Contents

1 Configuring Ethernet Interface

1.1 Introduction

Interfaces are important in implementing data switching on network devices. Orion_B26Q devices support two types of interfaces: physical ports and logical interfaces. A physical port is a hardware port on a device, such as the 100M Ethernet interface and Gigabit Ethernet interface. A logical interface, such as the loopback interface and tunnel interface, can be associated with a physical port or independent of any physical port. For network protocols, physical ports and logical interfaces are processed in the same way.

1.1.1 Basic Concepts

1. Interface Classification

Interfaces on Orion_B26Q devices fall into two categories:

- L2 interface (Switch or bridge mode)
- L3 interface (supported by L3 devices)

Common L2 interfaces are classified into the following types:

- Switch port
- L2 aggregate port (AP)

Common L3 interfaces are classified into the following types:

- Routed port
- L3 AP
- Switch virtual interface (SVI)
- Loopback interface
- Tunnel interface

2. Switch Port

A switch port is a single physical port on the device, and implements only the L2 switching function. The switch port is used to manage physical ports and L2 protocols related to physical ports.

3. L2 AP

An AP is formed by aggregating multiple physical ports. Multiple physical links can be bound together to form a simple logical link. This logical link is called an AP.

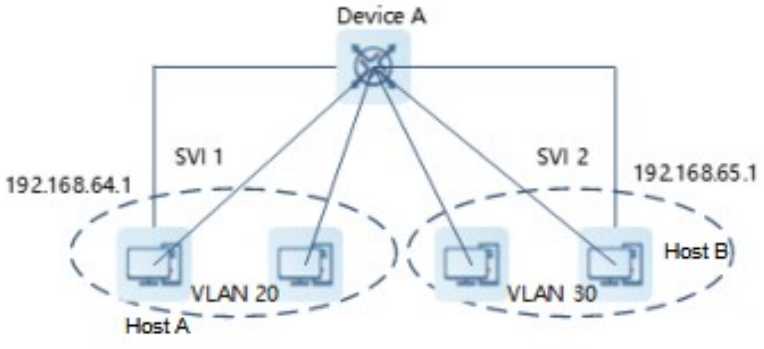
For L2 switching, an AP is equivalent to a switch port that combines bandwidths of multiple ports, thus expanding the link bandwidth. Frames sent over the L2 AP are balanced among the L2 AP member ports. If one member link fails, the L2 AP automatically transfers the traffic on the faulty link to other member links, improving reliability of connections.

4. SVI

The SVI can be used as the management interface of the local device, through which the administrator can manage the device. You can also create an SVI as a gateway interface, which is mapped to the virtual interface of each virtual local area network (VLAN) to implement routing across VLANs among L3 devices. You can run the **interface vlan** command to create an SVI and assign an IP address to this interface to set up a route between VLANs.

As shown in Figure 1-1, the hosts in VLAN 20 can directly communicate with each other without participation of L3 devices. If Host A in VLAN 20 wants to communicate with Host B in VLAN 30, SVI 1 of VLAN 20 and SVI 2 of VLAN 30 must be used.

Figure 1-1Schematic Diagram of SVI



5. Routed Port

A physical port on a L3 device can be configured as a routed port, which functions as the gateway interface for L3 switching. A routed port is unrelated with a specific VLAN. Instead, it just serves as an access port. The routed port cannot be used for L2 switching.

You can run the **no switchport** command to change a switch port to a routed port and assign an IP address to this port to set up a route. Note that all L2 features of the switch port will be deleted after you run the **no switchport** command.

Note

If a port is a L2 AP member port or a DOT1X port that is not authenticated, you cannot run the **switchport** or **no switchport** command to configure the switch port or routed port.

6. L3 AP

Like the L2 AP, a L3 AP is a logical port that aggregates multiple physical member ports. The aggregated ports must be the L3 ports of the same type. The AP functions as a gateway interface for L3 switching. Multiple physical links are combined into one logical link, expanding the bandwidth of a link. Frames sent over the L3 AP are balanced among the L3 AP member ports. If one member link fails, the L3 AP automatically transfers the traffic on the faulty link to other member links, improving reliability of connections.

A L3 AP cannot be used for L2 switching. You can run the **no switchport** command to change a L2 AP that does not contain any member port into a L3 AP, add multiple routed ports to this L3 AP, and then assign an IP address to this L3 AP to set up a route.

7. Loopback Interface

The loopback interface is a local L3 logical interface simulated by the software that is always **Up**. Packets sent to the loopback interface are processed on the device locally, including the route information. The IP address of the loopback interface can be used as the device ID of the Open Shortest Path First (OSPF) routing protocol, or as both the local address of telnet and the remote telnet access address. The procedure for configuring a loopback interface is similar to that for configuring an Ethernet interface. You can treat the loopback interface as a virtual Ethernet interface.

8. Tunnel Interface

The Tunnel interface implements the tunnel function. Over the Tunnel interface, transmission protocols (e.g., IP) can be used to transmit packets of any protocol. Like other logical interfaces, the tunnel interface is also a virtual interface of the system. Instead of specifying any transmission protocol or load protocol, the tunnel interface provides a standard point-to-point (P2P) transmission mode. Therefore, a tunnel interface must be configured for every single link.

1.1.2 Interface Configuration

You can run the **interface** command in the global configuration mode to enter the interface configuration mode. You can configure interface-related attributes in interface configuration mode.

If you enter the interface configuration mode of a non-existing logical interface, the interface will be created. You can also run the **interface range** or **interface range macro** command in the global configuration mode to configure the range (IDs) of interfaces. Interfaces defined in the same range must be of the same type and have the same features.

You can run the **no interface** command in global configuration mode to delete a specified logical interface.

1. Interface Numbering Rules

In stand-alone mode, the interface ID corresponding to a physical port consists of two parts: slot ID and port ID on the slot. For example, if the slot ID of the port is 2, and port ID on the slot is 3, the interface ID is 2/3. In virtual switch unit (VSU) mode or stack mode, the interface ID corresponding to a physical port consists of three parts: device ID, slot ID, and port ID on the slot. For example, if the device ID is 1, slot ID is 2, and port ID on the slot is 3, the interface ID is 1/2/3.

The device ID ranges from 1 to the maximum number of member devices supported.

The slot number rules are as follows: The static slot ID is 0, whereas the ID of a dynamic slot (pluggable module or line card) ranges from 1 to the number of slots. Assume that you are facing the device panel. Dynamic slots are numbered from 1 sequentially from front to rear, from left to right, and from top to bottom.

The ID of a port on the slot ranges from 1 to the number of ports on the slot, and is numbered sequentially from left to right.

You can select fiber or copper as the medium of a combo port. Regardless of the medium selected, the combo port uses the same port ID.

The ID of an AP ranges from 1 to the number of APs supported by the device.

The ID of an SVI is the ID of the VLAN corresponding to this SVI.

2. Configuring Interfaces Within a Range

You can run the **interface range** command in the global configuration mode to configure multiple interfaces at a time. Attributes configured in the **interface range** mode apply to all these interfaces.

