Interface

QSR-1920, QSR-2920, QSR-3920

Оглавление

1. INTERFACE BASIS

1.1. Overview

The interfaces can be classified into physical interface and logical interface. The physical interface includes Ethernet interface, E1 interface, CE1 interface, and 4G interface. The logical interface includes Ethernet subinterface, aggregation group interface, VLAN interface, loopback interface, null interface, and tunnel interface.

- Physical interface

The physical interfaces can be classified into fast Ethernet interface and slow WAN interface. Ethernet, characterized with highly flexible, relatively simple, and easy to realize, currently has become a most important LAN networking technology. The WAN interfaces are classified into E1 interface, CE1 interface, and synchronous/asynchronous serial interface. These interfaces can capsulate WAN link protocols such as HDLC and PPP. The device supports the following physical interfaces:

L2 Ethernet interface: also called port, is a physical interface. It works in layer 2, the data link layer. It only switches and forwards the received packets in layer 2.

L3 Ethernet interface: is a physical interface. It works in the network layer and can configure the IP address. It forwards the received packets in layer 3. That is, it can receives and transmits packets with the source IP address and destination IP address in the different network segment.

E1 interface: is a physical interface. It works in the physical layer. The highest rate 2 Mbps can be divided into 32 timeslots. It can transmit different data via TDM.

CE1 interface: is a physical interface. It works in the physical layer. The 2 Mbps E1 line is divided into 1 to 31 timeslots, providing 31 logical channels. Each channel is 64 kbps. Timeslot 0 transmits the signaling, which means that complete transparent transmission is impossible. Other 31 timeslots are used for data transmission.

Synchronous/Asynchronous serial interface: is a physical interface. It works in the physical layer and used for receiving and transmitting data. Synchronous serial interface: Clocks are only configured on the DCE port. In the V.35mode, the highest rate is 2 Mbps. In the V.24mode, the highest rate is 128 kbps. Asynchronous serial interface: The two ports must be configured with the same rate. In the V.35 or V.24 mode, the highest rate is 115200 bps.

3G interface: is the third generation mobile communications interface. It provides slow WAN access based on different access modes, which is a mainstream wireless mobile communications WAN access mode currently. It provides convenient, fast, and flexible networking method for users.

4G interface: is the fourth generation mobile communications interface and provides the high-speed wireless communication access mode. It provides the faster and better data communication service for the user. The networking mode is more flexible.

- Logical interface

The logical interface does not exist physically but it can achieve data switching, interacting, and forwarding. The device supports the following logical interfaces:

L3 Ethernet subinterface: is a logical interface. It works in the network layer and can configure the IP address and handle the L3 protocol. The VLAN tagged packets are received and transmitted on the L3 Ethernet interface. Users can configure multiple subinterfaces on one Ethernet interface. Therefore, packets from different VLANs can be forwarded from different subinterfaces, providing high flexibility for users.

Virtual Ethernet interface: is a logical interface. It can be divided into L3 VE interface (Virtual-Ethernet) and L2 VE interface (VE-Bridge). It is realized on the interface board, which applies to Ethernet protocol carrying other data link layer protocol.

Aggregation group interface: is a logical interface. It can be formed by binding multiple physical links between two devices. It works in the data link layer, expanding the link bandwidth and improving the link reliability.

VLAN interface: is a logical interface. It is bound with VLAN and forwards the packet between different VLANs.

loopback interface: is a logical interface. For the packets sent to the loopback interface, the device regards that the packets are sent to itself, so it does not forward the packets.

Null interface: is a logical interface. Any packet sent to null interface is dropped.

Tunnel interface: is a logical interface, providing the transmission link for the point-to-point mode.

For different interfaces, there are corresponding configuration modes. The related configuration modes of the interfaces include:

- Interface configuration mode, corresponds to L3 Ethernet interface, E1 interface, CE1 interface, 3G interface, synchronous/asynchronous serial interface, and all logical interfaces except the aggregation group interface.
- L2 Ethernet configuration mode: corresponds to L2 Ethernet interface, also called port.
- Aggregation group configuration mode: corresponds to the aggregation group interface.

This chapter mainly describes the common function configuration of various interfaces. For the featured function configuration of various interfaces, refer to the corresponding interface chapter.

1.2. Basic Function Configuration of Interfaces

Table 1-1 Basic function configuration list of interfaces

Configuration Task	
Configure the basic functions of the interfaces	Enter the interface configuration mode
	Enable/Disable the interface
	Configure the interface MTU
	Configure the interface description information
	Configure the interface logical bandwidth
	Configure the interface delay
	Configure the statistics interval of interface traffic.
	Configure the interface bandwidth utilization alarm

Configuration Task	
Configure the interface group function	Configure the interface group
Configure the interface status SNMP proxy concern layer	Configure the interface status SNMP proxy concern layer

1.2.1. Configure Basic Functions of Interfaces

Configuration Condition

None

Enter Interface Configuration Mode

Table 1-2 Enter the interface configuration mode

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	Mandatory

Note:

- If a logical interface is not created, the preceding command will be used to create the logical interface and then enter its configuration mode.

Enable/Disable Interface

Users can enable/disable an interface manually.

Table 1-3 Enable/Disable the interface

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	Either After entering the interface configuration mode, the follow-up configuration can take effect only on the current interface. After entering the L2 Ethernet interface configuration mode, the follow-up configuration can take effect only on the current port. After entering the aggregation group configuration mode, the follow-up configuration can take effect only on the aggregation group interface.
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Disable the interface	**shutdown**	Mandatory By default, the interface is enabled.
Enable the interface	**no shutdown**	Mandatory By default, the interface is enabled.

Note:

- The null interface does not support the function of disabling the interface.

Configure Interface MTU

The MTU configured on the interface takes effect at the same time for the ingress and egress packets, and the set values are the same. When the length of the received and sent packets exceeds the set value, the packets are dropped directly.

In contrast, the MTU configured on L3 Ethernet interface only takes effect for the egress packets. When the length of the sent packet exceeds the set value, the packet first performs the IP fragmenting, making the length of the fragmented packet not exceed the set value, and then send it out.

Table 1-4 Configure interface MTU

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	Either After entering the interface configuration mode, the follow-up configuration can take effect only on the current interface. After entering the interface configuration mode, the follow-up configuration can take effect only on the current port.
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	
Configure the interface MTU	**mtu** *mtu-size*	Mandatory The default MTU value varies for different interface types. For details, refer to the command manual.

Note:

- The null interface, loopback interface, tunnel interface, and aggregation group interface do not support the MTU configuration.
- The MTU value of the tunnel interface varies with MTU value of the egress interface.
- The actual valid port MTU is the multiples of 4 bytes. If the setting value is not the multiples of 4 bytes, the actual valid MTU = (setting value / 4) x 4. For example, if the set MTU is 1501 bytes, the actual valid MTU is 1500 bytes. If the length of the frame received and transmitted by the port exceeds the set MTU, the frame is dropped directly.

Configure Interface Description Information

Users can describe the interface through configuring the interface description information.

Table 1-5 Configure the interface configuration information

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	Either

Step	Command	Description
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	After entering the interface configuration mode, the follow-up configuration can take effect only on the current interface. After entering the interface configuration mode, the follow-up configuration can take effect only on the current port. After entering the aggregation group configuration mode, the follow-up configuration can take effect only on the aggregation group interface.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the interface description information	**description** *description-name*	Mandatory By default, the interface description information is not configured

Note:

- The null interface does not support the function of configuring the interface description.

Configure Interface Logical Bandwidth

The interface logical bandwidth affects the routing costs and QoS calculation, which does not affect the interface physical bandwidth. Generally, when the interface is connected to the WAN, it is recommended that the interface logical bandwidth and the actual bandwidth of the leased line be consistent.

Table 1-6 Configure the interface logical bandwidth

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the interface logical bandwidth	**bandwidth** *width-value*	Mandatory The default logical bandwidth varies for different interface types. For details, refer to the command manual.

Note:

- The interface logical bandwidth does not vary with the rate negotiated at the physical layer. For example, the gigabit-Ethernet port negotiates a rate as 100 M. The logical bandwidth still remains at the default value 1,000,000 kbps.
- The default logical bandwidth varies for different interface types. You can run the **show interface** *interface-name* command to check.
- The null interface, aggregation group interface, and L2 Ethernet interface do not support the function of configuring the logical bandwidth.

Configure Interface Delay

The interface delay configuration affects the calculation of the IRMP routing protocol cost, but does not affect the actual transmission delay of the interface. Users can change the cost of the routing protocol by configuring the interface delay.

Table 1-7 Configure the interface delay

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the interface delay	**delay** *delay-time*	Mandatory The interface delay is in the unit of 10 microseconds. The default delay varies for different interface types. The default delay value of the gigabit Ethernet interface is 1, that is, 10 microseconds (1x10 microseconds). If the configured delay is 2, that is 20 microseconds (2x10 microseconds).

Note:

- The default delay value varies for different interface types. You can run the **show interface** *interface-name* command to check.
- The null interface, aggregation group interface, and L2 Ethernet interface do not support the function of configuring the delay.

Configure Statistics Interval of Interface Traffic

The device measures the interface traffic regularly. Users can change the statistics interval of the interface traffic by manual configuration.

Table 1-8 Configure statistics interval of interface traffic

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	Either After entering the interface configuration mode, the follow-up configuration can take effect only on the current interface. After entering the interface configuration mode, the follow-up configuration can take effect only on the current port. After entering the aggregation group configuration mode, the follow-up configuration can take effect only on the aggregation group interface.
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the statistics interval for the average interface traffic rate	**load-interval** *interval*	Mandatory The default statistic interval is 300s.

Note:

- The null interface does not support the function of configuring the statistics interval of the interface traffic.

Configure Increasing or Reducing Interface Packet Statistics Length

In the compatibility test or actual application, the bandwidth calculation mode of the instrument or device interconnected with the local device is different from the local device. Here, you can adopt configuring the interface packet statistics length to correct, so as to keep consistency.

Table 1-9 Configure increasing or reducing the interface packet statistics length

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the interface to increase or reduce the packet statistics length	**packet account length** { **add** | **subtract** } *length*	Mandatory By default, do not configure increasing or reducing the packet statistics length on the interface.

Note:

The Null interface does not support the interface to configure increasing or reducing the packet statistics length.

Configure Interface Bandwidth Utilization Alarm

In the use of the device, the bandwidth utilization alarm threshold of the interface can be set to track and maintain the traffic capacity of the device.

Table 1-10 Configure the interface bandwidth usage alarm

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the interface bandwidth utilization alarm	**trap-threshold {input-rate | output-rate}** *rate1* **[resume-rate** *rate2***] [resume-duration** *cycle***]**	Mandatory By default, the function is not enabled on the interface.

1.2.2. Configure Interface Group Functions

Bind multiple interfaces as one interface group. Configuring various interface commands on the interface group is equivalent to configuring on all interfaces of the interface group, while it is not necessary to configure on each interface repeatedly. Display the information of one interface group is to display the information of all interfaces in the interface group.

Configuration Condition

Before configuring the interface group function, first complete the following task:

- The interfaces covered by the interface group should already exist.

Configure Interface Group

Table 1-11 Configure the interface group

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create the interface group in the enumeration mode	**interface group** *group-id* **enum** *interface-name1 interface-name2 … interface-nameN* [**point-to-point | multipoint**]	Mandatory By default, the interface group is not created.
Enter the global configuration mode	**exit**	-
Create the interface group in the specified scope	**interface group** *group-id* **range** | *start-interface-name end-interface-name* [**point-to-point** | **multipoint**]	Mandatory By default, the interface group is not created.

Note:

- The interface types in the interface group should be the same. The user can configure multiple interface groups as desired.
- The user can configure the commands supported by all types of interfaces in the interface group, but if the interfaces covered by the interface group do not support, the commands do not take effect and there may be no error prompt. Please check whether the commands take effect by viewing the configuration.
- If the interface group covers the logical interface and when the logical interface is deleted, the logical interface in the interface group is also deleted automatically.

1.2.3. Configure Interface Status SNMP Proxy Concerned Layer

In fact, the interface UP/DOWN status has two layers of status in the system. One is the L2 link layer status and the other is L3 protocol layer status. You can adopt the **show ip interface brief** command to view. Usually, the two status vary with the physical interface UO/DOWN, but when configuring keepalive gateway on the Ethernet interface, the L3 protocol layer status is controlled by the keepalive detection status.

If the SNMP proxy function is enabled on the device, the network management server can get the interface status information via the public mib. If SNMP Trap is enabled, the interface status change information can be sent to the network management server.

With the function command, you can set the SNMP proxy concerned interface status layer. By default, the SNMP proxy concerned interface status layer is L2 link layer, but to make the

interface status displayed by the network management server be consistent with the keepalive detection status when keepalive gateway is configured on the Ethernet interface, it is necessary to set the SNMP proxy concerned interface status is the L3 protocol layer. Therefore, in the environment enabled with keepalive detection (such as MSTP WAN line environment), it is suggested to configure **link-status-care l3**.

