secondary** D-Link(config-if)# **no ip address** *ip-address mask* **secondary**	Disable secondary IP addresses on a network interface.

10.1.2.2 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. 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 router. 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

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.

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

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

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.

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.

To configure ARP timeout, use the following command at interface configuration mode:

Command	Function
D-Link(config-if)# **arp timeout** *seconds* D-Link(config-if)# **arp timeout** *seconds*	Configure ARPtimeout.
D-Link(config-if)# **no arp timeout** D-Link(config-if)# **no arp timeout**	Restore to default configuration

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

10.1.2.3 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.

To disable IP routing, use the following commands at global configuration mode:

Command	Function
D-Link(config)# **no ip routing** D-Link(config)# **no ip routing**	Disable IP routing.
D-Link(config)# **ip routing** D-Link(config)# **ip routing**	Enable IP routing

10.1.2.4 Configuring Broadcast Packets Handling

A broadcast packet is a data packet destined for all hosts on a particular physical network. DES-7200 firmware 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.

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

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.

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.

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 configuration 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 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
D-Link(config-if)# **ip directed-broadcast** [*access-list-number*] D-Link(config-if)# **ip directed-broadcast** [*access-list-number*]	Enable directed broadcast to physical broadcast translation on an interface.
D-Link(config-if)# no ip directed-broadcast D-Link(config-if)# no ip directed-broadcast	Disable the translation

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
D-Link(config-if)# **ip broadcast-address** *ip-address* D-Link(config-if)# **ip broadcast-address** *ip-address*	Create a new broadcast address
D-Link(config-if)# no ip broadcast-address D-Link(config-if)# no ip broadcast-address	Disable a new broadcast address

10.1.3 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

10.1.3.1 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
D-Link# clear arp-cache D-Link# clear arp-cache	Clear the ARP cache.
D-Link# **clear ip route** {*network* [*mask*] | *}clear ip route {*network* [*mask*]|*}	Clear IP routing table

10.1.3.2 Displaying System and Network Status

You can display all the contents of IP routing tables, caches, and databases, which is helpful to solve network problems. You also can display information about node reachability 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
D-Link# **show arp** D-Link# **show arp**	Display the ARP table.
D-Link# show ip arp D-Link# show ip arp	Display the IP ARP cache.
D-Link# **show ip interface** [interface-type interface-number] D-Link# **show ip interface** [interface-type interface-number]	Show the interface information.
D-Link# **show ip route** [*network* [*mask*]] D-Link# **show ip route** [*network* [*mask*]]	Display the routing table

Command	Function
D-Link#show ip route D-Link#show ip route	Display the current state of the routing table in summary form.
D-Link# **ping** *ip-address* [**length** bytes] [**ntimes** *times*] [**timeout** *seconds*] D-Link# **ping** *ip-address* [**length** bytes] [**ntimes** *times*] [**timeout** *seconds*]	Test network node reachability.

10.1.4 IP Addressing Configuration Examples

It provides some IP addressing configuration examples as follow in this chapter:

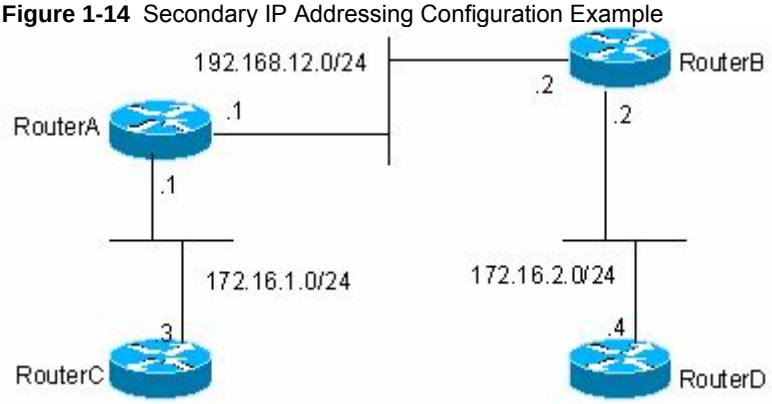
Secondary IP addressing configuration example

10.1.4.1 Secondary IP Addressing Configuration Example

- **Configuration Requirement**

It is shown the IP addresses allocation and network connections as following Figure1-2.

Figure 1-14 Secondary IP Addressing 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.

- **Detailed Configuration on 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 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.

Router A Configuration:

```
interface FastEthernet0/0
 ip address 172.16.3.1 255.255.255.0 secondary
 ip address 192.168.12.1 255.255.255.0
!
interface FastEthernet0/1
 ip address 172.16.1.1 255.255.255.0
```

```
!
router rip
 network 172.16.0.0
 network 192.168.12.0
```

Router B Configuration:

```
interface FastEthernet0/0
 ip address 172.16.3.2 255.255.255.0 secondary
 ip address 192.168.12.2 255.255.255.0
!
interface FastEthernet0/1
 ip address 172.16.2.1 255.255.255.0
!
router rip
 network 172.16.0.0
 network 192.168.12.0
```

10.2 IP Service Configuration

10.2.1 IP Services Configuration Task List

IP service configuration includes the following tasks which are all optional, you can perform them according to the network requirement:

Managing IP Connections

10.2.2 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. ICMP messages are sent by routers or access servers to hosts or other routers when a network problem is discovered. 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

10.2.2.1 Enabling ICMP Protocol Unreachable Messages

If the router receives a nonbroadcast packet destined for itself that uses an unknown protocol, it sends an ICMP protocol unreachable message back to the source. 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
D-Link(config-if)**# ip unreachables** D-Link(config-if)**# ip unreachables**	Enable the sending of ICMP protocol unreachable and host unreachable messages.
D-Link(config-if)**# no ip unreachables** D-Link(config-if)**# no ip unreachables**	Disable the sending of ICMP protocol unreachable and host unreachable messages.

10.2.2.2 Enabling ICMP Redirect Messages

Routes are sometimes less than optimal. For example, it is possible for the router to be forced to resend a packet through the same interface on which it was received. If the router resends a packet through the same interface on which it was received, it sends an ICMP redirect message to the originator of the packet telling the originator that the router is on a subnet directly connected to the receiving device, and that it must forward the packet to another system on 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
D-Link(config-if)**# ip redirects**D-Link(config-if)**# ip redirects**	Enable the sending of ICMP redirect messages. It is enabled by default.
D-Link(config-if)**# no ip redirects** D-Link(config-if)**# no ip redirects**	Disable the sending of ICMP redirect messages.

10.2.2.3 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
D-Link(config-if)**# ip mask-reply** D-Link(config-if)**# ip mask-reply**	Enable the sending of ICMP mask reply messages.
D-Link(config-if)**# no ip mask-reply** D-Link(config-if)**# no ip mask-reply**	Disable the sending of ICMP mask reply messages.

10.2.2.4 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 devices on a physical network must have the same protocol MTU.

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

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

10.2.2.5 Configuring IP Source Routing

DES-7200 supports IP source routing. The router 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
D-Link(config)# **ip source-route** D-Link(config)# **ip source-route**	Enable IP source routing
D-Link(config)# no ip source-route D-Link(config)# no ip source-route	Disable IP surce routing

Note that you have to use trap ip option packet to tell hardware to send option packet to software due to the hardware core restriction on DES-7200 serial switch.

11 Configuring IPv6

11.1 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**

11.1.1 IPv6 Address Format

The basic format of an IPv6 address is X : X : X : X : X : X : X : X, where X is a 4 hex integers (16 bits). Each digit contains 4 bits of information, each integer contains 4 hex digits and each address contains 8 integers, so it is total for 128 bits. Some legal IPv6 addresses are as follows:

```
2001:ABCD:1234:5678:AAAA:BBBB:1200:2100
800 : 0 : 0 :0 : 0 : 0 : 0 : 1
1080 : 0 : 0 : 0 : 8 : 800 : 200C : 417A
```

These integers are hex integers, where A to F denotes the 10 to 15 respectively. Each integer in the address must be denoted and the starting 0 need not be denoted. Some IPv6 address may contain a series of 0 (such as the example 2 and 3). Once this condition occurs, the ": :" is allowed to denote this series of 0. Namely, the address

```
800 : 0 : 0 : 0 : 0 : 0 : 0 : 1
```

can be denoted as:

```
800 :: 1
```

These two colons denote that this address can be extended to the complete 128-bit address. In this way, the 16-bit group can be replaced with two colons only when they are all 0 and the two colons can only present for one time.

In the mixture environment of IPv4 and IPv6, there is a mixture denotation method.The lowest 32 bits in an IPv6 address can be used to denote an IPv4 address. The address can be expressed in a mixture mode, i.e., X: X : X : X : X : d . d . d . d. Where, the X denotes a 16-bit integer, while d denotes a 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 . 10 . 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.

11.1.2 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:

11.1.2.1 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:

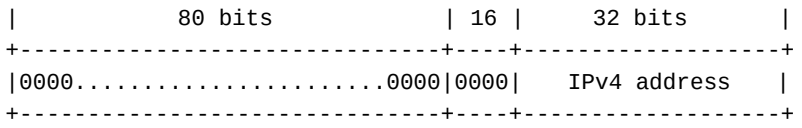
```
|   10     |
|  bits    |       38 bits           |         64 bits             |
+----------+-------------------------+-----------------------------+
|1111111011|    0     | subnet ID    |         interface ID        |
+----------+----------+--------------+-----------------------------+
```

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.

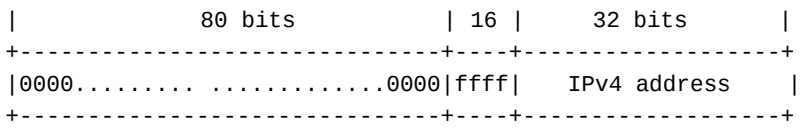
4. IPv4 Addresses-embedded IPv6 Addresses

The RFC2373 also defines 2 types of special IPv6 addresses embedded with IPv4 addresses:

- IPv4-compatible IPv6 address



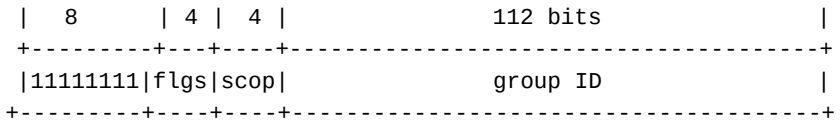
- IPv4-mapped IPv6 address



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.

11.1.2.2 Multicast Addresses

The format of the IPv6 multicast address is shown as follows:



- 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 multicase 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 is 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:FF**21:1234,**

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:

IPv6 Unicast or Anycast Address

prefix		Interface ID		
Multicast address of the corresponding requested node				←24 bits→
FF02	0	1	FF	Lower 24

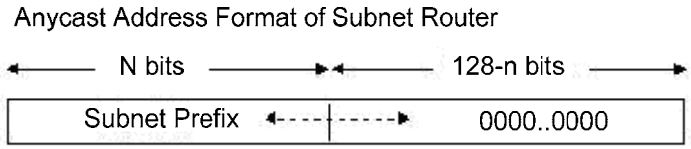
11.1.2.3 Anycast Addresses

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 packet 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.

Note 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.

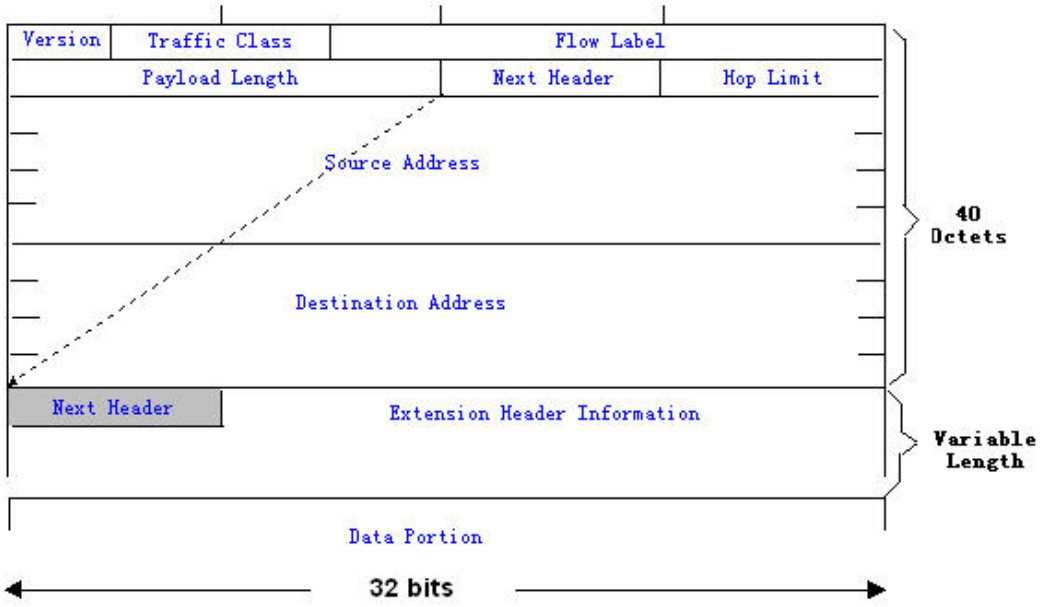
The RFC2373 predefines an anycast address, referred to as the anycast address of the subnet router. The following diagram shows the anycast address format of the subnet router, which consists of the subnet prefix followed by a series of 0 (as the interface identifier).

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.



11.1.3 IPv6 Packet Header Structure

- The format of the IPv6 packet header is shown as the figure below:



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 defines the following fields:

- Version :

The length is 4 bits. For IPv6, the field must be 6.

- Class (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 (Flow Label):

- 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 (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 (Next Header):

This field indicatesthe 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 indicates whether an IPv6 extended header exists.

- Hop Limit (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 reciever address of an IPv6 packet.

At present, the following extended header is defined for the IPv6:

- Hop-by-Hop Options (Hop-by-Hop Options):

This extended header must directly follow an IPv6 header. It contains the option data that must be checked by each nodes 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 node 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 corresponding 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 extented 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 tranfer 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.

11.1.4 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.

Note

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.

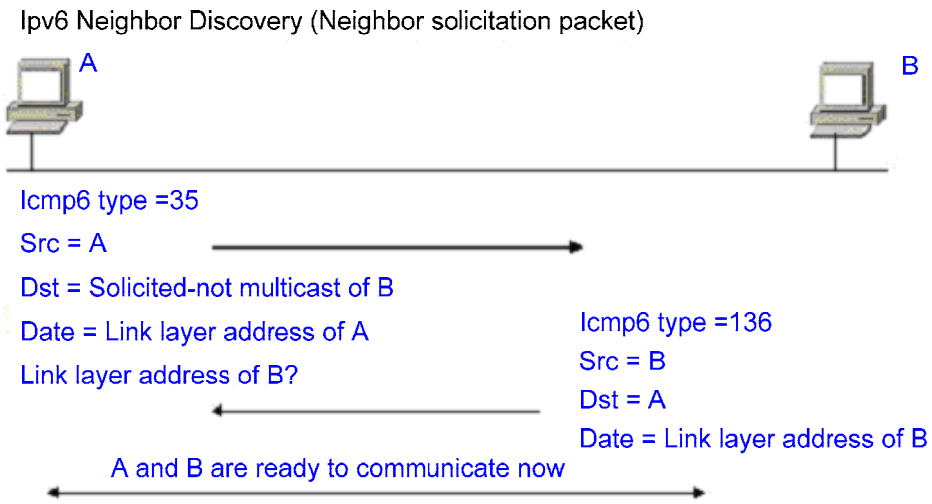
11.1.5 IPv6 Neighbor Discovery

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.

11.1.5.1 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 destionation 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:



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.

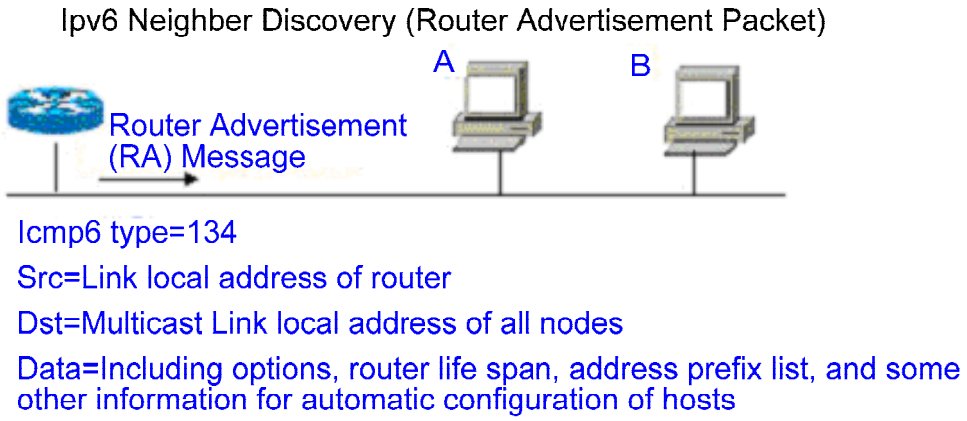
When one neighbor is considered that the reachable time is expired, should enable the Neighbor Unreachability Detection (NUD), which will occur only when it is necessary to send the unicast message to this neighbor. The NUD will not be enabled for the multicast message transmission.

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 (: : }.

11.1.5.2 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:



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.


Note

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.


Note

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.

11.2 IPv6 Configuration

The following will introduce the configuration of various function modules of the IPv6 respectively:

11.2.1 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.


Note

Once the interface of the IPv6 is created and the link of this interface is in the UP status, the system will generate. At present, the IPv6 doesn't support the configuration of the anycast address.

The configuration procedure of the IPv6 address is shown as follows:

Step 1	**configure terminal**	Enter the global configuration mode.
Step 2	**interface** *interface-id*	Enter the interface configuration mode.
Step 3	**ipv6 enable**	Enable the IPv6 protocol for an interface.If this command is not run, then the system automatically enable the IPv6 protocol when you configure an IPv6 address for an interface.

Step 4	**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-l 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.
Step 5	**End**	Return to the privilege mode.
Step 6	**show ipv6 interface vlan 1**	View the information related to the ipv6 interface.
Step 7	**copy running-config tartup-config**	Save the configuration.

Use the no ipv6 address *ipv6-prefixIprefix-length* command to delete the configured address. The following is an example of the configuration of the IPv6 address:

```
switch(config)# interface vlan 1
switch (config-if)# ipv6 enable
switch (config-if)# ipv6 address fec0:0:0:1::1/64
switch (config-if)# end
switch (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
```

11.2.2 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, and

The destination address of the message is not the router itself, and

The output interface of the next hop determined by the router for this message is the same as the interface this message received, namely, the next hop and the originator is of the same link, and

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 router.

Note

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:

Step 1	configure terminal	Enter the global configuration mode.
Step 2	interface vlan 1	Enter the SVI 1 interface configuration mode.
Step 3	ipv6 redirects	Open the IPv6 redirection function of this interface.
Step 4	End	Return to the privilege mode.
Step 5	show ipv6 interface vlan 1	View the information related to the interface configuration.
Step 6	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:

```
switch(config)# interface vlan 1
switch (config-if)# ipv6 redirects
switch (config-if)# end
switch # 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
```

11.2.3 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.

The following is the procedure to configure a static neighbor:

Step 1	configure terminal	Enter the global configuration mode.
Step 2	ipv6 neighbor *ipv6-address interface-id hardware-address*	Use this command to configure a static neighbor on this interface.
Step 3	end	Return to the privilege mode.
Step 4	show ipv6 neighbors	View the neighbor list.
Step 5	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:

```
switch(config)# ipv6 neighbor fec0:0:0:1::100 vlan 1 00d0.f811.1234
switch (config)# end
switch # 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
```

11.2.4 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:

Step 1	**configure terminal**	Enter the global configuration mode.
Step 2	**interface vlan** 1	Enter the configuration mode of the SVI 1.

Step 3	**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.
Step 4	**end**	Return to the privilege mode.
Step 5	show ipv6 interface vlan 1	View the IPv6 information of the SVI 1.
Step 6	**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:

```
switch(config)# interface vlan 1
switch (config-if)# ipv6 nd dad attempts 3
switch (config-if)#end
switch#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
```

11.2.5 Configuring Other Interface Parameters of Routers

The configuration parameters of the IPv6 in the interface of the routers is mainly comprised of 2 part, 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:

Step 1	configure terminal	Enter the global configuration mode.

Step 2	interface *interface-id*	Enter the interface configuration mode.
Step 3	ipv6 enable	Enalbe the IPv6 function.
Step 4	ipv6 nd ns-interval *milliseconds*	(Optional) Define the retransmission interval of the neighbor solicitation message.
Step 5	ipv6 nd reachable-time *milliseconds*	(Optional) Define the time when the neighbor is considered to be reacheable.
Step 6	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.
Step 7	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.
Step2	ipv6 nd ra-interval *seconds*	(Optional) Set the time interval for the router to send the router advertisement (RA) message periodically.
Step2	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).
Step2	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).
Step2	ipv6 nd suppress-ra	(Optional) Set whether suppress the router advertisement (RA) message in this interface.
Step2	end	Return to the privilege mode.
Step2	show ipv6 interface [*interface-id*] [ra-info]	Show the ipv6 interface of the interface or the information sent by this interface.
Step2	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*.

11.3 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.

```
switch#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

```
switch#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)

View the neighbor table information of the IPv6.
switch#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
```

12 Configuring IPv6 Tunnels

12.1 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 problem 1. The solution to problem2 is NAT-PT (Network Address Translation-Protocol Translation), which is not covered in this article.

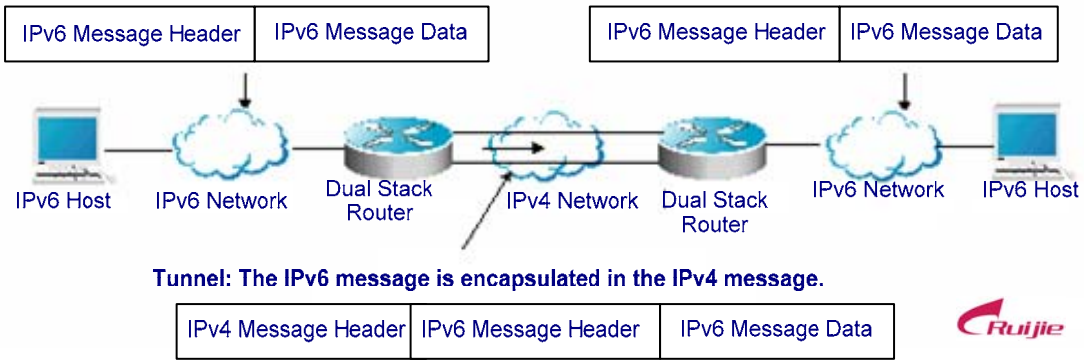
The IPv6 tunnel technology encapsulates IPv6 messages in IPv4 messages. In this way, IPv6 protocol packets can commuicate with each other via IPv4 networks. Therefore, with the IPv6 tunnel technology, isolated IPv6 networks can commuicate with each other via existing IPv4 networks, avoiding any modificaton 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

Note

The structure formed by connecting isolated IPv6 networks with the IPv6 tunnel technology is not the final network architecture of the IPv6. The technology is only for transition.

The model to use the tunnel technology is shown in the following figure:



The features of various tunnels are respectively introduced below.

12.1.2 Manually Configured Tunnel (IPv6 Manually Configured Tunnel)

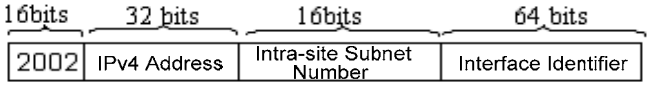
One manually configured tunnel is similar to one permanent link set up between two IPv6 domains via the backbone network of the IPv4.It is applicable for the relatively fixed connections that have a higher demand on security between two Area Border Routers or betwwn an Area Border Router and a host.

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.

12.1.3 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:



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 end 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 (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


Note

The IPv4 address embedded in the 6to4 address cannot be a private IPv4 address (i.e., the adderss 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 applicaton 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.

12.1.4 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.

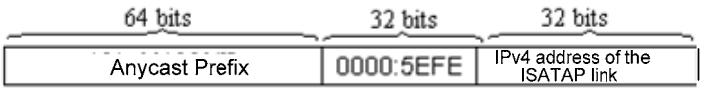
It is very possible that ISATAP is used with other transition technologies. Especially when used with the 6to4 tunnel technlogy, it can make the dual stack host of an internal network access an IPv6 backbone network very easily.

- 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:



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

12.2 IPv6 Tunnel Configuration

12.2.1 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, cofigure 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).

Note Be sure not to configure a manual tunnel with a same address as tunnel source and tunnel destination addresses on a switch.

Brief steps

1. config terminal
2. interface tunnel *tunnel-num*
3. tunnel mode ipv6ip
4. ipv6 enable
5. tunnel source {ip-address|type num}
6. tunnel destination *ip-address*
7. end

Detailed steps

Step1	configure terminal	Enter the global configuration mode.
Step2	interface tunnel *tunnel-num*	Specify a tunnel interface number to create a tunnel interface and enter the interface configuration mode.
Step3	tunnel mode ipv6ip	Specify that the type of a tunnel is the menually configured

		tunnel.
Step4	ipv6 enable	Enable the IPv6 function of the interface. You can also configure the IPv6 address to directly enalbe the IPv6 function of the interface.
Step5	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.
Step2	tunnel destination *ip-address*	Specify the destination address of a tunnel.
Step2	end	Return to the privilege mode.
Step2	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.

12.2.2 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.

Note

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

1. config terminal
2. interface tunnel *tunnel-num*
3. tunnel mode ipv6ip 6to4
4. ipv6 enable
5. tunnel source {ip-address|type num}
6. exit
7. ipv6 route 2002::/16 tunnel tunnel-number
8. end

Detailed steps

Step 1	**configure terminal**	Enter the global configuration mode.
Step 2	**interface tunnel** tunnel-num	Specify a tunnel interface number to create a tunnel interface and enter the interface configuration mode.
Step 3	**tunnel mode ipv6ip 6to4**	Specify that the type of a tunnel is the 6to4 tunnel.
Step 4	**ipv6 enable**	Enable the IPv6 function of the interface. You can also configure the IPv6 address to directly enalbe the IPv6 function of the interface.

Step 5	**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.
Step 6	**exit**	Return to the global configuration mode.
Step 7	**ipv6 route** *2002::/16* **tunnel** *tunnel-number*	Configure a satic 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.
Step 8	**end**	Return to the privilege mode.
Step 9	**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.

12.2.3 Configuring ISATAP Tunnel

This section introduces how to configure an ISATAP router.

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.

Note	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

1. config terminal
2. interface tunnel *tunnel-num*
3. tunnel mode ipv6ip isatap
4. **ipv6 address** *ipv6-prefixIprefix-length* **[eui-64]**
5. tunnel source interface-type num
6. no ipv6 nd suppress-ra
7. end

Detailed steps

Step 1	**configure terminal**	Enter the global configuration mode.
Step 2	**interface tunnel** *tunnel-num*	Specify a tunnel interface number to create a tunnel interface and enter the interface configuration mode.
Step 3	**tunnel mode ipv6ip isatap**	Specify that the type of a tunnel is the ISATAP tunnel.
Step 4	**ipv6 address** *ipv6-prefixIprefix-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.
Step 5	**tunnel source** *type num*	Specify the source interface number referenced by a tunnel. On the referenced interface, the IPv4 address must have been configured.
Step 6	**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.
Step 7	**end**	Return to the privilege mode.
Step 8	**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.

12.3 Verifying IPv6 Tunnel Configuration and Mmonitoring

This section introduces how to verify the configuration and actual running states of an IPv6 tunnel.

Brief steps

1. enable
2. show interface tunnel *number*
3. show ipv6 interface tunnel *mumber*
4. ping protocol destination
5. show ip route
6. show ipv6 route

Detailed steps

Step 1	**enable**	Enter the privilege configuration mode.
Step 2	**show interface tunnel** *tunnel-num*	View the information of a tunnel interface.
Step 3	**show ipv6 interface tunnel** *tunnel-num*	View the IPv6 information of a tunnel interface.
Step 4	**ping protocol destination**	Check the basic connectivity of a network.
Step 5	**show ip route**	View the IPv4 router table.
Step 6	**show ipv6 route**	View the IPv6 router table.

1. View the information of a tunnel interface.