The **interface range** command can be used to specify several range segments, and each range segment can be separated using a comma (,). The types of interfaces within all ranges specified in a command must be the same. The **macro** parameter is used to configure the macro corresponding to a range. For details, see "Configuring Macros of Interface Ranges".

When the **interface range** command is used, the parameter formats vary with different interface types. The common valid interface range formats are as follows:

- **FastEthernet** device/slot/{ start-port } - { end-port }.
- **GigabitEthernet** device/slot/{ start-port } - { end-port }.
- **TenGigabitEthernet** device/slot/{ start-port } - { end-port }.
- **FortyGigabitEthernet** device/slot/{ start-port } - { end-port }.
- **AggregatePort** { start-port } - { end-port }. The value range is from 1 to the maximum number of APs supported by the device.
- **vlan** vlan-ID-vlan-ID. The value range of VLAN ID is from 1 to 4094.
- **Loopback** loopback-start-ID-loopback-end-ID. The value range is from 1 to 2147483647.
- **Tunnel** tunnel-start-ID-tunnel-end-ID. The value range is from 0 to the maximum number of tunnel interfaces supported by the device minus 1.

3. Configuring Macros of Interface Ranges

You can define some macros to replace the interface ranges. Before using the **macro** parameter in the **interface range** command, you must first run the **define interface-range** command in the global configuration mode to define these macros.

In addition, you can run the **no define interface-range** *macro-name* command in the global configuration mode to delete the configured macros.

1.1.3 Interface Description and Administrative Status

You can configure a name for an interface to identify the interface and help you remember the functions of the interface.

You can enter the interface configuration mode to enable or disable an interface.

1. Interface Description

You can configure the name of an interface based on the purpose of the interface. For example, if you want to assign GigabitEthernet 1/1 for exclusive use by user A, you can describe the interface as "Port for User A."

2. Interface Administrative Status

In some cases, you may need to disable an interface. You can directly disable an interface by setting c. If an interface is disabled, it does not receive or send any frames, and the interface loses all its corresponding functions. You can also enable a disabled interface again by setting the management status. Two

administrative statuses are available for an interface: **Up** and **Down**. The administrative status of an interface is **Down** when the interface is disabled, and **Up** when the interface is enabled.

1.1.4 MTU of an Interface

You can configure the maximum transmission unit (MTU) of an interface to limit the length of a frame that can be received or forwarded through this interface.

You can set the system MTU to control the maximum length of frames that can be received or forwarded through all interfaces.

When a large amount of data is exchanged over an interface, a frame may be greater than a standard Ethernet frame in length. This type of frame is called jumbo frame. The MTU is the length of the valid data segment in a frame. It does not include the Ethernet encapsulation overhead.

If an interface receives or forwards a frame with a length greater than the MTU, this frame will be discarded.

1.1.5 Configuring Bandwidth of an Interface

The **bandwidth** command can be configured so that some routing protocols (for example, OSPF) can calculate the route metric and the Resource Reservation Protocol (RSVP) can calculate the reserved bandwidth. Modifying the interface bandwidth will not affect the data transmission rate of the physical port.

The **bandwidth** command is a routing parameter, and does not affect the bandwidth of a physical link.

1.1.6 Configuring Carrier Delay

The carrier delay refers to the delay after which the data carrier detect (DCD) signal changes from **Down** to **Up** or from **Up** to **Down**. If the DCD status changes during the delay, the system will ignore this change to avoid negotiation at the upper data link layer. If this parameter is set to a great value, nearly every DCD change is not detected. On the contrary, if the parameter is set to 0, every DCD signal change will be detected, resulting in poor stability.

If the DCD carrier is interrupted for a long time, the carrier delay should be set longer to accelerate convergence of the topology or route. On the contrary, if the DCD carrier interruption time is shorter than the topology or route convergence time, the carrier delay should be set to a greater value to avoid topology or route flapping.

1.1.7 Link Trap Policy

You can enable or disable the link trap function on an interface.

When the link trap function on an interface is enabled, the Simple Network Management Protocol (SNMP) sends link traps when the link status changes on the interface.

1.1.8 Interface Index Persistence

Like the interface name, the interface index also identifies an interface. When an interface is created, the system automatically assigns a unique index to the interface. The index of an interface may change after the device is restarted. You can enable the interface index persistence function so that the interface index remains unchanged after the device is restarted.

After interface index persistence is enabled, the interface index remains unchanged after the device is restarted.

1.1.9 Configuring Routed Port

A physical port on a L3 device can be configured as a routed port, which functions as the gateway interface for L3 switching. The routed port cannot be used for L2 switching. You can run the **no switchport** command to change a switch port to a routed port and assign an IP address to this port to set up a route. Note that all L2 features of the switch port will be deleted after you run the **no switchport** command.

1.1.10 Configuring L3 AP

Like a L3 routed port, you can run the **no switchport** command to change a L2 AP into a L3 AP on a L3 device, and then assign an IP address to this AP to set up a route. Note that you must delete all L2 features of an AP switch port before running the **no switchport** command.

A L2 AP with one or more member ports cannot be configured as a L3 AP. Similarly, a L3 AP with one or more member ports cannot be changed to a L2 AP.

1.1.11 Configuring Basic Attributes of Interfaces

You can configure the interface rate, duplex mode, flow control mode, and auto negotiation mode of an Ethernet physical port or AP.

1. Interface Rate

Generally, the rate of an Ethernet physical port is determined through auto negotiation with the peer device. The negotiated rate can be any rate within the interface capability. You can also configure any rate within the interface capability for the Ethernet physical port.

When you configure the rate of an AP, the configuration takes effect on all of its member ports. (All these member ports are Ethernet physical ports.)

2. Duplex Mode

The duplex mode of an Ethernet physical port or AP can be configured as follows:

- Full duplex: the interface can receive packets while sending packets.
- Half duplex: the interface can receive or send packets at a time.
- Auto negotiation: the duplex mode of the interface is determined through auto negotiation between the local interface and peer interface.

When you configure the duplex mode of an AP, the configuration takes effect on all of its member ports. (All these member ports are Ethernet physical ports.)