Configuration Condition

None

Table 1-12 Configure the interface status SNMP proxy concerned layer

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the network management layer of the interface status	**link-status-care** { **l2** | **l3** }	Mandatory By default, the interface status SNMP proxy concerned layer is L2 link layer.
Exit the global configuration mode	**exit**	-

1.2.4. Basic Monitoring and Maintaining of Interfaces

Table 1-13 Basic monitoring and maintaining of interfaces

Command	Description
clear interface *interface-name*	Clear the statistics information of the master interfaces and subinterfaces
clear interface *interface-name* **original statistics**	Clear the statistics information of the master interfaces
clear interface group *group-id*	Clear the statistics information of all interfaces in the interface group
show interface [*interface-name*]	Display the statistics information of the master interfaces and subinterfaces
show interface group *group-id*	Display the information of the interfaces in the interface group

Command	Description
show interface *interface-name* **original statistics**	Display the statistics information of the mater interfaces
show interface statistics [**input** | **output**]	Display the received and sent bit rate, bytes, packets and bandwidth usage statistics information of all interfaces
show running-config current-mode	Display the current interface configuration information

2. ETHERNET INTERFACE

2.1. Overview

Ethernet adopts the CSMA/CD media access mechanism, enabling any workstation to access the network at any time. Before transmitting data, the workstation first monitors whether the network is available. If no data is transmitted on the network, the workstation sends the information to be transmitted to the network. Ethernet, characterized with highly flexible, relatively simple, and easy to realize, currently has become a most important network technology.

Gigabit Ethernet, as a high-speed Ethernet technology, provides an efficient solution for improving the core network. The biggest advantage of this solution lies in that it inherits cost effective character of the traditional Ethernet technology. The gigabit Ethernet adopts the same frame format, frame structure, network protocol, full-/half-duplex work mode, flow control mode, and wiring system as the 10 M Ethernet. The gigabit Ethernet does not change the desktop application, operating system, application programs, and network management components of the traditional Ethernet, therefore it can be perfectly compatible with the 10 M/100 M Ethernet and protect the investment to a large extent. In addition, the IEEE standard supports the multimode fiber with a maximum distance of 550 m, single mode fiber with a maximum distance of 70 km, and coaxial cable with a maximum distance of 100 m. The gigabit Ethernet fills the gap of the 802.3 Ethernet/fast Ethernet standards.

The ten gigabit Ethernet standard is contained in the complementary standard IEEE 802.3ae of the IEEE802.3. It extends the IEEE 802.3 protocol and MAC standard, enabling them to support the 10 Gb/s transmission rate. In addition, through the WIS (WAN interface sublayer), the 10 gigabit Ethernet can be adjusted to a low transmission rate, which requires that the transmission format of the 10 gigabit Ethernet device and of the SONET (synchronous optic network) STS - 192c are compatible.

The Ethernet interfaces are classified into L2 Ethernet interface and L3 Ethernet interface.

Ethernet interface, also called L2 Ethernet interface or port, is a physical interface. It works at layer 2 in the OSI reference model-data link layer. It is mainly used to execute two basic operations:

Data frame forwarding: According to the MAC address (that is physical address) of the data frame, forward the data frame. Ethernet interface can only perform the L2 switching forwarding for the received packets, that is, can only receive and send the packets whose source IP and destination IP are at the same segment.

MAC address learning: Construct and maintain the MAC address table, used to support forwarding the data frames.

L3 Ethernet interface works at layer 3 in the OSI reference model-network layer. It configures the IP address, handles the L3 protocol, and provides the routing function.

According to the maximum rate supported by the port, the ports can be divided to the following three types:

Fastethernet: 100M port, can be abbreviated as Fa, such as fastethernet0/1 or Fa0/1;

Gigabitethernet: 1000M port, can be abbreviated as Gi, such as gigabitethernet0/25 or Gi0/25;

Tengigabitethernet: 10 Gigabit port, can be abbreviated as Te, such as tengigabitethernet1/1 or Te1/1.

According to the media type of the port, the port type can be divided to copper (electrical port) and fiber (optical port).

L2 Ethernet interface and L3 Ethernet interface differ in functions, resulting in different configuration modes. L2 Ethernet interface and L3 Ethernet interface correspond to L2 Ethernet configuration mode and L3 Ethernet configuration mode, respectively.

2.2. Ethernet Interface Function Configuration

Table 2-1 Function configuration list of Ethernet interface

Configuration Task	
Configure basic functions of Ethernet interface	Configure the rate and duplex mode
	Configure the switching of Ethernet interface fiber and electrical modes
Configure features of L3 Ethernet interface	Configure the MAC address of the Ethernet interface
	Configure the automatic negotiation of the Ethernet interface fiber mode
Configure features of L2 Ethernet interface	Enter the L2 Ethernet interface configuration mode
	Enter the batch configuration mode of L2 Ethernet interface
	Configure the port MDIX (Media Dependent Interface Crossover) mode
	Configure the port media type
	Configure the head-of-line blocking
	Configure the port flow control
	Configure the delay time
	Configure automatic energy-saving of the port
	Configure the status flap detection of the port
	Enable port loopback test

Configuration Task	
	Configure the storm suppression parameter
	Configure the action executed after the storm suppression
	Configure the UNI/NNI attribute of the port
	Configure the uni port connectivity

2.2.1. Configure Basic Functions of Ethernet interface

Configuration Condition

None

Configure Rate and Duplex Mode

The interface rate can be set in the following two methods:

One is to set the fixed rate according to the port rate capability set. The optional parameters include **10** (10M), **100** (100M), **1000** (1000M), **10000** (10000M), 10000 (10000M), 40000 (40000M).

The other is to set the rate as **auto** (auto-negotiation), specifying that the rate is negotiated by the local end and the peer port.

Similarly, the port duplex mode can be set in the following two methods:

One is to set the duplex mode according to the capability set of the port duplex mode. The optional parameters include **full** (full-duplex mode), indicating that the port can send packets when receiving the packets; **half** (half-duplex mode), indicating that the port can only receive or send packets at one moment, but cannot perform at the same time;

The other is to set the duplex mode as **auto** (auto-negotiation), indicating that the duplex mode is negotiated automatically by the local end and the peer port.

Table 2-2 Configure the rate and duplex mode of the port

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	Either After entering the interface configuration mode, the follow-up configuration can take effect only on the current interface. After entering the interface configuration mode, the follow-up configuration can take effect only on the current port.
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	
Configure the port rate	**speed** { **10** | **100** | **1000** | **10000** | **auto** }	Mandatory By default, the port rate is set to **auto**.
Configure the duplex mode of the port	**duplex** { **auto** | **full** | **half** }	Mandatory By default, the duplex mode of the port is set to **auto**.

Configure Switching of Ethernet Fiber and Electrical Modes

Table 2-3 Configure the switching of Ethernet fiber and electrical modes

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	Either After entering the interface configuration mode, the follow-up configuration can take effect only on the current interface. After entering the interface configuration mode, the follow-up configuration can take effect only on the current port.
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	

Step	Command	Description
Configure the interface media type	**media-type** { **auto** | **copper** | **fiber** }	Mandatory By default, the media type of the electrical port is **copper**, the media type of the optical port is fiber.

2.2.2. Configure Features of L3 Ethernet Interface

Configuration Condition

None

Configure the MAC Address of the Ethernet Interface

Table 2-4 Configure the MAC address of the Ethernet interface

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the MAC address	**mac-address** *mac-address-value*	Mandatory By default, the MAC address of the Ethernet interface is the factory defaults.
Restore the MAC address	**no mac-address**	Restore the MAC address of the Ethernet interface to the factory defaults.

Note:

- The MAC address is 48 bytes. The preceding command can be only used to set the unicast MAC address. The MAC address of the interface cannot be set to all 0, broadcast address, or multicast address.

Configure Automatic Negotiation of Ethernet Interface Fiber Mode

Table 2-5 Configure the automatic negotiation of the optical Ethernet interface mode

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the automatic negotiation of the Ethernet interface fiber mode	**fiber-mode negotiation** { **enable** | **disable** }	Mandatory By default, the automatic negotiation of the Ethernet interface fiber mode is set to disable.

2.2.3. Configure Features of L2 Ethernet Interface

Enter the L2 Ethernet Interface Configuration Mode

To configure on the specified port, first enter the L2 Ethernet interface configuration mode of the port and then execute the corresponding configuration command.

Table 2-6 Enter the L2 Ethernet interface configuration mode

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Mandatory

Note:

- The naming rule of the port number is S/P (Slot/Port). Slot indicates the slot on the device, numbered from 0. If there is fixed port, slot 0 is reserved for the fixed port. The service slot is numbered from 1. Port indicates the physical port on the device or service card. The port on each device and service card is numbered from 0.
- The naming rule of the port name *interface-name* is port type + port number. For example, gigabitethernet0/0 indicates the fixed port numbered 1 and the type is 1000 M port.

Enter Batch Configuration Mode of L2 Ethernet Interface

When performing the same configuration on multiple ports, to improve the configuration efficiency and reduce the repeated steps, select entering the batch configuration mode of the L2 Ethernet interface, including the following three cases: single port, such as gigabitethernet0/1; successive ports, using “-” to indicate one section of successive ports, such

as gigabitethernet0/3-0/5, indicating port 0/3, 0/4, 0/5; single port and successive ports, using comma to separate, such as “gigabitethernet0/1, 0/3-0/4, 0/6”, indicating port 0/1, 0/3, 0/4, 0/6.

Table 2-7 Enter the batch configuration mode of the L2 Ethernet interface

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the batch configuration mode of the L2 Ethernet interface	**interface** *interface-list*	Mandatory

Configure Port MDIX Mode

We can send and receive signals only after connecting the local end and the peer port. Therefore, the MDIX mode is used with connection cables.

The cables connecting ports are divided to two types: straight-through cable and crossover cable. To support the two types of cables, provide three kinds of MDIX modes: **normal**, **cross**, and **auto**.

The optical port can only support straight-through cable. Therefore, MDIX mode can only be set as **normal**.

The electrical port is formed by eight pins. You can change the roles of the pins by setting the MDIX mode. When setting as **normal**, use pin 1 and 2 to send signals, and pin 3, 6 to receive signals; when setting as **cross**, use pin 1, 2 to receive signals, pin 3, 6 to send signals; when setting as **auto**, the local and peer electrical ports automatically negotiate the functions of the pins by connecting the cables.

When using the straight-through cable, the MDIX modes of the local and peer ports cannot be the same.

When using crossover cable, the MDIX modes of the local and peer ports should be the same or at least one is **auto**.

Table 2-8 Configure port MDIX mode

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	-
Configure the mode of receiving and transmitting signal via the network cable	**mdix** { **auto | cross | normal** }	Mandatory By default, the MDIX mode of the electrical port is set to **auto** and the MDIX mode of the optical port is set to **normal**.

Configure Port Flow Control

When the sending or receiving buffer is full and if the duplex mode of the port is half-duplex, send the blocking signals back to the source end by the back pressure mode; if the duplex mode of the port is full-duplex mode, the port informs the source end to stop sending by the flow control mode.

Table 2-9 Configure the port flow control

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	-
Configure the port flow control	**flowcontrol** { **on | off** }	Mandatory By default, the flow control function of the port is disabled.

Note:

The local flow control can be realized only when the local and peer ends both enable the flow control function.

Configure Delay Time

When the port changes from Up to Down, first enter the set suppression time period and the switching of the port status is not felt by the system; and then after the set suppression time, report the port status change to the system. In this way, we can avoid the unnecessary running cost caused by the frequent switching of the ports status in short time.

Table 2-10 Configure delay time

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	-
Configure the delay time	**link-delay** *link-delay-value*	Mandatory By default, the delay report time of the port changing from Up to Down is 0, that is, disable the delay report function; when the port changes from Up to Down, report and process immediately.

Configure Port Status Flap Detection

When the port changes from Down to Up and if the port status flap detection is configured and it meets the detection condition, it is regarded that the status flap happens to the specified port or called Link-Flap and the port is automatically disabled and set as Error-Disabled.

Table 2-11 Configure the port status flap detection

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the port status flap detection	**errdisable flap-setting cause link-flap max-flaps** *max-flaps-number* **time** *time-value*	Mandatory By default, the trigger condition of executing Link-Flap is within 10s. The detected port becomes Up for at least 5 times.

Note:

- When the port is disabled by the Link-Flap function and set as Error-Disabled and if it is necessary to recover automatically, you can configure the command **errdisable recovery cause** to set the above function.

Configure Storm Suppression Parameters

Limit the broadcast, multicast or unknown unicast traffic on the port by configuring the storm suppression parameters. When the broadcast and unknown unicast traffic on the port exceeds the set threshold, the system drops the excessive packets, so as to make the proportion of the broadcast and unknown unicast traffic on the port reduce to the limited range and ensure the normal running of the network services.

Table 2-12 Configure the storm suppression parameters

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	-
Configure the storm suppression parameters	**storm-control bps** *bps-value*	Mandatory By default, the port storm suppression parameters are not configured.

Note:

- storm-control bps bps-value supports suppressing the total flow of the unknown unicast and broadcast packets.

Configure Port UNI/NNI Type

Uni port is the connection port between the user device and network; nni port is the connection interface between networks. On one device, the nni port and uni port or nni ports are interconnected; uni ports are separated from each other.

Table 2-13 Configure the UNI/NNI attribute of the port

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	-
Configure the UNI/NNI attribute of the port	**port-type** { **nni** | **uni** }	Mandatory By default, the UNI/NNI type of the port is **nni**.

Configure Connectivity of uni Port

By default, all uni ports of one device are separated from each other. However, to realize the intercommunication between the specified multiple uni ports, but not change the separation relation between these uni ports and other uni ports, you can configure the connectivity of the uni port.

When configuring the connectivity on the specified uni port, you can only set whether the uni port can forward packets to other uni ports, not affecting whether other uni ports can forward packets to the specified uni port. Therefore, to realize the intercommunication among multiple uni ports, you should configure as community on these uni ports respectively.

Table 2-14 Configure the connectivity of uni port

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	-
Configure the connectivity of uni port	**uni-isolate** { **community | isolated** }	Mandatory

Step	Command	Description
		By default, the uni port cannot forward packets to other uni ports.

Note:

- The command can only take effect on the uni port.