```
Switch# 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.

```
Switch# 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
```

12.4 IPv6 Tunnel Configuration Instances

The folloing chapters/sections introduce IPv6 tunnel configuration instances.

Manual tunnel configuration instance

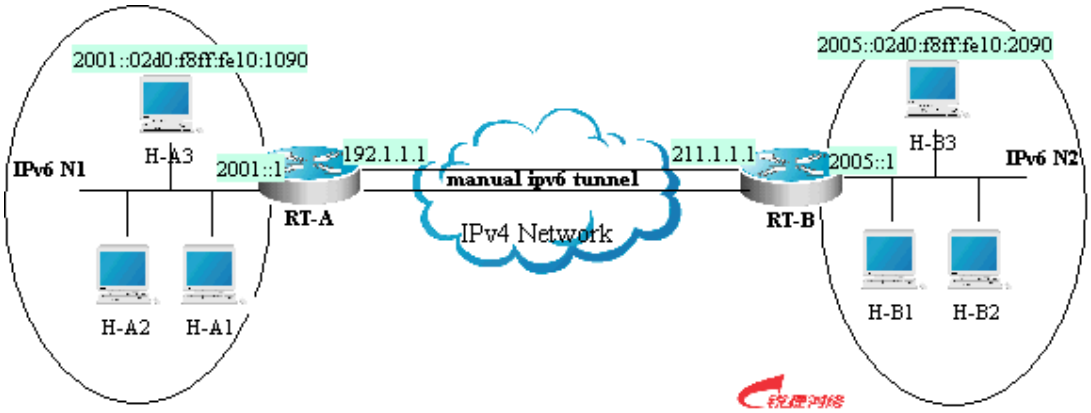
Manual IPv6 Tunnel Configuration Instance

6to4 Tunnel Configuration Instance

ISATAP tunnel configuration instance

ISATAP and 6to4 tunnel configuration instance

12.4.1 Manual IPv6 Tunnel Configuration Instance



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

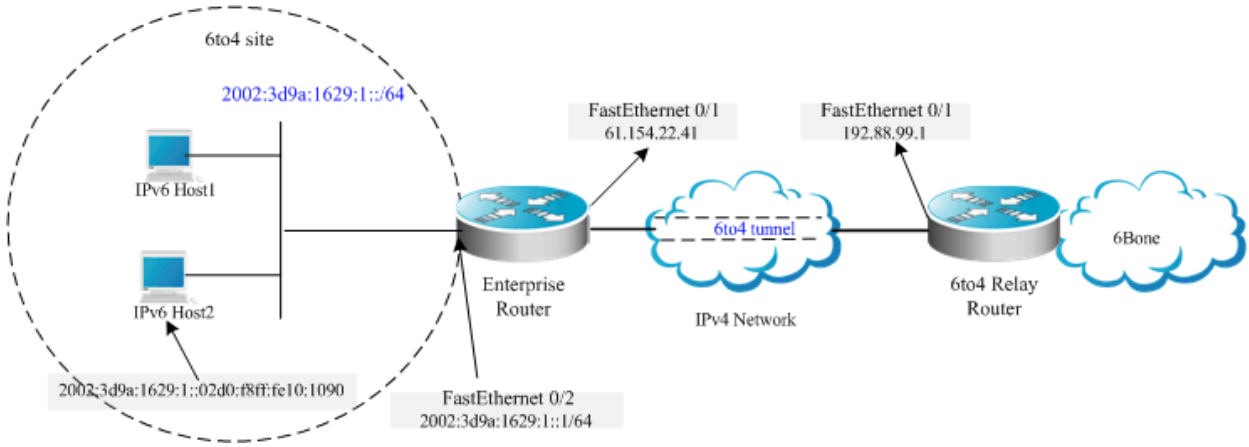
```
! Connect the interfaces of the IPv4 network
  interface FastEthernet 2/1
   no switchport
ip address 192.1.1.1 255.255.255.0
! Connect the interfaces of the IPv6 network
interface FastEthernet 2/2
no switchport
ipv6 address 2001::1/64
no ipv6 nd suppress-ra (optional)
! Configure manual tunnel interface
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
```

12.4.2 6to4 Tunnel Configuration Instance



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

Note

When configurating 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

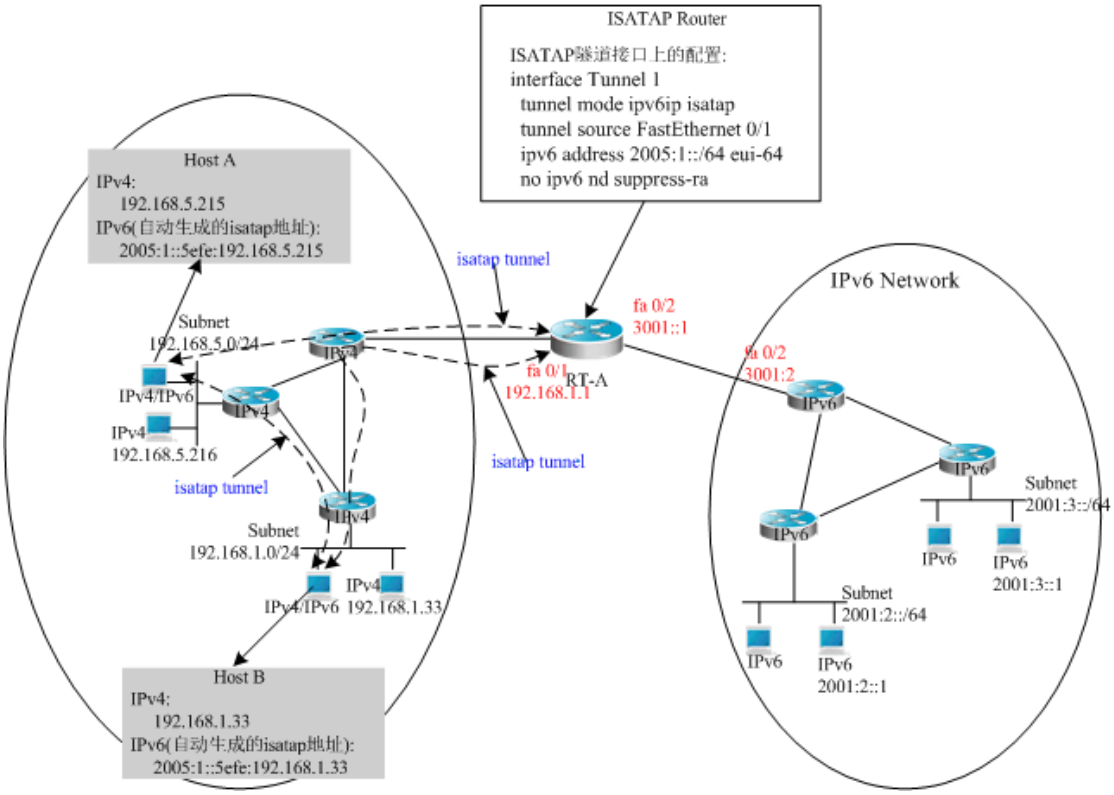
```
! Connect the interfaces of the IPv4 network
interface FastEthernet 0/1
no switchport
```

```
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
```

12.4.3 ISATAP Tunnel Configuration Instance



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 responsibel for the message forwarding function of the ISATAP host inside the site and the IPv6 host outside the site.

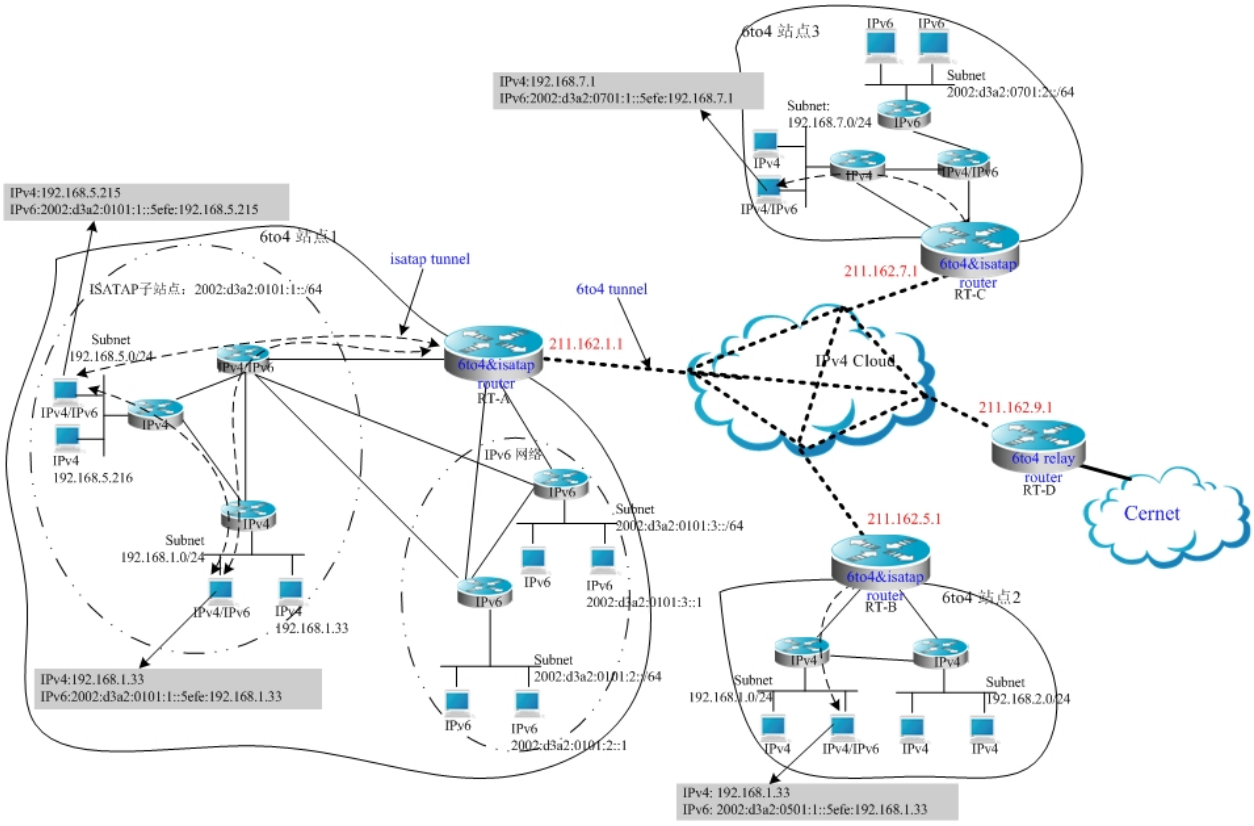
In the above figure, when Host A and Host B send router requests to ISATAP Router, ISATAP Router will respond with a router advertisement message. After receiving the message, the hosts will be automatically configured and they also generate their own ISATAP addresses respectively. Then, the IPv6 communication between Host A and Host B will be done via the ISATAP tunnel. When Host A or Host B needcommunicate 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 FastEthernet0/1
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 FastEthernet0/2
no switchport
ipv6 address 3001::1/64
```

```
! Configure the route to the IPv6 network
    ipv6 route 2001::/64 3001::2
```

12.4.4 Configuration Instance for Composite Application of ISATAP and 6to4 Tunnels



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.

Instruction:

Note

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.

The configurations of Area Border Routers in the 6to4 site shown in the above figure are introduced respectively below. Note: 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 site
interface FastEthernet0/1
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 FastEthernet0/2
no switchport
2002:d3a2:0101:10::1/64
! Connect interface 2 of the IPv6 network
interface FastEthernet0/2
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 FastEthernet0/1
no switchport
ip address 192.168.10.1 255.255.255.0
! Connect interface 2 of the IPv4 network  inside the site
interface FastEthernet0/2
no switchport
ip address 192.168.20.1 255.255.255.0
! Configure isatap tunnel interface
interface Tunnel 1
tunnel mode ipv6ip isatap
tunnel source FastEthernet 0/1
ipv6 address 2002:d3a2:0501:1::/64 eui-64
no ipv6 nd suppress-ra
! Configure 6to4 tunnel interface
interface Tunnel 2
tunnel mode ipv6ip 6to4
ipv6 enable
tunnel source GigabitEthernet 0/1
```

```
! Configure the route to the 6to4 tunnel
ipv6 route 2002::/16 Tunnel 2
! Configure the routeto the 6to4 relay router RT-D to access the Cernet network
ipv6 route ::/0 2002:d3a2::0901::1
```

RT-C configuration:

```
! Connect the interfaces of the Internet 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 FastEthernet0/1
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 FastEthernet0/2
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 FastEthernet0/1
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
```

13 LCD Configuration

13.1 Overview

The LCD provides an intuitive presentation of the state of a switch. The operation is very easy and performed by use of keys. In this way, even if a user has no knowledge about CLI commands, the user can know the running state of the current switch. When the swithc works abnormally, the display can inform the user of the abnormal information timely.

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.

In the normal state, the switch prints 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 waring information. The information will not disapper from the display until the user push the selection key (enter).

13.1.1 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 condtion occurs.

1. Menu key (Menu) Stops showing the current state and begins to 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.

Push the Menu key to begin showing the menu. Selected line background colors deepen in the display. If no key remains unpushed for a period, information will be shown circularly again and the next screen of the shown content in the last circle is shown. If a user pushs one of the four keys, then the following condtion occurs.

5. Menu key (Menu) Stops showing the current state and begins to show the main menu.

6. 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.

7. 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.

8. 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 diplay shows generated warning messages.If a warning message need be shown in multiple screens, then the display shows the content of the waring message in screens circularly. If multiple waring 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:

9. Menu key (Menu) Stops showing the waring message and begins to show the main menu.

10. 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.

11. Page Up key (Pgup) All the waring 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.

12. Page Down key (Pgdn) Waring 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.

13.2 LCD Configuration Task List

13.2.1 Configuring Warning Information Queue Length

Afer a warning message is generated, the LCD keeps showing the new warning message unless a user pushs the key Enter.The user can browse history warning messages through menu items after pushing the key Enter.The command can be used to configurate the length of a warning message.

The current version of DES-7200 saves 100 history warning messages by default. To configurate the length of a history warning message, run the following command in the global configuration mode:

Command	Function
D-Link(config)**# lcd trap-number** *num*	Set a new length of a waring message
D-Link(config)**# no lcd trap-number**	Restore to the default setting

13.3 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 warnig message to 200

14 Configuring MAC Address

14.1 Managing the MAC Address List

14.1.1 Overview

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

14.1.1.1 Dynamic Address

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

When the switch receives a packet, if the destination MAC address of the packet has been learned by the switch, the packet will be sent only to the port associated with the MAC. Otherwise, the packet will be sent to all other ports.

The switch 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 switch 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 switch 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 switch 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 switch is reset, all dynamic addresses that the switch has learned will be lost. The switch need to learn these addresses again.

14.1.1.2 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 switch reloads.

14.1.1.3 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 switch is reset.

If you want the switch 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 switch.

14.1.1.4 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.

14.1.2 Configuring MAC Address

14.1.2.1 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

14.1.2.2 Setting the Address Aging Time

Setting the Address Aging Time

Command	Function
D-Link(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.

14.1.2.3 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 (**clear mac address-table dynamic address** *mac-address*), remove all addresses on the specified physical port or port channel (**clear mac address-table dynamic interface** *interface-id*), or

remove all addresses on a specified VLAN (**clear mac address-table dynamic vlan** *vlan-id*).

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

14.1.2.4 Adding and Removing Static Address Entries

You add a static address to the address table by specifying the destination MAC unicast address and the VLAN from which it is received. Packets received with this destination address are forwarded to the interface specified with the interface-id.

Adding a Static Address:

Command	Function
D-Link(config)#mac-address-table static *mac-add* vlan vlan-id interface interface-id	Add a static address to the MAC address table. For *mac-addr*, specify the destination MAC unicast address to add to the address table. For *vlan-id*, specify the VLAN for which the packet with the specified MAC address is received. For *interface-id*, specify the interface to which the received packet is forwarded. Valid interfaces include physical ports or Aggregate Port. 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. This example shows how to add the static address 00d0.f800.073c to the MAC address table.

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:

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

14.1.2.5 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 switch.

Adding a filtering address:

Command	Function
D-Link(config)#mac-address-table filtering *mac-addr* vlan *vlan-id*	For *mac-addr*, specify the destination MAC unicast address to add to the address table. the address table. For *vlan-id*, specify the VLAN for which the packet with the specified MAC address is received.

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 add the filtering address 00d0.f800.073c to the MAC address table.

When a packet is received in VLAN 1 with this MAC address as its destination address, the packet is discarded:

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

14.1.3 Viewing MAC Addresses Table Entries

Viewing MAC addresses table entries of the switch:

Command	Function
D-Link#show mac-address-table	Show all types of MAC addresses (including dynamic address, static address and filtering address)
D-Link#show mac-address-table aging-time	Show the current aging time
D-Link#show mac-address-table dynamic	Show only dynamic MAC addresses
D-Link#show mac-address-table static	Show only static MAC addresses
D-Link#show mac-address-table filtering	Show only filtering MAC addresses
D-Link#show mac-address-table interface	Show all types of MAC addresses for the specified interface
D-Link#show mac-address-table vlan	Show all types of MAC addresses for the specified VLAN
D-Link#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:

```
D-Link#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:

```
D-Link#show mac-address-table count
Dynamic Address Count 30
Static  Address Count 0
Filter  Address Count 0
Total Mac Addresses 30
Total Mac Address Space Available: 8159
```

Show the current aging time:

```
D-Link#show mac-address-table aging-time
Aging time    : 300
```

14.2 Configuring MAC Address Notification

14.2.1 Overview

MAC address notification enables you to track users on a network by storing the MAC address activity on the switch. After the trap is enabled, whenever the switch learns or removes a MAC address, an SNMP notification can be generated and sent to the NMS (Network Management Workstation).If a notification about adding MAC address has been generated, you know a new user (marked by the MAC address) is using the switch. 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 switch) has been generated, you know that a user does not use the switch any more.

When there are many users on the switch, a lot of notifications about MAC address changing will be generated (for example, the switch powers on). You can set a trap interval time to bundle the notification traps and reduce network traffics. 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 on, if you enable MAC address notification traps on an interface, the changing of MAC address on that interface will generate the traps, and the changing of MAC address on other interfaces that you disable the traps will not generate the traps. The switch can send the traps about adding address, or deleting address, or both on the specified interface. When the global switch is turned off, the switch will not send any MAC address notification traps on any interface.

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

14.2.2 Configuring MAC Address Notification Traps

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

Configuring MAC address notification traps of the switch:

Command	Function
D-Link(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. *community-string* - Specify the community string to send with the notification traps. The string is used for authentication
D-Link(config)#snmp-server enable traps mac-notification	Enable the switch to send MAC address traps.
D-Link(config)#mac-address-table notification	Turn on the MAC address notification global switch.
D-Link(config)#mac-address-table notification {interval *value* | history-size *value*}	interval *value* :Specify the notification trap interval in seconds between each trap sent to the NMS. The range is 0 to 3600 seconds; the default is one second. history-size *value* :Specify the maximum number of entries in the MAC address notification history table. The range is 0 to 200, and the default is 50.
D-Link(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 switch from sending MAC address notification traps, use the **no snmp-server enable traps mac-notification** command in the global configuration mode. To disable the

MAC address notification traps on a specified interface, use the **no snmp trap mac-notification** {**added** | **removed**} interface configuration command.

To disable the MAC address notification feature, use the **no mac address-table notification** command in the global 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.

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

14.2.3 Viewing MAC Address change Notification information

In the privileged mode, you can view the MAC address notification traps by using one or more of the commands listed in the following table:

Command	Function
D-Link#**show mac-address-table notification**	Show the global configuration of MAC address change notification function
D-Link#**show mac-address-table notification interface**	Show the enable status of MAC address change notification on the interface
D-Link#**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:

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

D-Link#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
……


D-Link#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
```

14.3 IP and MAC Address Binding

14.3.1 Overview

If you have bound an IP address with a specified MAC address, when the switch 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 switch with address binding. Notice that the feature has priority over 802.1X, port-based security and ACL.

14.3.2 Configuring IP and MAC Address Bind

In the privileged mode, follow these steps to configure the IP and MAC address binding:

Command	Function
D-Link(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* command in the global configuration mode.

14.3.3 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 global configuration mode.

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

15 Configuring MIB

This appendix lists all MIBs supported by this model of switch, including:

A List of MIBs

Obtaining MIB Files

15.1 A List of MIBs

Standard MIBs supported:

BRIDGE-MIB (RFC1493)

EtherLike-MIB(RFC1643)

IF-MIB(RFC2863)

RFC1213-MIB

RMON1-MIB (supports four groups: RMON etherStats, etherHistory, alarms and events)

SNMPv2-MIB

SNMPv3-MIB (Support USM and VACM)

Private MIB

Displaying the supported MIB in the system:

You can use the command of show snmp mib to view the the supported MIB in current system:

D-Link**#show snmp mib**

sysDescr

sysObjectID

sysUpTime

sysContact

sysName

sysLocation

sysServices

sysORLastChange

ifNumber

ifEntry

ifEntry.ifIndex

ifEntry.ifDescr

ifEntry.ifType

ifEntry.ifMtu

ifEntry.ifSpeed

ifEntry.ifPhysAddress

ifEntry.ifAdminStatus

ifEntry.ifOperStatus

ifEntry.ifLastChange

ifEntry.ifInOctets

ifEntry.ifInUcastPkts

ifEntry.ifInNUcastPkts

ifEntry.ifInDiscards

ifEntry.ifInErrors

ifEntry.ifInUnknownProtos

ifEntry.ifOutOctets

ifEntry.ifOutUcastPkts

ifEntry.ifOutNUcastPkts

ifEntry.ifOutDiscards

ifEntry.ifOutErrors

ifEntry.ifOutQLen

ifEntry.ifSpecific

.....