3. Flow Control

Two flow control modes are defined for an interface:

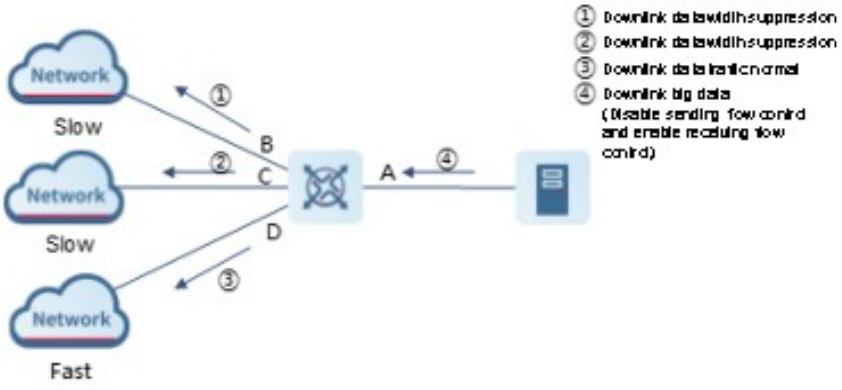
- Symmetric flow control mode: Generally, after flow control is enabled on an interface, the interface processes the received flow control frames, and sends the flow control frames when congestion occurs on the interface. The received and sent flow control frames are processed in the same way. This is called symmetric flow control mode.
- Asymmetric flow control mode: In some cases, an interface on a device is expected to process the received flow control frames to ensure that no packet is discarded due to congestion, and not to send the flow

control frames to avoid decreasing the network speed. In this case, you need to configure the asymmetric flow control mode to separate the procedure for receiving flow control frames from the procedure for sending flow control frames.

- When you configure the flow control mode of an AP, the configuration takes effect on all of its member ports. (All these member ports are Ethernet physical ports.)

As shown in Figure 1-1, Port A of the device is an uplink port, and Ports B, C and D are downlink ports. Assume that Port A is enabled with the functions of sending and receiving flow control frames. Port B and Port C are connected to different slow networks. If a large amount of data is sent on Port B and Port C, Port B and Port C will be congested, and consequently congestion occurs in the inbound direction of Port A. Therefore, Port A sends flow control frames. When the uplink device responds to the flow control frames, it reduces the data flow sent to Port A, which indirectly slows down the network speed on Port D. In this case, you can disable the function of sending flow control frames on Port A to ensure the bandwidth usage of the entire network.

Figure 1-1Interface Flow Control Diagram



4. Auto Negotiation Mode

- The auto negotiation mode of an interface can be On or Off. The auto negotiation state of an interface is not completely equivalent to the auto negotiation mode. The auto negotiation state of an interface is jointly determined by the interface rate, duplex mode, flow control mode, and auto negotiation mode.
- When you configure the auto negotiation mode of an AP, the configuration takes effect on all of its member ports. (All these member ports are Ethernet physical ports.)

Note

- Generally, if one of the interface rate, duplex mode, and flow control mode is set to **Auto**, or the auto negotiation mode of an interface is **On**, the auto negotiation state of the interface is **On**, that is, the auto negotiation function of the interface is enabled. If none of the interface rate, duplex mode, and flow control mode is set to **Auto**, and the auto negotiation mode of an interface is **Off**, the auto negotiation function of the interface is disabled.
- For a 100M fiber port, the auto negotiation function is always disabled. For a Gigabit copper port, the auto negotiation function is always enabled, that is, the auto negotiation state is **On**.

1.1.12 Automatic Module Detection

If the interface rate is set to auto, the interface rate can be automatically adjusted based on the type of the inserted module.

Currently, the automatic module detection function can be used to detect only small form-factor pluggable (SFP) and enhanced SFP (SFP+) modules. The SFP module is a Gigabit module, whereas the SFP+ module is a 10 Gigabit module. If an SFP module is inserted, the interface works in Gigabit mode. If an SFP+ module is inserted, the interface works in 10 Gigabit mode.

Note

The automatic module detection function takes effect only when the interface rate is set to auto.

1.1.13 Protected Port

In some application environments, it is required that communication be disabled between some ports on the device. For this purpose, you can configure some ports as protected ports. You can also disable routing between protected ports. After ports are configured as protected ports, the protected ports cannot communicate with each other, but can communicate with non-protected ports. Protected ports work in either of the two modes.

- In the first mode, L2 switching is blocked but routing is allowed between protected ports, which is the default mode.
- In the second mode, L2 switching and routing are both blocked between protected ports.

When two protected ports are configured as a pair of mirroring ports, frames sent or received by the source port can be mirrored to the destination port. Currently, only an Ethernet physical port or AP can be configured as a protected port. When an AP is configured as a protected port, all of its member ports are configured as protected ports. By default, the L3 routing between protected ports is not blocked. In this case, you can run the **protected-ports route-deny** command to block the routing between protected ports.

1.1.14 Port Errdisable Recovery

Some protocols support the port errdisable recovery function to ensure security and stability of the network. For example, in the port security protocol, when you enable port security and configure the maximum number of security addresses on the port, a port violation event is generated if the number of addresses learned on this port exceeds the maximum number of security addresses. Protocols, such as the Spanning Tree Protocol (STP), DOT1X, and REUP, support the similar functions, and a violating port will be automatically shut down to ensure security. Also, if frequent port flapping occurs, a violating port will be shut down.

When a port is disabled because it is set to the errdisable state by the REUP link state tracking group function, the port can be restored only by REUP at a scheduled time or by running the REUP errdisable recovery command in the global configuration mode. In other scenarios, you can run the errdisable recovery command in the global configuration mode to recover all the ports in errdisable state and enable these ports. You can manually recover a port, or automatically recover a port at a scheduled time. You can run the **shutdown** or **no shutdown** command to recover all the ports in the errdisable state and enable these ports.

1.1.15 Optical Module Alarm Detection

After this function is configured, you can view the optical module alarm information of an interface by using the management information base (MIB). When events such as insertion or removal of an optical module, optical module exceptions, and optical module exception clearing are detected, related TRAP messages are sent.

The exceptions include overhigh/overlow transmit power of the optical module, overhigh/overlow receive power of the optical module, inter-integrated circuit (IIC) fault of the optical module, unsupported module type, and the like.

After the alarm detection function is enabled and a corresponding detection period is configured, the SNMP device periodically monitors the optical module status on an interface. When any of the above events is detected, the SNMP device sends a related TRAP message. The SNMP device sends a TRAP message immediately for the optical module insertion or removal, but sends a TRAP message in the next period for optical module exceptions and optical module exception clearing. Only one TRAP message is sent for the same exceptions. The exception will be notified periodically, and the exception clearing event will be notified once only. You can disable the periodic notification function by using the repeated notification mode switch.

1.1.16 Optical Module Antifake Detection

You can configure the optical module antifake detection function to check whether the optical module in use is supplied by Orion_B26Q Networks.

If the optical module is not supplied by Orion_B26Q Networks, the data communication may be affected. If the optical module antifake detection function is enabled, the device can automatically identify an optical module that is not supplied by Orion_B26Q Networks and generate an alarm when such module is inserted to the Orion_B26Q device.

This function is disabled by default. You can enable this function through configuration.

Each optical module supplied by Orion_B26Q Networks has a unique antifake code. The device can read this antifake code to determine whether the module is supplied by Orion_B26Q Networks. If not, the device will generate syslogs and send trap messages.