2.2.4. Ethernet Interface Monitoring and Maintaining

Table 2-15 Ethernet interface monitoring and maintaining

Command	Description
clear interface { *interface-list* | **switchport** } **statistics**	Clear the packet and traffic statistics information of the port
clear interface interface-name	Clear the statistics information of the specified L3 Ethernet interface
show errdisable flap-values	Display the current setting of triggering executing Link-Flap function
show interface { *interface-list* | **switchport** [**brief** [down | up]] }	Display all information or abstract information of the Ethernet interface or virtual switch link member port
show interface *interface-list* **statistics**	Display the packet and traffic statistics information of the port
show interface switchport statistics [**packet | rate**]	Display the packet and traffic statistics information of all ports on the device
show port-type [*interface-list* | { **uni** | **nni** } [*interface* interface-*list*]]	Display the UNI/NNI attribute information of the port

2.3. Typical Configuration Example of Ethernet Interface

2.3.1. Configure Storm Suppression Function

Network Requirements

- Configure the storm suppression function on the port of Device to suppress the total packets, realizing that PC2 can access Internet normally when PC1 sends lots of broadcast and unknown unicast.

Network Topology

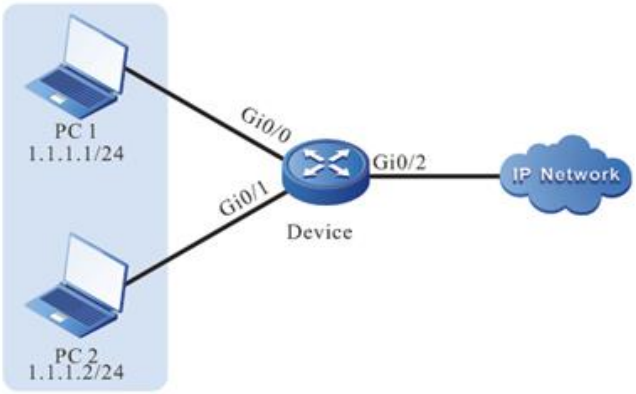

Figure 2-1 Networking of configuring storm suppression

Configuration Steps

Step 1: Configure VLAN and port link type on Device.

#Create VLAN2 on Device.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/0 and gigabitethernet0/1 on Device as Access, permitting the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet0/0,0/1 0/1,0/2
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

#Configure the link type of port gigabitethernet0/2 on Device as Trunk, permitting the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet0/2
Device(config-if-gigabitethernet0/2)#switchport mode trunk
Device(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/2)#exit
```

Step 2: Configure the storm suppression function

#Adopt bps limitation mode to suppress the broadcast, unknown unicast and multicast packets on port gigabitethernet0/0 and the suppression rate is 1024 kbps.

```
Device(config)#interface gigabitethernet 0/0
Device(config-if-gigabitethernet0/0)# storm-control broadcast bps 1024
Device(config-if-gigabitethernet0/0)# storm-control unicast bps 1024
Device(config-if-gigabitethernet0/0)#exit
```

Step 3: Check the result

#View the storm suppression information of port gigabitethernet 0/0 on Device.

```
router#show interface gigabitethernet 0/0


gigabitethernet0/1 configuration information
    Description     :
    Status          : Enabled
    Link            : Up
    Set Speed       : Auto
    Act Speed       : 1000
    Def Speed       : Auto
    Set Duplex      : Auto
    Act Duplex      : Full
    Def Duplex      : Auto
    Set Flow Control : Off
    Act Flow Control : Off
    Mdix            : Auto
    Mtu             : 1824
    Port mode       : LAN
    Port ability    : 10M HD,10M FD,100M HD,100M FD,1000M FD
    Link Delay      : No Delay
    Storm Control   : Unicast Bps 1024
    Storm Control   : Broadcast Bps 1024
    Storm Control   : Multicast Disabled
    Storm Action    : Logging
    Port Type       : Nni
    Pvid            : 2
    Set Medium      : Copper
    Act Medium      : Copper
  Mac Address       : 001f.ce22.7f19
```

#When PC1 sends lots of broadcast and unknown unicast, PC2 also can access Internet normally.

3. AGGREGATION GROUP INTERFACE

3.1. Overview

Aggregation group interface is one logical interface. When enabling the link aggregation function on multiple ports, the multiple ports with the same link aggregation feature form the aggregation group and are abstracted to aggregation group interface; meanwhile, the multiple ports with the same attribute are called the member ports of the aggregation group. It is mainly used to expand the link bandwidth and improve the connection reliability.

3.2. Aggregation Group Interface Function Configuration

Table 3-1 Function configuration list of aggregation group interface

Configuration Task	
Configure the basic functions of the aggregation group interface	Enter the aggregation group configuration mode

3.2.1. Configure Basic Functions of Aggregation Group Interface

Configuration Condition

None

Enter the aggregation group configuration mode

Table 3-2 Enter the aggregation group configuration mode

Step	**Command**	**Description**
Enter the global configuration mode	**configure terminal**	-
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	Mandatory

Note:

- Before entering the specified aggregation group configuration mode, first create the corresponding aggregation group.

3.2.2. Aggregation Group Interface Monitoring and Maintaining

Table 3-3 Monitoring and maintaining of aggregation group interface

Command	Description
clear link-aggregation *link-aggregation-id* **statistics**	Clear the packet and traffic statistics information of the specified aggregation group
show link-aggregation [*link-aggregation-id* | **brief**]	Display all information of the aggregation group
show link-aggregation *link-aggregation-id* **statistics**	Display the packet and traffic statistics information of the specified aggregation group
show port-type link-aggregation *link-aggregation-id* | { **uni** | **nni** } **link-aggregation** *link-aggregation-id*	Display the UNI/NNI attribute information of the specified aggregation group

4. VLAN INTERFACE

4.1. Overview

VLAN interface is one logical interface, used to be bound with VLAN and complete the packet forwarding between different VLANs. One VLAN can only be bound to one VLAN interface. One VLAN interface also can only be bound with one VLAN.

4.2. VLAN Interface Function Configuration

Table 4-1 VLAN interface function configuration list

Configuration Task	
Configure the basic functions of the VLAN interface	Configure VLAN interface

4.2.1. Configure VLAN Interface

Configuration Condition

None

Configure VLAN Interface

Table 4-2 Configure the VLAN interface

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create the VLAN interface	**interface vlan** *vlan-id*	Mandatory By default, the VLAN interface is not configured.

Note:

- There is no order requirement for creating VLAN interface, creating VLAN and adding physical port to VLAN.
- For how to create a VLAN and add the physical port to the VLAN, refer the VLAN chapter in the configuration manual.

4.2.2. VLAN Interface Monitoring and Maintaining

Table 4-3 VLAN interface monitoring and maintaining

Command	Description
clear interface vlan *vlan-id*	Clear the statistics information of the specified VLAN interface
show interface vlan *vlan-id*	Display the information of the specified VLAN interface
show interface vlan *vlan-id* **original statistics**	Display the statistics information of the specified VLAN interface

4.3. Typical Configuration Example of VLAN Interface

4.3.1. Configure VLAN Interface

Network Requirements

- Configure the VLAN interface on Device to realize the intercommunication between PC1 and PC2 of different VLANs.

Network Topology

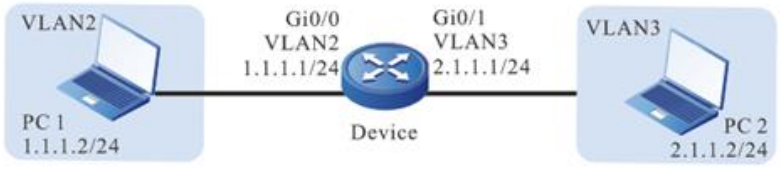

Figure 4-1 Networking of configuring VLAN interface

Configuration Steps

Step 1: Configure VLAN and port link type on Device.

Create VLAN2 and VLAN3 on Device.

```
Device#configure terminal
Device(config)#vlan 2-3
```

Configure the link type of port gigabitethernet0/0 and gigabitethernet0/1 on Device as Access. Port gigabitethernet0/0 permits the services of VLAN2 to pass and gigabitethernet0/1 permits the services of VLAN3 to pass.

```
Device(config)#interface gigabitethernet 0/0
Device(config-if-gigabitethernet0/0)#switchport mode access
Device(config-if-gigabitethernet0/0)#switchport access vlan 2
Device(config-if-gigabitethernet0/0)#exit
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
```

```
Device(config-if-gigabitethernet0/1)#switchport access vlan 3
Device(config-if-gigabitethernet0/1)#exit
```

Step 2: Configure the VLAN interface and IP address on Device.

Create VLAN2 interface on Device whose IP address is 1.1.1.1 and subnet mask is 255.255.255.0; create VLAN3 interface whose IP address is 2.1.1.1 and subnet mask is 255.255.255.0.

```
Device(config)#interface vlan 2
Device(config-if-vlan2)#ip address 1.1.1.1 255.255.255.0
Device(config-if-vlan2)#exit
Device(config)#interface vlan 3
Device(config-if-vlan3)#ip address 2.1.1.1 255.255.255.0
Device(config-if-vlan3)#exit
```

Step 3: Check the result.

#View the information of VLAN interface on Device.

```
Device#show interface vlan 2
vlan2:
    line protocol is up
    Flags: (0xc008063) BROADCAST MULTICAST ARP RUNNING
    Type: ETHERNET_CSMACD
    Internet address: 1.1.1.1/24
    Broadcast address: 1.1.1.255
    Metric: 0, MTU: 1500, BW: 1000000 Kbps, DLY: 10 usec, VRF: global
    Reliability 255/255, Txload 1/255, Rxload 1/255
    Ethernet address is 0045.1023.0032
    Last clearing of "show interface" counters never
    input peak rate 2595920 bits/sec,  1 week 0 day ago
    output peak rate 484 bits/sec,  22 hours 59 minutes 1 second ago
    5 minutes input rate 0 bits/sec, 0 packets/sec, bandwidth utilization -
    5 minutes output rate 0 bits/sec, 0 packets/sec, bandwidth utilization -
    0 packets received; 0 packets sent
    0 bytes received; 0 bytes sent
    0 multicast packets received
    1 multicast packets sent
    0 input errors; 0 output errors
    0 collisions; 0 dropped
```