15.2 Obtaining MIB Files

Log on http://ietf.org/rfc.html to obtain information about the standard MIB.

Log on the internet to obtain information about the private MIBs

16 Configuring MSTP

16.1 MSTP Overview

16.1.1 STP and RSTP

16.1.1.1 STP and RSTP Overview

This switch can support both the STP protocol and the RSTP protocol and comply with the IEEE 802.1D and the IEEE 802.1w standard.

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 can make the switch of one LAN play the roles below:

- 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).

16.1.1.2 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.

16.1.1.3 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 former 2 bytes is shown as the table below. Of which, the former 4 bits denote the priority, while the latter 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

16.1.1.4 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.

16.1.1.5 Port Roles and Port States

Each port will play a Port Role in the network and be used to represent different acts in the network topology.

- **Root port:** The port that provides the shortest path to the Root Bridge.
- **Designated port:** The port by which each LAN is connected to the root bridge.
- **Alternate port:** The alternate port of the root port which will change into the root port once the root port fails.
- **Backup port:** The backup port of the Designated port. If two ports are connected to one LAN for the bridge, the port with higher priority is the Designated port, while that with lower priority is the Backup port.
- **Disable port:** The port that is not in the active status. Namely, the port whose operation state is down is assigned to this role.

The following is the schematics of various port roles such as the R1w-2-1, the R1w-2-2 and the R1w-2-3:

R = Root port D = Designated port A = Alternate port B = Backup port

Unless otherwise stated, the priority of the port will be lowered from left to right.

Figure R1w-2-1

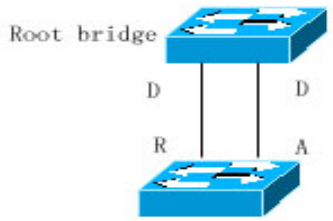
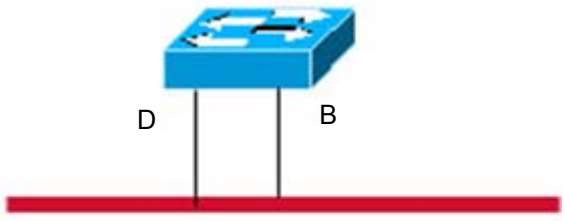
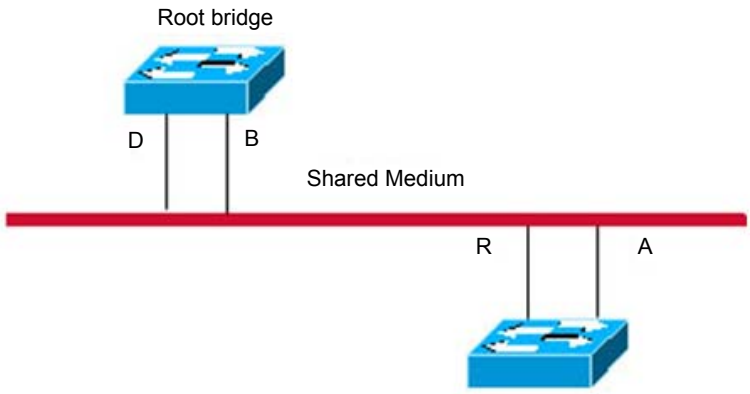


Figure R1w-2-2



Shared Medium

Figure R1w-2-3



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

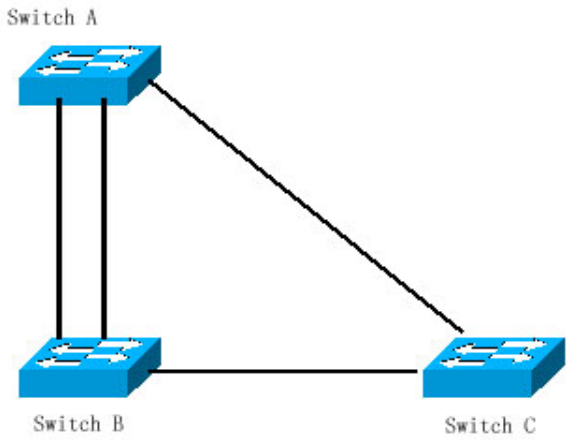
- **Discarding:** It will neigh forward the received frame nor learn about the source Mac address.
- **Learning:** It will not forward the received frame, but learn about the source Mac address, so it is a transitional status.
- **Forwarding:** It will forward the received frame and learn about the source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

16.1.1.6 Spanning of Network Topology Tree (Typical Application Solution)

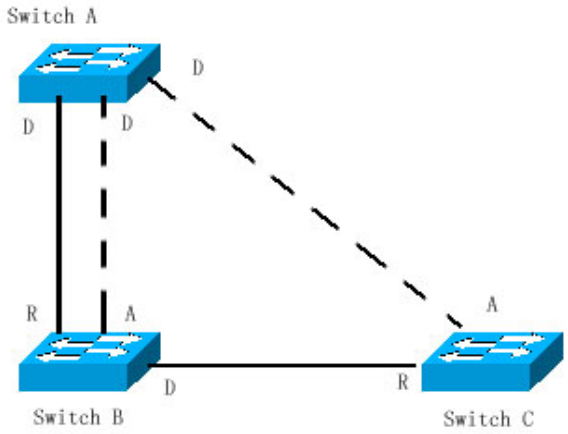
We now describe how the STP and RSTP protocol spans a tree-type structure by the mixed network topology. As is shown in Figure R1w-3-1 below, the bridge IDs of the Switch A, B and C are assumed to be increasing. Namely, the Switch A presents the highest priority. There is the 1000M link between switch 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 R1w-3-1



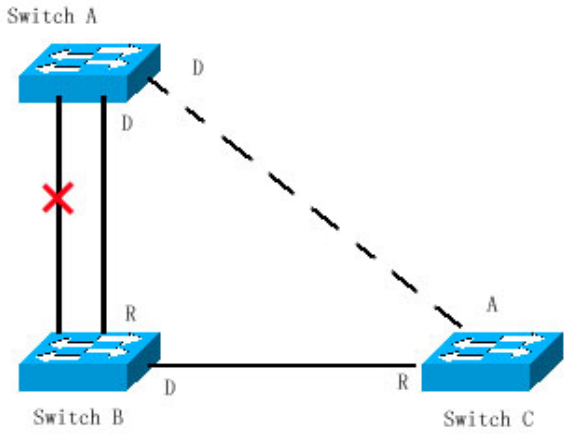
If all of three Switches open the Spanning Tree protocol, they will select the root bridge as the Switch A by switching the BPDU. Once Switch B detects that two ports are connected to Switch A, it will select the port with the highest priority as the root port, while another one is selected as the Alternate 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 R1w-3-2 after the port roles are selected.

Figure R1w-3-2



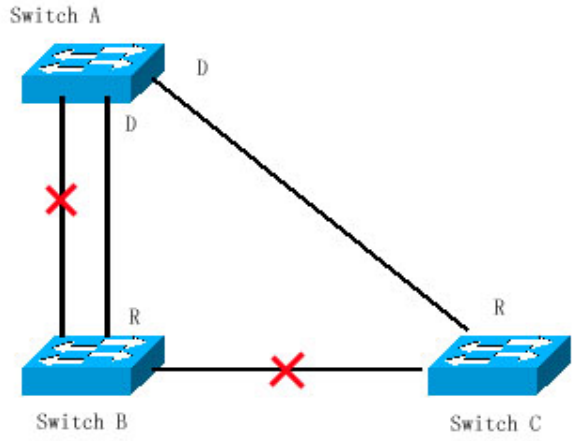
If the failure of the active path between Switch A and Switch B occurs, the alternate path will take action immediately to generate corresponding Figure R1w-3-3.

Figure R1w-3-3



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 R1w-3-4.

Figure R1w-3-4



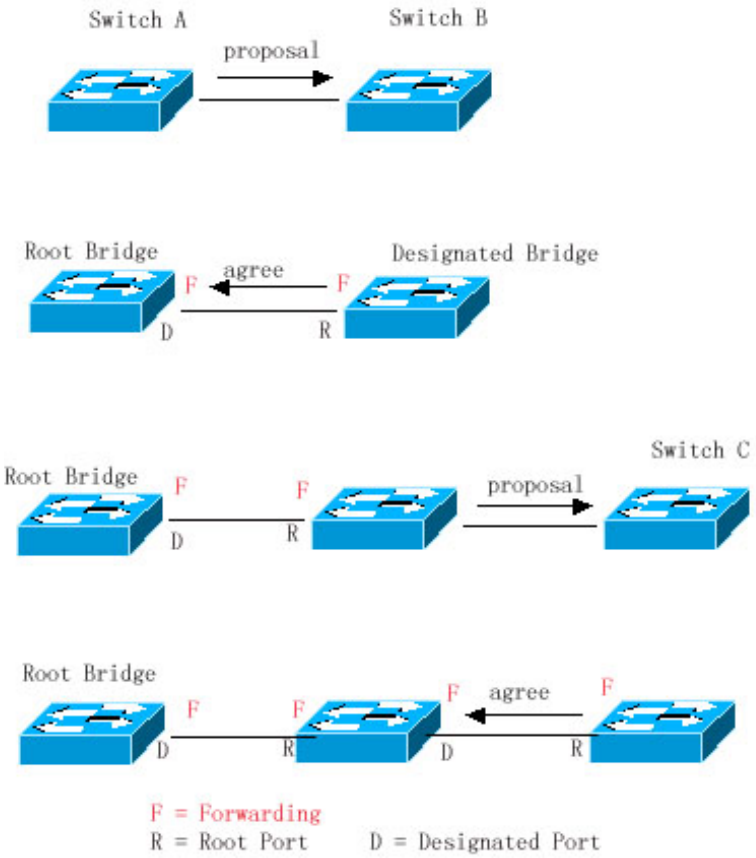
16.1.1.7 Quick Convergence of RSTP

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 R1w-4-1, 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 R1w-4-1



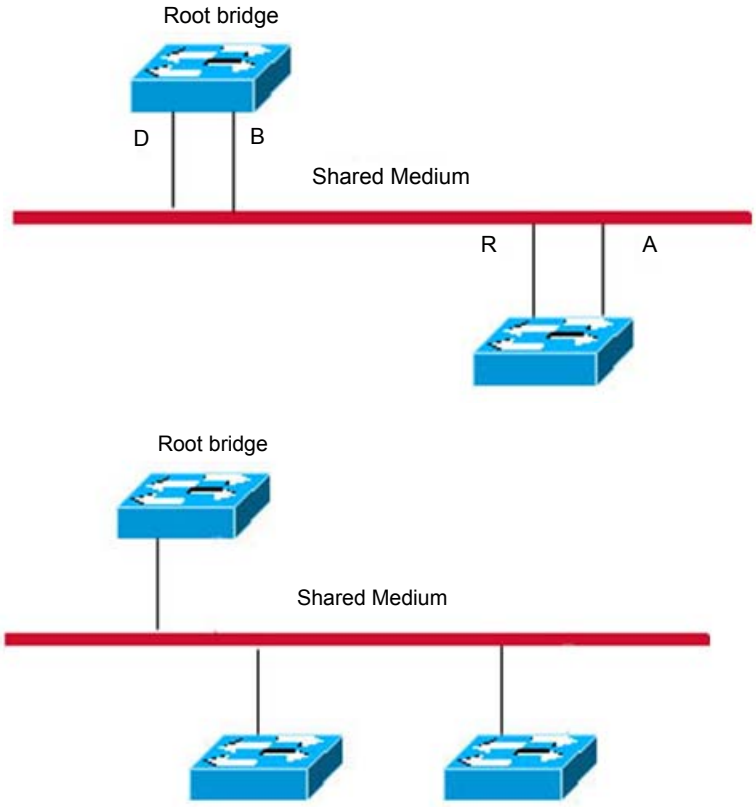
Note

Above shake-hand process is conditional, that is the port should be a point-to-point connect. In order to maximize the efficiency of your switches, it had better not make the switches set up the non point-to-point connect.

Other than Figure *R1w-2-3*, other schematics in this chapter are the point-to-point connection. The following lists the example figure of the non point-to-point connection.

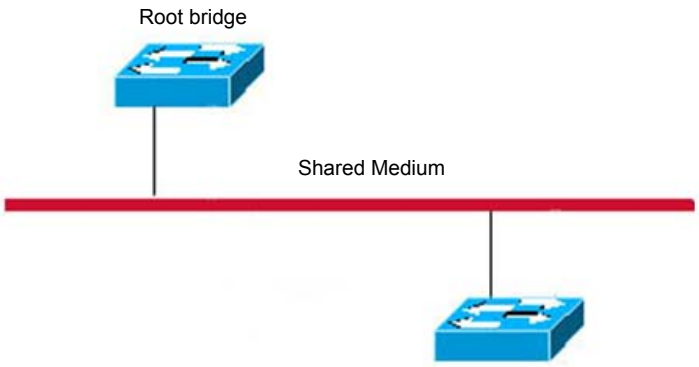
Example of Non Point-to-point Connection:

Figure R2w-2-1



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

Figure R2w-2-2



16.1.1.8 Compatibility of RSTP and STP

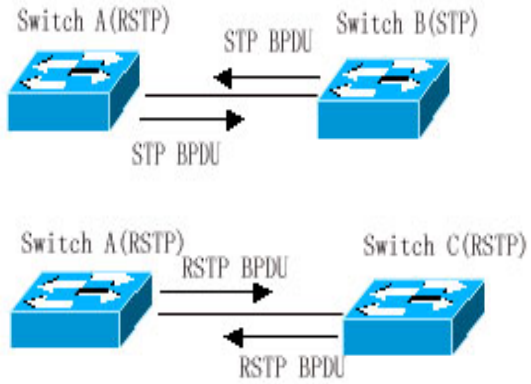
The RSTP protocol is completely compatible with the STP protocol, and will judge whether the bridge connected with supports the STP protocol or the RSTP protocol by the version number of received BPDU automatically. It can only take the forwarding method of the STP to carry out the forwarding after 30s 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 R1w-1-1, 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 (as Figure R1w-1-2), 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 switches can run by the RSTP protocol as shown in Figure R1w-1-3.

Figure R1w-1-3

Protocol Migration



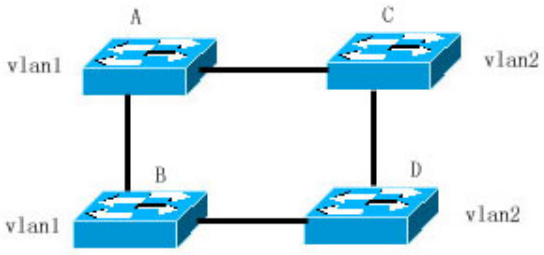
16.1.2 MSTP Overview

This switch 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:

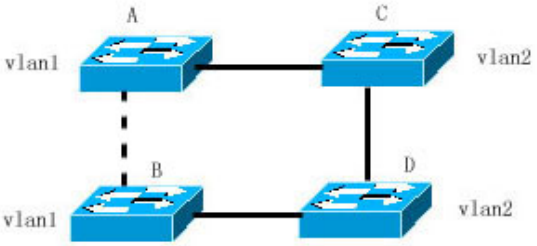
As is shown in Figure *mstp-1*, the switch A and B are within the vlan1, while the switch C and D are within the vlan2, and then form the loop.

Figure mstp-1



For some specified configuration, it will cause the DISCARDING of the path between the switch A and B (as Figure *mstp-2*). For the switch C and D don't include vlan1, it can't forward the data packet of vlan1, so the vlan1 of switch A fails to communicate with the vlan1 of switch B.

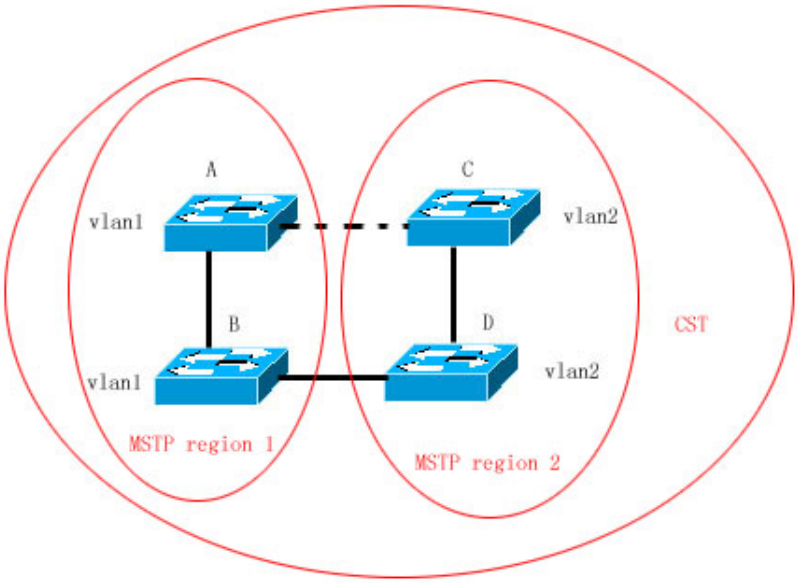
Figure mstp-2



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 switch, 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 *mstp-3*: the switch 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 switches respectively and there is no loop between them, so one path DISCARDING is selected according to related configuration.

Figure mstp-3



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

16.1.2.1 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 switch 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 switch is the same as itself, it will consider that the switch 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.

16.1.2.2 Spanning Tress within MSTP region (IST)

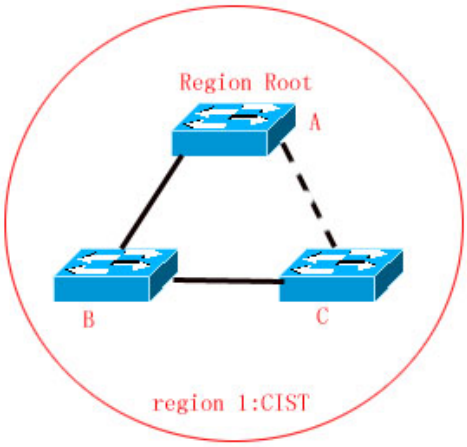
After the MSTP region is partitioned, each region will select separate root bridge of various instances and the port role of various ports for each switch according to such parameters as the bridge priority and port priority. Finally, it will specify whether this port is FORWARDING or DISCARDING within 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 switch A, B and C form the loop within the region 1.

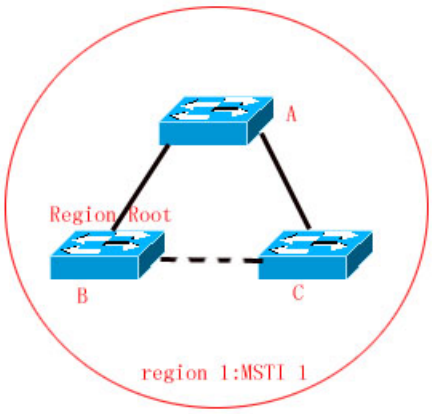
As is shown in Figure *mstp-4-1*, switch A with the highest priority is selected as the Region Root in the CIST (instance 0). Then, the path between switch A and C is DISCARDING according to other parameters. Hence, for the vlan group of the instance 0, only the path from switch A to B and switch A to C is available, which breaks the loop of the vlan group.

Figure mstp-4-1



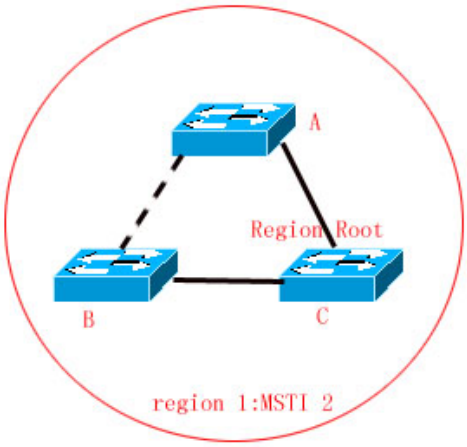
As is shown in Figure *mstp-4-2*, switch B with the highest priority is selected as the Region Root in the MSTI 1 (instance 1). Then, the path between switch B and C is DISCARDING according to other parameters. Hence, for the vlan group of the instance 1, only the path from switch A to B and switch B to C is available, which breaks the loop of the vlan group.

Figure mstp-4-2



As is shown in Figure *mstp-4-3*, switch C with the highest priority is selected as the Region Root in the MSTI 2 (instance 2). Then, the path between switch A and B is DISCARDING according to other parameters. Hence, for the vlan group of the instance 2, only the path from switch A to B and switch A to C is available, which breaks the loop of the vlan group.

Figure mstp-4-3

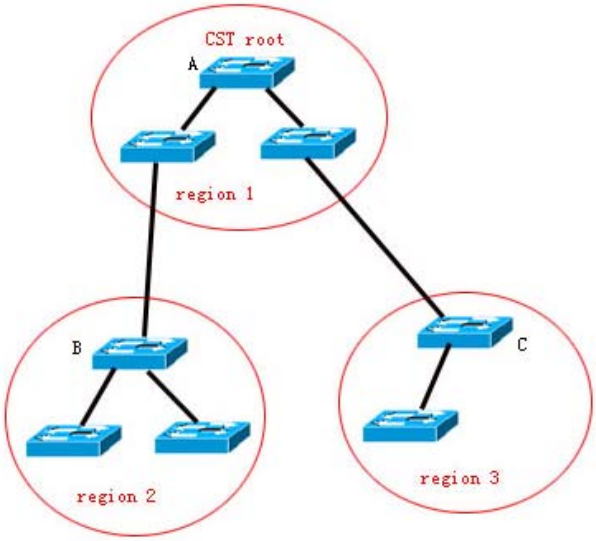


It should note that the MSTP protocol doesn't concern with which vlan the port is of, so users should configure corresponding path cost and priority for related port according to actual vlan configuration, to prevent the MSTP protocol from breaking the loop unexpected.

16.1.2.3 Spanning Tree between MSTP regions (CST)

For CST, each MSTP region is equivalent to a large-sized switch, and different MSTP regions also span a large-sized network topology tree, referred to as the CST (common spanning tree). As is shown in Figure *mstp-4*, for the CST, the switch A with the smallest bridge ID is selected as the root of the whole CST (CST root). Furthermore, it is the CIST regional root within this region. In region 2, the root path cost fro switch B to CST root is selected as the CIST regional root within this region for it is the shortest. In this way, the region 3 selects the switch C as the CIST regional root.

Figure mstp-4



The CIST regional root needs not to be the switch with the smallest bridge ID within this region, which means the switch with the minimum root path cost to the CST root within this region.

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 switch of this Region as much as possible!

16.1.2.4 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 with 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**. Within the region, the hop count will be reduced 1 when it passes through one switch starting from the region root bridge, until it reaches to 0, which denotes that this BPDU information is timeout, the switch will discard the BPDU 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.

16.1.2.5 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 the RSTP and STP*** section.

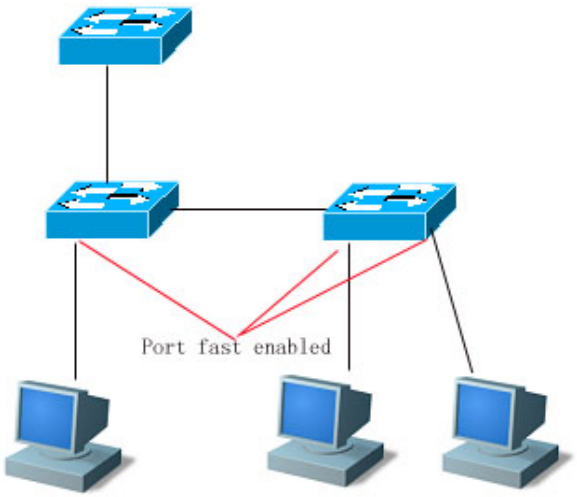
For the RSTP protocol, it will process the CIST part of the MSTP BPDU, so it is not necessary for the MSTP to send the RSTP BPDU to be compatible with it.

Each switch that runs the STP or RSTP protocol is a separate region, but will not form the same region with any switch.

16.2 Optional Features of MSTP

16.2.1 Understanding Port Fast

If the port of the switch 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 switch can be set as the Port Fast enabled.



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.

16.2.2 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.

16.2.3 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.

16.2.4 Understanding tc-protection

Tc-protection can only be enabled or disabled globally. In default cases, it is enabled.

In the enabled status, the corresponding switch performs a deletion operation within a period (four seconds) after receiving a TC-BPDU message. It also checks whether another TC-BPDU message is received within the period. If yes, the switch performs deletion again, thus avoiding frequently deleting MAC address tables and ARP tables.