1.1.17 Splitting and Combination of 40G/100G Interfaces

The 40G/100G Ethernet interface is a high-bandwidth interface. It is mainly used on devices at the convergence layer or core layer to increase the interface bandwidth. 40G/100G interface splitting means splitting one 40G/100G interface into four 10G/25G interfaces. In this case, the 40G/100G interface becomes unavailable, and the four 10G/25G interfaces forward data independently. 40G/100G interface combination means combining four 10G/25G interfaces into one 40G/100G interface. In this case, the four 10G/25G interfaces become unavailable, and only the 40G/100G interface forwards data. Unavailable interfaces cannot forward data. You can flexibly adjust the bandwidth by combining or splitting interfaces.

1.1.18 Configuring Interface Traffic Statistics

By default, virtual interfaces such as sub-interfaces and SVIs do not support interface traffic statistics collection, while the Ethernet port and Ethernet AP support interface traffic statistics collection, but do not support IP traffic statistics collection. When you need to locate a network fault or monitor the network operation status, you can enable the interface traffic statistics collection function and IP traffic statistics collection function. And run he **show interface** *interface-type interface-number* command to view the packet statistics of the specified interface and IP packet statistics.

Note

Enabling the interface traffic statistics collection function and IP traffic statistics collection function consumes system resources. You are advised to configure the functions as required.

1.1.19 EEE

Energy Efficient Ethernet (EEE) is an Ethernet solution that saves energy When EEE is enabled, the port enters low power consumption mode when the Ethernet connection is idle, thus saving energy.

Low Power Idle (LPI) is the low power consumption mode. After a port enters LPI mode, it reduces signals significantly, and sends only signals that are sufficient to maintain the connection on the port to save energy.

According to the Ethernet standards or specifications, interfaces with a bandwidth of 100M or above have the active idle state. An interface will consume much power if it maintains connection without being affected by data transmission. Therefore, the power consumption is high no matter whether any data is transmitted on the link. Even if no data is transmitted, the port will always send the idle signals to retain the connection state of the link.

EEE enables a port of the device to enter the LPI mode for the purpose of saving energy. In LPI mode, the power consumption is low when the link is idle. The EEE technology can also quickly change the LPI state of a port to the normal state, providing high-performance data transmission.

After enabled with EEE, the port automatically enters LPI mode if the port is always **Up** without sending or receiving any packet in a period of time. The port recovers the working mode when it needs to send or receive packets, thus saving energy. To make the EEE function take effect, the peer port must also support the EEE function.

Note

Only a copper port working in 100M or 1000M rate mode supports the EEE function.

The EEE function takes effect only on the port enabled with auto negotiation.

1.1.20 Port Flapping Protection

When flapping occurs on a port, a lot of hardware interruptions occur, consuming a lot of CPU resources. On the other hand, frequent port flapping damages the port. You can configure the flapping protection function to protect ports.

By default, the port flapping protection function is enabled. You can disable this function as required. When flapping occurs on a port, the port detects flapping every 2s or 10s. If flapping occurs six times within 2s on a port, the device displays a prompt. If 10 prompts are displayed continuously, that is, port flapping is detected continuously within 20s, the port is shut down (the violation cause shows **Link Dither**). If flapping occurs 10 times within 10s on a port, the device displays a prompt without shutting down the port.

1.1.21 Interface Syslog

You can use the syslog function to determine whether to display information about interface changes or exceptions.

You can enable or disable the syslog function as required. By default, this function is enabled. When an interface becomes abnormal, for example, the interface status changes, or the interface receives error frames, or flapping occurs, the system displays prompts to notify users.

1.1.22 Configuring the MAC Address of an Interface

By default, each Ethernet interface has a globally unique Media Access Control (MAC) address. The MAC addresses of Ethernet interfaces can be modified if required. However, MAC addresses in the same LAN must be unique.

To configure the MAC address of an Ethernet interface, run the **mac-address** command in interface configuration mode:

Note

Configuration of MAC addresses may affect internal communication in a LAN. Therefore, you are not advised to configure MAC addresses by yourself unless necessary.

1.1.23 VLAN Encapsulation Flag on Interfaces

Virtual local area network (VLAN) is a logical network divided on a physical network and corresponds to the L2 network in the ISO model. In 1999, IEEE released the 802.1Q protocol draft for standardizing the VLAN implementation solution.

The VLAN technology enables the network administrator to divide one physical LAN into multiple broadcast domains (or VLANs). Each VLAN contains a group of workstations with the same requirements and each VLAN has the same attributes as the physical LAN. As VLANs are logically divided, workstations in the same VLAN do not need to be placed in the same physical space, that is, these workstations may belong to different physical LAN network segments. Multicast and unicast traffic in a VLAN will not be forwarded to other VLANs. This helps control traffic, reduces device investment, simplifies network management, and improves the network security.

VLAN is a protocol used to solve Ethernet broadcast and security problems. During packet transmission, a VLAN header is added to Ethernet frames. In addition, VLAN IDs are used to classify users to different work groups to restrict L2 exchange between users in different work groups. Each work group is a VLAN. VLANs can be used to restrict the broadcast scope and form virtual work groups to manage networks dynamically.

To ensure communication with hosts in a VLAN, you can configure the 802.1Q (VLAN protocol) VLAN encapsulation flag on the Ethernet interface or sub-interface. In this case, when packets are sent over the Ethernet interface, the corresponding VLAN header will be encapsulated. When packets are received, the VLAN header will be deleted from the packet.

1.1.24 Configuring the FEC Mode of an Interface

Forward error correction (FEC) is an error code correction method employing the following working principle: The sender adds a redundancy error-correcting code to the data for sending. The receiver performs error detection on the data based on the error-correcting code. If an error is found, the receiver corrects the error. FEC improves signal quality but also causes signal delay. Users can enable or disable this function according to the actual situation.

There are three FEC modes: rs mode, base-r mode, and auto mode. Different types of interfaces support different FEC modes, depending on the specific products.

1.1.25 Configuring the Sampling Period of Ethernet Interface Statistics

The default statistics sampling period of an Ethernet interface or Ethernet sub-interface is 5 seconds, which means that interface statistics are updated every 5 seconds. In scenarios with high requirements for real-time statistics, you can prolong the sampling period.

A shorter sampling period indicates higher system performance consumption. Therefore, the sampling period must be adjusted as required. If the number of physical ports exceeds 500, you are advised to set the sampling period to a value greater than 10s.

1.1.26 Configuring Enhanced Name Display for Interfaces

After enhanced name display for interfaces is enabled in the standard MIB node, the value of an interface name node in the standard MIB does not contain spaces. In addition, the ifName node displays the full name of the interface, which does not contain spaces. By default, the value and interface name of the interface name node in the standard MIB contain spaces, and the ifName node displays the short name of the interface.

1.1.27 Including Interframe Gaps in Interface Packet Rate Statistics

By default, interframe gaps are not included in the statistics of packet sending/receiving rate of Orion_B26Q device. You can enable the function of including interframe gaps in interface packet rate statistics, if you want to view the statistics at the physical layer, which contains the number of bytes of packets and the interframe gap. The packet sending/receiving rate at the physical layer refers to the sending/receiving rate of packets that contains interframe gaps.