```
    Unknown protocol 0
Device#show interface vlan 3
vlan3:
    line protocol is up
    Flags: (0xc008063) BROADCAST MULTICAST ARP RUNNING
    Type: ETHERNET_CSMACD
    Internet address: 2.1.1.1/24
    Broadcast address: 2.1.1.255
    Metric: 0, MTU: 1500, BW: 1000000 Kbps, DLY: 10 usec, VRF: global
    Reliability 255/255, Txload 1/255, Rxload 1/255
    Ethernet address is 0045.1023.0032
    Last clearing of "show interface" counters never
    input peak rate 2595920 bits/sec,  1 week 0 day ago
    output peak rate 484 bits/sec,  22 hours 59 minutes 1 second ago
    5 minutes input rate 0 bits/sec, 0 packets/sec, bandwidth utilization -
    5 minutes output rate 0 bits/sec, 0 packets/sec, bandwidth utilization -
    0 packets received; 0 packets sent
    0 bytes received; 0 bytes sent
    0 multicast packets received
    1 multicast packets sent
    0 input errors; 0 output errors
    0 collisions; 0 dropped
    Unknown protocol 0
```

#PC1 can ping PC2.

5. E1 INTERFACE

5.1. Overview

With the emerging of the PCM (Pulse Code Modulation), the TDM (Time Division Multiplexing) has been extensively applied in the digital communication system. Currently, two TDM systems exist in the digital communication system. One is the E1 system recommended by ITU-T, which is extensively applied in Europe and China. The other is the T1 system recommended by ANSI, which is mainly applied in North America and Japan. The T1 rate is 1.544 Mbit/s and the E1 rate is 2.048 Mbit/s.

PCM coding theory and rule: The PCM digital interface uses the G.703 standard, performing asymmetric or symmetric transmission via the 75 Ω coaxial cables or 120 Ω twisted-pair cables. HDB3 codes containing timing relationship are the transmission codes. The receiving end recovers the timing by decoding and achieves clock synchronization.

The E1 interface follows the G.703 unframed structure standard. All 2.048 Mbit/s bandwidth are used for data transmission. When the E1 interface is used for the frame structure, it can be used for G.704 CCS structure and G.704 CAS structure. G.704 CCS structure TS16 can transmit data, but G.704 CAS structure TS16 transmits signaling, instead of data. In both G.704 CCS structure and G.704 CAS structure modes, TS0 cannot transmit data. TS16 indicates timeslot 16 on the E1 channel and TS0 indicates timeslot 0 on the E1 channel.

When the E1 interface is used, all timeslots can be bound as an interface in random. This logical interface is the same as the synchronous serial port, supporting the link layer protocol such as PPP and HDLC.

5.2. E1 Interface Function Configuration

Table 5-1 Function configuration list of the E1 interface

Configuration Task	
Configure the basic functions of the E1 interface	Configure the E1 framing CAS mode
	Configure the E1framing CCS mode
Configure other features of the E1 interface	Configure the E1 data line CRC-4 verification mode
	Configure E1 interface data frame CRC verification mode
	Configure the E1 transmit clock source
	Configure the E1 matching impedance
	Configure the E1 line code
	Configure the E1 looping mode

5.2.1. Configure Basic Functions of E1 Interface

Configuration Condition

None

Configure E1 Framing CAS Mode

When configuring the E1 framing mode, TS0 is used to transmit frame synchronous signal, CRC-4, and peer end asynchronous alarm indicator and TS16 is used to transmit CAS multiframe alignment signal and multiframe peer end asynchronous alarm indicator. Thus, other 30 timeslots are used to transmit data.

Table 5-2 Configure E1 framing CAS mode

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the timeslot	**timeslot** *timeslot-range*	Mandatory By default, the interface is the unframed mode.

Note:

- When configuring the framing mode, the start timeslot number must be greater than the end timeslot number. Otherwise, the configuration is invalid.

Configure E1 Framing CCS Mode

When configuring the E1 framing mode, TS0 is used to transmit frame synchronous signal, CRC-4, and peer end asynchronous alarm indicator and TS16 is used to transmit data, that is, the CCS mode. Thus, a total of 31 timeslots on the E1 channel are used to transmit data.

Table 5-3 Configure the E1 framing CCS mode

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the TS16	**ts16**	Mandatory By default, the interface is the CAS mode.

Note:

- When configuring the interface working in the CCS mode, the interface must be in the framing mode. CCS indicates the common channel signaling and CAS indicates the channel associated signaling.

5.2.2. Configure Other Features of E1 Interface

Configuration Condition

None

Configure E1 Data Line CRC-4 Verification Mode

The E1 supports protocols such as PPP and HDLC. The CRC4 is used to check the data frame. The following commands can be used to configure data CRC4 verification mode.

Table 5-4 Configure E1 data line CRC4 verification mode

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the CRC-4 verification mode	**crc4** { **rcrc4** | **tcrc4** }	Mandatory By default, the E1 interface receiving and transmitting CRC-4 are not configured.

Note:

- This command cannot be configured in non-framing mode.

Configure E1 Data Line CRC Verification Mode

The E1 supports protocols such as PPP and HDLC. The CRC is used to check the data frame. The following commands can be used to configure data frame CRC verification mode.

Table 5-5 Configure E1 interface data frame CRC verification mode

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the CRC verification mode of the data frame	**crc** { **32** | **16** }	-

Configure E1 Transmit Clock Source

During the data transmission, both frame synchronization and clock synchronization must be ensured. Packet loss may occur when the clock is not synchronized. Therefore, to ensure clock synchronization, a unified clock must be used. One end is configured with an internal clock and the other end is configured with a line clock. Thus, a unified clock is ensured on the line.

Table 5-6 Configure E1 transmit clock source

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the transmit clock source	**clock source** { **internal** | **line** }	Mandatory By default, the E1 interface transmit clock is the line clock.

Configure E1 Matching Impedance

The E1 is the standard dual-line circuit. One is used to receive data and the other is used to send data. Meanwhile, two cables are used. One is 75 Ω unbalanced coaxial cables and the other is 120 Ω balanced twisted-pair cables. The following command can be used to configure the line matching impedance.

Table 5-7 Configure the E1 matching impedance

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the matching impedance	**resistance** { **120** | **75** }	Mandatory By default, the matching impedance of the interface is 75 Ω.

Configure E1 Line Coding

The E1 receiving and transmitting directions are independent without interfering each other. The E1 adopts the differential transmission mode, which has a stronger ability of resisting common-mode interference and a transmission distance of 1 km. Because the clock is extracted from the line clock, an independent clock line is not required. The E1 line transmits the baseband signal, generally HDB3 (High Density Bipolar 3) codes or AMI. Both the preceding two codes are ternary return to zero codes.

Table 5-8 Configure the E1 line coding

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the E1 interface line coding	**linecode** { **ami** | **hdb3** }	Mandatory By default, the interface line coding is HDB3 coding.

Configure E1 Looping Mode

Different looping modes are used to diagnose the line status. The local loop is used to diagnose whether exceptions occur to the local device for receiving and transmitting data. The remote loop is used to diagnose whether exceptions occur to the remote device for receiving and transmitting data.

Table 5-9 Configure the E1 looping mode

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the interface looping mode	**loopback** { **local** | **remote** }	Mandatory By default, the looping mode for the E1 interface is not configured.

Note:

- When configuring the interface looping, the interface transmit clock source must be configured as the internal clock.

5.2.3. E1 Interface Monitoring and Maintaining

Table 5-10 The E1 interface monitoring and maintaining

Command	Description
clear interface *interface-name*	Clear related statistics of the E1 interface *interface-name*
show controllers e1 *slot/unit*	Display related information of the E1 controller
show interface *interface-name*	Display all configuration parameters and current running status information of the E1 interface *interface-name*
show running-config	View the configuration of the E1 interface

5.3. Typical Configuration Example of E1 Interface

5.3.1. Configure E1 Unframed Mode

Network Requirements

- Use a cable to connect the E1 interface of Device1 and Device2. The E1 interface is configured as the unframed mode by default. The interface encapsulation type is PPP to enable the intercommunication between Device1 and Device2.

Network Topology

Figure 5-1 Networking of the E1 unframed mode

Configuration Steps

Step 1: Configure the clock mode for the E1 interface. Device1 is configured with an internal clock and Device2 in configured with an external clock. The external clock is the default setting, which does not need to be configured manually.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#interface serial1/0
Device1(config-if-serial1/0)#clock source internal
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#interface serial1/0
```

Step 2: Configure the IP addresses for all interfaces.

#Configure Device1.

```
Device1(config-if-serial1/0)#ip address 1.0.0.1 255.255.255.0
Device1(config-if-serial1/0)#exit
Device1(config)#exit
```

#Configure Device2.

```
Device2(config-if-serial1/0)#ip address 1.0.0.2 255.255.255.0
Device2(config-if-serial1/0)#exit
Device2(config)#exit
```

Step 3: Check the result.

#View the interface status of serial1/0 on Device1.

```
Device1#show interface serial 1/0
serial1/0:
    line protocol is up
    Flags: (0x80080f1) POINT-TO-POINT MULTICAST RUNNING
    Type: PPP
    Internet address: 1.0.0.1/24
```

```
Destination Internet address: 1.0.0.2
Metric: 0, MTU: 1500, BW: 2048 Kbps, DLY: 20000 usec, VRF: global
Reliability 255/255, Txload 1/255, Rxload 1/255
Last clearing of "show interface" counters is 0 hour 0 minute 0 second ago
input rate 0 bit/sec, 0 packet/sec, bandwidth utilization 0.00%
output rate 0 bit/sec, 0 packet/sec, bandwidth utilization 0.00%
0 packets received; 0 packets sent
0 bytes received; 0 bytes sent
0 multicast packets received
0 multicast packets sent
0 input errors; 0 output errors
0 collisions; 0 dropped
 encap-type: simply PPP
 LCP:OPENED
 IPCP:OPENED   NDSPCP:INITIAL
  rxFrames 0, rxChars 0
  txFrames 0, txChars 0
  rxNoOctet 0, rxAbtErrs 0, rxCrcErrs 0
  rxOverrun 0, rxLenErrs 0, txUnderrun 0
  DCD=up
  rate=2048000 bps
```

#Ping the IP address of the peer interface serial1/0 on Device1 and can be pinged through.

```
Device1#ping 1.0.0.2


Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 1.0.0.2 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

Note:

- The encapsulation type of the E1 interface is PPP by default. Therefore, the encapsulation type does not need to be configured for the interfaces. Run the **show interface** command, it can be observed that **Type** is set to *PPP*. If other WAN protocols need to be configured, refer to WAN protocol-related documentation.
- In the E1 unframed mode, a 2 M interface is generated. This mode is mainly applied in DDN (Digital Data Network).

5.3.2. Configure E1 Framing CAS Mode

Network Requirements

- Use a cable to connect the E1 interface of Device1 and Device2. The E1 interface is configured as framing CAS mode with timeslot 16 transmitting signaling. The framing mode is CAS by default. The interface encapsulation type is HDLC to enable the intercommunication between Device1 and Device2.

Network Topology

Figure 5-2 Networking of configuring E1 framing CAS mode

Configuration Steps

Step 1: When configuring timeslots of the E1 interface, both Device1 and Device2 use timeslot from 1 to 20.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#interface serial1/0
Device1(config-if-serial1/0)#timeslot 1-20
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#interface serial1/0
Device2(config-if-serial1/0)#timeslot 1-20
```

Step 2: Configure the clock mode for the E1 interface. Device1 is configured with an internal clock and Device2 in configured with an external clock. The external clock is the default setting, which does not need to be configured manually.

#Configure Device1.

```
Device1(config-if-serial1/0)#clock source internal
```

Step 3: Configure the IP addresses for all interfaces.

#Configure Device1.

```
Device1(config-if-serial1/0)#ip address  1.0.0.1 255.255.255.0
Device1(config-if-serial1/0)#exit
Device1(config)#exit
```

#Configure Device2.

```
Device2(config-if-serial1/0)#ip address 1.0.0.2 255.255.255.0
```

```
Device2(config-if-serial1/0)#exit
Device2(config)#exit
```

Step 4: Check the result.

View the interface status of serial1/0 on Device1.

```
Device1#show interface serial 1/0
serial1/0:
    line protocol is up
    Flags: (0x80080f1) POINT-TO-POINT MULTICAST RUNNING
    Type: PPP
    Internet address: 1.0.0.1/24
    Destination Internet address: 1.0.0.2
    Metric: 0, MTU: 1500, BW: 1216 Kbps, DLY: 20000 usec, VRF: global
    Reliability 255/255, Txload 1/255, Rxload 1/255
    Last clearing of "show interface" counters is 0 hour 0 minute 0 second ago
    input rate 0 bit/sec, 0 packet/sec, bandwidth utilization 0.00%
    output rate 0 bit/sec, 0 packet/sec, bandwidth utilization 0.00%
    0 packets received; 0 packets sent
    0 bytes received; 0 bytes sent
    0 multicast packets received
    0 multicast packets sent
    0 input errors; 0 output errors
    0 collisions; 0 dropped
     encap-type: simply PPP
     LCP:OPENED
     IPCP:OPENED   NDSPCP:INITIAL
       rxFrames 0, rxChars 0
       txFrames 0, txChars 0
       rxNoOctet 0, rxAbtErrs 0, rxCrcErrs 0
       rxOverrun 0, rxLenErrs 0, txUnderrun 0
       DCD=up
      rate=1216000 bps
```

Ping the IP address of the peer interface serial1/0 on Device1 and can be pinged through.

```
Device1#ping 1.0.0.2
```

```
Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 1.0.0.2 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

Note:

- When the E1 interface is configured as the framing mode, timeslots used by both ends must be the same. For example, in the preceding case, Device 1 uses timeslots from 1 to 20 and Device 2 must also use the timeslots from 1 to 20. Otherwise, the port cannot be up.
- When the E1 interface is configured as the framing mode, if the E1 interface is in the CAS mode, then the peer interface must also be configured in the CAS mode. Otherwise, the interface cannot be up.
- The encapsulation type of the E1 interface is PPP by default. Therefore, the encapsulation type does not need to be configured for the interfaces. Run the **show interface** command, it can be observed that **Type** is set to *PPP*. If other WAN protocols need to be configured, refer to WAN protocol-related documentation.
- The typical application of the CAS mode of the E1 interface is as follows: The digital trunk, as the voice switch, considers the E1 interface as 32 64 kbit/s. However, timeslot 16 (configurable) is used to transmit signaling.

5.3.3. Configure E1 Framing CCS Mode

Network Requirements

- Use a cable to connect the E1 interface of Device1 and Device2. The E1 interface is configured as framing CCS mode with timeslot 16 transmitting data. The interface encapsulation type is PPP to enable the intercommunication between Device1 and Device2.

Network Topology

Figure 5-3 Networking of E1 framing CCS mode

Configuration Steps

Step 1: When configuring timeslots of the E1 interface, both Device1 and Device2 use timeslot from 1 to 20.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#interface serial1/0
Device1(config-if-serial1/0)#timeslot 1-20
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#interface serial1/0
```

```
Device2(config-if-serial1/0)#timeslot 1-20
```

Step 2: Configure TS16 and CCS mode for the E1 interface.

#Configure Device1.

```
Device1(config-if-serial1/0)#ts16
```

#Configure Device2.

```
Device2(config-if-serial1/0)#ts16
```

Step 3: Configure the clock mode for the E1 interface. Device1 is configured with an internal clock and Device2 in configured with an external clock. The external clock is the default setting, which does not need to be configured manually.

#Configure Device1.

```
Device1(config-if-serial1/0)#clock source internal
```

Step 4: Configure the IP addresses for all interfaces.

#Configure Device1.

```
Device1(config-if-serial1/0)#ip address  1.0.0.1 255.255.255.0
Device1(config-if-serial1/0)#exit
Device1(config)#exit
```

#Configure Device2.

```
Device2(config-if-serial1/0)#ip address 1.0.0.2 255.255.255.0
Device2(config-if-serial1/0)#exit
Device2(config)#exit
```

Step 5: Check the result.