16.3 Configuring MSTP

16.3.1 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
Relations between vlan and instances	All vlans belong to instance 0. Only instance 0 exists.

You can reset spanning tree parameters to default configurations (not including disabling span) through the **spanning-tree reset** command.

16.3.2 Open and Close Spanning Tree Protocol

Once opening the Spanning-tree protocol, the switch will start to run the Spanning-tree protocol. This switch will run the MSTP protocol by default.

The default status of the switch is to close the Spanning-tree protocol.

In the privileged mode, perform these steps to open the Spanning Tree protocol:

Command	Function
D-Link**# configure terminal**	Enter the global configuration mode.
D-Link(config)**# spanning-tree**	Open the Spanning tree protocol.
D-Link(config)**# end**	Return to the privileged EXEC mode.
D-Link**# show spanning-tree**	Check the configuration entities.

Command	Function
D-Link# **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.

16.3.3 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 switch is not compatible with that of other manufacturers.

Note

When you switch to the RSTP or STP mode from the MSTP mode, all information of related MSTP Region will be cleared.

The switch adopts the MSTP mode by default.

In the privileged mode, perform these steps to open the Spanning Tree protocol:

Command	Function
D-Link# **configure terminal**	Enter the global configuration mode.
D-Link(config)# **spanning-tree mode** *mstp/rstp/stp*	Switch the Spanning Tree mode.
D-Link(config)# **end**	Return to the privileged EXEC mode.
D-Link# **show spanning-tree**	Check the configuration entities.
D-Link# **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.

16.3.4 Configuring Switch Priority

The setting of the switch priority concerns with which switch is the root of the whole network, as well as the topology of the whole network. It is recommended that administrators set the core switch with higher priority (smaller value), which will facilitate the stability of the whole network. You can assign different switch priorities for various instances, by which various instances can run separate spanning tree protocol. The switches between different regions only concern with the priority of the CIST (instance 0).

The same as Bridge ID, priorities can be set to 16 values, being multiples of 4096 including 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 switch priority:

Command	Function
D-Link# **configure terminal**	Enter the global configuration mode.

Command	Function
D-Link(config)# **spanning-tree [mst** *instance-id]* **priority** *priority*	For the configuration of the switch 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.
D-Link(config)# **end**	Return to the privileged EXEC mode.
D-Link# **show running-config**	Check the configuration entities.
D-Link# **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.

16.3.5 Configuring Port Priority

When two ports are connected to the shared medium, the switch 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.

The same as those of switches, priorities can be set to 16 values, being multiples of 16 including 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224 and 240.The default value is 128.

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

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

16.3.6 Configuring Path Cost of Port

The switch selects the Root port according to the minimal sum of the path cost from the port to the root bridge, so the setting of the port path cost concerns with the root port of this switch. 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
D-Link# **configure terminal**	Enter the global configuration mode.
D-Link(config)# **interface** *interface-id*	Enter he configuration mode of this interface, the legal interface contains the physical port and the Aggregate Link.
D-Link(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.
D-Link(config-if)# **end**	Return to the privileged EXEC mode.
D-Link# **show spanning-tree [mst instance-id]interface** *interface-id*	Check the configuration entities.
D-Link# **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.

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

If this port Path Cost is the default value, the switch 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
D-Link# **configure terminal**	Enter the global configuration mode.
D-Link(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.
D-Link(config)# **end**	Return to the privileged EXEC mode.
D-Link# **show running-config**	Check the configuration entities.
D-Link# **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.

16.3.8 Configuring Hello Time

Configure the time interval of the BPDU message is sent Periodically. The default value is 2s.

In the privilege mode, perform these steps to configure the Hello Time:

Command	Function
D-Link# **configure terminal**	Enter the global configuration mode.
D-Link(config)# **spanning-tree hello-time** *seconds*	Configure the hello time, whose value range is 1-10s, 2s by default.
D-Link(config)# **end**	Return to the privileged EXEC mode.
D-Link# **show running-config**	Check the configuration entities.
D-Link# **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.

16.3.9 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
D-Link# **configure terminal**	Enter the global configuration mode.
D-Link(config)# **spanning-tree forward-time** *seconds*	Configure the forward delay time, whose value range is 4-30s, 15s by default.
D-Link(config)# **end**	Return to the privileged EXEC mode.
D-Link# **show running-config**	Check the configuration entities.
D-Link# **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.

16.3.10 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
D-Link# **configure terminal**	Enter the global configuration mode.
D-Link(config)# **spanning-tree max-age** *seconds*	Configure the max age time, whose value range is 6-40s, 20s by default.
D-Link(config)# **end**	Return to the privileged EXEC mode.
D-Link# **show running-config**	Check the configuration entities.
D-Link# **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.

Note

In addition to the value range of themselves, there are some Constraint relationship among the Hello Time, Forward-Delay Time and Max-Age Time as follows:
2*(Hello Time + 1.0 seconds) <= Max-Age Time <= 2*(Forward-Delay – 1.0seconds). The configured three parameters should meet above condition. Otherwise, it may cause the topology instability.

16.3.11 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 Maximum-Hop Count:

Command	Function
D-Link# **configure terminal**	Enter the global configuration mode.
D-Link(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.
D-Link(config)# **end**	Return to the privileged EXEC mode.
D-Link# **show running-config**	Check the configuration entities.
D-Link# **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.

16.3.12 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 Section 1.1.1.7 Quick Convergence of RSTP. If you don't set this value, the switch 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
D-Link# **configure terminal**	Enter the global configuration mode.
D-Link(config)# **interface** *interface-id*	Enter into the interface configuration mode.
Switch(config-if)# **spanning-tree link-type** point-to-point	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.
D-Link(config-if)# **end**	Return to the privileged EXEC mode.
D-Link# **show running-config**	Check the configuration entities.
D-Link# **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.

16.3.13 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 the RSTP and STP.

Command	Function
D-Link# **clear spanning-tree detected-protocols**	Execute the version check forcibly to all ports.
D-Link# **clear spanning-tree detected-protocols interface** *interface-id*	Execute the version check forcibly to a specific port.

16.3.14 Configuring MSTP Region

To enable several switches be of the same MSTP region, it is necessary to make these switches possess the same name, revision number and instance-vlan corresponding table.

You can configure vlans included in instances 0-64. The remaining vlan 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
D-Link# **configure terminal**	Enter the global configuration mode.
D-Link(config)# **spanning-tree mst configuration**	Enter the configuration mode.
D-Link(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

Command	Function
	be transferred to the instance 0.
D-Link(config-mst)# **name** *name*	Specify the MST configuration name, this string can present up to 32 bytes.
D-Link(config-mst)# **revision** *version*	Specify the MST revision number, whose range is 0-65535. The default value is 0.
D-Link(config-if)#**show**	Verify MST configuration entries.
D-Link(config-if)# **end**	Return to the privileged EXEC mode.
D-Link# **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:

```
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 35
Switch(config-mst)# name region1
Switch(config-mst)# revision 1
Switch(config-mst)# show
Pending MST configuration
Name [region1]
Revision 1
Instance Vlans Mapped
-------- --------------------
0 1-9,21-4094
1 10-20
-------------------------------
Switch(config-mst)# exit
Switch (config)#
```

16.3.15 Configuring Maximum-Hop Count

Configure the Maximum-Hop Count to specify how many switches 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
D-Link# **configure terminal**	Enter the global configuration mode.
D-Link(config)# **spanning-tree max-hops** *hop-count*	Configure the Maximum-Hop Count, whose range is 1-40, 20 by default.
D-Link(config)# **end**	Return to the privileged EXEC mode.
D-Link# **show running-config**	Check the configuration entities.
D-Link# **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.

16.4 Configuring MSTP Optional Features

16.4.1 Default Setting of Optional Features for Spanning Tree

Default setting of optional features is disabled.

16.4.2 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
D-Link# **configure terminal**	Enter the global configuration mode.
D-Link(config)# **interface** *interface-id*	Enter he configuration mode of this interface, the legal interface contains the physical port and the Aggregate Link.
D-Link(config-if)# **spanning-tree portfast**	Open the portfast of this interface.
D-Link(config-if)# **end**	Return to the privileged EXEC mode.
D-Link# **show spanning-tree interface** *interface-id* **portfast**	Check the configuration entities.
D-Link# **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.

16.4.3 Opening 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
D-Link# **configure terminal**	Enter the global configuration mode.
D-Link(config)# **spanning-tree portfast bpduguard default**	Open the BPDU guard global.
D-Link(config)# **interface** *interface-id*	Enter he configuration mode of this interface, the legal interface contains the physical port and the Aggregate Link.
D-Link(config-if)# **spanning-tree portfast**	Open the portfast of this interface.
D-Link(config-if)# **end**	Return to the privileged EXEC mode.
D-Link# **show running-config**	Check the configuration entities.
D-Link# **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.

16.4.4 Open BPDU Filter

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

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

Command	Function
D-Link# **configure terminal**	Enter the global configuration mode.
D-Link(config)# **spanning-tree portfast bpdufilter default**	Open the BPDU filter global.
D-Link(config)# **interface** *interface-id*	Enter he configuration mode of this interface, the legal interface contains the physical port and the Aggregate Link.
D-Link(config-if)# **spanning-tree portfast**	Open the portfast of this interface.
D-Link(config-if)# **end**	Return to the privileged EXEC mode.
D-Link# **show running-config**	Check the configuration entities.
D-Link# **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.

16.4.5 Running tc_protection

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

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

If you want to switch off the tc_protection, you can use the global configuration command **no spanning-tree tc-protection** to configure.

16.5 Showing the configuration and status of MSTP

MSTP provides the following commands to check the configuration and operation information. The functions are shown as below:

Command	Meaning
show spanning-tree	Show parameters of the MSTP and topology information of spanning-tree
show spanning-tree mst configuration	Show the configuration of the MSTP.
show spanning-tree mst *instance-id*	Show the MSTP information of this instance.
show spanning-tree mst *instance-id* **interface** *interface-id*	Show the MSTP information of corresponding instance for specified interface.
show spanning-tree interface *interface-id*	Show the MSTP information of all instances for specified interface.
show spanning-tree forward-time	Show forward-time
show spanning-tree Hello time	Show Hello time
spanning-tree max-hops	Show max-hops
spanning-tree tx-hold-count	tx-hold-count
spanning-tree pathcost method	Show pathcost method

17 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.


Note

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 conform to the OSPFv2.

17.1 OSPFv3 Protocal 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 implemention in the OSPFv3 in contrast to the OSPFv2.

17.1.1 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 accorrdingly. 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 informaton 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.


Note

By 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 exsist 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 use 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 prefic 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 databse

description message, then you are unable to normally establish the adjacency relation.If there is an irrecognizable 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 unknowm LSA type. By using the information recorded in the LSA header, we can determine how to handle received irrecoganizable LSA type.

17.1.2 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, then it must have been directly started under the interface configuration mode.In the OSPFv2, the inteface 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. If a configuration interface participates in the running of OSPFv3, then the OSPFv3 will automatically run.In the OSPFv2, the interface must be directly started under the route configuration mode for the OSPF protocol to run.
4. In the enviroment where the OSPFv3 runs, when it is allowed to run multiple OSPF entieis 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.

17.1.3 Router ID Configuration

Each device running the OSPFv3 process must be identified with a router ID in the IPv4 address format.

Unlie 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.

17.1.4 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 supoort the IPSec authentication mechanism.

17.2 OSPFv3 Basic Configuration

The OSPFv3 protocol of D-Link Corporation has the following features:

- Supports broadcast and point-to point networks (configured as point-to-point Ethernet interface);
- Supports virtual links;
- Supports passive interfaces;
- Supports an interface to select a participant OSPF entity;
- Supports sub intervals (Stub area);
- Supports route redistribution;
- Supports route information filtering;

- Supports route information aggregation;
- Supports management instance setting;

To be implemeted:

- Supports NSSA areas;
- Supports authentication. The OSPFv3 will use the IPSec authentication mechanism.

Default OSPFv3 configuration:

Router ID		**Undefined**
Interface Configuration	Interface type	Broadcast netwokr
	Interface cost	Undefined
	hello message sending interval	10 seconds
	Adjacency router dead-interval	4 times the hello interval.
	LSA sending delay	1 seconds
	LSA retransmit interval.	5 seconds
	priority	1
	MTU check of databse description messages	Enable
Virtual Link	Virtual Link	Undefined
	hello message sending interval	10 seconds
	Adjacency router 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	Disable.
	External route Convergence	Disable.
Management Distance	Intra-area route	110
	Inter-area route	110
	External route	110
Auto cost		Enable Defaul 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 time between evey two calculations: 10 seconds
Route redistribution		Disable.
Route information filtering		Disable.
Passive interface		Disable.

To run the OSPFv3, follow these steps in the privileged mode:

Command	Function
configure terminal	Enter the global configuration mode.
ipv6 router ospf	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 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.

Note

In the interface configuration mode, starting an interface participating in the OSPFv3 will directly start an OSPFv3 route process.

17.3 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 ospf network {**broadcast** | **point-to-point**}	Set the network type of an interface. The default is the broadcast network type.
ipv6 ospf cost *cost*	(Optional) Define the cost of an interface.
ipv6 ospf hello-interval *seconds*	(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*	(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*	(Optional) Set link-state retransmit-interval.
ipv6 ospf retransmit-interval *seconds*	(Optional) Set the LSA transmit delay on an interface.
ipv6 ospf priority *number*	(Optional) Set the priority of an interface. The priority is used to select Designated Routers (DR) and Backup Designated Routers (BDR).
ipv6 ospf mtu-ignore	(Optional) Disable the interface to check MTU when it receives a database description message.

Command	Function
ip ospf database-filter all out	(Optional) Set an interface not to flood LSA information out. By default, the OSPF floods the received LSA information out from all the interfaces in a same area, excluding the interface receiving the LSA information.

You can use the no mode of the above commands to invalidate configured contents.

Note

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 neighbours. Otherwise, it will be impossible to establish a the adjacency relation. These parameters includes the following:

instance, hello-interval and dead-interval.

17.4 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 use of this hierarchical structure, each device is allowed to keep the the link state databse in the area where it resides and the topology inside the area invisible to outside.In this way, the link state databse of each device can be always in a resonable 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 has 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 (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 amout of AS external route information to enter an NSSA in other ways, namely, to enter the NSSA by the way of type 7 LSAs.

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* **nssa** [**no-redistribution**] [**default-information-originate**] [**no-summary**]	Configure a NSSA. no-redistribution: When the Layer 3 device is a NSSA ABR, you can use this keyword to import the routing information into normal area, but not into the NSSA. This originates the LSA of defaulted type 7 in the NSSA. This option only takes effect on NSSA ABR and NSSA ASBR, between which, however, there is a difference. On ABR, whether there is a default route or not in the routing table, the LSA of the defaulted route type-7 will be created. On the other hand, this is only created when there is a default route in the routing table on ASBR. **no-summarization**: Stop the Area Board Router (ABR) on the NSSA area from sending summarization-LSAs information to the NSSA area.
area *area-id* **default-cost** *cost*	Configure the cost of the default route sent to a stub area or NSSA.

You can use the no mode of the above commands to invalidate configured contents.

17.5 Configuring OSPFv3 Virtual Connection

In the OSPF, all areas must connect to the backbone area to ensure the commumication with other areas.If 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.

Note

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.

17.6 Configuring OSPFv3 Route Information Convergence

If there is no route convergence, each device in a network should maintain the informatin of routes to each network.By use of convergence, you can integrate some information and reduce the burden inside Layer 3 devices and network bandwidth.With the increase in network size, the importance of route convergence is higher.

DES-7200 supports two route convergence configurations: inter-area convergence and eternal route convergence.

17.6.1 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**] [**cost** *cost*]	Configure inter-area convergence.

Use **no area** *area-id* **range** {*ipv6-prefix* /*prefix-length*} to delete configured inter-area convergence.

17.6.2 Configuring External Route Convergence

It is allowed to configure external route convergence in the following conditions:

1. When an ASBR in a non- NSSA redistributes generated type 5 LSAs;
2. When an ASBR in an NSSA redistributes generated type type 7 LSAs;
3. When an ABR in an NSSA converts type 7 LSAs into type 5 LSAs.

To configure external route convergence, run the following command in the OSPFv3 configuration mode:

Command	Function
summary-prefix *prefix* [**advertise**|**not-advertise**] [**cost** *cost*] [**tag** *tag-value*]	Configure external route convergence.

Use **no summary-prefix** *prefix* to delete configured external route convergence.

Note

At present, our company does not support the application of the tag parameter.

17.7 Configuring OSPFv3 Default Route

In the OSPF protocol, there are multiple ways to generate the default route.

Refer to *Configuring OSPFv3 Area Parameter*. In a stub area, the default route indicated by a type 3 LSA will be automatically generated. In an NSSA, you can generate the default route indicated by a type3 LSA by using the **no-summary** parameter of the **area nssa** command. Likely, you can generat the default route indicated by a type7 LSA by using the **default-information-originate** parameter.

Additionally, through configuration, you can generate the default route indicated by a type5 LSA and pubish it inside the whole OSPF AS.In the OSPFv3 configuration mode, run the following command:

Command	Function
default-information originate [**always**] [**metric** *metric-value*] [**metric-type** *type-value*] [**route-map** *map-tag*]	Configure the generated default route.

Youcan use the **no default-information originate** command to delete the generated default route.

Note

1. The command is not allowed to be configured on the devices in an stub area.
2. Once you configure the command, the device will automatically compile ASBRs.

17.8 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 + 0.5 ≈ 10.

Currently, D-Link products do not support the setting of the bandwidth for network interfaces, but 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.

Note

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.

17.9 Configuring OSPFv3 Management Distance

A management distance indicates the confidence of one route information source and its range is from 1 to 255. The larger the value of a management distance, the lower the confidence.

OSPFroute information includes intra-area routes, inter-area routes and external routes. The OSPF allows configuring different management distances for different types of route information.

To change the OSPFv3 management distance, run the following command in the OSPFv3 configuration mode:

Command	Function
distance {*distance* | **ospf** {[**inter-area** *dist1*] [**inter-area** *dist2*] [**external** *dist3*]}}	Configure the OSPFv3 management distance.

17.10 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 datagase periodly 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:

Command	Function
timers lsa-group-pacing *seconds*	Adjust the pace interval of link-state information (LSAs) refresh, aging, check and calculation recorded in the OSPFv3 route process.

When the OSPFv3 process has much LSA information to interact with neighbours, the LSA information may form multiple updating messages to be sent to neighbours. To avoid the congestion of sending message queues and make CPU less busy, you can control the interval to send these updaing messages by the following commands:

If you need adjust the interval to interact LSA information, then run the following commands in the OSPFv3 configuration mode:

Command	Function
timers pacing flood *milliseconds*	Configure the time interval to update LSA messages.
timers pacing retransmission *milliseconds*	Configure the time interval to retrasmit LSA messages.

17.10.1 Configuring OSPFv3 Route Redistribution

Route information restribution can restribute 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*] [**tag** *tag-value*] [**route-map** *map-tag*]	Redistribute the route information of other protocols and select to set the conditions for redistribution. At present, the OSPFv3 supports static routes and connect routes.
default-metric *number*	Configure the default measurement value of distribution information.

You can use the **no redistribute** *protocol* mode to cancel route information redistribution.


Note

If you use the route-map parameter of the **redistribute** command and the matching rule of the parameter is associated with a prefix-list or you use a prefix-list which the **distribute-list out** command is associated to, then because the rules of these prefix-lists themselves change, please run the **clear ipv6 ospf redistribute** command to update the generated LSAs for restribution.


Note

At present, our company does not support the application of the tag parameter.

17.10.2 Configuring OSPFv3 Route Information Filtering

If you do not want to receive some route information or you do not want to notify neighbours of some route information, then you can filter the information by using the prefix list based on the IPv6.

To configure the filtering of the OSPFv3 transceiving route information, run the following command in the OSPFv3 configuration mode:

Command	Function
distribute-list prefix-list *list-name* {**in** [*interface-type interface-number*] | **out** [*protocol*]}	According to prefix lists, filter transceiving route information. **in**: filtering input; **out**: filtering output.

You can use the **no distribute-lsit** {**in**|**out**} command to cancel the filtering.


Note

If you use the distribute-list in command and the rules for prefix-list which distribute-list in is associated to change, then please run the clear ipv6 ospf force-spf command to redo the SPF calculation.

17.10.3 Configuring OSPFv3 Passive Interface

To prevent other Layer 3 devices in the network from learing 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 configurd 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 configuraion 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 configuraton of a passive interface.

17.11 OSPFv3 Debug and Monitoring

The OSPFv3 process supports plenty of debug commands and monitoring commands.

17.11.1 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 packet-in	Show that the OSPFv3 receives a message.
debug ipv6 ospf packet-out	Show that the OSPFv3 sends a message.
debug ipv6 ospf packet-event	Show that an error occurs when the OSPFv3 processes a received message.
debug ipv6 ospf negotiation-process	Show the proces when an adjacency relation is established between this device and neighbours.
debug ipv6 ospf if-state	Show interface state machine events and changes.
debug ipv6 ospf nbr-state	Show neighbour state machine events and changes.
debug ipv6 ospf kernel-route	Show the interaction with the kernel route table.

Use the above **undebug** commands to disable the above enabled **debug** commands.

Note

The debug commands are provided fortechnicians.

Running a debug command wil affect the performance of the system in a certain extent.

Therefore, after running debug commands, be sure to use undebug commnads to protect the performance of the system.

17.11.2 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.

Command	Function
show ipv6 ospf area [*area-id*]	Show the area information of the OSPFv3 process.
show ipv6 ospf area-range	Show the area aggregation address range information of the OSPFv3 process.
show ip ospf border-routers	Show the information of ABRs and ASBRs in the AS where the OSPFv3 is running.
show ipv6 ospf [*area-id*] **database** **show ipv6 ospf** [*area-id*] **database adv-router** *router-id* [**internal**] **show ipv6 ospf** [*area-id*] **database self-originate** [**internal**] **show ipv6 ospf** [*area-id*] **database internal** [**adv-router** *router-id* | **self-originate**] **show ipv6 ospf** [*area-id*] **database router** [*link-state-id*] [**adv-router** *router-id* | **self-originate**] **show ipv6 ospf** [*area-id*] **database network** [*link-state-id*] [**adv-router** *router-id* | **self-originate**] **show ipv6 ospf** [*area-id*] **database inter-prefix** [*link-state-id*] **show ipv6 ospf** [*area-id*] **database inter-prefix** [*link-state-id*] **adv-router** *router-id* [*IPv6 prefix*] **show ipv6 ospf** [*area-id*] **database inter-prefix** [*link-state-id*] **self-originate** [*IPv6 prefix*] **show ipv6 ospf** [*area-id*] **database inter-prefix** [*link-state-id*] *IPv6 prefix* [**adv-router** *router-id* | **self-originate**] **show ipv6 ospf** [*area-id*] **database inter-router** [*link-state-id*] **show ipv6 ospf** [*area-id*] **database inter-router** [*link-state-id*] **adv-router** *router-id* [*destination-router-id*] **show ipv6 ospf** [*area-id*] **database inter-router** [*link-state-id*] **self-originate** [*destination-router-id*] **show ipv6 ospf** [*area-id*] **database inter-router** [*link-state-id*] *destination-router-id* [**adv-router** *router-id* | **self-originate**] **show ipv6 ospf** [*area-id*] **database external** [*link-state-id*] **show ipv6 ospf** [*area-id*] **database external** [*link-state-id*] **adv-router** *router-id* [*IPv6 prefix*] **show ipv6 ospf** [*area-id*] **database external** [*link-state-id*] **self-originate** [*IPv6 prefix*] **show ipv6 ospf** [*area-id*] **database external** [*link-state-id*] *IPv6 prefix* [**adv-router** *router-id* | **self-originate**]	Show the database information.of the OSPFv3 process

Command	Function
show ipv6 ospf [*area-id*] **database nssa-external** [*link-state-id*] **show ipv6 ospf** [*area-id*] **database nssa-external** [*link-state-id*] **adv-router** *router-id* [*IPv6 prefix*] **show ipv6 ospf** [*area-id*] **database nssa-external** [*link-state-id*] **self-originate** [*IPv6 prefix*] **show ipv6 ospf** [*area-id*] **database nssa-external** [*link-state-id*] *IPv6 prefix* [**adv-router** *router-id* | **self-originate**] **show ipv6 ospf** [*area-id*] **database link** [*link-state-id*] **show ipv6 ospf** [*area-id*] **database link** [*link-state-id*] **adv-router** *router-id* [**interface** *interface*] **show ipv6 ospf** [*area-id*] **database link** [*link-state-id*] **self-originate** [**interface** *interface*] **show ipv6 ospf** [*area-id*] **database link** [*link-state-id*] **interface** *interface* [**adv-router** *router-id* | **self-originate**] **show ipv6 ospf** [*area-id*] **database intra-prefix** [*link-state-id*] **show ipv6 ospf** [*area-id*] **database intra-prefix** [*link-state-id*] **adv-router** *router-id* [**ref-lsa** {**router** | **network**}] **show ipv6 ospf** [*area-id*] **database intra-prefix** [*link-state-id*] **self-originate** [**ref-lsa** {**router** | **network**}] **show ipv6 ospf** [*area-id*] **database intra-prefix** [*link-state-id*] **ref-lsa** {**router** | **network**} [**adv-router** *router-id* | **self-originate**]	
show ipv6 ospf distribute-list	Show the filtering list information of the OSPFv3 process.
show ipv6 ospf flood-list [*interface-type interface-number*]	Show the LSA updating list information on the OSPFv3 process interface.
show ipv6 ospf interface [*interface-type interface-number*]	Show the interface information of the OSPFv3 process
show ipv6 ospf neighbor [**detail**] [*neighbor-id* | *interface-type interface-number* [*neighbor-id*]]	Show the neighbour information of the OSPFv3 process.
show ipv6 ospf redistribute-info	Show the restribution configuration information of the OSPFv3 process.
show ipv6 ospf request-list [[*interface-type interface-number*] [*neighbor-id*]]	Show the neighbour LSA request list information of the OSPFv3 process.
show ipv6 ospf retransmission-list [[*interface-type interface-number*] [*neighbor-id*]]	Show the neighbour LSA retransmission list information of the OSPFv3 process.
show ipv6 ospf summary-prefix	Show the external route convergence address range information of the OSPFv3 process.
show ipv6 ospf virtual-links	Show the virtual link information of the OSPFv3 process.