After this function is enabled, the size of the interframe gap is fixed to 20 bytes. (The interframe gap consists of 12 bytes and the preamble consists of 8 bytes.) An error exists because the chip collects statistics on the frame gap of 20 bytes, but the command statistics exclude the frame gap.

1.2 Configuration Task Summary

The Ethernet interface configuration includes the following tasks:

(1) Configuring Basic Features

(2) (Optional) Configuring Interface Attributes

1.3 Configuring Basic Features

1.3.1 Overview

- Create a specified logical interface and enter the configuration mode of this interface, or enter the configuration mode of an existing physical or logical interface.
- Create multiple specified logical interfaces and enter interface configuration mode, or enter configuration mode of multiple existing physical or logical interfaces.
- The interface indexes remain unchanged after the device is restarted.
- Configure the interface description so that users can directly learn information about the interface.
- Enable or disable the link trap function of an interface.
- Configure the interface administrative status, and enable or disable an interface.
- Split a 40G interface or combine four 10G interfaces into one 40G interface.

- Enable enhanced name display for interfaces.

1.3.2 Restrictions and Guidelines

- The **no** form of the command can be used to delete a specified logical interface or logical interfaces in a specified range, but cannot be used to delete a physical port or physical ports in a specified range.
- The **default** form of the command can be used in the interface configuration mode to restore default settings of a specified physical port or a logical interface, or interfaces or ports in a specified range.
- The errdisbale ports can be recovered by using the **shutdown** or **no shutdown** command. To prevent unwanted link flapping caused by frequent operation of the **shutdown/no shutdown** command, there should be a certain time interval (which must be greater than the carrier delay of the interface) before/after configuring the **shutdown**/**no shutdown** command twice on an interface.

1.3.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Configure a single interface.

interface *interface-type interface-number*

The physical port has been created by default.

(4) (Optional) Configure interfaces within a range.

interface range { *port-range* | **macro** *macro-name* }

The port range is not specified by default.

(5) (Optional) Configure interface index persistence.

snmp-server if-index persist

The interface index persistence function is disabled by default.

(6) (Optional) Configure splitting and combination of 40G interfaces.

split interface *interface-type interface-number*

The 40G interface is unsplit by default.

(7) (Optional) Configure the port flapping protection function.

physical-port dither protect

The port flapping protection function is enabled by default.

(8) (Optional) Configure the syslog information printing function for the interface.

logging [**link-updown** | **error-frame** | **link-dither** | **res-lack-frame** | **crc-frame**]

The interface information printing function is disabled by default.

(9) Enter the interface configuration mode.

interface *interface-type interface-number*

(10) (Optional) Configure the description of an Interface.

description *interface-name*

No interface name is configured by default.

(11) (Optional) Configure the LinkTrap function of an interface.

snmp trap link-status

The LinkTrap notification sending function for interface status changes is enabled by default.

(12) (Optional) Configure the administrative status of an interface.

shutdown

The interface is in **Up** state by default.

1.4 Configuring Interface Attributes

1.4.1 Overview

- Enable the device to connect and communicate with other devices through the switch port or routed port.
- Adjust various interface attributes on the device.

1.4.2 Restrictions and Guidelines

- You can select either fiber or copper as the medium type of an interface when both medium types are available. Once the medium type is selected, all interface attributes, including the status, duplex mode, and rate, are configured for the interface of the selected medium type. If the interface type is changed, the attributes of the new interface type are the default attributes. You can reconfigure these attributes as required.
- When the FEC function is enabled at one end of the link, it must be also enabled at the other end. If the QSFP28-100G-LR4 optical module is used without affecting the negotiation status of the two ends, the FEC function is disabled by default and should not be enabled according to the IEEE standard protocol. If the QSFP28 optical modules other than QSFP28-100G-LR4 are used, the FEC function is enabled by default, and disabling this function may lead to packet errors.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Configure the system MTU.

system mtu *mtu-value*

Configuring the MTU of the system will update the MTU effective values of all the Ethernet interfaces (including the APs) of the system. However, if the interface is configured with an MTU, the MTU configured for the interface will take effect.

The MTU of the system is not configured by default.

(4) (Optional) Configure the forwarding plane MTU.

mtu forwarding *number*

The command works on all the physical ports only and controls only the forwarding of L2 packets. After the command is configured, the protocol MTU is inconsistent with the chip forwarding MTU, which may cause problems such as flow interruption and protocol exception in some scenarios. For example, in the IPv6 scenario, if the global fwd_mtu configuration is smaller than the default interface value when the default MTU is configured for the interface, the IPv6 packet cannot be sent and received normally, and the network will be interrupted. You are advised to use the **system mtu** command instead of this command unless there are special scenario requirements.

(5) (Optional) Configure optical module antifake detection.

fiber antifake { **ignore** | **enable** }

The optical module antifake detection function is disabled by default.

(6) (Optional) Configure the sampling period of Ethernet interface statistics.

ethernet-port counter sample-period [*interval*]

The sampling period of Ethernet interface statistics is 5s by default.

(7) (Optional) Configure the sampling period of Ethernet sub-interface statistics.

ethernet-subport counter route-sample-period [*interval*]

The sampling period of Ethernet sub-interface statistics is 5s by default.

(8) (Optional) Include interframe gaps in port rate statistics.

flow-statistics include-interframe enable

The packet sending and receiving rate statistics are cleared and recalculated after you run this command.

The function of including interframe gaps in interface packet rate statistics is disabled by default.

(9) Enter the interface configuration mode.

interface *interface-type interface-number*

(10) (Optional) Configure a L3 AP.

no switchport

(11) (Optional) Configure the rate of an interface.

speed [**10** | **100** | **1000** | **10G** | **40G** | **auto**]

If an interface is an AP member port, the rate of this interface is determined by the rate of the AP. When the interface exits the AP, it uses its own rate configuration. You can run the **show interfaces** command to view the rate configuration. The rate options available to an interface vary with the type of the interface. For example, you cannot set the rate of an SFP interface to 10 Mbps.

(12) (Optional) Configure the duplex mode of an interface.

duplex { **auto** | **full** | **half** }

(13) (Optional) Configure the flow control mode of an interface.

flowcontrol { **auto** | **off** | **on** | **receive** { **auto** | **off** | **on** } | **send** { **auto** | **off** | **on** } }

Flow control is disabled by default.

(14) (Optional) Configure the auto negotiation mode of an interface.

negotiation mode { **on** | **off** }

The auto negotiation mode is disabled by default.

(15) (Optional) Configure the MTU of an interface.

mtu *num-value*

By default, the MTU of an interface is usually 1500 bytes. The configuration varies with different interface types. The actual conditions of the specific interface prevail.

(16) (Optional) Configure the bandwidth of an interface.

bandwidth *kilobits*

No interface bandwidth is configured by default.

(17) (Optional) Configure the carrier delay of an interface.

carrier-delay { [**milliseconds**] *delay-interval* | **up** [**milliseconds**] *up-interval* **down** [**milliseconds**] *down-interval* }

The carrier delay of an interface is 2s by default.