#View the interface status of serial1/0 on Device1.

```
Device1#show interface serial 1/0
serial1/0:
    line protocol is up
    Flags: (0x80080f1) POINT-TO-POINT MULTICAST RUNNING
    Type: PPP
    Internet address: 1.0.0.1/24
    Destination Internet address: 1.0.0.2
```

```
Metric: 0, MTU: 1500, BW: 1280 Kbps, DLY: 20000 usec, VRF: global
Reliability 255/255, Txload 1/255, Rxload 1/255
Last clearing of "show interface" counters is 0 hour 0 minute 0 second ago
input rate 0 bit/sec, 0 packet/sec, bandwidth utilization 0.00%
output rate 0 bit/sec, 0 packet/sec, bandwidth utilization 0.00%
0 packets received; 0 packets sent
0 bytes received; 0 bytes sent
0 multicast packets received
0 multicast packets sent
0 input errors; 0 output errors
0 collisions; 0 dropped
 encap-type: simply PPP
 LCP:OPENED
 IPCP:OPENED   NDSPCP:INITIAL
  rxFrames 0, rxChars 0
  txFrames 0, txChars 0
  rxNoOctet 0, rxAbtErrs 0, rxCrcErrs 0
  rxOverrun 0, rxLenErrs 0, txUnderrun 0
  DCD=up
 rate=1280000 bps
```

Ping the IP address of the peer interface serial1/0 on Device1 and can be pinged through.

```
Device1#ping 1.0.0.2


Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 1.0.0.2 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

Note:

- When the E1 interface is configured as the framing mode, timeslots used by both ends must be the same. For example, in the preceding case, Device 1 uses timeslots from 1 to 20 and Device 2 must also use the timeslots from 1 to 20. Otherwise, the interface cannot be up.
- When the E1 interface is configured as the framing mode, if the E1 interface is in the CCS mode, then the peer interface must also be configured in the CCS mode. Otherwise, the interface cannot be up.
- The encapsulation type of the E1 interface is PPP by default. Therefore, the encapsulation type does not need to be configured for the interfaces. Run the **show interface** command, it can be observed that **Type** is set to *PPP*. If other WAN protocols

need to be configured (for example, PPP protocol), refer to WAN protocol-related documentation.

- The typical application of the CCS mode of the E1 interface is as follows: The digital trunk, as the voice switch, considers the E1 interface as 32 64 kbit/s. However, timeslot 16 (configurable) is used to transmit data.

6. CE1 INTERFACE

6.1. Overview

CE1 means channelized E1. A 2.048Mbit/s E1 is used as multiple 64 kbit/s and its combination, such as 128 kbit/s and 256 kbit/s. The difference between CE1 and E1 lies in that timeslots cannot be divided for the E1 but can be divided for CE1. CE1 has a total of 32 timeslot and each timeslot is 64 kbit/s. It can be divided into N x 64 kbit/s. Timeslot 0 of CE1 is used to transmit synchronous information. CE1 and E1 can be interconnected, but CE1 must be used as E1 in this case, that is, timeslots cannot be divided. The link layer supports the link layer protocols such as PPP and HDLC.

6.2. CE1 Interface Function Configuration

Table 6-1 Function configuration list of the CE1 interface

Configuration Task	
Configure the basic functions for the CE1 interface	Configure the CE1 framing mode
	Configure the CE1 unframed mode
Configure other feature for the CE1 interface	Configure the CE1 data line CRC-4 verification mode
	Configure the CE1 transmit clock source
	Configure the CE1 matching impedance
	Configure the CE1 line coding mode
	Configure the CE1 looping mode

6.2.1. Configure Basic Functions of CE1 Interface

Configuration Condition

None

Configure CE1 Framing Mode

When configuring the CE1 framing mode, CE1 at this time is the E1 in the CCS mode. But the difference between CE1 and E1 lies in that timeslots of CE1 can be divided into multiple channels to transmit data independently. The E1 can be only divided into one channel, but this channel has a bandwidth of N x 64 kbit/s. However, the CE1 can be divided into multiple N s 64 kbit/s.

Table 6-2 Configure the CE1 interface

Step	Command	Description
Enter the CE1 controller configuration mode	**controller e1** *slot/unit*	-
Enter the channel	**channel-group** *channel-group-number* **timeslots** *timeslots-range*	Mandatory By default, the CE1 channel is not configured.

Note:

- When configuring the framing mode, the start timeslot number must be smaller than the end timeslot number. Otherwise, the configuration is invalid.
- If a timeslot is configured for both two channels, this configuration is invalid and interfaces cannot be generated.
- During the configuration, the timeslot scope must match the channel group number. The timeslot of the channel group is defined by the service provider.

Configure CE1 Unframed Mode

Configuring CE1 unframed mode equals to the transparent 2 M mode of the E1 interface. All the 32 timeslots are used to transmit data and the bandwidth is 2048 kbps.

Table 6-3 Configure the CE1 unframed mode

Step	Command	Description
Enter the CE1 controller configuration mode	**controller e1** *slot/unit*	-
Configure the unframed CE1 interface of transparent 2 M	**unframed**	Mandatory By default, the unframed mode is not configured.

Note:

- If other channels are configured, the unframed mode cannot be configured any more.

6.2.2. Configure Other Features of CE1 Interface

Configuration Condition

None

Configure CE1 Data Line CRC4 Check Mode

The CE1 interface supports the protocols such as PPP and HDLC. CRC4 can be used to verify the data frame. The following command can configure the data CRC4 verification mode.

Table 6-4 Configure the CE1 data line CRC4 check mode

Step	Command	Description
Enter the CE1 controller configuration mode	**controller e1** *slot/ unit*	-
Configure the CRC-4 verification mode	**framing** { **crc4** | **default** | **no-crc4** }	Mandatory By default, the CRC-4 verification is used only when data is transmitted.

Configure CE1 Transmit Clock Source

During the data transmission, both frame synchronization and clock synchronization must be ensured. Packet loss may occur when the clock is not synchronized. Therefore, to ensure clock synchronization, a unified clock must be used. One end is configured with an internal clock and the other end is configured with a line clock. Thus, a unified clock is ensured on the line.

Table 6-5 Configure the CE1 transmit clock source

Step	Command	Description
Enter the CE1 controller configuration mode	**controller e1** *slot/ unit*	-
Configure the transmit clock source	**clock source** { **internal** | **line** }	Mandatory By default, the transmit clock of the CE1 interface is the line clock.

Configure CE1 Matching Impedance

The CE1 is the standard dual-line circuit. One is used to receive data and the other is used to send data. Meanwhile, two cables are used. One is 75 Ω unbalanced coaxial cables and the other is 120 Ω balanced twisted-pair cables. The following command can be used to configure the line matching impedance.

Table 6-6 Configure the CE1 matching impedance

Step	Command	Description
Enter the CE1 controller configuration mode	**controller e1** *slot/ unit*	-
Configure the matching impedance	**resistance** { **120** | **75** }	Mandatory By default, the matching impedance of the interface is 75 Ω.

Configure CE1 Line Coding

The CE1 receiving and transmitting directions are independent without interfering each other. The CE1 adopts the differential transmission mode, which has a stronger ability of resisting common-mode interference and a transmission distance of 1 km. Because the clock is extracted from the line clock, an independent clock line is not required. The CE1 line transmits the baseband signal, generally HDB3 (High Density Bipolar 3) codes or AMI. Both the preceding two codes are ternary return to zero codes.

Table 6-7 Configure the CE1 line coding

Step	Command	Description
Enter the CE1 controller configuration mode	**controller e1** *slot/ unit*	-
Configure the CE1 interface line coding	**linecode** { **ami** | **hdb3** }	Mandatory By default, the interface line coding is HDB3 coding.

Configure CE1 Looping Mode

Different looping modes are used to diagnose the line status. The local loop is used to diagnose whether exceptions occur to the local device for receiving and transmitting data. The remote loop is used to diagnose whether exceptions occur to the remote device for receiving and transmitting data.

Table 6-8 Configure the CE1 looping mode

Step	Command	Description
Enter the CE1 controller configuration mode	**controller e1** *slot unit*	-
Configure the interface looping mode	**loopback** { **local** | **remote** }	Mandatory By default, the looping mode for the CE1 interface is not configured.

Note:

- When configuring the interface looping, the interface transmit clock source must be configured as the internal clock.

6.2.3. CE1 Interface Monitoring and Maintaining

Table 6-9 The CE1 interface monitoring and maintaining

Command	Description
clear interface *interface-name*	Clear related statistics of the CE1 interface interface-name
show controllers e1 *slot/ unit*	Display related information of the CE1 controller
show interface *interface-name*	Display all configuration parameters and current running status information of the CE1 interface *interface-name*
show running-config	View the configuration of the CE1 interface

6.3. Typical Configuration Example of CE1 Interface

6.3.1. Configure CE1 Unframed Mode

Network Requirements

- Use a cable to connect the CE1 interface of Device1 and Device2. The CE1 interface is configured as the unframed mode by default. The interface encapsulation type is HDLC to enable the intercommunication between Device1 and Device2.

Network Topology

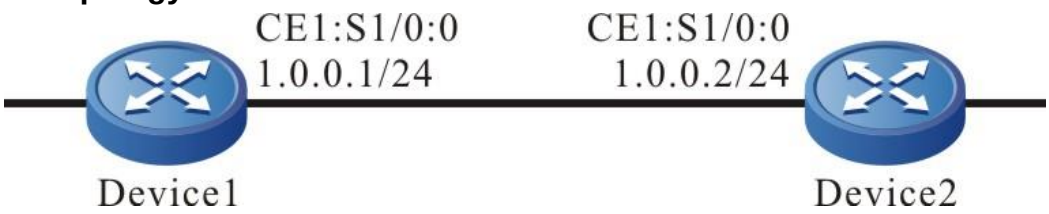

Figure 6–1 Networking of the CE1 unframed mode

Configuration Steps

Step 1: Configure the clock mode for the CE1 controller. Device1 is configured with an internal clock and Device2 in configured with an external clock. The external clock is the default setting, which does not need to be configured manually.

#Configure the CE1 interface of Device1.

```
Device1#configure terminal
Device1(config)#controller e1 1/0
Device1(config-controller)#clock source internal
```

#Configure the CE1 interface of Device2.

```
Device2#configure terminal
Device2(config)#controller e1 1/0
```

Step 2: Configure the unframed mode in the CE1 controller and the interface serial1/0:0 is automatically generated.

#Configure the CE1 interface of Device1.

```
Device1(config-controller)#unframed
Device1(config-controller)#exit
```

#Configure the CE1 interface of Device2.

```
Device2(config-controller)#unframed
Device2(config-controller)#exit
```

Step 3: Configure the IP addresses for all interfaces.

#Configure the IP address for serial1/0:0 created in Step 2 on Device1.

```
Device1(config)#interface serial 1/0:0
Device1(config-if-serial1/0:0)#ip address  1.0.0.1 255.255.255.0
Device1(config-if-serial1/0:0)#exit
Device1(config)#exit
```

Configure the IP address for serial1/0:0 created in Step 2 on Device2.

```
Device2(config)#interface serial 1/0:0
Device2(config-if-serial1/0:0)#ip address  1.0.0.2 255.255.255.0
```

```
Device2(config-if-serial1/0:0)#exit
Device2(config)#exit
```

Step 4: Check the result.

#View the status of serial1/0:0 on Device1.

```
Device1#show interface serial 1/0:0
serial1/0:0:
    line protocol is up
    Flags: (0x80080f1) POINT-TO-POINT MULTICAST RUNNING
    Type: PPP
    Internet address: 1.0.0.1/24
    Destination Internet address: 1.0.0.2
    Metric: 0, MTU: 1500, BW: 2048 Kbps, DLY: 20000 usec, VRF: global
    Reliability 255/255, Txload 1/255, Rxload 1/255
    Last clearing of "show interface" counters is 0 hour 0 minute 0 second ago
    input rate 0 bit/sec, 0 packet/sec, bandwidth utilization 0.00%
    output rate 0 bit/sec, 0 packet/sec, bandwidth utilization 0.00%
    0 packets received; 0 packets sent
    0 bytes received; 0 bytes sent
    0 multicast packets received
    0 multicast packets sent
    0 input errors; 0 output errors
    0 collisions; 0 dropped
     encap-type: simply PPP
     LCP:OPENED
     IPCP:OPENED   NDSPCP:INITIAL
       rxFrames 0, rxChars 0
       txFrames 0, txChars 0
       rxNoOctet 0, rxAbtErrs 0, rxCrcErrs 0
       rxOverrun 0, rxLenErrs 0, txUnderrun 0
       DCD=up
       rate=2048000 bps
```

Ping the IP address of the peer interface serial1/0 on Device1.

```
Device1#ping 1.0.0.2


Press key (ctrl + shift + 6) interrupt it.
```

```
Sending 5, 76-byte ICMP Echos to 1.0.0.2 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

Note:

- In the CE1 unframed mode, the ":" contained in the generated interface name followed by number 0.
- The encapsulation type of the CE1 interface is PPP by default. Therefore, the encapsulation type does not need to be configured for the interfaces. Run the **show interface** command, it can be observed that **Type** is set to *PPP*. If other WAN protocols need to be configured, refer to WAN protocol-related documentation.

6.3.2. Configure CE1 Framing Mode

Network Requirements

- Use a cable to connect the CE1 interface of Device1 and Device2. The CE1 interface is configured as the framing mode. The interface encapsulation type is PPP to enable the intercommunication between Device1 and Device2.

Network Topology

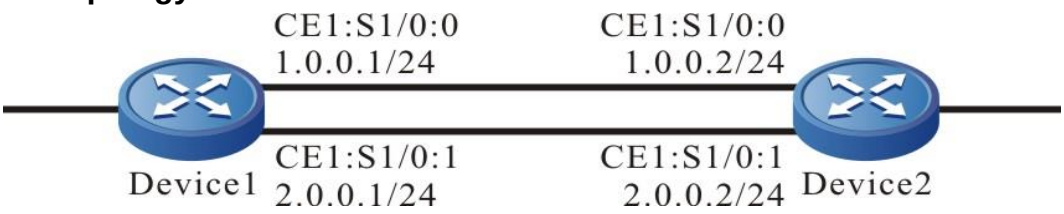

Figure 6–2 Networking of configuring the CE1 framing mode

Configuration Steps

Step 1: Configure the framing mode for the CE1 controller. Channel 0 uses timeslots form 0 to 10 and channel 1 uses timeslots from 11 to 20. serial1/0:0 and serial1/0:1 are automatically generated.

#Configure the CE1 interface of Device1.

```
Device1#configure terminal
Device1(config)#controller e1 1/0
Device1(config-controller)#channel-group 0 timeslots  1-10
Device1(config-controller)#channel-group 1 timeslots  11-20
```

#Configure the CE1 interface of Device2.

```
Device2#configure terminal
Device2(config)#controller  e1 1/0
Device2(config-controller)#channel-group 0 timeslots 1-10
Device2(config-controller)#channel-group 1 timeslots 11-20
Device2(config-controller)#exit
```

Step 2: Configure the clock mode for the CE1 controller. Device1 is configured with an internal clock and Device2 in configured with an external clock. The external clock is the default setting, which does not need to be configured manually.