18 Network Communication Detection Tools

18.1 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
D-Link**#ping** [**ip**] [*address* [**length** *length*] [**ntimes** *times*] [**timeout** *seconds*]]	Ping network connectivity Test tools

A normal ping function can run in the user EXEC mode and privileged EXEC mode. By default, it sends five packets with the length of 100 bytes to a specified IP address. During the specified period (by default, 2 seconds), if there is a response, then one "!" displays. If no response, then one "." Displays, In the end, the system outputs a piece of statistics.This is a normal ping example:

```
D-Link #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
```

Extended ping functions can only run in the privileged EXEC mode. In an extended ping, you can specify the number, length and delay of sent packets. Like the normal ping function, the system outputs a piece of statistics in the end. This is an extended ping example:

```
D-Link#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
D-Link#
```

18.2 Traceroute Connectivity Test

By running the traceroute command, the system can show all the gateways passed by the packets for test from the source address to the destination address. The traceroute command is used to check connectivity of networks and exactly locate a failure (if any).The rule for network transfer is as follows: Everytime when one packet passes one gateway, the data of the TTL domain in the packet subtracts 1. When the data of the TTL domain is 0, the gateway discards the packet and sends an incorrect packet with a unreachable address back to the source address.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 untill the packet reachs 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
D-Link**#traceroute** [*protocol*] [*destination*]	Trace the network route for packet sending

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

1. Traceroute example where network connectivity is good:

```
D-Link#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
D-Link#
```

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 vey useful for network analysis.

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

```
D-Link#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
  D-Link#
```

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.

19 Configuring QOS

19.1 QOS Overview

19.1.1 Basic Framework of QoS

Traditional switches 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 switch now is exerting its performance of data forwarding and the use of its switching bandwidth is maximized.

The switch 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 implementation with this switch is based on the DiffServ architecture of IETF. 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:

1. 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.
2. 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 switch and router have 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, switches, routers, 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 equipment. To reduce the processing overhead on the backbone network, such assignment is often used on the network edge. Based on the class information, switches 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.

19.1.2 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:

1. 1. 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.
2. 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.


Tip

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.

3. 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.


Tip

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:

4. 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.
5. 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.
6. 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.

19.1.3 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.

19.1.4 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.

19.1.5 Queuing

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.

19.1.6 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.

19.2 QOS Configuration

19.2.1 Default QOS configuration

Make clear the following points of QoS before starting the configuration:

1. One interface can be associated with at most one policy-map.
2. One policy-map can have multiple class-map.
3. One class-map can be associated at most one ACL, and all ACEs in that ACL must have the same filter domain template.
4. The amount of ACEs associated with one interface meets the constraint described in the section "Configuring secure ACL".

The QoS function is disabled by default. All the packets have the same processing. 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

19.2.2 Configuring the Qos Trust Mode of an Interface

By default, the QoS trust mode of an interface is disabled.

Command	Description
configure terminal	Enter 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:

```
D-Link(config)#interface gigabitEthernet 0/4
D-Link(config-if)#mls qos trust dscp
D-Link(config-if)#end
D-Link#show mls qos interface g0/4
 Interface        : GigabitEthernet 0/4
 Attached input  policy-map:
 Default COS: trust dscp
 Default COS: 0
D-Link#
```

19.2.3 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 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:

```
D-Link#configure terminal
D-Link(config)#interface g0/4
D-Link(config-if)#mls qos cos 6
D-Link(config-if)#end
D-Link#show mls qos interface g0/4
 Interface        : GigabitEthernet 0/4
 Attached input  policy-map:
 Default COS: trust dscp
 Default COS: 6
D-Link#
```

19.2.4 Configuring Class Maps

You may create and configure Class Maps through the following steps:

Command	Description
configure terminal	Enter 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* | a*cl-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.

```
D-Link(config)#ip access-list extended acl_1
D-Link(config-ext-nacl)#permit tcp any any eq 80
D-Link(config-ext-nacl)#exit
D-Link(config)#class-map class1
D-Link(config-cmap)#match access-group acl_1
D-Link(config-cmap)#end
```

19.2.5 Configuring Policy Maps

You may create and configure Policy Maps through the following steps:

Command	Description
configure terminal	Enter 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.
police *rate-bps burst-byte*	Limit the bandwidth of the dataflow and specify the

Command	Description
[**exceed-action** {**drop** | **dscp** *dscp-value*}] **no police**	action for the excessive bandwidth part, where *rate-bps* is the limited bandwidth per second (kbps), *burst-byte* is the limited burst bandwidth (Kbyte), **drop** means dropping the message of the excessive bandwidth part, **dscp** *dscp-value means changing the* DSCP value of the message in excessive bandwidth part, and *dscp-valu*e value range varies with specific products.

Tip

If the same Policy Map is applied on multiple interfaces, the rate bandwidth configured with it will be shared by those interfaces. To have one interface exclusively occupy the rate bandwidth configured with the policies in the Policy Maps, it is possible to configure Policy Maps that is solely associated with the interface (as long as the name of the Policy Maps is different from others, while the associated classes can be the same).

For example, the following steps create a policy-map named policy1 and associate it with interface gigabitethernet 1/1.

```
D-Link(config)#policy-map policy1
D-Link(config-pmap)#class class1
D-Link(config-pmap-c)#set ip dscp 48
D-Link(config-pmap-c)#exit
D-Link(config-pmap)#exit
D-Link(config)#interface gigabitethernet 1/1
D-Link(config-if)#switchport mode trunk
D-Link(config-if)#mls qos trust cos
D-Link(config-if)#service-policy input policy1
```

19.2.6 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 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.

19.2.7 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 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:

```
D-Link#configure terminal
D-Link(config)#mls qos scheduler sp
D-Link(config)#end
D-Link#show mls qos scheduler
Global Multi-Layer Switching scheduling
 Strict Priority
D-Link#
```

19.2.8 Configuring Output Round-Robin Weight

You may set the output round-robin weight through the following steps:

Command	Description
configure terminal	Enter 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

```
D-Link#configure terminal
D-Link(config)#wrr-queue bandwidth 1 2 3 4 5 6 7 8
D-Link(config)#end
D-Link#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
D-Link(config)#
```

19.2.9 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 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

```
D-Link#configure terminal
D-Link(config)#priority-queue cos-map 1 2 4 6 7 5
D-Link(config)#end
D-Link#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
```

19.2.10 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 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:

```
D-Link#configure terminal
D-Link(config)#mls qos map cos-dscp 56 48 46 40 34 32 26 24
D-Link(config)#end
D-Link#show mls qos maps cos-dscp
cos dscp
--- ----
0   56
1   48
2   46
3   40
4   34
5   32
6   26
7   24
```

19.2.11 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 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:

```
D-Link#configure terminal
D-Link(config)#mls qos map dscp-cos 0 32 56 to 6
D-Link(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
D-Link(config)#
```

19.2.12 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 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:

```
D-Link#configure terminal
D-Link(config)#mls qos map ip-precedence-dscp 56 48 46 40 34 32 26 24
D-Link(config)#end
D-Link#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
```

19.3 QOS Displaying

19.3.1 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:

```
D-Link#show class-map
 Class Map cc
   Match access-group 1
D-Link#
```

19.3.2 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, where *policy-name* is the name of the selected policy map. When the class *class-name* is specified, it show the class map bound with the policy map.

For example:

```
D-Link#show policy-map
 Policy Map pp
    Class cc
D-Link#
```

19.3.3 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:

```
D-Link#show mls qos interface gigabitEthernet 0/4
 Interface        : GigabitEthernet 0/4
 Attached input  policy-map: pp
 Default COS: trust dscp
 Default COS: 6
D-Link#show mls qos interface policers
Interface        : GigabitEthernet 0/4
Attached input  policy-map: pp
D-Link#
```

19.3.4 Showing mls qos queueing

You may show the QoS queue information through the following steps:

Command	Description
show mls qos queuing	Show the QoS queue information, CoS-to-queue map, wrr weight and drr weight;

For example:

```
D-Link#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
```

19.3.5 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:

```
D-Link#show mls qos scheduler
Global Multi-Layer Switching scheduling
 Strict Priority
D-Link#
```

19.3.6 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:

```
D-Link#show mls qos maps cos-dscp
cos dscp
--- ----
0   0
1   8
2   16
3   24
```

```
4   32
5   40
6   48
7   56
D-Link#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
D-Link#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
```

19.3.7 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]

```
D-Link# show mls qos rate-limit
Interface       : GigabitEthernet 0/4
  rate limit input bps = 100 burst = 100
```

Contents

20 Configuring RMON

20.1 Overview

RMON is the standard monitoring specification of Internet Engineering Task Force (IETF). Through this specification, network managers can exchange network monitoring data. RMON place a detector on the network node, and the network management platform determines which information the detector will report, such as the monitored statistic information, time segment for collecting history information and more. A network device like a switch or router is a node in the network. If the RMON function is implemented, the functionality of RMON detector will be available to monitor the information of the location with that node.

The RMON has evolved through three phases. Phase 1 involves the remote monitoring of Ethernet, phase 2 is added with the token ring function, which is called the token ring remote monitoring module, and phase 3 is called the RMON2, with the RMON function advancing to a higher level of protocol monitoring.

The RMON in phase 1 (referred as RMON1 below) includes nine groups, any of which is optional (instead of required), but the use of some groups requires the support of the others.

The switch implements the contents in groups 1, 2, 3 and 9: statistical group, history group, alarm group and event group.

20.1.1 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 includes an Ethernet statistical table, whose contents are packets dropped, packets broadcast, CRC errors, block size, conflicts and so on.

20.1.2 History

History is the second group in RMON. It collects and measures, records and stores network values regularly for subsequent handling. History includes two small groups: HistoryControl and EthernetHistory. The former one is used to set control information such as sampling interval. The latter is used for managers to provide the history data of other statistics information, such as network segment traffic, error packet, broadcast packet, utilization, and collision times.

20.1.3 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.

20.1.4 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.

20.2 List of RMON Configuration Tasks

20.2.1 Configuring Statistical Group

You may use the following command to add a statistical entry:

Command	Function
D-Link(config-if)**#rmon collection stats** *index* **[owner** *ownername***]**	Add a statistical entry
D-Link(config-if)**#no rmon collection stats** *index*	Delete a statistical entry

The current version of DES-7200 supports only the statistics of Ethernet interfaces. The index value shall be an integer within 1-65535. At most 100 statistical entries can be configured currently.

20.2.2 Configuring History Control Group

You may use the following command to add a history control entry:

Command	Function
D-Link(config-if)**#rmon collection history** *index* **[owner** *ownername***] [buckets** *bucket-number***] [interval** *seconds***]**	Add a history control entry
D-Link(config-if)**#no rmon collection history** *index*	Delete a history control entry

The current version of DES-7200 supports only the Ethernet records. The index value shall be within 1-65535. At most 10 control entries can be configured.

Bucket-number: The data source to be used and the interval are specified for the control entry. Sampling will be done once in every sampling interval. The sampling results are saved. The bucket-number determines the maximum number of samples saved. When it reaches the maximum, the oldest records will be overwritten by new ones. The Bucket-number is within the range 1-65535, 0 by default.

Interval: Interval for sampling. The default value is 1800 seconds. Its value range is 1-3600.

20.2.3 Configuring Alarm Group and Event Group

You may use the following command to configure the alarm table:

Command	Function
D-Link(config)**#rmon alarm** *number variable interval* **{absolute | delta } rising-threshold** value [event-number] **falling-threshold** *value* [event-number] **[owner** *ownername***]**	Add a history control entry
D-Link(config)**# rmon event** *number* **[log] [trap** *community***] [***description-string***]**	Add an event group entry
D-Link(config)**#no rmon alarm** *number*	

Command	Function
D-Link(config)#no **rmon event** *number*	

number: index of the alarm table (event table), ranging 1-65535.

variable: Variable to be monitored in the alarm table. It must be of integer type.

Interval: Interval for sampling, ranging 0-2147483647

The keyword "absolute" means comparing the value in every sample with the upper and lower thresholds; the keyword "delta" means comparing the difference from the last sample with the upper and lower thresholds.

"value" defines the upper and lower thresholds.

event-number: When it is out of the lower or upper threshold, the event with index event-number will be triggered.

The keyword "log" means the action triggered is to record event.

The keyword "trap" means the action triggered is to send the trap message to the management station.

Community: Authentication name for sending trap

description-string: description of the event

20.2.4 Showing RMON Status

Command	Function
D-Link(config)# **show rmon alarms**	Show alarm group
D-Link(config)# **show rmon events**	Show event group
D-Link(config)# **show rmon history**	Show history group
D-Link(config)# **show rmon statistics**	Show statistics group

20.3 Examples of RMON Configurations

20.3.1 Example of Configuring Statistical Group

If you desire to take statistics for Ethernet port 3, run the following commands:

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

20.3.2 Example of Configuring History Group

If you desire to take statistics for the history information of Ethernet port 3 every 10 minutes, run the following commands:

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

20.3.3 Example of Configuring Alarm Group and Event Group

You desire to configure the alarm function for a MIB that supports statistics. 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”.

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

20.3.4 Example of Showing rmon Status

20.3.4.1 show rmon alarms

```
D-Link# 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
```

20.3.4.2 show rmon events

```
D-Link# 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
```

20.3.4.3 show rmon history

D-Link# 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
.......
```

20.3.4.4 show rmon statistics

```
D-Link#  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
```

21 System Log Configuration

21.1 Overview

During the operation of a router, 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. To facilitate the administrator to read and manage those log messages, they can be tagged with timestamp and serial number and classified with priorities.

21.1.1 Log Message Format

The format of 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

Note

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.

21.2 Log Configuration

21.2.1 Log Switch

The log switch is turned on by default. If it is turned off, the router 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
D-Link(config)# **logging on**	Turn on the log switch
D-Link(config)# **no logging on**	Turn off the log switch


Note

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.

21.2.2 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
D-Link(config)# **logging buffered** [*buffer-size* | *level*]	Record log in memory buffer
Red-Gian# **termninal monitor**	Allow log to be displayed on VTY window
D-Link(config)# **logging** *host*	Send log to the syslog sever in the network
D-Link(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.

"termninal 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.


Note

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.


Note

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.

21.2.3 Turning on 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
D-Link(config)# **service timestamps** *message-type* [**uptime|datetime**]	Enable the timestamp in the log information
D-Link(config)# **no service timestamps** *message-type* [**uptime|datetime**]	Disable the timestamp in the log information

There are two formats of timestamps: router startup time (uptime) or router date (datetime). 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.

21.2.4 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
D-Link(config)#**no service sequence-numbers**	Delete sequential number in the log messages
D-Link(config)# **service sequence-numbers**	Add sequential number in the log messages

21.2.5 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
D-Link(config)# **logging console** *level*	Set the level of log information that is allowed to be displayed on the console
D-Link(config)# **logging monitor** *level*	Set the level of log information that is allowed to be displayed on the VTY window (such as telnet window)
D-Link(config)# **logging buffered** [*buffer-size* | *level*]	Set the level of log information that is allowed to be recorded in memory buffer
D-Link(config)# **logging file flash:***filename* [*max-file-size*] [*level*]	Set the level of log information that is allowed to be recorded in extended flash
D-Link(config)# **logging trap** *level*	Set the level of log information that is allowed to be sent to syslog server

The log information of 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 to be displayed on specified device, the log information is at or below the set level will not be displayed. For example, after the command "logging console 6" is executed, all log information at or below level 6 will not 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.

21.2.6 Configuring 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
D-Link(config)# **logging facility** *facility-type*	Configure the log information device value
D-Link(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 DES-7200 is 23.

21.2.7 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 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
D-Link(config)# **logging source interface** *interface-type interface-number*	Configure the source port of log information
D-Link(config)# **logging source ip** *A.B.C.D*	Configure the source IP address of log messages

21.3 Log Monitoring

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

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

21.3.1 Examples of Log Configurations

Here is a typical example to enable the logging function:

```
!
hostname r36
!
interface FastEthernet 0/0
 ip address 192.168.200.42 255.255.255.0
 duplex auto
speed auto
!
interface FastEthernet 0/1
 duplex auto
 speed auto
!
interface Null 0
!
service sequence-numbers         //Enable sequential number
service timestamps debug datetime //Enable debug information timestamp, in date
format
service timestamps log   datetime //Enable log information timestamp, in date
format
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
!
line con 0
line aux 0
line vty 0 4
login
!
!
end
```

22 Managing the Switch

22.1 Overview

This chapter describes how to manage the switch.

- Access Control by Command Authorization
- Logon Authentication Control
- System Time Configuration
- Scheduled Restart
- Configuring a System Name and Prompt
- Title Configuration
- Viewing System Information
- Serial port rate configuration
- Using Telnet on the Switch

Note

For more detailed CLI commands, please see the CLI command references.

22.2 Access Control by Command Authorization

22.2.1 Overview

A simple way of providing 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 proprietary encryption algorithm.

22.2.2 Default Password and Privilege Level Configuration

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

22.2.3 Configuring or Changing Passwords of Different Levels

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

Command	Purpose
D-Link(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.
D-Link(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.
D-Link# **enable** [*level*] and D-Link# **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.

22.2.4 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.

22.2.5 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
D-Link(config-line)# **password** *password*	Specify the line password
D-Link(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.

22.3 Logon Authentication Control

22.3.1 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 switch 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 switch, we can authenticate users according to the username and password pairs stored centrally on a RADIUS server instead of local files. The switch 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.

22.3.2 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
D-Link(config)# **username** *name* **[password** *password* | **password** *encryption-type encrypted password*]	Establish the username identity authentication by using the encryption password.
D-Link(config)# **username** *name* **[privilege** *level*]	Set the privilege level for the user (optional).

22.3.3 Configuring Line Logon Authentication

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

Command	Function
D-Link(config-line)**#login local**	Set local authentication for line logon in AAA mode.
D-Link(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.

22.4 System Time Configuration

22.4.1 Overview

Every switch has its system clock, which provides the date (yeah, month, day) and time (hour, minute, second) and the week. When you use a switch for the first time, you must configure the system clock 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.

22.4.2 Setting the System Time and Date

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

Command	Function
D-Link**#clock set** *hh:mm:ss date month year* or D-Link**#clock set** *hh:mm:ss month date year*	Set the date and clock for the system.

For example: To change the system clock as 2002-12-25, 08:00:00

```
D-Link#clock set 10:10:12 20 Jun 2003 ⇐Set the system date and time
D-Link#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.

22.4.3 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:

```
D-Link#sh clock     ⇐Show the current time of the system
clock: 2003-5-20 11:11:34
```

22.5 Scheduled Restart

22.5.1 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. For example, if you need to reload the system in 10 minutes for test, you can configure the switch with **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. 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 in 12:00 a.m. on January 1, 2006, you 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

22.5.2 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	Purpose
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):

```
D-Link# reload at 12:00 11 Nov midday  ⇐Set the date and time to restart the
system
D-Link#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
```

22.5.3 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	Purpose
D-Link**# reload in** *mmm* **[***reload-reason***]**	Configure the system reload in *mmm* minutes, where the reload reason is described in *reload-reason* (if inputted)
D-Link**# 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):

```
D-Link# reload in 125 test  ⇐Set the system restart time
```

Or

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

22.5.4 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.

Deleting the Configured Restart Scheme

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

Command	Purpose
D-Link**# reload cancel**	Delete the configured restart scheme.

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

22.6 Configuring a System Name and Prompt

22.6.1 Overview

For easy management of the switch, 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 “Switch”. The default switch system name and prompt are both “Switch”.

22.6.2 Configuring a System Name

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

Command	Purpose
D-Link(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. In the following example, the switch name will be changed into DES-7200:

```
D-Linkt#configure terminal     ⇐Enter the global configuration mode.
D-Link(config)#hostname DES-7200⇐Set the switch name as DES-7200
DES-7200(config)#              ⇐The name has been modified successfully.
```

22.6.3 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 “Switch”. You can configure a system prompt with the **prompt** command in the global configuration mode.

Command	Purpose
D-Link# **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.

22.7 Title Configuration

22.7.1 Overview

When the user logs in to the switch, 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 daily notice is for all users that are connected to the switch. When a user logs in to the switch, the notice message will first be shown on the terminal. 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.

22.7.2 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 switch. You may configure the message of the day in the global configuration mode:

Command	Purpose
D-Link(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

Command	Purpose
	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:

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

22.7.3 Configuring a Login Banner

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

Command	Purpose
D-Link(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: 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 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.":

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

22.7.4 Displaying a Banner

The message of a banner displays on all connected terminals at login.

```
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:
```

In which, “Notice: In this example, "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.

22.8 Viewing System Information

22.8.1 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.

22.8.2 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	Purpose
D-Link# **show version**	Show system information and version

22.8.3 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	Purpose
D-Link# **show version devices**	Show current device information on the switch
D-Link# **show version slots**	Show slot and module information on the switch

22.9 Console Rate Setting

22.9.1 Overview

The switch has a console interface, through which it is possible to manage the switch. When it is the first time to use the switch, it is required to configure it through the console interface. You can change the baud rate of the serial port according to your requirement. Notice that the baud rate on the terminal must be the same with the baud rate of the serial port on the switch.

22.9.2 Setting Console Rate

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

Command	Purpose
D-Link(config-line)# **speed** *speed*	Set the console transmission rate, in bps. For the serial interface, you can only set the transmission rate as one

Command	Purpose
	of 9600, 19200, 38400, 57600 and 115200, 9600 by default.

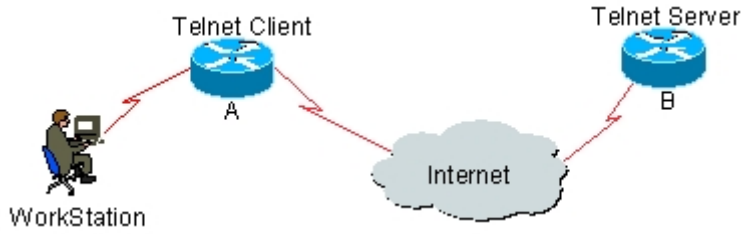
This example shows how to configure the baud rate of the serial port to 57600 bps:

```
D-Link#configure terminal          ⇐Enter the global configuration mode.
D-Link(config)#line console 0      ⇐ Enter the console line configuration
mode
D-Link(config-line)#speed 57600    ⇐Set the console rate as 57600
D-Link(config-line)#end            ⇐ Return to the privileged mode.
D-Link#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
```

22.10 Using Telnet on the Switch

22.10.1 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.



22.10.2 Using Telnet Client

You may use the telnet command on the switch to log onto a remote device:

Command	Purpose
D-Link**# telnet** *host-ip-address*	Log onto a remote device through telnet.

The example below shows how to establish the telnet session and manage the remote switch, where the IP address of the remote switch is 192.168.65.119:

```
D-Link#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:
```

23 Configuring SNMP

23.1 SNMP Related Information

23.1.1 Overview

The Simple Network Manger Protocol, shorted as SNMP, has become a network administration standard RFC1157 since August 1998. Thanks to the supports from numerous vendors, SNMP has become a factual network administration standard and is applicable in the interconnection environment of multiple vendors' systems. The SNMP enables network administrators to perform information query, network configuration, fault locating and capacity planning. Network monitoring and administration are the basic functions of SNMP.