(18) (Optional) Configure the load interval of an interface.

load-interval *seconds*

The interval of load calculation for an interface is 10s by default.

(19) (Optional) Configure a protected port.

switchport protected

A protected port is not configured for the port by default.

(20) (Optional) (In global configuration mode) Configure L3 routing blocking between protected ports.

protected-ports route-deny

The L3 routing blocking function between protected ports is disabled by default.

(21) (Optional) Configure port errdisable recovery.

errdisable recovery [**interval** *interval* | **cause** *link-state*]

The port errdisable recovery function is disabled by default.

(22) (Optional) Configure the interface traffic statistics collection function.

statistics { **enable** | **ip enable** }

The IP traffic statistics collection function is disabled for all the interfaces by default.

(23) (Optional) Create an Ethernet sub-interface.

interface gigabitethernet 0/1.1

No Ethernet sub-interface is created by default.

(24) (Optional) Configure the FEC mode of an interface.

fec mode { **rs | base-r** | **none** | **auto** }

By default, the FEC mode of an interface depends on the interface type, and a specific FEC mode is subject to the actual product.

1.5 Monitoring

This section describes the **show** commands used for checking the running status of a configured function to verify the configuration effect.

You can run the **clear** commands to clear information.

Caution

Services may be interrupted due to loss of vital information if you run the **clear** command during device operation.

The administrator can run the **line-detect** command to check the operating status of a cable. Line detection helps determine the operating status of a cable when the cable is short-circuited, disconnected, or in another abnormal state.

Specification

Only a physical port using copper as the medium supports line detection. A physical port using fiber as the medium or an AP does not support line detection.

When line detection is performed on an operational interface, the interface will be temporarily disconnected, and then re-connected.

Table 1-1Ethernet Interface Monitoring

Command	Purpose
show interfaces [*interface-type interface-number*]	Displays all the statuses and configuration information of a specified interface.
show interfaces [*interface-type interface-number*] **status err-disabled**	Displays the interface errdisable status.
show interfaces [*interface-type interface-number*] **link-state-change statistics**	Displays the link status change time and count of a specified port.
show interfaces [*interface-type interface-number*] **switchport**	Displays the administrative and operational states of switch interfaces (non-routed interfaces).
show interfaces [*interface-type interface-number*] **description** [**up** | **down**]	Displays the description and status of a specified interface.
show interfaces [*interface-type interface-number*] **counters** [**up** | **down**]	Displays the statistics of a specified port, among which the displayed rate may contain an error of ±0.5%.
show interfaces [*interface-type interface-number*] **counters increment** [**up** | **down**]	Displays the number of packets added in the previous sampling interval.
show interfaces [*interface-type interface-number*] **counters error** [**up** | **down**] [**nozero**]	Displays the statistics about error packets.

Command	Purpose
show interfaces [*interface-type interface-number*] **counters rate** [**up | down**] [**nozero**]	Displays the packet sending/receiving rate of the interface.
show interfaces [*interface-type interface-number*] **counters rate physical-layer** [**up** | **down**] [**nozero**]	Displays the packet sending/receiving rate of an interface at the physical layer. The packet sending/receiving rate at the physical layer refers to the sending/receiving rate of packets that contains interframe gaps.
show interfaces [*interface-type interface-number*] **counters summary** [**up** | **down**] [**nozero**]	Displays a summary of interface packets.
show interfaces [*interface-type interface-number*] **counters drops** [**up | down**]	Displays the statistics of discarded packets of an interface.
show interfaces [*interface-type interface-number*] **line-detect**	Displays the line detection status. Line detection helps determine the operating status of a cable when the cable is short-circuited, disconnected, or in another abnormal state.
show interfaces [*interface-type interface-number*] **usage** [**up | down**]	Displays the bandwidth usage of an interface.
show interface [*interface-type interface-number*] **mtu forwarding**	Displays the information of the forwarding plane MTU.
show mgmt virtual	Displays the information of the virtual management port.
show vlans	Displays the information of a VLAN sub-interface.
show interfaces [*interface-type interface-number*] **transceiver**	Displays the basic information about the optical module on a specified interface.
show interfaces [*interface-type interface-number*] **transceiver alarm**	Displays the current fault alarms of the optical module on a specified interface. If no fault occurs, **None** is displayed.
show interfaces [*interface-type interface-number*] **transceiver diagnosis**	Displays the current measurement values of optical module diagnosis parameters of a specified interface.
show split summary	Displays the splitting and combination information of 40G/100G interfaces.
clear counters [*interface-type interface-number*]	Clears the statistics of a specified interface.

Command	Purpose
clear link-state-change statistics [*interface-type interface-number*]	Clears the statistics of link status changes of an interface.
show interfaces [*interface-type interface-number*] **troubleshooting**	Displays the diagnosis information of an interface.
show interfaces [*interface-type interface-number*] **fault-info**	Displays the fault information of an interface, including the fault cause and occurrence time.

1.6 Configuration Examples

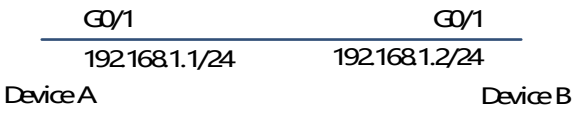
1.6.1 Configuring Interface Attributes

1. Requirements

Interconnect two devices, and configure the basic attributes of the device interfaces.

2. Topology

Figure 1-1Interface Attribute Topology



3. Notes

- Connect two devices through the switch ports.
- Configure an SVI on each of the two devices, and assign IP addresses in the same network segment to the two SVIs.
- Enable interface index persistence on the two devices.
- Enable the link trap function on the two devices.
- Configure the interface administrative status on the two devices.

4. Procedure

Configure as follows on Device A.

```
DeviceA> enable
DeviceA # configure terminal
DeviceA(config)# snmp-server if-index persist
DeviceA(config)# interface vlan 1
DeviceA(config-if-VLAN 1)# ip address 192.168.1.1 255.255.255.0
DeviceA(config-if-VLAN 1)# exit
DeviceA(config)# interface gigabitethernet 0/1
```

```
DeviceA(config-if-GigabitEthernet 0/1)# snmp trap link-status
DeviceA(config-if-GigabitEthernet 0/1)# shutdown
```

Configure as follows on Device B.

```
DeviceB# configure terminal
DeviceB(config)# snmp-server if-index persist
DeviceB(config)# interface vlan 1
DeviceB(config-if-VLAN 1)# ip address 192.168.1.2 255.255.255.0
DeviceB(config-if-VLAN 1)# exit
DeviceB(config)# interface gigabitethernet 0/1
DeviceB(config-if-GigabitEthernet 0/1)# snmp trap link-status
DeviceB(config-if-GigabitEthernet 0/1)# shutdown
```

5. Verification

Perform verification on Device A and Device B as follows:

- Run the **shutdown** command on the interface GigabitEthern 0/1, and check whether GigabitEthern 0/1 and SVI 1 are in **Down** state.
- Run the **shutdown** command on the interface GigabitEthern 0/1, and check whether a trap message indicating the **Down** state of this interface is sent.
- Restart the device, and check whether the interface index of GigabitEthern 0/1 is the same as that before the restart.