#Configure the CE1 interface of Device1.

```
Device1(config-controller)#clock source internal
Device1(config-controller)#exit
```

Step 3: Configure the IP addresses for all interfaces.

#Configure the IP addresses for serial1/0:0 and serial1/0:1 created in Step 2 on Device1.

```
Device1(config)#interface serial 1/0:0
Device1(config-if-serial1/0:0)#ip address 1.0.0.1 255.255.255.0
Device1(config-if-serial1/0:0)#exit
Device1(config)#interface serial 1/0:1
Device1(config-if-serial1/0:1)#ip address  2.0.0.1 255.255.255.0
Device1(config-if-serial1/0:0)#exit
Device1(config)#exit
```

#Configure the IP addresses for serial1/0:0 and serial1/0:1 created in Step 2 on Device2.

```
Device2(config)#interface serial 1/0:0
Device2(config-if-serial1/0:0)#ip address 1.0.0.2 255.255.255.0
Device2(config-if-serial1/0:0)#exit
Device2(config)#interface serial 1/0:1
Device2(config-if-serial1/0:1)#ip address 2.0.0.2 255.255.255.0
Device2(config-if-serial1/0:1)#exit
Device2(config)#exit
```

Step 4: Check the result.

#View the status of serial1/0:0 and serialer1/0:1 on Device1.

```
Device1#show interface serial 1/0:0
serial1/0:0:
    line protocol is up
    Flags: (0x80080f1) POINT-TO-POINT MULTICAST RUNNING
    Type: PPP
    Internet address: 1.0.0.1/24
    Destination Internet address: 1.0.0.2
    Metric: 0, MTU: 1500, BW: 640 Kbps, DLY: 20000 usec, VRF: global
    Reliability 255/255, Txload 1/255, Rxload 1/255
```

```
    Last clearing of "show interface" counters is 0 hour 0 minute 2 seconds ago
    input rate 0 bit/sec, 0 packet/sec, bandwidth utilization 0.00%
    output rate 0 bit/sec, 0 packet/sec, bandwidth utilization 0.00%
    1 packets received; 1 packets sent
    12 bytes received; 12 bytes sent
    0 multicast packets received
    0 multicast packets sent
    0 input errors; 0 output errors
    0 collisions; 0 dropped
     encap-type: simply PPP
     LCP:OPENED
     IPCP:OPENED   NDSPCP:INITIAL
       rxFrames 1, rxChars 14
       txFrames 1, txChars 14
       rxNoOctet 0, rxAbtErrs 0, rxCrcErrs 0
       rxOverrun 0, rxLenErrs 0, txUnderrun 0
       DCD=up
       rate=640000 bps

Device1#show interface serial 1/0:1
Serial1/0:1:
    line protocol is up
    Flags: (0x80080f1) POINT-TO-POINT MULTICAST RUNNING
    Type: PPP
    Internet address: 2.0.0.1/24
    Destination Internet address: 2.0.0.2
    Metric: 0, MTU: 1500, BW: 640 Kbps, DLY: 20000 usec, VRF: global
    Reliability 255/255, Txload 1/255, Rxload 1/255
    Last clearing of "show interface" counters is 0 hour 0 minute 2 seconds ago
    input rate 0 bit/sec, 0 packet/sec, bandwidth utilization 0.00%
    output rate 0 bit/sec, 0 packet/sec, bandwidth utilization 0.00%
    1 packets received; 1 packets sent
    12 bytes received; 12 bytes sent
    0 multicast packets received
    0 multicast packets sent
    0 input errors; 0 output errors
    0 collisions; 0 dropped
```

```
encap-type: simply PPP
LCP:OPENED
IPCP:OPENED   NDSPCP:INITIAL
 rxFrames 1, rxChars 14
 txFrames 1, txChars 14
 rxNoOctet 0, rxAbtErrs 0, rxCrcErrs 0
 rxOverrun 0, rxLenErrs 0, txUnderrun 0
 DCD=up
 rate=640000 bps
```

#On Device1, ping the address of the peer interface serial 1/0:0 and serial 1/0:1, and the ping can be connected.

```
Device1#ping 1.0.0.2


Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 1.0.0.2 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.

Device1#ping 2.0.0.2


Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 2.0.0.2 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

Note:

- serial1/0:0 and serial1/0:1 in the network topology are two logical interfaces on a physical interface. Because the two interfaces communicate independently, two solid lines in the topology indicates two logical channels, which is a physical channel actually.
- When the CE1 interface is configured as the framing mode, timeslots used by both ends must be the same. For example, in the preceding case, Device 1 uses timeslots from 1 to 10 and timeslots from 11 to 20 and Device 2 must also use the timeslots from 1 to 10 and timeslots from 11 to 20. Otherwise, the port cannot be up.
- In the CE1 unframed mode, the ":" contained in the interface name indicates the channel number.
- The encapsulation type of the CE1 interface is PPP by default. Therefore, the encapsulation type does not need to be configured for the interfaces. Run the **show interface** command, it can be observed that **Type** is set to *PPP*. If other WAN protocols need to be configured, refer to WAN protocol-related documentation.

7. POS INTERFACE

7.1. Overview

SONET (Synchronous Optical Network) is the synchronous transmission machinism defined by ANSI, one globalized standard transmission protocol, and adopts the optical transmission.

SDH (Synchronous Digital Hierarchy) defined by CCIT adopts the synchronous multiplexing mode and flexible mapping structure, and can directly add/drop the low-speed tributary signal from the SDH signal, but does not need to use lots of multiplexing/demultiplexing devices, so as to reduce the signal loss and device investment.

POS (Packet Over SONET/SDH) is one technology applied in the MAN and WAN. It supports grouping data, such as support IP data grouping. POS directly maps the packet with variable length to the SDH/ SONET synchronous load, uses the SDH/SONET physical-layer transmission standard, and provides one high-speed, reliable, and point-to-point data connection. The POS interface can use the PPP and HDLC protocol at the data link layer and uses the IP protocol at the network layer. For different devices, the interface transmission rates may be different. For example, STM-1, STM-4, each level of rate is the four multiples of the lower level.

7.2. POS Function Configuration

Table 7-1 POS function configuration list

Configuration tasks	
Configure the basic functions of the POS interface	Configure the transmit clock source of the POS interface
	Configure the POS interface loopback
	Configure the payload scramble of the POS interface
Configure the other features of the POS interface	Configure the flag bytes in the SDH frame of the POS interface
	Configure the delay of the POS interface replying the line or channel event
	Configure the line error code alarm threshold of the POS interface
	Configure the data frame CRC check mode of the POS interface
	Configure the line frame format of the POS interface

Configuration tasks	
	Configure the J0 and J1 track flag transmit mode of the POS interface
	Configure the J0 and J1 track character string content of the POS interface

7.2.1. Configure the Basic Functions of the POS Interface

Network Condition

None

Configure the Transmit Clock Source of the POS Interface

During the data transmission, it is necessary to ensure the frame synchronous and clock synchronous. If the clock is not synchronous, it may cause packet loss, so it is necessary to unify the clock to ensure the clock synchronous during the transmission.

The clock adopted by the POS transmit port usually adopt two modes:

Internal clock: The oscillator in the card generates the transmit clock;

External clock:Take the clock extracted by the receiving port from the line as the transmit clock.

Table 7–2 Configure the transmit clock source of the POS interface

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the transmit clock source	**clock source** { **internal** | **line** }	Mandatory By default, the transmit clock of the POS interface is the line clock.

Configure POS Interface Loopback

When diagnosing the line status, use various loops. The local loop is used to diagranose whether the data receiving and sending of the device are normal. The remote loop is used to diagnose whether the data receiving and sending of the remote device are normal.

Table 7-3 Configure the POS interface loopback

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the interface loopback	**loopback** { **local** | **remote** }	Mandatory By default, the POS interface does not set loopback.

Note:

- When configuring the POS loopback mode as the local loopback, you should configure the transmit clock source as the internal clock.

Configure Payload Scramble of POS Interface

To make the receiving end extract the clock from the line effectively, SDH performs the X^7+X^6+1 scramble for the data in the whole STM-1 frame in the multiplexing segment. Meanwhile, in the channel (VC4), you also can set whether to perform the $X^{43}+1$ scramble for the payload in the container. The command is used to enable or disable the payload scramble.

Table 7-4 Configure the payload scramble of the POS interface

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the interface to enable the payload scramble	**pos scramble-atm**	Mandatory By default, the interface enables the payload scramble.

7.2.2. Configure Other Features of the POS Interface

Network Condition

None

Configure the Flag Byte in the SDH Frame of the POS Interface

The layers in the SDH are all set with different flags, used to indicate various information. On the POS interface, you can use the command to set the flags.

Table 7-5 Configure the flag byte in the SDH frame of the POS interface

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the value of the frame flag byte	**pos flag** { **c2** / **j0** / **j1** } *flag-value*	Mandatory The default rules of the line flag of the c2 cost byte are as follows: HDLC is encapsulated (no matter whether to perform the payload scramble) as 0xCF; the PPP of the payload scamble is encapsulated as 0x16; do not encapsulate the payload scamble PPP as 0xCF. By default, the j0 transmit mode is single-byte mode and the default value of j0 is 0x01. By default, the j1 transmit mode is single-byte mode and the default value of j1 is 0x00.

Configure Response Line or Channel Event Delay of the POS Interface

The line status depends on the interface status. The change of the interface status is triggered by the line status event. When no event happens, the interface regards that the line connection is normal and the DCD signal on the interface is UP. After the event happens, the interface DCD will change to status to down without delay. You can use the command to set the interface response line or channel event delay.

Table 7-6 Configure the response line or channel event delay of the POS interface

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the delay of the response line or channel event	**pos delay trigger** { **line** / **path** } *time*	Mandatory By default, the delay of the response line or channel event is 0ms.

Configure the Line Error Code Alarm Threshold of the POS Interface

The configuration is to set the thresholds of the line error code SD and SF alarms.

Table 7-7 Configure the line error code alarm threshold of the POS interface

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the line error code alarm threshold	**pos threshold** { **sd-ber** | **sf-ber** } *threshold-number*	Mandatory By default, the SD threshold is 10^{-6}, the SF threshold is 10^{-3}.

Configure the Data Frame CRC Check Mode of the POS Interface

The protocols supported by POS are PPP and HDLC. After each data frame, you can adopt CRC to check the data frame. The command can be used to configure the data CRC check mode.

Table 7-8 Configure the data frame CRC check mode of the POS interface

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the CRC check mode of the data frame	**crc** { **32** | **16** | **none** }	Mandatory By default, the CRC check length of the POS interface is 32 bits(4bytes).

Configure the Line Frame Format of the POS Interface

There are two frame structures adopted by POS:

STM-N (N = 1, 4, 16.....) in the SDH system

OC-N (N = 3, 12, 48.....) in the SONET system

With the command, you can set the frame format of the line transmission.

Table 7-9 Configure the line frame format of the POS interface

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the line frame format	**pos framed** { **sonet** | **sdh** }	Mandatory By default, the frame format of the POS interface is SDH.

Configure the J0 and J1 Track Flag Transmit Mode of the POS Interface

In the SDH/SONET field cost and channel cost, the track flags are set. SDH/SONET defines that the track flag can be single-byte mode and multi-byte mode (16bytes/64bytes). By default, POS adopts the single-byte mode and its content can be set via the **pos flag** command. To configure the multi-byte mode, you can use the command.

Table 7-10 Configure the J0 and J1 track flag transmit mode of the POS interface

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the J0 and J1 track flag transmit mode	**overhead** { **j0** / **j1** } **length** { **16/64** | **1** }	By default, the J0 and J1 track flag transmit mode is the single-byte mode.

Configure J0 and J1 Track Character String Content of the POS Interface

In the SDH/SONET field cost and channel cost, the track flags are set. SDH/SONET defines that the track flag can be single-byte mode and multi-byte mode (16bytes/64bytes). If the track flag is the multi-byte mode, you can use the command to configure the character string content of the track flag

Table 7-11 Configure the J0 and J1 track character string content of the POS interface

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the J0 and J1 track flag transmit mode	**overhead** { **j0** / **j1** } **length** { **16/64** | **1** }	Mandatory By default, the J0 and J1 track flag transmit mode is the single-byte mode.
Configure the J0 and J1 track transmit, expect receiving character string content	**overhead** { **j0** / **j1** } { **transmit** / **expect** } *string*	Mandatory By default, the J0 and J1 track transmit, expect receiving character string content is null.

7.2.3. POS Monitoring and Maintaining

Table 7-12 POS monitoring and maintaining

Command	Description
show controller pos *slot / sub-slot / unit*	Display the internal information of the POS drive

7.3. POS Typical Configuration Example

7.3.1. Configure POS Interface

Network Requirements

- Device1 and Device2 can be interconnected via the POS interface directly.

Network Topology

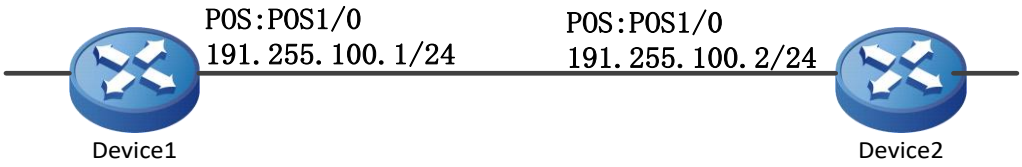

Figure 7-1Configure the POS interface

Configuration Steps

Step 1: Configure the line clock of the POS interface of Device1 as the internal clock, and the POS interface of Device2 adopts the default line clock.

Configure Device1.