The SNMP is a application layer protocol in the client/server mode, including three parts:

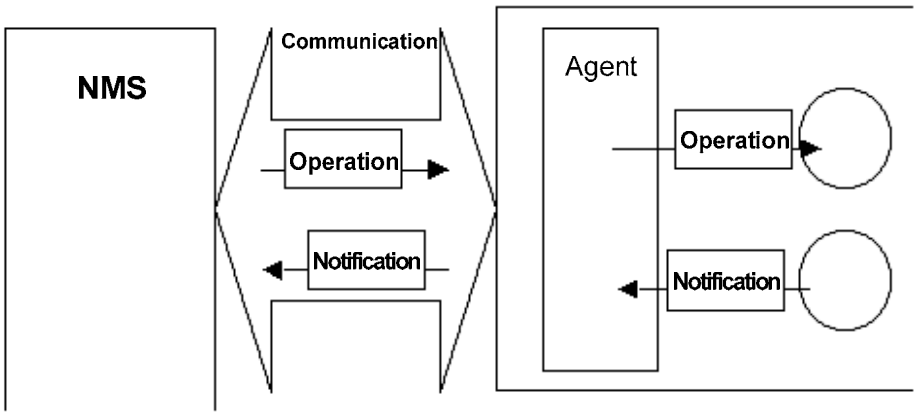
- SNMP network manager
- SNMP agent
- MIB management information base

The SNMP network manager is a system that works with the SNMP to contrl and monitor and network, called known as Network Management System (NMS). The network platforms that generally run on the NMS are HP OpenView, CiscoView and CiscoWorks 2000. D-Link Corporation has developed the network management software D-View for its network devices. All these popular network management software can be used to easily perform monitoring and management for network devices.

The SNMP Agent is the software that runs on the managed device to receive, handle and respond to the monitoring and control messages from the NMS. It also proactively sends some messages to NMS.

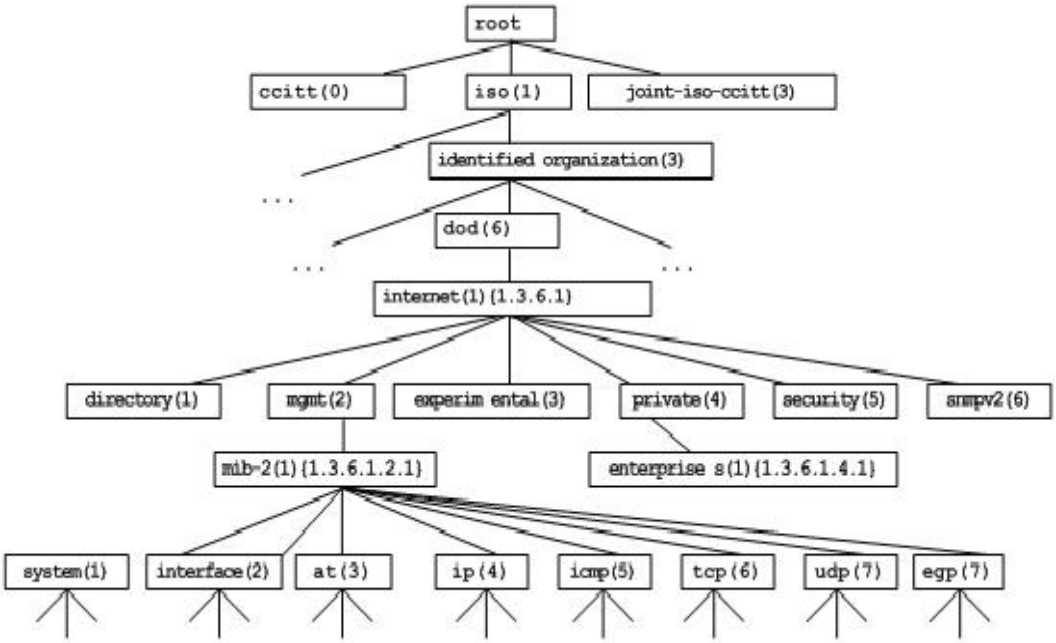
The diagram below illustrates the relationship between NMS and Agent:

Figure 1-15 Relationship between NMS and Agent



The Management Information Base (MIB) is a virtual network management information base. There is a great deal information for the managed network devices. In order to uniquely identify a specific managed unit in the SNMP message, the MIB has a tree hierarchy to describe the managed units in the network devices. Nodes on the tree indicate specific managed units. The example below shows a MIB object naming tree. To indicate a unique node system in the network devices, a string of numerals {1.3.6.1.2.1.1} is used as the object identifier of the managed unit. The MIB is the set of the object identifiers of the network devices.

Figure 1-16 Hierarchical Structure of MIB



23.1.2 SNMP Versions

Currently, the SNMP has the following versions:

- SNMPv1: The Simple Network Management Protocol, is the first formal SNMP version, 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 with during transmission
2. Insuring that the data is from a valid source data
3. Encrypting packets to insure the data confidentiality

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.

The SNMPv2C is added with the get-bulk operation mechanism and can return more detailed error information type for the NMS. 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 SNMPv1 managers and SNMPv2C managers can exist at the same time, so an SNMP agent must be able to recognize both SNMPv1 and SNMPv2C messages, and return correct version's message.

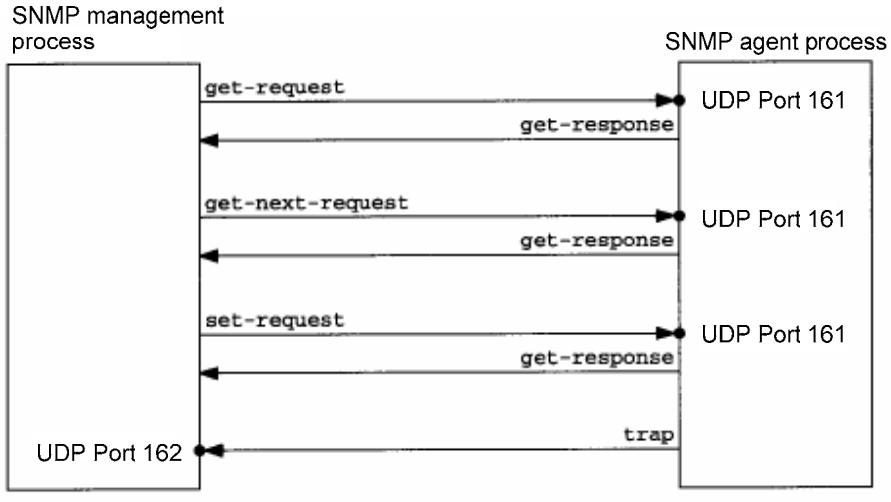
23.1.3 SNMP Management Operations

In the interaction information between NMS and Agent in SNMP, six operation types are defined:

1. get-request operation: NMS gets one or more parameter values from Agent
2. get-next-request operation: NMS gets next parameter of one or more parameter from Agent
3. get-bulk operation: NMS gets batch parameter values from Agent
4. set-request operation: NMS sets one or more parameter values for Agent
5. get-response operation: Agent returns one or more parameter values, as the response of the Agent to any of the above 3 operations for NMS
6. trap operation: Agent proactively sends messages to notify events occurring to NMS

The first 4 messages are sent from NMS to Agent, whereas the last two are from Agent to NMS (note: the SNMPv1 does not support the get-bulk operation). These operations are detailed below respectively.

Figure 1-17 Types of SNMP messages



The first 3 operations from NMS to Agent and the response operation of the Agent are implemented on UDP port 161. The trap operation from Agent is implemented on UDP port 162.

23.1.4 SNMP Security

In the SNMPv1 and SNMPv2 versions, authentication name is used to determine the right for using MIB objects. In order for the switch management, the community string defined on the NMS must match at least one of the community strings defined on the switch.

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.

23.1.5 SNMP Engine ID

Gives read and write access to authorized management stations to all variables in MIB 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:

1. The first four octets are assigned with the private enterprise number in HEX by IANA.
2. 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

23.2 SNMP Configuration

The configuration of the SNMP is completed in the global mode of network devices. It is required to enter into the global configuration mode first to make SNMP configuration.

23.2.1 Configuring Authentication Name and Access Rights

The SNMPv1/SNMPv2C works with Community-based security plan, where the SNMP agent accepts only the management operations with the same authentication name (Community-String), and does not respond to the SNMP messages with unmatched authentication name of the network device and then drops the messages. The authentication name is like the password between NMS and Agent.

- It is possible to configure the access list association to manage only the NMS of the specified IP addresses.
- It is possible to configure the community operation rights as ReadOnly or ReadWrite.
- Specify the view name for the view-based management. By default, no view is configured, allow access to all MIB objects
- It is possible to specify the manager IP address of the authentication name. If not, it means no restriction for using the manager IP address of the authentication name. By default, there is no restriction for this.

To configure the SNMP authentication name, execute the following command in the global configuration mode:

Command	Function
D-Link(config)# **snmp-server community** *string* [**view** *view-name*] [**ro** | **rw**] **[host** *host-ip***]**	Configure authentication name and rights

It is possible to configure one or more entries to specify different community names, so that the network device can provide NMS management with different rights. To delete the community name and rights, execute the **no snmp-server community** command in the global configuration mode.

23.2.2 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.

- It is possible to configure including/excluding view.
- It is possible to set read-only view and writable view for a group of users.
- For SNMPv3 users, it is possible to specify the security level, for authentication or not, and for encryption or not.

To configure the MIB view and group, execute the following command in the global configuration mode:

Command	Function
D-Link(config)**#snmp-server view** *view-name oid-tree* {**include | exclude**}	Create a MIB view to include or exclude the associated MIB objects.
snmp-server group *groupname* **{v1 | v2c |v3 {auth | noauth | priv}} [read** *readview***][write** *writeview***]**	Create a group and associated 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.

23.2.3 Configurting SNMP User

The security management can be implemented with user-based security module. The user-based management requires the configuration of user information. The NMS must have legal users to be able to communicate with the agents.

For SNMPv3 users, it is possible to specify the security level, authentication algorithm (MD5 or SHA) and authentication password, and encryption algorithm (only DES now) and encryption password.

To configure the SNMP user, execute the following command in the global configuration mode:

Command	Function
D-Link(config)**# snmp-server user** *username groupname* **{v1 | v2 | v3 [encrypted] [auth { md5|sha }** *auth-password* **] [priv des56** *priv-password***]}**	Configure the user information

Delete the specified user by using the **no snmp-server user** *username groupname* command.

23.2.4 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
D-Link(config)# **snmp-server host** *host-addr* **traps** {**version** {**1**|**2c** |**3** [**auth | noauth | priv**]} *community-string* [*type*]	Configure the SNMP host address, message type, authentication name (or username under SNMPv3), security level (only supported by SNMPv3), and more

23.2.5 Configuring SNMP Agent Parameters

It is possible to 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, execute the following command in the global configuration mode:

Command	Function
D-Link(config)**#snmp-server contact** *text*	Configure the contact of the system
D-Link(config)**#snmp-server location** *text*	Configure the location of the system

Command	Function
D-Link(config)**#snmp-server chassis-id** *number*	Configure the sequential number of the system

23.2.6 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. In the global configuration mode, execute the following commands:

Command	Function
D-Link(config)**#snmp-server packetsize** *byte-count*	Configure the maximum packet size of the agent

23.2.7 Stopping SNMP Agent

The SNMP agent service is a service provided by DES-7200 and can be started or stopped at any time. To stop it, execute the following commands in the global configuration mode:

Command	Function
D-Link(config)**#no snmp-server**	Stop SNMP agent service

23.2.8 Configuring Agent to Sent Trap to NMS Proactively

TRAP is the message automatically sent by Agent to NMS unsolicitedly, and is used to report some critical and important events. By default it is not allowed for Agent to send traps. To enable it, execute the following command in the global configuration mode:

Command	Function
D-Link(config)**#snmp-server enable traps** [*type*][*option*]	Allow Agent to sent trap proactively
D-Link(config)**#no snmp-server enable traps** [*type*][*option*]	Forbid Agent to sent trap proactively

23.2.9 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
D-Link(config)**#snmp-server trap-source** *interface*	Specify the source port for sending Trap messages
D-Link(config)# **snmp-server queue-length** *length*	Specify the length of each Trap message queue
D-Link(config)# **snmp-server trap-timeout** *seconds*	Specify the interval for sending Trap messages

23.3 SNMP Monitoring and Maintenance

23.3.1 Checking the Current SNMP Status

To monitor the SNMP status and troubleshoot SNMP configurations, 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.

```
D-Link#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
   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:

Displayed messages	Description
Bad SNMP version errors	SNMP version is incorrect
Unknown community name:	The authentication name is unrecognized.
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

23.3.2 Checking the MIB Objects Supported by Current SNMP Agent

In the privileged user mode, execute **show snmp mib** to check the MIB objects supported by the current agent.

```
D-Link#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
```

23.3.3 Checking SNMP Users

In the privileged user mode, execute **show snmp user** to check the SNMP users configured in the current agent.

```
D-Link#show snmp user

User name: test
Engine ID: 800013110300000000000
storage-type: permanent    active
Security level: auth priv
Auth protocol: SHA
Priv protocol: DES
Group-name: g1
```

23.3.4 Checking SNMP Views and Groups

In the privileged user mode, execute **show snmp group** to check the groups configured in the current agent.

```
D-Link#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:
```

In the privileged user mode, execute **show snmp view** to check the views configured in the current agent.

```
D-Link#show snmp view
default(include) 1.3.6.1
test-view(include) 1.3.6.1.2.1
```

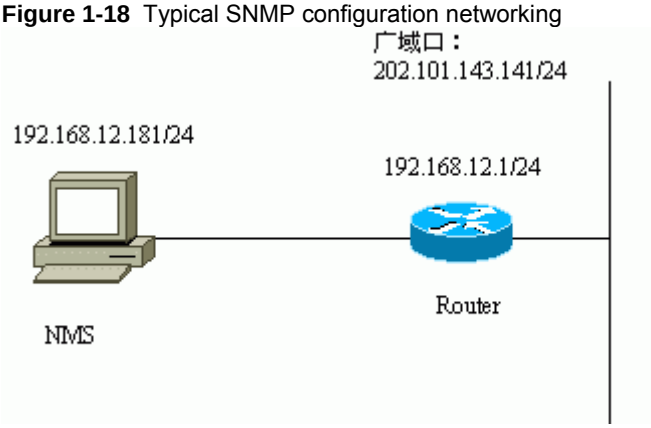
23.4 SNMP Configuration Examples

23.4.1 Typical Configuration Example

■ **Configuration requirements**

As shown in the diagram, the network device and NMS are connected through Ethernet. The IP address of the NMS is 192.168.12.181, and that of the network device is 192.168.12.1. The NMS has network management software running (HP OpenView, for example).

Figure 1-18 Typical SNMP configuration networking



■ **Specific Network Device Configurations**

Start the SNMP agent service:

```
D-Link(config)#snmp-server community public RO
```

Execute the above command in the global configuration mode, and then the network device will start the SNMP agent service. Now, the NMS can implement SNMP monitoring for the network devices. However, this configures only the read-only right and does not allow modification of the network device configuration. All other configurations are optional.

To enable the read-write function, execute the following command:

```
D-Link(config)#snmp-server community private RW
```

Below are some basic SNMP agent parameters configured on the network device. The NMS gets to know the basic system information of the network device by getting these parameters. This configuration is optional.

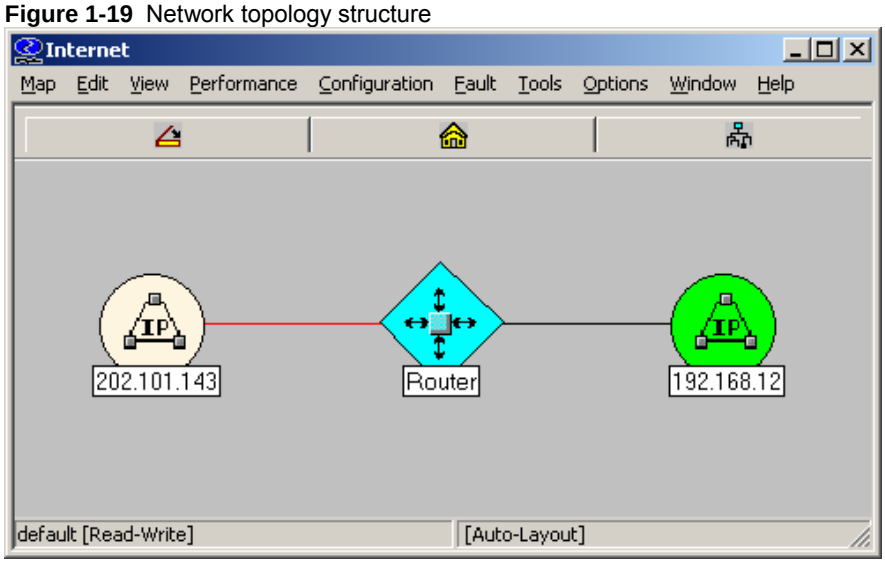
```
D-Link(config)#snmp-server location fuzhou
D-Link(config)#snmp-server contact wugb@i-net.com.cn
D-Link(config)#snmp-server chassis-id 1234567890 0987654321
```

The command below allows the network device to proactively send some traps to the NMS. This configuration is optional.

```
D-Link(config)#snmp-server enable traps
D-Link(config)#snmp-server host 192.168.12.181 public
```

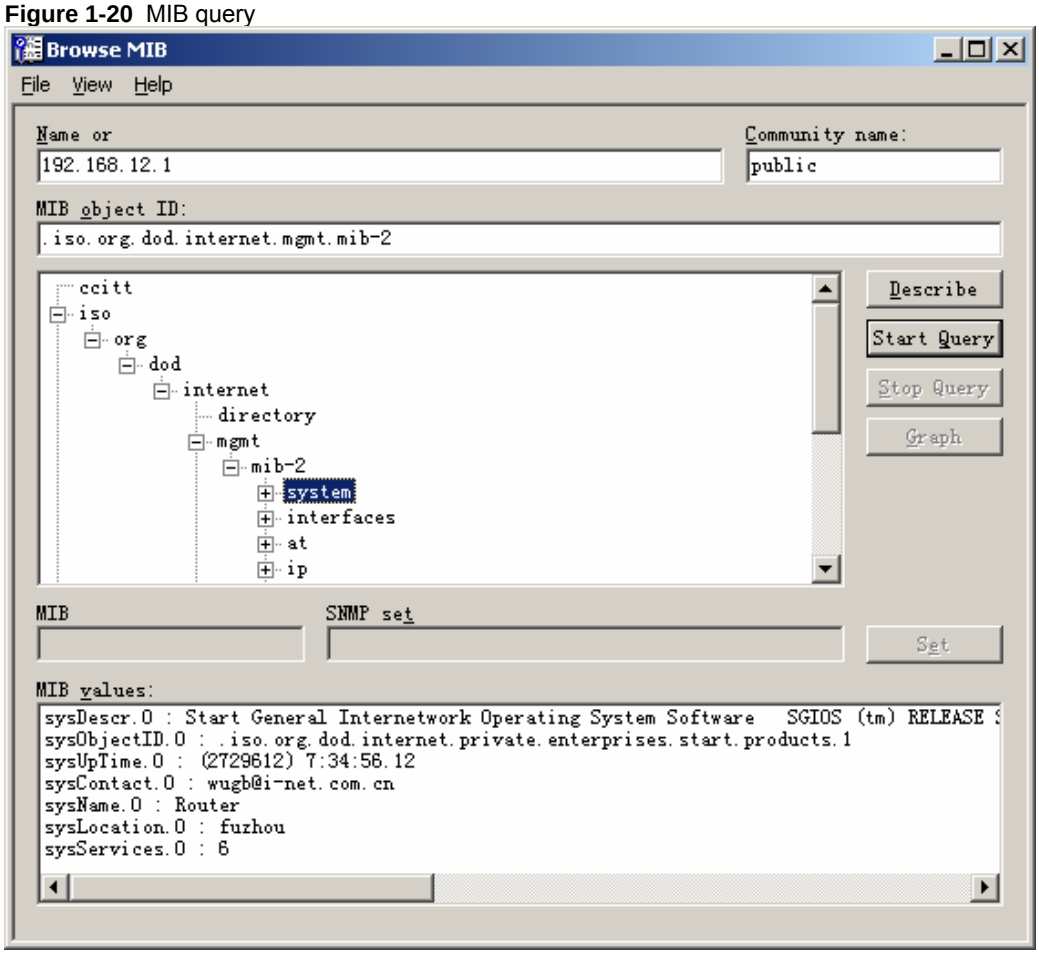
Now, the SNMP agent of the network device is configured completely. The NMS can now monitor and manage the network device. Regarding HP OpenView, for example, the network topology map will be generated, as shown below.

Figure 1-19 Network topology structure



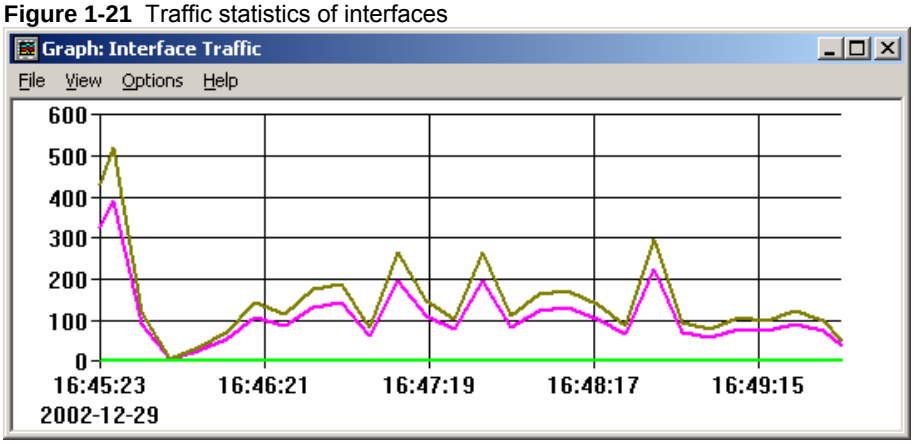
Now it is possible to query or set the managed units in the network device. Click the TOOL->SNMP MIB Brower menu on the HP OpenView to display the following dialog box. Enter the IP address 192.168.12.1 in the Name field and "public" in the Community Name field. Select the specific managed unit of the 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 1-20 MIB query



The HP OpenView features powerful network management function, such as the traffic statistical chart of the network interfaces. For details of other SNMP functions, see the document of the network management software, no more details here.

Figure 1-21 Traffic statistics of interfaces



23.4.2 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:

```
D-Link(config)#access-list 1 permit 192.168.12.181
D-Link(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.

23.4.3 Example of SNMPv3 Related Configurations

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 authentication and the authentication key is des-priv. Meanwhile, configure the switch to send trap message to 192.168.65.199 in the form of SNMPv3. The user name is **v3user**. The trap message is sent in authentication & encryption mode, with the MD5 being authentication mode and the authentication password being **md5-auth**; the encryption algorithm is des, with the encryption key as using **des-priv** as the encryption password.

```
D-Link(config)# snmp-server view v3userview 1.3.6.1.2.1 include
D-Link (config)# snmp-server group v3usergroup v3 priv read v3userview write
v3userview
D-Link (config)# snmp-server user v3user v3usergroup v3 auth md5 md5-auth priv
des56 des-priv
D-Link (config)# snmp-server host 192.168.65.199 traps version 3 priv v3user
```

24 Simple Network Time Protocol (SNTP)

24.1 Overview

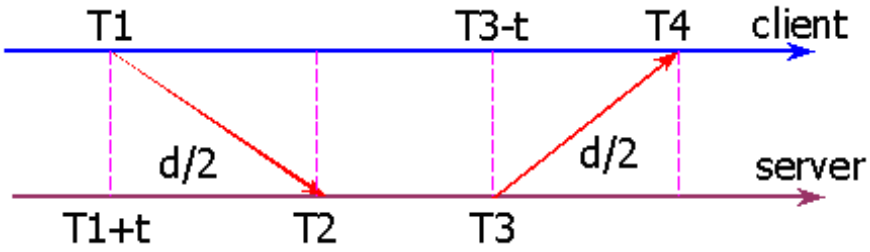
Currently, a communication protocol is commonly used on the Internet to synchronize the time on the network, that is, the Network Time Protocol (NTP). As the simplified version of the NTP protocol, the Simple Network Time Protocol (SNTP) is another such protocol.

The NTP can work with various platforms and operating systems and it uses a very exact algorithm, so it is nearly immune to delay and dither, as it provides 1-50 ms accuracy. The NTP also provides the authentication mechanism, featuring a high security. However, the NTP has a complicated algorithm and has a high requirement for the system.

As the simplified version of the NTP, the SNTP uses a simpler algorithm for time calculation and features a high performance. Its accuracy can usually reach about 1s, which can meet the needs in most cases.