Device A:

```
DeviceB # show interfaces gigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is administratively down  , line protocol is DOWN
Hardware is GigabitEthernet, address is 00d0.f865.de9b (bia 00d0.f865.de9b)
Interface address is: no ip address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Bridge, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  Rxload is 1/255, Txload is 1/255
  Queue    Transmitted packets     Transmitted bytes       Dropped packets
Dropped bytes
      0                     0                     0                     0
0
      1                     0                     0                     0
0
      2                     0                     0                     0
0
      3                     0                     0                     0
0
      4                     0                     0                     0
0
```

```
      5                     0                     0                     0
0
      6                     0                     0                     0
0
      7                     4                   440                     0
0
  Switchport attributes:
    interface's description:""
    lastchange time:0 Day:20 Hour:15 Minute:22 Second
    Priority is 0
    admin medium-type is Copper, oper medium-type is Copper    admin duplex mode
is AUTO, oper duplex is Unknown
    admin speed is AUTO, oper speed is Unknown
    flow control admin status is OFF, flow control oper status is Unknown
    admin negotiation mode is OFF, oper negotiation state is ON
    Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
  Port-type: access
    Vlan id: 1
   10 seconds input rate 0 bits/sec, 0 packets/sec
   10 seconds output rate 0 bits/sec, 0 packets/sec
    4 packets input, 408 bytes, 0 no buffer, 0 dropped
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    4 packets output, 408 bytes, 0 underruns , 0 dropped
0 output errors, 0 collisions, 0 interface resets
A# show interfaces vlan 1
Index(dec):4097 (hex):1001
VLAN 1 is UP  , line protocol is DOWN
Hardware is  VLAN, address is 00d0.f822.33af (bia 00d0.f822.33af)
Interface address is: 192.168.1.1/24
ARP type: ARPA, ARP Timeout: 3600 seconds
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Ethernet-II, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  Rxload is 0/255, Txload is 0/255
```

Device B:

```
DeviceB# show interfaces gigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is administratively down  , line protocol is DOWN
Hardware is GigabitEthernet
Interface address is: no ip address, address is 00d0.f865.de9b (bia
00d0.f865.de9b)
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Bridge, loopback not set
  Keepalive interval is 10 sec , set
```

```
  Carrier delay is 2 sec
  Rxload is 1/255, Txload is 1/255
  Queue    Transmitted packets     Transmitted bytes       Dropped packets
Dropped bytes
      0                     0                     0                     0
0
      1                     0                     0                     0
0
      2                     0                     0                     0
0
      3                     0                     0                     0
0
      4                     0                     0                     0
0
      5                     0                     0                     0
0
      6                     0                     0                     0
0
      7                     4                   440                     0
0
  Switchport attributes:
    interface's description:""
    lastchange time:0 Day:20 Hour:15 Minute:22 Second
    Priority is 0
    admin medium-type is Copper, oper medium-type is Copper
    admin duplex mode is AUTO, oper duplex is Unknown
    admin speed is AUTO, oper speed is Unknown
    flow control admin status is OFF, flow control oper status is Unknown
    admin negotiation mode is OFF, oper negotiation state is ON
    Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
  Port-type: access
    Vlan id: 1
   10 seconds input rate 0 bits/sec, 0 packets/sec
   10 seconds output rate 0 bits/sec, 0 packets/sec
    4 packets input, 408 bytes, 0 no buffer, 0 dropped
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    4 packets output, 408 bytes, 0 underruns , 0 dropped
0 output errors, 0 collisions, 0 interface resets
B# show interfaces vlan 1
Index(dec):4097 (hex):1001
VLAN 1 is UP  , line protocol is DOWN
Hardware is  VLAN, address is 00d0.f822.33af (bia 00d0.f822.33af)
Interface address is: 192.168.1.2/24
ARP type: ARPA, ARP Timeout: 3600 seconds
  MTU 1500 bytes, BW 1000000 Kbit
```

```
Encapsulation protocol is Ethernet-II, loopback not set
Keepalive interval is 10 sec , set
Carrier delay is 2 sec
Rxload is 0/255, Txload is 0/255
```

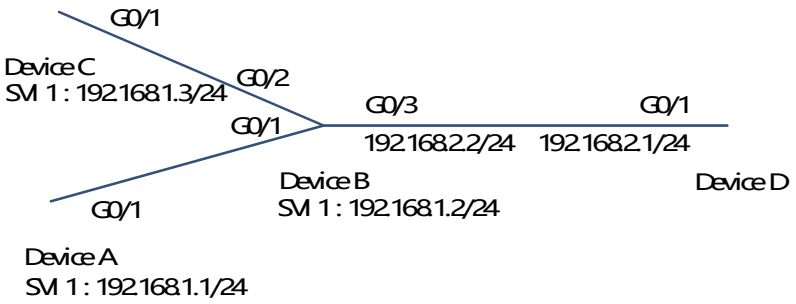
1.6.2 Configuring Interconnection Interfaces

1. Requirements

Interconnect two devices, and configure attributes of the device interfaces.

2. Topology

Figure 1-1Interconnection Interface Configuration Topology



3. Notes

- On Device A, configure GigabitEthernet 0/1 as a switch port in access mode, with the default VLAN ID as 1. Configure SVI 1, assign an IP address to SVI 1, and set up a route to Switch D.
- On Device B, configure GigabitEthernet 0/1 and GigabitEthernet 0/2 as switch ports in trunk mode, with the native VLAN ID as 1. Configure SVI 1, and assign an IP address to SVI 1. Configure GigabitEthernet 0/3 as a routed port, and assign an IP address in another network segment to this port.
- On Device C, configure GigabitEthernet 0/1 as a switch port in access mode, with the default VLAN ID as 1. Configure SVI 1, and assign an IP address to SVI 1.
- On Device D, configure GigabitEthernet 0/1 as a routed port, assign an IP address to this port, and set up a route to Switch A.