```
Device1#configure terminal
Device1(config)#interface pos1/0
Device1(config-if-pos1/0)#clock source internal
Device1(config-if-pos1/0)#exit
```

Step 2: Enter the POS interface of Device1 and Device2 to configure the IP address and adopt the default PPP link protocol.

Configure Device1.

```
Device1(config)#interface pos1/0
Device1(config-if-pos1/0)#ip address 191.255.100.1 255.255.255.0
Device1(config-if-pos1/0)#exit
Device1(config)#exit
```

Configure Device2.

```
Device2#configure terminal
Device2(config)#interface pos1/0
Device2(config-if-pos1/0)#ip address 191.255.100.2 255.255.255.0
```

```
Device2(config-if-pos1/0)#exit
Device2(config)#exit
```

Step 3: Check the result.

#View the POS interface status.

```
Device1#show interface pos 1/0
pos1/0:
    line protocol is up
    Flags: (0x80080f1) POINT-TO-POINT MULTICAST RUNNING
    Type: PPP
    Internet address: 191.255.100.1/24
    Destination Internet address: 191.255.100.2
    Metric: 0, MTU: 1500, BW: 155000 Kbps, DLY: 20000 usec, VRF: global
    Reliability 255/255, Txload 1/255, Rxload 1/255
    Last clearing of "show interface" counters is 0 hour 0 minute 0 second ago
    input rate 0 bit/sec, 0 packet/sec, bandwidth utilization 0.00%
    output rate 0 bit/sec, 0 packet/sec, bandwidth utilization 0.00%
    8 packets received; 0 packets sent
    688 bytes received; 0 bytes sent
    0 multicast packets received
    0 multicast packets sent
    0 input errors; 0 output errors
    0 collisions; 0 dropped
     encap-type: simply PPP
     LCP:OPENED
     IPCP:OPENED   NDSPCP:INITIAL
     rxFrames: 8, rxChars 688
     txFrames: 0, txChars 0
     rxNoOctet 0, rxAbtErrs 0, rxCrcErrs 0
     rxOverrun 0, rxLenErrs 0, txUnderrun 0
     DCD: UP
```

On the POS interface of Device1, you can see that the DCD and link protocol status are up.

#On Device1, ping the POS interface address of the peer Device2 to detect the connectivity.

```
Device1#ping  191.255.100.2

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 191.255.100.2 , timeout is 2 seconds:
!!!!!
```

```
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

You can ping the peer POS interface address, indciating that the configuration is correct and the communication can be performed.

Note:

- The POS interface can encapsulate the HDLC and PPP protocol. By default, the PPP protocol is encapsulated.
- If two POS interfaces can be connected via the SDH network of the carrier, both of the two POS interfaces adopt the default line clock.

8. 4G INTERFACE

8.1. 4G Overview

4G is short for 4th Generation. It is evolved from the third generation communication technology, that is, LTE (Long Term Evolution). The importing of various core technologies, such as OFDM (Orthogonal Frequency Division Multiplexing) and MIMO (Multiple Input Multiple Output), improves the communication efficiency and transmission rate in the LTE network. With the advantages of high bandwidth, high rate and low delay, LTE brings better data transmission service for the wireless communication. It will also bring more revolutionary change, such as VoLTE (Voice over LTE) and MBMS (Multimedia Broadcast Multicast Service).

LTE mainly has two mainstream network modes, that is, LTE-TDD and LTE-FDD. LTE-TDD mainly adopts the Time Division Multiplexing technology and the main advantage is that the uplink and downlink rate can be adjusted by configuring the uplink and downlink timeslot ratio. It has high utilization for the fragmental bands, applicable to the asymmetrical transmission services. The disadvantage is the poor immunity. LTE-FDD mainly adopts the Frequency Division Multiplexing technology. The uplink and downlink transmission adopts different bands to ensure the stability of the communication rate and strong immunity. The disadvantage is the low band utilization. In the 20M spectrum bandwidth, the LTE uplink and downlink theoretical rates are 50Mb/s, 100Mb/s respectively. With the updating of the LTE technology, the rate is also improved continuously.

With the evolution of the mobile communication technology, the network difference is gradually reduced, bringing more colorful services for the user.

8.1.1. 4G Application Scenario

The data communications in the 4G wireless network is available when the 4G communication modules, such as a USB adapter and 3G board card, are inserted into the device. If there is no 4G network or the 4G network coverage is not stable, the module can switch to 2G/3G network. The specific application scenario is shown in the following figure.

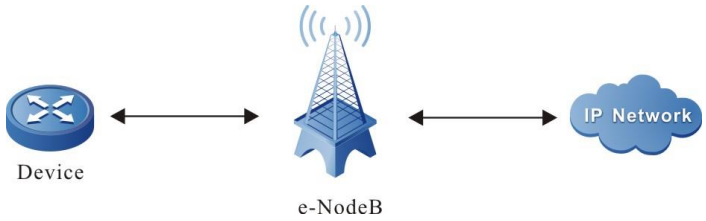

Figure 8-1 4G application scenario

Viewing from the preceding figure, the device achieves the wireless communication with the operator base station via the 4G communication modules and achieves data interaction with the WAN finally via the operator. Different 4G communication modules and different SIM cards determine different operators and different network modes. However, viewing from the overall application scenario, the data communications methods differ slightly.

8.2. 4G Function Configuration

Table 8-1 4G configuration list

Configuration Task	
Configure the 4G dialing access point	Configure the APN dialing access point
Configure the 4G dialing parameters	Configure the user name and password
	Configure the authentication type
Configure the SIM card safety function	Enable the PIN code function
	Authenticate the PIN code manually
	Authenticate the PIN code automatically
	Modify the PIN code
	Unblock the PIN code
	Configure IMSI binding function
Select the network mode	Select the forced mode
	Select the auto mode
Configure the multi-account dialing function	Configure the multi-account dialing function
Configure the waiting timeout of the dialing connection	Configure the time of waiting for the dialing connection
Configure 4G to switch to 3G dynamically	Configure 4G to switch to 3G dynamically

Configuration Task	
Configure system id to be bound with username	Configure system id to be bound with username

8.2.1. Configure 4G Dialing Access Point

The APN access point name is provided by the carrier. During dialing, the carrier determines the accessed server and sets up the data connection by resolving the access point name.

Configuration Condition

The carrier needs to support the APN access function.

Configure Dialing Access Point

Configure the dialing access point according to the dialing requirement of the carrier, mainly setting the access server name.

Table 8-2 Configure the dialing access point

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the 4G interface mode	**interface fastcellular** *interface-name*	-
Configure the 4G dialing access point	**dialer config apn** *apn-name*	Optional By default, *apn-name* is CMNET.

8.2.2. Configure 4G Dialing Parameters

The carrier determines the access server, authenticates and sets up the connection by resolving the user name and password.

The authentication type configuration of the 4G interface needs to be consistent with that of the server.

Configuration Condition

The carrier needs to support the access function via the user name and password.

Configure Dialing User Name and Password

Configure the user name and password according to the dialing requirement of the carrier.

Table 8-3 Configure the dialing user name and password

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the 4G interface mode	**interface fastcellular** *interface-name*	-
Configure the 4G dialing user name and password	**dialer config username** *user-name* password *pwd*	Optional By default, *user-name* is a and *pwd* is a.

Configure Dialing Authentication Type

It needs to be consistent with the authentication type of the server. If the server does not need the authentication type, do not affect the dialing process after 4G interface configuration.

Table 8-4 Configure dialing authentication type

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the 4G interface mode	**interface fastcellular** *interface-name*	-
Configure the 4G dialing authentication type	**dialer config authtype {chap | pap | pap_chap}**	Optional By default, the authentication type is CHAP.

8.2.3. Configure 4G Dialing IP Type

Configure the IP type as IPv4 or IPv6. After dialing successfully, you can get the corresponding IP address.

Configuration Condition

The operator needs to support the IPv6 network.

Configure IP Type

Table 8-5 Configure the IP type used by dialing

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the 4G interface mode	**interface fastcellular** *interface-name*	-
Configure the IP type of the 4G dialing	**dialer config ipfamily {ipv4 | ipv6 | ipv4v6}**	Optional By default, it is IPv4 type.

8.2.4. Configure SIM Card Safety Function

SIM card safety function mainly provides PIN code protection and IMSI binding, protecting the right of using the 4G module.

The SIM (subscriber identity module), also called the subscriber identity card, records the user identity data and information.

PIN (Personal Identification Number) code is the personal identity password of the SIM card. The PIN code is set to 1234 or 0000 by default. If the PIN code is enabled, a four-digit PIN code must be entered when powering on. The PIN code can be changed, which is used to protect your own SIM card from being used by others.

PUK (PIN Unlocking Key) is the unblocking code of the PIN code. When the SIM card is locked caused by entering wrong PIN code, you can unblock it using the PUK code.

A unique IMSI (International Mobile Subscriber Identification Number) is allocated to every SIM card. This code is valid at any places including the roaming area on the network. The IMSI binding function binds the unique identifier of the SIM card with the slot number.

Warning:

- When the PIN code is wrongly entered for three consecutive times, the SIM card will be locked. At this time, you can use the PUK code to unblock it. However, if the PUK code is wrongly entered for ten consecutive times, the SIM card will be locked permanently.

Configuration Condition

None

Enable PIN Code

The right of using the SIM card is protected by enabling the PIN code. You must enter the correct PIN code to use the SIM card.

Table 8-6 Enable the PIN code

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the 4G interface mode	**interface fastcellular** *interface-name*	-
Configure the 4G PIN code protect	**pin-code pin-enable** *pin code*	Mandatory By default, do not enable the PIN code protect function.

Authenticate PIN Code Manually

PIN code manual authentication means PIN code authentication by entering the command manually every time.

Table 8-7 Authenticate the PIN code manually

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the 4G interface mode	**interface fastcellular** *interface-name*	-
Configure the 4G PIN code authentication	**pin-code pin-check** *pin code*	Mandatory By default, do not configure the manual authentication PIN code.

Authenticate PIN Code Automatically

In the PIN code automatic authentication mode, the PIN code is verified by presetting the PIN code. The user only needs to configure the PIN code for one time and the device will use the configured PIN code for authentication.

Table 8-8 Authenticate the PIN code automatically

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the 4G interface mode	**interface fastcellular** *interface-name*	-
Configure the 4G auto authentication PIN code function	**pin-code pin-check auto** *pin code*	Mandatory By default, do not configure the auto authentication PIN code.

Change PIN Code

Changing the PIN code allows the new PIN code set by the user. After the PIN code is changed, the new PIN code is used for authentication.

Table 8-9 Change the PIN code

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the 4G interface mode	**interface fastcellular** *interface-name*	-
Change the 4G PIN code	**pin-code pin-change** *pin code new pin code*	Mandatory By default, do not change the PIN code.

Unblock PIN Code

If the SIM card is locked by entering the wrong PIN code for three consecutive times, the user can enter the PUK code to unblock it and set new PIN code.

Table 8-10 Unblock the PIN code

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the 4G interface mode	**interface fastcellular** *interface-name*	-
Unlock and set the new PIN code via the PUK code	**pin-code puk-check** *puk code pin code*	Mandatory By default, do not configure the unblock PIN code

Configure IMSI Binding Function

The user can specify the SIM card to the 4G interface in the fixed slot by the IMSI binding function, and the 4G interfaces in other slots cannot use the SIM card. This function is only available for this device.

Table 8-11 Configure the IMSI binding function

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the 4G interface mode	**interface fastcellular** *interface-name*	-
Perform the IMSI binding for the specified 4G interface SIM card	**dialer condition imsi-band** { **current-imsi** | *imsi* }	Mandatory By default, do not enable the IMSI binding function

8.2.5. Select Network Mode

The optional network configuration modes provided by the device include auto mode, LTE mode, WCDMA mode, TD-SCDMAmode, and CDMA mode. The auto mode indicates that the module automatically adapts to the current network and performs the network switching according to the preferred mode automatically. The other mode is the forced mode, mainly used when the 3G/4G signal coverage is stable in the customer scenario and the user has the specified requirement for the rate. Usually, the auto mode is recommended.

Configuration Condition

None

Select Network Mode

The user can configure as desired.

Table 8-12Select network mode

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the 4G interface mode	**interface fastcellular** *interface-name*	-
Configure the network mode	**dialer condition mode { auto | lte | wcdma | tdscdma | cdma}**	Optional By default, enable the auto mode.

8.2.6. Configure Multi-account Dialing Function

The multi-account dialing function is mainly used: In the auto dialing mode, when the default dialing configuration in the 4G interface fails to dial in the set time, automatically switch to multi-account list. The carrier needs to support the function.

Configuration Condition

None

Configure Multi-account List

To create the multi-account list, configure the desired dialing parameter.

Table 8-13 Configure the multi-account list

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the sub list configuration mode	**multi-dialer** *multi-list-name*	*multi-list-name*: Up to 10 lists can be configured. The length of the list name cannot exceed 20.

Step	Command	Description
Enter the sub item configuration mode	**config-list** *list-id*	*list-id*: optional value 1-2
Configure the dialing parameter sub item	**apn** *apn-name* **username** *user-name* **password** *pwd* **authtype {chap | pap | ap_chap}**	Optional By default, do not configure.

Configure 4G Interface to Associate with Multi-account List

The default dialing configuration in the interface is still the preferred dialing configuration. After configuring the 4G interface to associate with the multi-account list, the created multi-account list can take effect.