Since the SNTP packets and the NTP packets are exactly the same, the SNTP Client implemented by this switch is fully compatible with the NTP Server.

SNTP Principle: Measurement of Network Delay and Clock offset



Originate Timestamp	T1	time request sent by client
Receive Timestamp	T2	time request received at server
Transmit Timestamp	T3	time reply sent by server
Destination Timestamp	T4	time reply received at client

t is the time different between server and client.

d is the trip time between them.

Because

T2 = T1 + t + d / 2;

So

T2 - T1 = t + d / 2;

And because

T4 = T3 – t + d / 2;

So

T3 - T4 = t – d / 2;

Now

d = (T4 - T1) - (T3 - T2);

t = ((T2 - T1) + (T3 - T4)) / 2;

With the result of “t” and “d”, the SNTP Client can calculate the current time.

As a result, the current time is T4 + t

24.2 Configuring SNTP

This section describes how to configure SNTP.

24.2.1 Default SNTP Configuration

By default, the SNTP configurations are as follows:

Item	Default value
SNTP status	Disable; the SNTP service is disabled.
IP address of the NTP Server	0
SNTP synchronization interval	1800s
Local time zone	+8, that is, East 8

24.2.2 Enabling SNTP

In the privileged mode, you can enable SNTP by performing the following steps:

Step 1	Enter the global configuration mode.
	`RedGiant#config`
Step 2	Enable SNTP and instantly synchronize the clock. In future, whenever this command is executed, the clock will be synchronized immediately, not waiting for the scheduled synchronization. (To prevent frequent time synchronization, the immediate synchronization interval shall not be less than 5 seconds.)
	`Switch(config)# sntp enable`
Step 3	Return to the privileged mode.
	`RedGiant(config)#End`
Step 4	Show the current configuration.
	`RedGiant#show running-config`
Step 5	save the configuration.
	`Copy running-config startup-config`

To disable SNTP, use the **no sntp enable** global configuration command.

24.2.3 Configuring NTP Server Address

Since the SNTP packets and the NTP packets are exactly the same, the SNTP Client is fully compatible with the NTP Server. There are many NTP Servers on the network. You can select one with short network delay as the NTP Server on the switch.

To obtain the specific NTP server address, log in to http://www.ntp.org/,

for example, 192.43.244.18 (time.nist.gov).

In the privilege mode, perform these steps to configure the DHCP Server IP address:

Step 1	Enter the global configuration mode.
	`RedGiant#config`
Step 2	Configure the IP address of SNTP Server.
	`RedGiant(config)#sntp server <ip-addr>`
Step 3	Return to the privileged mode.
	`RedGiant(config)#End`
Step 4	Show the current configuration.
	`RedGiant#show running-config`
Step 5	save the configuration.
	`Copy running-config startup-config`

24.2.4 Configure the SNTP synchronization interval

The SNTP Client needs to synchronize with the NTP Server at periodical intervals for calibrating the clock periodically. You can configure the interval for synchronization between the switch and the NTP Server by performing the following steps.

Step 1	Enter the global configuration mode
	`RedGiant#config`
Step 2	Set the periodical synchronization interval, in seconds, range 60-65535 seconds, 1800 seconds by default
	`RedGiant(config)#sntp interval <seconds>`
Step 3	Return to the privileged mode.
	`RedGiant(config)#End`
Step 4	Show the current configuration.
	`RedGiant#show running-config`
Step 5	save the configuration
	`Copy running-config startup-config`

24.2.5 Configuring Local Time Zone

The time obtained from the communication of the SNTP is the GMT. To obtain the accurate local time, you need to set the local time zone to adjust the standard time.

Step 1	Enter the global configuration mode.
	`RedGiant#config`
Step 2	Configure the time zone, within the range of -23 ~ 23, where the negative number means the west and the positive number means the east. East zone. For example, 8 means the east 8th zone, -8 means the west 8th zone, and 0 means 0 means the Greenwich standard time. The default is Beijing Time, that is, East 8.
	`RedGiant(config)#clock time-zone <time-zone>`

Step 3	Return to the privileged mode.
	`RedGiant(config)#End`
Step 4	Show the current configuration.
	`RedGiant#show running-config`
Step 5	save the configuration.
	`Copy running-config startup-config`

You can restore the default value by using the no clock time-zone command.

24.3 Showing SNTP

The steps are as follows:

Step 1	Show the related parameters of SNTP.
	`RedGiant#show sntp`
Step 2	Use the show system-guard to view the configuration parameters of the system guard:

	`RedGiant#show sntp`
	`SNTP state : ENABLE ;SNTP is enabled or not`
	`SNTP server : 192.168.4.12 ;NTP Server`
	`SNTP sync interval : ----- Synchronization interval`
	`Time zone : +8 ;local time zone`

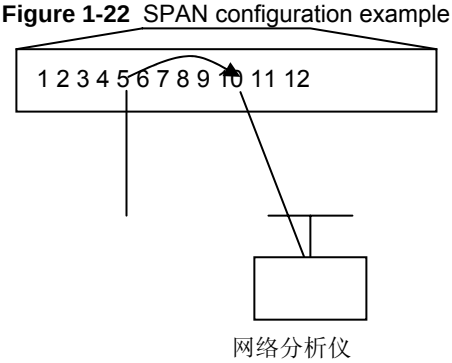
25 Configuring SPAN

25.1 Overview

You can copy the packets from one port to another port connected with a network analysis device or RMON analyzer by using the SPAN to analyze the communication on the port. The SPAN mirrors all the packets sent/received at a port to a physical port for analysis.

For example, all the frames on Gigabit port 5 are mirrored to Gigabit port 10, as shown in Figure 1-1. Although the network analyzer connected to port 10 is not directly connected to port 5, it can receive all the frames at port 5.

Figure 1-22 SPAN configuration example



Through the SPAN, you can monitor all the frames incoming/outgoing the source port, including the route input frames.

SPAN does not affect the normal message exchange between switches. It only copies all ingoing frames and outgoing frames from the source port to the destination port. However, a destination port with excessive traffic volume, for example, when one 100Mbps destination port monitors a 1000Mbps port, may cause frames to be dropped.

25.2 SPAN Concepts and Terms

This section describes the concepts and terms related to SPAN configuration.

25.2.1 SPAN Session

One SPAN session is the combination of one destination port and source port. You can monitor the input, output, and bi-directional frames of one or multiple interfaces.

You may configure one or more SPAN sessions. Both switched port and routed port can be configured as the source or destination ports. The SPAN session does not affect the normal operation of the switch.

You can configure the SPAN session on one disabled port, but the SPAN does not take effect until you enable the destination and source ports. The **Show monitor session** *session number* command allows you to show the operation status of the SPAN session.

One SPAN session does not take effect immediately after power-on, but until the destination port becomes operable.

25.2.2 Frame Type

The SPAN session includes the following frame types:

Received frame: Received frames include all known unicast frames and routing frames, and each received frame is copied to the destination port. In one SPAN session, you can monitor the input frames of one or multiple source ports. The inputted frames from the source port may be dropped due to some reasons, for example, port security, but this does not affect the function of the SPAN, and the frames are still sent to the destination port.

Transmitted frames: All known unicast frames from the source port will be copied to the destination port. In one SPAN session, you can monitor the input frames of one or multiple source ports. The inputted frames to the source port from other ports may be dropped due to some reasons, but the frames are still sent to the destination port.

Bi-directional frame: It includes the two types of frames mentioned above. In one SPAN session, you can monitor the input and output frames of one or multiple source ports.

25.2.3 Source Port

The source port (also known as the monitored interface) is a switched port or routed port, and is monitored for network analysis. In one SPAN session, you can monitor input, output and bi-directional frames. There is no restriction for the maximum number of the source ports.

A source port has the following features:

It can be a switched port, routed port or AP.

It cannot be a destination port at the same time.

It can specify the input/output directions of the monitored frames.

The source port and destination port can reside on the same VLAN or different VLANs.

25.2.4 Destination Port

The SPAN session has a destination port (also known as the monitoring port), which is used to receive the frames copied from the source port.

The destination source port has the following features:

It can be a switched port or routed port. Meanwhile, the sessions 2-n of the DES-7200 switch also support AP as the destination SPAN port.

When the SPAN session is activated, the destination port does not participate in the STP.

25.2.5 SPAN Traffic

You can use the SPAN to monitor all network communications, including multicast frames and BPDU frames.

25.2.6 Interfaces between the SPAN and Other Functions

The SPAN interacts with the following functions.

Spanning Tree Protocol (STP) — When the SPAN session is activated, the destination port does not participate in the STP. When the SPAN session is disabled, the destination port can participate in the STP.

25.3 Configuring SPAN

This section describes how to configure the SPAN on your switch, covering:

25.3.1 Configuring SPAN

Table 1-1 Default SPAN Configuration

Function	Default Configuration
SPAN status	Disabled

25.3.2 SPAN Configuration Guide

Please follow the rules below in configuring the SPAN.

The network analyzer should be connected to the monitoring interface.

The DES-7200 series switches support 1-n sessions. For sessions 2-n, the tag behavior of the ingoing mirrored messages (messages entering into the switch) is the same as that of the outgoing messages. In other words, if the input messages are untagged, the mirrored messages will also be untagged, and vice versa. The input mirrored message at layer-3 exchange is the same as the input messages, whereas for the output mirror messages, the VID and the messages after the source MAC will be modified. The mirroring behavior of session 1 is just like that of D-Link's DES-7200 series.

The destination port cannot be a source port, and the source port cannot be a source port.

You can configure one disabled port as a destination port or source port, but the SPAN function does not take effect until the destination port and source port have been enabled again.

The **no monitor session** *session_number* global configuration command allows you to delete the source or destination port from the SPAN session.

The SPAN destination port does not participate in the STP. The SPAN monitoring frames also include BPDU, so the BPDU frames received by the SPAN destination port are all copied from the SPAN source port.

When the SPAN is enabled, the configuration change has the following result.

- If you change the VLAN configuration of the source port, the configuration takes effect immediately.
- If you change the VLAN configuration of the destination port, the configuration does not take effect until the SPAN session is deleted.
- If you have disabled the source port or destination port, the SPAN does not take effect.
- If you add the source port or destination port into an AP, this will cause the cancellation of the source or destination port of SPAN.

25.3.3 Creating a SPAN Session and Specifying the Monitoring Port and Monitored Port

Specify a SPAN session and the destination port and the source port.

Command	Function
D-Link(config)#monitor session *session_number* source interface *interface-id* [,| -] {both | rx | tx}	Specify the source port. For *session_number*, specify 1. For *interface-id*, specify the appropriate interface ID.
D-Link(config)#monitor session *session_number* destination interface *interface-id*	Specify the source port. For *session_number*, specify 1. For *interface-id*, specify the appropriate interface ID.

To delete the SPAN session, use the **no monitor session** *session_number* global configuration command. To delete the SPAN session, use the **no monitor session** *session_number* global configuration command. You can use the **no monitor session** *session_number* **source interface** *interface-id* global configuration command or the **no monitor session** *session_number* **destination interface** *interface-id* command to delete the source port or destination port.

The following example shows how to create one SPAN session: session 1. First, clear the configuration of the currently session 1, and then set to mirror the frames of port 1 to port 8. **The Show monitor session** privileged command allows you to verify your configuration.

```
D-Link(config)# no monitor session 1
D-Link(config)# monitor session 1 source interface gigabitEthernet 3/1 both
D-Link(config)# monitor session 1 destination interface gigabitEthernet 3/8
D-Link(config)# end
D-Link# show monitor session 1
sess-num: 1
src-intf:
GigabitEthernet 3/1 frame-type Both
dest-intf:
GigabitEthernet 3/8
```

25.3.4 Deleting a Port from the SPAN Session

Delete the source port from a SPAN session.

Command	Function
D-Link(config)#no monitor session *session_number* source interface *interface-id* [,| -] [both | rx | tx]	Specify the source port to delete. For *session_number*, specify 1. For *interface-id*, specify the appropriate interface ID.

You can use the **no monitor session** *session_number* **source interface** *interface-id* global configuration mode to delete the source port from a SPAN session. The following example shows how to delete port 1 from session 1 and verify your configuration.

```
D-Link(config)# no monitor session 1 source interface gigabitethernet 1/1 both
D-Link(config)# end
D-Link# show monitor session 1
sess-num: 1
dest-intf:
GigabitEthernet 3/8
```

25.3.5 Specifying the Source/Destination MAC of the Mirror Frame

The function is supported only by the S20.

In the privileged mode, follow these steps to specify the source MAC of the mirrored frame and the destination MAC.

Command	Function
D-Link(config)# no monitor session *session_number* **[source interface** *interface-id* **[both | rx | tx] | destination interface** *interface-id* **] | mac {source** *mac-addr*| **destination** *mac-addr* **} [both | rx | tx]** **{source|destination}** *mac-address* **[both | rx | tx]**	Configure the source MAC to be mirrored and the destination MAC.

Execute the **no monitor session** *session_number* **mac** {**source | destionation**} **[both | rx | tx]** global configuration command to delete the source and destination MAC of the mirrored frame.

25.4 Showing the SPAN Status

The show monitor privileged command allows you to show the current SPAN status. The following example illustrates how to show the current status of SPAN session 1 by using the show monitor privileged command.

```
D-Link# show monitor session 1
sess-num: 1
src-intf:
GigabitEthernet 3/1 frame-type Both
dest-intf:
GigabitEthernet 3/8
```

26 Module Hot-Plugging/Unplugging

26.1 Overview

The DES-7200 series switches of D-Link support hot-plugging/unplugging of modules. You may plug and unplug modules while the switch is powered on, without affecting the normal system operation or other modules.

26.2 Module Hot-Plugging/Unplugging Configuration

This chapter includes:

- Plugging or Unplugging Modules
- Installing or Uninstalling Modules
- Viewing Module Information

26.2.1 Plugging or Unplugging Modules

You may plug modules while the switch is operating (hot-plugging/unplugging). The operation of the other modules will not be affected. When the modules are plugged into the slots, the management software of the switch will attempt to install the module driver automatically.

Note

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.

26.2.2 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:

Step 1	configure terminal	Enter the global configuration mode.

Step 2	install slot-num moduletype	Install the module of a specified type in a slot
Step 3	end	Return to the privileged mode.

Note

The installation of driver does not need physical presence of the module. This means that you may "pre-configure" the switch. You may run the "install" command to virtualize the module of a specified type and then configure it. When the module is plugged in the slot, all configurations take effect automatically.

You may uninstall a running module. Once uninstalled, all configurations for that module will be lost and the module will be deactivated, unless you manually install the driver for the module, or unplug it and then plug it back again.

In the global configuration mode, execute the following commands to uninstall a module manually:

Step 1	configure terminal	Enter the global configuration mode.
Step 2	no install *slot-num*	Uninstall the module in a slot
Step 3	end	Return to the privileged mode.

26.2.3 Viewing Module Information

In the privileged user mode, execute the following commands to check the details of a module so as to uninstall it manually:

Step 1	show version module detail	View module information

```
D-Link #show version module detail
Device             : 1
Slot               : 1
User Status        :  installed
Software Status    : ok
Online Module      :
       Type        : M8606-24SFP/12GT7200-24G
       Ports       : 24
       Version     : 01-01-05-02
Configured Module  :
       Type        : M8606-24SFP/12GT7200-24G
       Ports       : 24
       Version     : 01-01-05-02

Device             : 1
Slot               : 2
User Status        : installed
Software Status    : ok
Online Module      :
       Type        : M8606-2XFP7200-2XG
       Ports       : 2
       Version     : 01-01-05-02
Configured Module  :
```

```
       Type        : M8606-2XFP7200-2XG
       Ports       : 2
       Version     : 01-01-05-02

Device             : 1
Slot               : 3
User Status        : installed
Software Status    : ok
Online Module      :
       Type        : M8606-24GT/12SFP7200-24
       Ports       : 24
       Version     : 01-01-05-02
Configured Module  :
       Type        : M8606-24GT/12SFP7200-24
       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        : M6806-24SFP/12GT
       Ports       : 24
       Version     :

       Device      : 1
       Slot        : M1
       Status      : master
       Online Module:
       Type        : M86067200-CM-CM1
       Ports       : 0
       Version     : 01-01-05-02
```

27 Redundant Management Configuration

27.1 Overview

The DES-7200 series switches of D-Link support 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.

27.2 Configuring Redundant Management

This chapter includes:

- Automatic selection of master management board
- Manual selection of master management board

27.2.1 Automatic Selection of Master Management Board

The DES-7200 series switches support 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.

Note

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.

27.2.2 Manual Selection of Master Management Board

The DES-7200 series 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:

Step 1	***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.

```
D-Link#
D-Link#redundancy  force-switchover
D-Link#
```

In the global configuration mode, execute the following commands to configure the priority of the management board:

Step 1	**configure terminal**	This command is executed immediately without the necessity for global configuration mode.
Step 2	**main-cpu prefer [M1|M2]**	Specify the management board in which slot shall be started preferentially
Step 3	**end**	Return to the privileged EXEC mode.
Step 4	**write memory**	Save the configuration.
Step 5	**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.

```
D-Link #
D-Link # configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
D-Link (config)#main-cpu  prefer  m2
2006-04-22 09:26:00  @5-CONFIG:Configured from outband
D-Link # show main-cpu  preference
main-cpu preference : M2
D-Link #
```

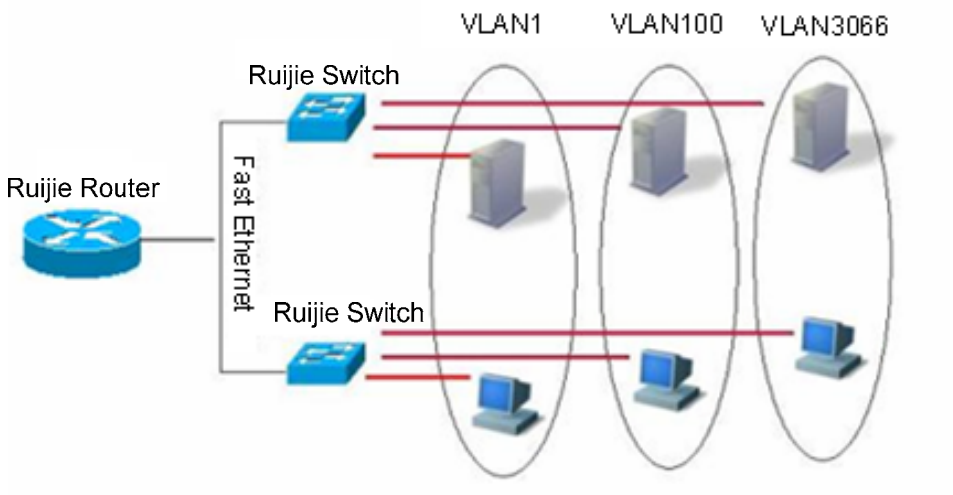
28 Configuring VLAN

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

28.1 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 unitcast, broadcast and multicast and frames on L2 are forwarded and distributed within a VLAN, not directly to another VLAN. Therefore, if the host connected to a port wants to communicate with a host in another VLAN, a router or L3 switch is needed between them, as shown in 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.



Same as a physical network, the VLAN is usually connected to an IP subnet. A typical example is that all the hosts in one IP subnet belong to the same VLAN. The communication between VLANs must go through a L3 device (router or L3 switch). Our L3 switch 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.

28.1.1 Supported VLAN

The supported VLANs conform to the IEEE802.1q standards. Up to 4094 VLANs are supported with the IDs ranging from VLAN 1 to VLAN 4094. VLAN 1 is the defaulted one that cannot be deleted. DES-7200 switches support up to 4093 VLANs.

28.1.2 VLAN Member Type

You can determine the frames that can pass a port by configuring the member type of the port in the VLAN and the multiple VLANs of the port. 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 switch, and it can forward the frames of all the VLANs. However, you can impose restriction by setting allowed-VLANs.

28.2 Configuring VLAN

One VLAN is identified by its VLAN ID.In the switch, you can add, delete, and modify a VLAN, of which the VLAN ID must be in the range of VLAN2-VLAN 4094. VLAN 1 is created by the switch automatically and cannot be deleted.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.

28.2.1 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.

28.2.2 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 and Inactive

28.2.3 Creating/Modifying a VLAN

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

Command	Funtion
D-Link(config)# **vlan** *vlan-id*	Enter one VLAN ID. If you enter a new VLAN ID, the switch will create it for you. If you enter an existing VLAN ID, the switch modifies the appropriate VLAN.
D-Link(config)#**name** *vlan-name*	(Optional) Name the VLAN. If you skip this step, the switch 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:

```
D-Link# configure terminal
D-Link(config)# vlan 888
D-Link(config-vlan)# name test888
D-Link(config-vlan)# end
```

28.2.4 Deleting a VLAN

You cannot delete the default VLAN (VLAN 1).

In the priviledged mode, you can delete a VLAN.

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

28.2.5 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
D-Link(config-if)**#switchport mode access**	Define the VLAN member type of the interface (L2 ACCESS port)
D-Link(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:

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

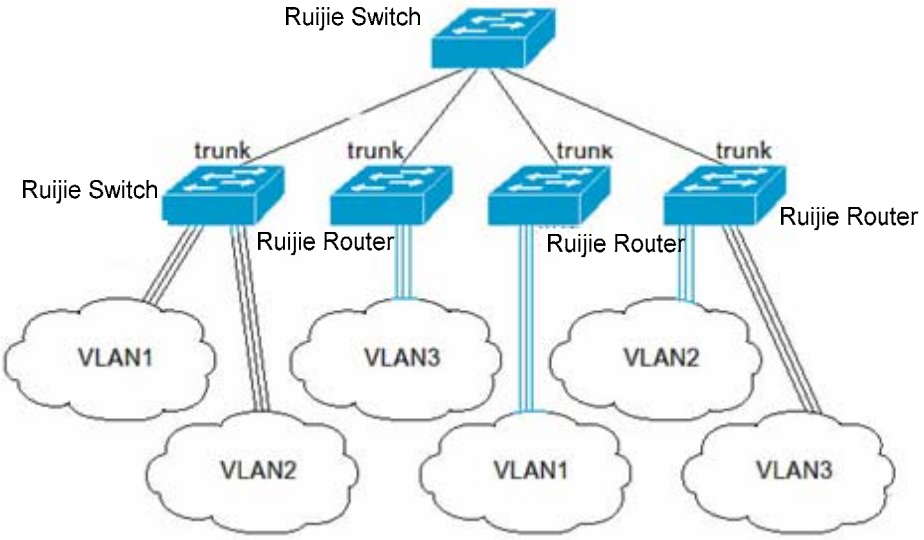
The following example shows how to verify the configuration:

```
D-Link (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
```

28.3 Configuring VLAN Trunks

28.3.1 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 over one link.The trunk of the D-Link switches uses capsulation of 802.1Q. The following diagram shows one network connected with trunks.



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
D-Link(config-if)#**switchport mode access**	Set one interface to the access mode
D-Link(config-if)#**switchport mode trunk**	Set one interface to the Trunk mode

As the trunk, the port belongs to one native VLAN. 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.

28.3.2 Configuring a Trunk Port

28.3.2.1 Trunk Port Basic Configuration

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

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

28.3.3 Defining the Allowed VLAN List of a Trunk Port

By default, one Trunk port can output all the traffics of all the VLANs (1-4093) supported by the switch. 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
D-Link(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 "-", for example, 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:

```
D-Link(config)# interface fastethernet1/15
Switch(config-if)# switchport trunk allowed vlan remove 2
D-Link(config-if)# end
D-Link# show interfaces fastethernet1/15 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
```

28.3.4 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 priviledged mode, you can configure a native VLAN for a Trunk port.

Command	Function
D-Link(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.