4. Procedure

Configure as follows on Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface GigabitEthernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# switchport mode access
DeviceA(config-if-GigabitEthernet 0/1)# switchport access vlan 1
DeviceA(config-if-GigabitEthernet 0/1)# exit
DeviceA(config)# interface vlan 1
DeviceA(config-if-VLAN 1)# ip address 192.168.1.1 255.255.255.0
```

```
DeviceA(config-if-VLAN 1)# exit
DeviceA(config)# ip route 192.168.2.0 255.255.255.0 VLAN 1 192.168.1.2
```

Configure as follows on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# interface GigabitEthernet 0/1
DeviceB(config-if-GigabitEthernet 0/1)# switchport mode trunk
DeviceB(config-if-GigabitEthernet 0/1)# exit
DeviceB(config)# interface GigabitEthernet 0/2
DeviceB(config-if-GigabitEthernet 0/2)# switchport mode trunk
DeviceB(config-if-GigabitEthernet 0/2)# exit
DeviceB(config)# interface vlan 1
DeviceB(config-if-VLAN 1)# ip address 192.168.1.2 255.255.255.0
DeviceB(config-if-VLAN 1)# exit
DeviceB(config)# interface GigabitEthernet 0/3
DeviceB(config-if-GigabitEthernet 0/3)# no switchport
DeviceB(config-if-GigabitEthernet 0/3)# ip address 192.168.2.2 255.255.255.0
DeviceB(config-if-GigabitEthernet 0/3)# exit
```

Configure as follows on Device C.

```
DeviceC> enable
DeviceC# configure terminal
DeviceC(config)# interface GigabitEthernet 0/1
DeviceC(config-if-GigabitEthernet 0/1)# port-group 1
DeviceC(config-if-GigabitEthernet 0/1)# exit
DeviceC(config)# interface aggregateport 1
DeviceC(config-if-AggregatePort 1)# switchport mode access
DeviceC(config-if-AggregatePort 1)# switchport access vlan 1
DeviceC(config-if-AggregatePort 1)# exit
DeviceC(config)# interface vlan 1
DeviceC(config-if-VLAN 1)# ip address 192.168.1.3 255.255.255.0
DeviceC(config-if-VLAN 1)# exit
```

Configure as follows on Device D.

```
DeviceD> enable
DeviceD# configure terminal
DeviceD(config)# interface GigabitEthernet 0/1
DeviceD(config-if-GigabitEthernet 0/1)# no switchport
DeviceD(config-if-GigabitEthernet 0/1)# ip address 192.168.2.1 255.255.255.0
DeviceD(config-if-GigabitEthernet 0/1)# exit
DeviceD(config)# ip route 192.168.1.0 255.255.255.0  GigabitEthernet 0/1
192.168.2.2
```

5. Verification

Perform verification on Device A, Device B, Device C, and Device D as follows:

- On Switch A, ping the IP addresses of interfaces of the other three devices. Verify that you can access the other two on each device.

- Verify that Device B and Device D can be pinged mutually.
- Verify that the interface status is correct. Check the PIM-DM routing tables of Device A and Device B and confirm whether the multicast packets can be received. Device A is taken as an example below:

Check on Device A.

```
DeviceA# show interfaces gigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is UP  , line protocol is UP
Hardware is GigabitEthernet, address is 00d0.f865.de90 (bia 00d0.f865.de90)
Interface address is: no ip address
  MTU 1500 bytes, BW 100000 Kbit
  Encapsulation protocol is Ethernet-II, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  Ethernet attributes:
    Last link state change time: 2012-12-22 14:00:48
    Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50
seconds
    Priority is 0
    Admin medium-type is Copper, oper medium-type is Copper
    Admin duplex mode is AUTO, oper duplex is Full
    Admin speed is AUTO, oper speed is 100M
    Flow control admin status is OFF, flow control oper status is OFF
    Admin negotiation mode is OFF, oper negotiation state is ON
Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
  Bridge attributes:
Port-type: access
Vlan id: 1
  Rxload is 1/255, Txload is 1/255
  10 seconds input rate 0 bits/sec, 0 packets/sec
  10 seconds output rate 67 bits/sec, 0 packets/sec
    362 packets input, 87760 bytes, 0 no buffer, 0 dropped
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    363 packets output, 82260 bytes, 0 underruns , 0 dropped
    0 output errors, 0 collisions, 0 interface resets
```

Check on Device B.

```
DeviceB# show interfaces gigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is UP  , line protocol is UP
Hardware is GigabitEthernet, address is 00d0.f865.de91 (bia 00d0.f865.de91)
Interface address is: no ip address
  MTU 1500 bytes, BW 100000 Kbit
  Encapsulation protocol is Ethernet-II, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
```

```
  Ethernet attributes:
    Last link state change time: 2012-12-22 14:00:48
    Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50
seconds
    Priority is 0
    Admin medium-type is Copper, oper medium-type is Copper
    Admin duplex mode is AUTO, oper duplex is Full
    Admin speed is AUTO, oper speed is 100M
    Flow control admin status is OFF, flow control oper status is OFF
    Admin negotiation mode is OFF, oper negotiation state is ON
Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
  Bridge attributes:
    Port-type: trunk
    Native vlan: 1
    Allowed vlan lists: 1-4094
Active vlan lists: 1
  Rxload is 1/255, Txload is 1/255
  10 seconds input rate 0 bits/sec, 0 packets/sec
  10 seconds output rate 67 bits/sec, 0 packets/sec
362 packets input, 87760 bytes, 0 no buffer, 0 dropped
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
363 packets output, 82260 bytes, 0 underruns , 0 dropped
0 output errors, 0 collisions, 0 interface resets
```

Check on Device C.

```
DeviceC# show interfaces gigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is UP  , line protocol is UP
Hardware is GigabitEthernet, address is 00d0.f865.de92 (bia 00d0.f865.de92)
Interface address is: no ip address
  MTU 1500 bytes, BW 100000 Kbit
  Encapsulation protocol is Ethernet-II, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  Ethernet attributes:
Last link state change time: 2012-12-22 14:00:48
Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50
seconds
Priority is 0
Admin medium-type is Copper, oper medium-type is Copper
Admin duplex mode is AUTO, oper duplex is Full
Admin speed is AUTO, oper speed is 100M
Flow control admin status is OFF, flow control oper status is OFF
Admin negotiation mode is OFF, oper negotiation state is ON
Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
  Rxload is 1/255, Txload is 1/255
```

```
  10 seconds input rate 0 bits/sec, 0 packets/sec
  10 seconds output rate 67 bits/sec, 0 packets/sec
362 packets input, 87760 bytes, 0 no buffer, 0 dropped
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
363 packets output, 82260 bytes, 0 underruns , 0 dropped
0 output errors, 0 collisions, 0 interface resets
```

Check on Device D.

```
DeviceD# show interfaces gigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is UP  , line protocol is UP
Hardware is GigabitEthernet, address is 00d0.f865.de93 (bia 00d0.f865.de93)
Interface address is: 192.168.2.1/24
  MTU 1500 bytes, BW 100000 Kbit
  Encapsulation protocol is Ethernet-II, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  Ethernet attributes:
Last link state change time: 2012-12-22 14:00:48
Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50
seconds
Priority is 0
Admin medium-type is Copper, oper medium-type is Copper
Admin duplex mode is AUTO, oper duplex is Full
Admin speed is AUTO, oper speed is 100M
Flow control admin status is OFF, flow control oper status is OFF
Admin negotiation mode is OFF, oper negotiation state is ON
Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
  Rxload is 1/255, Txload is 1/255
  10 seconds input rate 0 bits/sec, 0 packets/sec
  10 seconds output rate 67 bits/sec, 0 packets/sec
362 packets input, 87760 bytes, 0 no buffer, 0 dropped
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
363 packets output, 82260 bytes, 0 underruns , 0 dropped
0 output errors, 0 collisions, 0 interface resets
```