28.4 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:

```
D-Link# 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

D-Link#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
```

29 Configuring VRRP

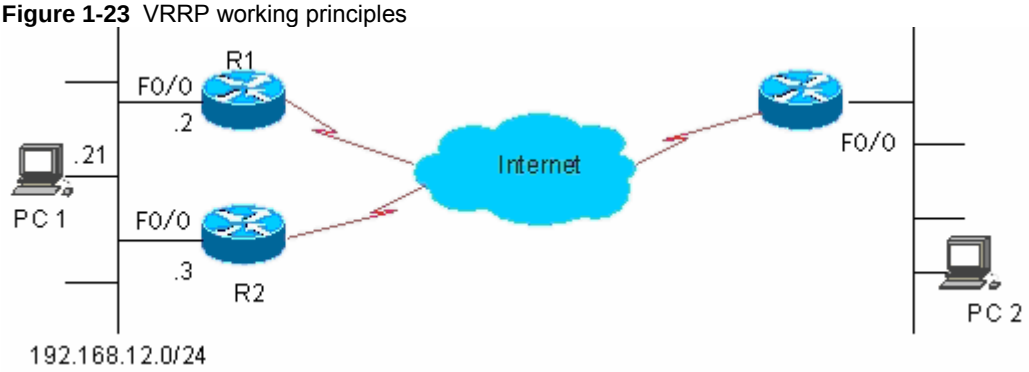
29.1 Overview

The VRRP is designed to implement uninterrupted services in case of IP transmission failure. Specifically, it is used to prevent the failure of the first-hop route when the first-hop route cannot be dynamically learned by the source host in the LAN. Multiple routers in the VRRP group are mapped to a virtual router. The VRRP ensures there is one and only one router that is presenting the virtual router to send packets. The host sends packets to the virtual router. The router that forwards packets is regarded as the master router. If that router cannot work due to some cause, the one in standby status will be selected to replace it and become the master router. 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 applicati0on group through multiple routers, but only one router acts as the master router at any time to undertake the route forwarding function. The others are in the backup roles. The switching between those multiple routers in the VRRP application group is fully transparent for the host in the LAN. The RFC 2338 defines the router switching rules:

1. The VRRP protocol adopts the preempt method to select the master router. 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 router is selected, other routers will be taken as the backup routers and the status of the master router will be monitored by the VRRP message sent from the master router. When the master router works normally, it will send a VRRP multicast message every other time, referred to as the advertisement message to notify the backup router, and the master router is in normal working status. If the backup router within the group doesn't receive the message from the master router for a long time, the status itself will be switched to the Master. If there is more than one backup router within the group, repeat the preempt process in step 1. In this process, the router with the maximum priority will be selected as the master router to execute the VRRP backup function.

Figure 1-23 VRRP working principles



Once a master router is elected in a VRRP backup group, the hosts in the LAN will execute route forwarding through that master router. The communication process is illustrated in Figure 1-1. As shown in Figure 1-1, routers 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 router 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 router but does not know whether router R1 or R2 is playing the role. The master router is elected between routers R1 and R2 in the VRRP group. Once the master router fails, the other router automatically becomes the master.

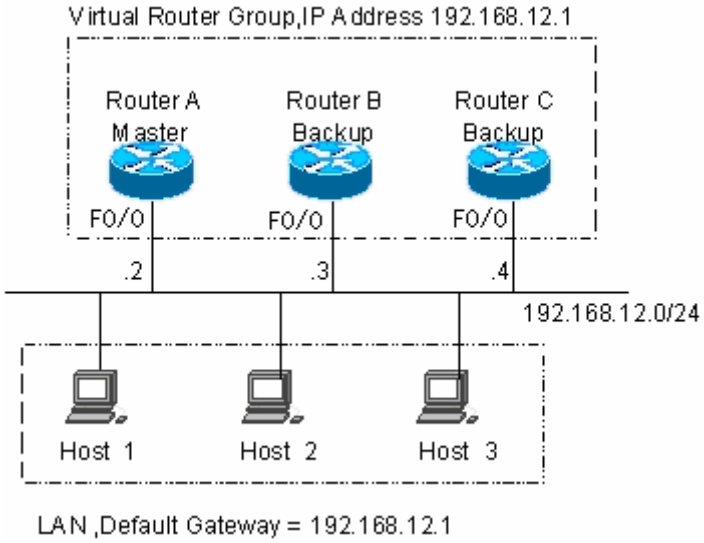
29.2 VRRP Applications

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.

29.2.1 Route redundancy

The basic VRRP applications are illustrated in Figure 1-2.

Figure 1-24 Basic VRRP applications

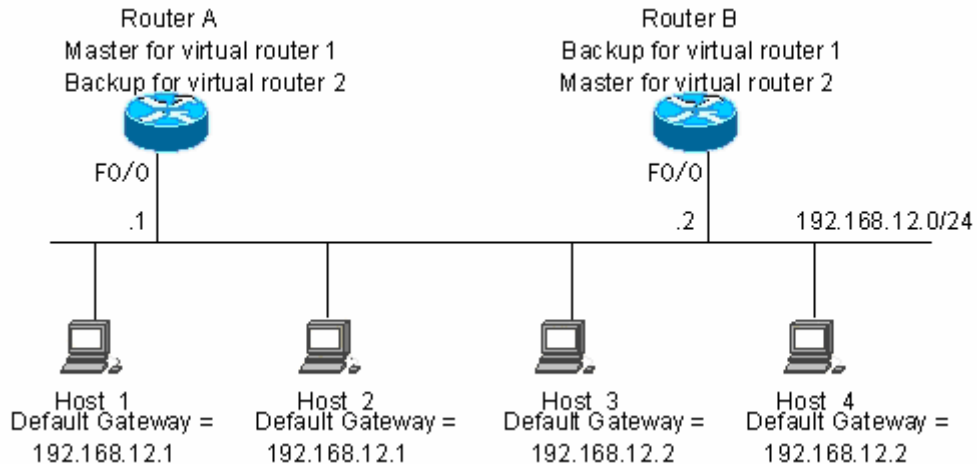


As shown in Figure 1-2, routers A, B and C are connected with the LAN through Ethernet interfaces, on which the VRRP is configured. They are in the same VRRP group with virtual IP address 192.168.12.1. Router A is elected as the master router of the VRRP, and routers B and C are standby. Hosts 1, 2 and 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 router (router A in Figure 1-2). Once router A fails, one will be elected between routers B and C to undertake the forwarding function of the virtual router, thus resulting in the simple route redundancy.

29.2.2 Load balancing

The advanced VRRP applications are illustrated in Figure 1-3.

Figure 1-25 Advanced VRRP applications



As shown in Figure 1-3, two virtual routers are configured. For virtual router 1, router A uses IP address 192.168.12.1 of Ethernet interface Fa0/0 as the IP address of the virtual router. In this way, router A becomes the master router and router B standby. For virtual router 2, router B uses IP address 192.168.12.2 of Ethernet interface Fa0/0 as the IP address of the virtual router. In this way, router B becomes the master router and router A standby. In the LAN, hosts 1 and 2 use the IP address 192.168.12.1 of virtual router 1 as the default gateway, while hosts 3 and 4 use the IP address 192.168.12.2 of virtual router 2 as the default gateway. In this VRRP application, router A and router B provide the route redundancy to share the traffic from the LAN, that is, load balancing.

29.3 VRRP configuration

29.3.1 VRRP configuration task list

The VRRP is applicable for the multicast or broadcast LANs, such as Ethernet. The configuration of the VRRP is concentrated on the Ethernet interfaces. The configuration tasks are as follows:

- Enable VRRP backup function (required)
- Set the authentication string of the VRRP backup group (optional)
- Set the broadcast interval of the VRRP backup group (optional)
- Set the preemption mode of router in the VRRP backup group (optional)
- Set the priority of router in the VRRP backup group (optional)
- Set the interface to be monitored by the VRRP backup group (optional)
- Set the VRRP broadcast timer learning function (optional)

- Set the description string of router 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.

29.3.2 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
Router(config-if)# **vrrp** *group* **ip** *ipaddress* **[secondary]**	Enable VRRP
Router(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.

Tip

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.

29.3.3 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
Router(config-if)# **vrrp** *group* **authentication** *string*	Set the authentication string of the VRRP.
Router(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.

29.3.4 Set the broadcast interval of the VRRP backup group

Command	Purpose
Router(config-if)# **vrrp** *group* **timers advertise** *interval*	Set the master router VRRP advertisement interval

Command	Purpose
Router(config-if)# **no vrrp** *group* **timers advertise** [*interval*]	Restore default for the master router VRRP advertisement interval

If the current router becomes the master router 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.

Tip

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.

29.3.5 Set the preemption mode of router in the VRRP backup group

If the VRRP group is working in the preemption mode, once a router finds its priority is higher than the Master priority, it will preempt to become the master router of the VRRP group. If the VRRP group is not working in the preemption mode, even if a router finds its priority is higher than the Master priority, it will not preempt to become the master router 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 router has the highest priority and thus automatically become the master router in the VRRP group.

Command	Purpose
Router(config-if)# **vrrp** *group* **preempt** [**delay** *second*s]	Set the preemptive mode for the VRRP group
Router(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.

29.3.6 Set the priority of router in the VRRP backup group

The VRRP stipulates the role of every router in the backup is determined by the priority parameter of the router. In the preemption mode, the router with the highest priority and virtual IP address obtained will become the active (master) router, and the other routers with lower priorities in the same backup group will become the backup (or listening) routers. Once the VRRP function is enabled, the default priority of the VRRP group is 100.

Command	Purpose
Router(config-if)# **vrrp** *group* **priority** *level*	Set the priority of the VRRP backup group.
Router(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).

29.3.7 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
Router(config-if)# **vrrp** *group* **track** *interface-type number* [*interface –priority*]	Set the interface to be monitored by the VRRP backup group
Router(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.


Tip

The monitored interface only allows layer-3 routable logical interfaces (such as Routed Port, SVI, Loopback and Tunnel).

29.3.8 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 router and Master router.

Command	Purpose
Router(config-if)# **vrrp** *group* **timers learn**	Set the timer learning function
Router(config-if)# **no vrrp** *group* **timers learn**	Cancel the timer learning function

By default, the VRRP group timer learning function is not set.


Tip

In case the advertisement interval in the VRRP advertisement received by the VRRP backup router is inconsistent with the advertisement interval configured locally, if the timer learning function is not configured on the VRRP backup router, the VRRP backup router will drop the VRRP advertisement; otherwise, the VRRP backup router receives the VRRP advertisement and use the advertisement interval to calculate the failure judgment interval of the VRRP Master router.

29.3.9 Set the description string of router in the VRRP backup group

This command will set the descriptor for the VRRP group to facilitate identifying the VRRP group.

Command	Purpose
Router(config-if)# **vrrp** *group* **description** *text*	Set the description string of the VRRP group
Router(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.


Tip

If blanks are contained in the VRRP backup group description string, quotation marks (") must be used to identify the description string.

29.4 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.

29.4.1 show vrrp

DES-7200 has the following **show vrrp** commands to check the VRRP status of the local router.

Command	Purpose
Router# **show vrrp** [**brief |** *group*]	Check the current VRRP status
Router# **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

```
Router#show vrrp
FastEthernet 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
FastEthernet 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
```

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.

2. show vrrp brief

```
Router#show vrrp brief
Interface        Grp Pri Time  Own Pre State   Master addr     Group addr
FastEthernet 0/0   1   100   -    -   P  Backup  192.168.201.213 192.168.201.1
FastEthernet 0/0   2   120   -    -   P  Master  192.168.201.217 192.168.201.2
```

The displayed messages above include the Ethernet name, VRRP backup group number configured on the interface, status, priority, preemption mode, virtual IP address and Master router IP address.

3. show vrrp interface

```
Router#show vrrp interface FastEthernet 0/0
FastEthernet 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
FastEthernet 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
Router#
```

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.

29.4.2 debug vrrp

DES-7200 has the following **debug vrrp** commands to provide the VRRP status debugging information of the local router.

Command	Purpose
Router# **debug vrrp error**	Turn on VRRP error prompt debugging switch
Router# **no debug vrrp error**	Turn off VRRP error prompt debugging switch
Router# **debug vrrp events**	Turning on the VRRP event debugging switch
Router# **no debug vrrp events**	Turning off the VRRP event debugging switch

Command	Purpose
Router# **debug vrrp packets**	Turning on the VRRP message debugging switch
Router# **no debug vrrp packets**	Turning off the VRRP message debugging switch
Router# **debug vrrp state**	Turning on the VRRP state debugging switch
Router# **no debug vrrp state**	Turning off the VRRP status debugging switch
Router# **debug vrrp**	Enables the IP debug switch
Router# **no debug vrrp**	Turn off the VRRP debugging switch

Here are some examples of the command:

1. debug vrrp

```
Router#debug vrrp
Router#
VRRP Grp 1 Advertisement priority 120, ipaddr 192.168.201.213
VRRP Grp 1 Event - Advert higher or equal priority
%VRRP-6-STATECHANGE: FastEthernet 0/0 Grp 1 state Master -> Backup
VRRP Grp 1 Advertisement from 192.168.201.213 has invalid virtual address
192.168.1.1
%VRRP-6-STATECHANGE: FastEthernet 0/0 Grp 1 state Backup -> Master
Router#
```

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

```
Router#debug vrrp error
Router#
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

```
Router#debug vrrp events
Router#
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
Router#
```

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

```
Router#debug vrrp packets
Router#
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.

```
Router#debug vrrp packets
Router#
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

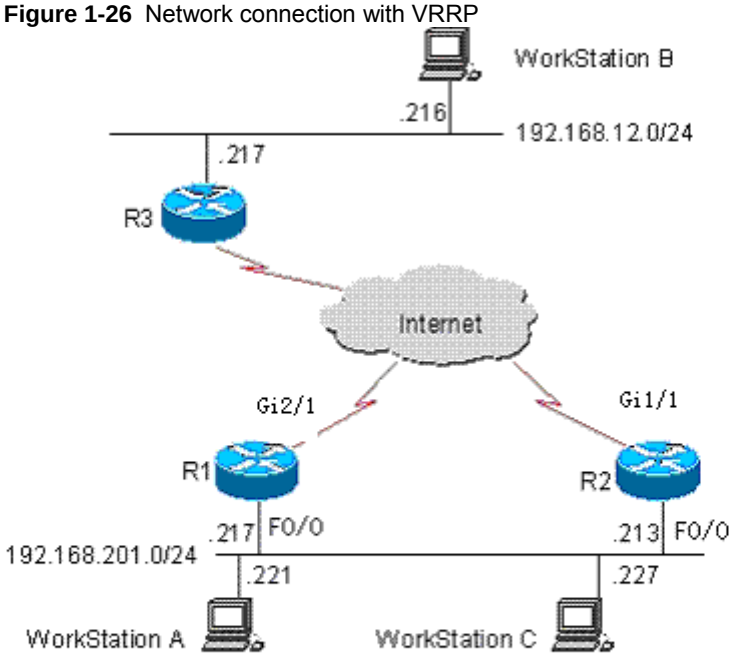
```
Router#debug vrrp state
VRRP State debugging is on
Router#
%VRRP-6-STATECHANGE: FastEthernet 0/0 Grp 2 state Master -> Backup
%VRRP-6-STATECHANGE: FastEthernet 0/0 Grp 2 state Backup -> Master
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/0
Switch(config-if)#no shutdown
Switch(config-if)#end
Router#
%VRRP-6-STATECHANGE: FastEthernet 0/0 Grp 2 state Master -> Init
Router#
```

The above displayed information indicates the VRRP group status on Fastethernet 0/0 is shifting among Master, Backup and Init.

29.5 Example of Typical VRRP Configuration

In the connections shown in Figure 1-4, VRRP backup is configured on routers R1 and R2 to provide the VRRP service for internal network segment 192.168.201.0 /24. Router R3 is not configured with VRRP but just the common routing functions. The configurations below provide the related VRRP settings of routers R1 and R2.

Figure 1-26 Network connection with VRRP



In the configuration example below, the configurations of router R3 remain unchanged, as detailed below:

```
!
!
hostname "R3"
!
!
!
interface FastEthernet 0/0
 no switchport
 ip address 192.168.12.217 255.255.255.0
!
interface gigabitEthernet 1/1
 no switchport
 ip address 60.154.101.5 255.255.255.0
!
interface gigabitEthernet 2/1
 no switchport
 ip address 202.101.90.61 255.255.255.0
!
router ospf
 network 202.101.90.0 0.0.0.255 area 10
 network 192.168.12.0 0.0.0.255 area 10
 network 60.154.101.0 0.0.0.255 area 10
!
!
!
end
```

29.5.1 Example of Single VRRP Backup Group

Establish the connections according to Figure 1-4. 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 router. In normal cases, router R1 is the active router to function as the gateway (192.168.201.). When router R1 becomes unreachable due to power-off or failure, router R2 takes its place to function as the gateway (192.168.201.1). The configurations for routers R1 and R2 are described as follows.

Router R1 configuration:

```
!
!
hostname "R1"
!
!
interface FastEthernet 0/0
 no switchport
 ip address 192.168.201.217 255.255.255.0
 vrrp 1 priority 120
 vrrp 1 timers advertise 3
 vrrp 1 ip 192.168.201.1
!
interface gigabitEthernet 2/1
 no switchport
 ip address 202.101.90.63 255.255.255.0
!
router ospf
 network 202.101.90.0 0.0.0.255 area 10
 network 192.168.201.0 0.0.0.255 area 10
!
```

Router R2 configuration:

```
!
hostname "R2"
!

interface FastEthernet 0/0
 no switchport
 ip address 192.168.201.213 255.255.255.0
 vrrp 1 ip 192.168.201.1
 vrrp 1 timers advertise 3
!
interface gigabitEthernet 1/1
 no switchport
 ip address 60.154.101.3 255.255.255.0
!
!
router ospf
 network 60.154.101.0 0.0.0.255 area 10
 network 192.168.201.0 0.0.0.255 area 10
!
!
```

```
end
```

As shown above, routers R1 and R2 are in the same VRRP backup group 1, point to the same virtual router IP address (192.168.201.1) and are both in the VRRP preemption mode. Since the VRRP backup group priority of router R1 is 120 but that of R2 is the default value 100, router R1 acts as the VRRP Master router in normal cases.

29.5.2 Example of configuration to monitor interface with VRRP

Establish the connections according to Figure 1-4. 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 router. Different from the above configuration example, router R1 is configured with VRRP to monitor interface GigabitEthernet 2/1. In normal cases, router R1 is the active router to function as the virtual gateway (192.168.201.). When router R1 becomes unreachable due to power-off or failure, router R2 takes its place to function as the virtual gateway (the virtual router address 192.168.201.1). Especially, when the WAN interface GigabitEthernet 2/1 of router R1 is unavailable, router R1 will decrease its priority in the VRRP backup group so that router 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 router R1 resumes normal, router R1 restores its priority in the VRRP backup group, becomes active and functions as the virtual gateway once again. The configurations for routers R1 and R2 are described as follows.

Router R1 configuration:

```
!
!
hostname "R1"
!
!
interface FastEthernet 0/0
 no switchport
 ip address 192.168.201.217 255.255.255.0
 vrrp 1 priority 120
 vrrp 1 timers advertise 3
 vrrp 1 ip 192.168.201.1
 vrrp 1 track GigabitEthernet 2/1 30
!

interface gigabitEthernet 2/1
 no switchport
 ip address 202.101.90.63 255.255.255.0
!
router ospf
 network 202.101.90.0 0.0.0.255 area 10
 network 192.168.201.0 0.0.0.255 area 10
!
!
end
```

Router R2 configuration:

```
!
!
```

```
hostname "R2"
!
interface FastEthernet 0/0
 no switchport
 ip address 192.168.201.213 255.255.255.0
 vrrp 1 ip 192.168.201.1
 vrrp 1 timers advertise 3
!
interface gigabitEthernet 1/1
 no switchport
 ip address 60.154.101.3 255.255.255.0
!
router ospf
 network 60.154.101.0 0.0.0.255 area 10
 network 192.168.201.0 0.0.0.255 area 10
!
!
end
```

As shown above, routers R1 and R2 are in the same VRRP backup group 1, 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 routers R1 and R2 are 3 seconds. In normal cases, since the VRRP backup group priority of router R1 is 120 but that of R2 is the default value 100, router R1 acts as the VRRP Master router. If router R1 in the Master status finds its WAN interface GigabitEthernet 2/1 is unavailable, router R1 decreases its priority in the VRRP backup group from 90 to 30, so that router R2 can become the Master router. 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 router R1 becomes the master router once again.

29.5.3 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 1-4. 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. Router R1 acts as the master router in backup group 2 and as the backup router in backup group 1; router R2 acts as the backup router in backup group 2 and as the master router in backup group 1. The configurations for routers R1 and R2 are described as follows.

Router R1 configuration:

```
!
!
hostname "R1"
!
interface FastEthernet 0/0
 no switchport
 ip address 192.168.201.217 255.255.255.0
 vrrp 1 timers advertise 3
 vrrp 1 ip 192.168.201.1
```

```
 vrrp 2 priority 120
 vrrp 2 timers advertise 3
 vrrp 2 ip 192.168.201.2
 vrrp 2 track GigabitEthernet 2/1 30
!
interface gigabitEthernet 2/1
 no switchport
 ip address 202.101.90.63 255.255.255.0
!
router ospf
 network 202.101.90.0 0.0.0.255 area 10
 network 192.168.201.0 0.0.0.255 area 10
!
!
end
```

Router R2 configuration:

```
!
!
hostname "R2"
!
!
interface Loopback 0
 ip address 20.20.20.5 255.255.255.0
!
interface FastEthernet 0/0
 no switchport
 ip address 192.168.201.213 255.255.255.0
 vrrp 1 ip 192.168.201.1
 vrrp 1 timers advertise 3
 vrrp 1 priority 120
 vrrp 2 ip 192.168.201.2
 vrrp 2 timers advertise 3
!

interface gigabitEthernet 1/1
 no switchport
 ip address 60.154.101.3 255.255.255.0
!
router ospf
 network 60.154.101.0 0.0.0.255 area 10
 network 192.168.201.0 0.0.0.255 area 10
!
!
!
end
```

It is shown that routers R1 and R2 are mutual backup, and the two are acting as the master routers in VRRP backup groups 1 and 2 respectively to provide different virtual gateway functions.

29.6 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 routers 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.

30 Configuration of Anti-attack System Guard

30.1 Overview

As is well known, several hacker attacks and the intrusion of network virus start from scanning active hosts within the network. Furthermore, a large number of scanning messages will occupy the network bandwidth greatly, which causes the network communication failure.

For this reason, the layer 3 switches of D-Link Corporation provides the anti-scanning function to prevent the hacker scanning and the Worm.Blaster-like attack, and reduce the CPU load of the layer 3 switches.

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 switches. 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 above two attacks, our switches can adjust corresponding parameters such as the attack threshold and the isolated time of the attacked host on each interface, to facilitate administrators to manage the configuration finely. If the configuration of each interface is identical, administrators can set a batch of ports by the **interface range** function.

30.2 Configuration of Anti-attack System Guard

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.

30.2.1 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
- Check the related information of anti-attack system guard

30.2.2 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
end	Return to the privileged EXEC 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.

30.2.3 Configure Isolated Time of Unauthorized Attack User

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 EXEC 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.

30.2.4 Configuring Threshold to Judge whether it is an Attacked Users

There is two attack methods that affect the performance of the switches: 1. Scan a batch of the 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. 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 EXEC mode.
show system-guard	Check the configuration entities.
copy running-config startup-config	Save the configuration.

Note

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.

30.2.5 Set the maximum monitored IPs

You can set the maximum quantity of the attacked hosts monitored by the switches. 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 EXEC mode.
show system-guard	Check the configuration entities.
copy running-config startup-config	Save the configuration.


Note

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** to set.

30.2.6 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 and mask for anti-attack function. Up to 255 exceptional IP entries are supported.
end	Return to the privileged EXEC mode.
show system-guard exception-ip	Show all exceptional IP entries.
copy running-config startup-config	Save the configuration.

The "no" option of this command will delete 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:

```
Switch(config)#no system-guard all-eip
```

To delete an exceptional IP:

```
Switch(config)#no system-guard 192.168.5.145  255.255.255.0
```


Note

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 (see section 2.7).

30.2.7 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, the **clear system-guard** denotes to clear all isolated user; the **clear system-guard interface** *interface-id* denotes to clear all users on this port. While the **clear system-guard interface** *interface-id* **ip-address** *ip-address* denotes to clear the specified IP user in this interface.

30.2.8 View Related Information of System Guard

30.2.8.1 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:

```
Switch#show system-guard
detect-maxnum number   : 100   ---------------The maximum quantity of the hosts
monitored by the switches
isolated host number   : 11   ---------------The maximum quantity of the hosts
isolated by the switches

inteface  state   isolate time  same-attack-pkts   scan-attack-pkts
--------------------------- ----------------   ------------------
Fa 0/1    ENABLE    120             20                 10
Fa 0/2    DISABLE   110             21                 11
……

Switch#show system-guard interface Fa 0/1

detect-maxnum number   : 100   ---------------The maximum quantity of the hosts
monitored by the switches
isolated host number   : 11   ---------------The maximum quantity of the hosts
isolated by the switches

inteface  state   isolate time  same-attack-pkts   scan-attack-pkts
--------------------------- ----------------   ------------------
Fa 0/1    ENABLE    120             20                 10
```

30.2.8.2 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

```
Switch # 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.

30.2.8.3 View User that being Monitored

Command	Meaning
show system-guard detect-ip [interface *interface-id***]**	View the IP that is being Monitored.

```
Switch # show system-guard isolated-ip
interface    ip-address     same 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
```

30.2.8.4 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.

```
Switch # show system-guard isolated-ip
Exception IP Address    Exception Mask
--------------------   ---------------
192.168.5.145           255.255.255.0
192.168.4.11            255.255.255.0
```