Table 8-14 Configure the 4G interface to associate with the multi-account list

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the 4G interface mode	**interface fastcellular** *interface-name*	-
Configure the 4G interface to associate with the multi-account list	**multi-dialer** *multi-list-name*	Optional By default, do not configure the 4G interface to associate with the multi-account list

8.2.7. Configure the Timeout of Waiting for Dialing Connection

The configuration depends on the factors, such as the quality of wireless communication links and the time used by the operator to allocate bandwidth resources. For example, when the link communication quality is poor, the operator is allocating the IP address for the 4G device end, and the device terminal is actively disconnecting the dial request because waiting for getting the IP address times out. In this case, the probability of the dialing success can be improved by reasonably adjusting the waiting timeout parameter.

Configuration Condition

None

Configure the Time of Waiting for Dialing Connection

The user configures it according to the actual situation.

Table 8-15 Configure the time of waiting for the dialing connection

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the 4G interface mode	**interface fastcellular** *interface-name*	-
Configure the time of waiting for the dialing connection	**dialer condition connect-time** *time*	Optional The unit of *time* is second, the value range is 10-90, and the default value is 30.

8.2.8. Configure Switching 4G to 3G Dynamically

4G is online for a long time, and as a result, lots of ins resources are occupied. The configuration can automatically switch to the 3G mode during idle or when the interface is shutdown, so as to release the resources.

Configuration Condition

None

Configure Switching 4G to 3G Dynamically

The user configures it according to the actual situation.

Table 8-16 Configure switching 4G to 3G dynamically

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the 4G interface mode	**interface fastcellular** *interface-name*	-
Configure switching 4G to 3G dynamically	**dialer condition disconnect { standby-cdma | standby-tdscdma | standby- wcdma [delay-time** *delay-time*] }	Mandatory By default, the function is disabled.

8.2.9. Configure system id to Be Bound with username

The configuration can bind the system id of the device with the dialing parameter **username**.

Configuration Condition

None

Configure system id to Be Bound with username

The user configures it according to the actual situation.

Table 8-17 Configure system id to be bound with username

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the 4G interface mode	**interface fastcellular** *interface-name*	-
Configure system id to be bound with username	**dialer condition sysid-band**	Mandatory By default, system id is not bound with username.

8.2.10. 4G Monitoring and Maintaining

Table 8-18 4G monitoring and maintaining

Command	Description
show fastcellular *interface-name* **{ phyinfo {all | hardware | network | profile | radio | security} | dialer condition }**	Display the 4G module hardware information, network information, and SIM card information of all interfaces, as well as the error statistics information of the dialing
show multi-list[*multi-list-name***]**	Display the association, dialing status and current configuration content of the current backup dialing configuration list and interface

8.3. Typical Configuration Example of 4G Network

8.3.1. 4G Dialing-on-Demand Typical Configuration Example

Network Requirements

- Device1 is connected to the specified private network via the dialing-on-demand mode.
- Device1 serves as the node device, the operator device serves as LAC, and Device2 serves as LNS. Set up the L2TP tunnel between LAC and Device2.

Network Topology

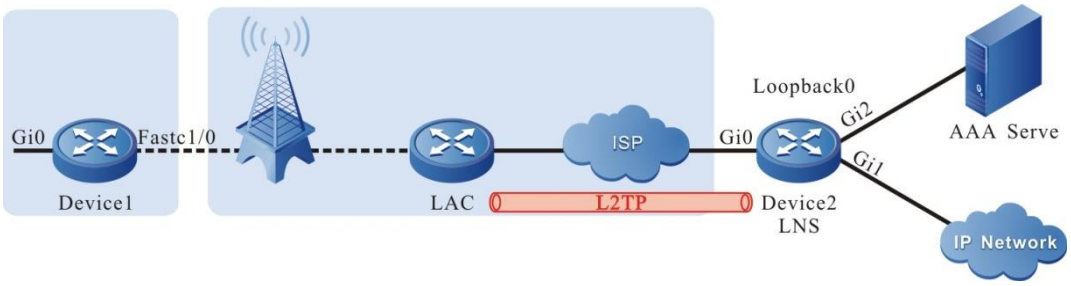

Figure 8-2 4G dialing-on-demand configuration view

Device	Interface	IP address	Device	Interface	IP address
Device1	Gi0	172.16.2.1/24	Device2	Loopback0	64.19.245.250 /24
AAA		130.255.12.28/24		Gi0	125.71.215.223/24
				Gi1	26.1.1.1/24
				Gi2	130.255.100.29/24

Configuration Steps

Step 1: Configure the IP address and route of the interface (omitted).

Step 2: Configure the 4G interface.

#Configure the dialing user name and password of Device1 4G interface fastcellular1/0. Configure the interface to the dialing-on-demand mode, getting the IP address via DHCP.

```
Device1#configure terminal
Device1(config)#interface fastcellular1/0
Device1(config-if-fastcellular1/0)#dialer config username test@jsyh.vpdn.sc password 0 admin
Device1(config-if-fastcellular1/0)#dialer-group ip any
Device1(config-if-fastcellular1/0)#ip address dhcp
Device1(config-if-fastcellular1/0)#exit
```

Step 3: Configure the default route on Device1, and the egress interface is fastcellular1/0.

#Configure the default route of Device1.

```
Device1(config)#ip route 0.0.0.0 0.0.0.0 fastcellular1/0
```

Note:

- 4G private network can be connected via APN and domain name, which depends on the carrier. In the example, it is connected via the domain name mode.
- If configuring the **dialer mode auto** command to enable auto dialing on the 4G interface, do not need to trigger dialing via the data flow. If configuring the **dialer-group ip any** command to enable dialing on demand on the 4G interface, it is necessary to trigger dialing via the data flow. Select one of two dialing modes according to the actual situation.
- If configuring the **dialer-group ip access-list [name]/[number]** command on the 4G interface, you can specify the interested flow to trigger the 4G interface dialing.
- Configure the **dialer interval-time [*time*]** command on the 4G interface, and you can modify the interval of two dialings. By default, it is 10s, and it is suggested to use the default value.
- If configuring the **dialer idle-timeout 0** command on the 4G interface, you can set the 4G line not to time out forever. By default, the timeout time is 120s.
- If configuring the **ip dhcp router-option disable** command to disable the function of auto adding the default route via DHCP on the 4G interface, do not add the default route of the egress interface automatically after the 4G interface automatically dials successfully.
- If configuring the **ip address dhcp [A.B.C.D]** command on the 4G interface, you can specify the subnet mask length of the IP address got by the 4G interface.

Step 4: Configure AAA.

#Configure Device2.

Use Radius to authenticate, name the authentication list, authorization list as ppp, configure the Radius sercer address, authentication port, statistics port, and Radius server password.

```
Device2#configure terminal
Device2(config)#aaa new-model
Device2(config)#aaa authentication ppp ppp radius none
Device2(config)#aaa authorization network ppp radius
Device2(config)#radius-server host 130.255.12.28 auth-port 1812 acct-port 1813 priority 0 key 0 a
```

Step 5: Configure the L2TP tunnel.

#Configure Device2.

Configure the virtual template virtual-template 1.

```
Device2(config)#interface virtual-template 1
Device2(config-if-virtual-template1)#encapsulation ppp
Device2(config-if-virtual-template1)#ppp mtu adaptive proxy
Device2(config-if-virtual-template1)#ppp authentication chap ppp
Device2(config-if-virtual-template1)#ppp authorization ppp
Device2(config-if-virtual-template1)#ip unnumber loopback0
Device2(config-if-virtual-template1)#exit
```

Enable the VPDN function and configure the VPDN group.

```
Device2(config)#vpdn enable
Device2(config)#vpdn-group 1
Device2(config-vpdn)#accept-dialin
Device2(config-vpdn-acc-in)#protocol l2tp
Device2(config-vpdn-acc-in)#virtual-template 1
Device2(config-vpdn-acc-in)#exit
```

Configure only accepting the L2TP connection request of LAC with the host name GGSNCD01 (optional).

```
Device2(config-vpdn)#terminate-from hostname GGSNCD01
```

Configure the authentication password of the L2TP tunnel. The password should be the same as the L2TP password provided by the carrier.

```
Device2(config-vpdn)#l2tp tunnel password admin
```

Step 6: Check the result.

#On Device2, view the L2TP tunnel set with the LAC.

```
Device2#show vpdn detail
```

L2TP MaxTun 6000, MaxSes 6000:

tunnel free num: 5999

TUNNELS:

LocID LocName RemID RemName RemAddr Vpdn Port Sess State

78 Router 78 GGSNCD01 115.169.201.159 1 1701 1 ESTAB

session free num: 1999

SESSIONS:

LocID TunID RemID IfName User SysId Imsi/calling-noState

30 78 386 virtual-access2 test1@jsyh.vpdn.sc - 460110500000920 ESTAB

L2TP total Tunnel and Session Information. Tunnel 1 Session 1

#After dialing successfully, the 4G interface of Device1 can get the IP address and the protocol is UP.

Device1#show interface fastcellular 1/0

Fastcellular1/0:

line protocol is up

Flags: (0xc208063) BROADCAST MULTICAST ARP RUNNING

Type: ETHERNET_CSMACD

Internet address: 64.19.245.249/30

Broadcast address: 64.19.245.251

Metric: 0, MTU: 1500, BW: 100000 Kbps, DLY: 100 usec, VRF: global

Reliability 255/255, Txload 1/255, Rxload 1/255

Ethernet address is 001f.ceb8.d858

Last clearing of "show interface" counters never

input peak rate 596 bits/sec, 1 hour 58 minutes 8 seconds ago

output peak rate 715 bits/sec, 1 hour 58 minutes 8 seconds ago

5 minutes input rate 0 bit/sec, 0 packet/sec

5 minutes output rate 0 bit/sec, 0 packet/sec

618 packets received; 1807 packets sent

4 multicast packets received

29 multicast packets sent

0 input errors; 0 output errors

0 collisions; 0 dropped

Unknown protocol 0

Rate: auto Duplex: auto

rxframes 618, rx bytes 52160, rx arps 21

txframes 1807, tx bytes 308654, tx arps 25

```
rx errors 0, tx errors 0
```

#On Device1, ping the address of the virtual interface virtual-access2 on Device2, and view whether the ping can be connected.

```
Device1#ping 64.19.245.250

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 64.19.245.250 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 316/502/1066 ms.
```

Device1 can ping the address of the virtual interface virtual- access2 of Device2.

8.3.2. 4G VPDN Typical Configuration Example

Network Requirements

- Device1 is connected to the specified private network environment via the domain name.
- Device1 serves as the network site device, the carrier device serves as LAC, and Device2 serves as LNS. Set up the L2TP tunnel between LAC and Device2.
- Associate Track on the 4G interface of Device1, used to detect the link status between the site router and LNS.

Network Topology

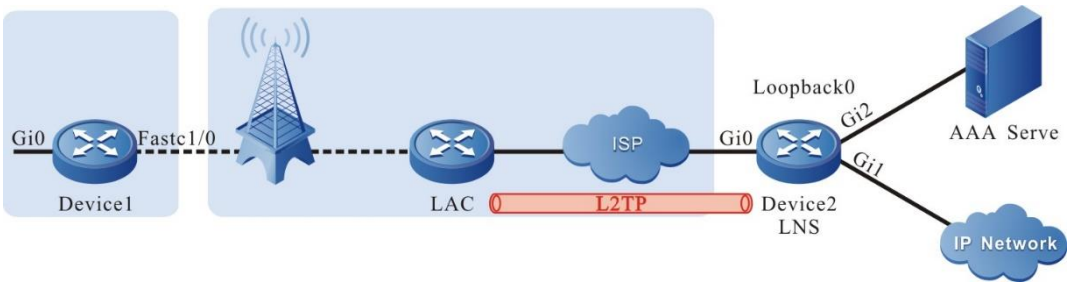

Figure 8-3 4G VPDN typical configuration view

Device	Interface	IP address	Device	Interface	IP address
Device1	Gi0	172.16.2.1/24	Device2	Loopback0	64.19.245.250 /24
AAA		130.255.12.28/24		Gi0	125.71.215.223/24
				Gi1	26.1.1.1/24
				Gi2	130.255.100.29/24

Configuration Steps

Step 1: Configure the IP address and route of the interface (omitted).

Step 2: Configure the 4G interface.

#Configure the dialing user name and password of Device1 4G interface fastcellular1/0. Configure the interface as the auto dialing mode and get IP address via DHCP.

```
Device1#configure terminal
Device1(config)#interface fastcellular1/0
Device1(config-if-fastcellular1/0)#dialer config username test@jsyh.vpdn.sc password 0 admin
Device1(config-if-fastcellular1/0)#dialer mode auto
Device1(config-if-fastcellular1/0)#ip address dhcp
Device1(config-if-fastcellular1/0)#exit
```

Note:

The 4G private network can be connected via the APN and domain name. The specific mode depends on the carrier. In the example, use the domain name mode to access.

Step 3: Configure AAA.

#Configure Device2.

Use Radius to authenticate. The authentication list and authorization list are named as ppp. Configure the address, authentication port, statistics port, and Radius server password of the Radius server.

```
Device2(config)#aaa new-model
Device2(config)#aaa authentication ppp ppp radius none
Device2(config)#aaa authorization network ppp radius
Device2(config)#radius-server host 130.255.12.28 auth-port 1812 acct-port 1813 priority 0 key 0 a
```

Step 4: Configure the L2TP tunnel.

#Configure Device2.

Configure the virtual template virtual-template 1.

```
Device2(config)#interface virtual-template 1
Device2(config-if-virtual-template1)#encapsulation ppp
Device2(config-if-virtual-template1)#ppp mtu adaptive proxy
Device2(config-if-virtual-template1)#ppp authentication chap ppp
Device2(config-if-virtual-template1)#ppp authorization ppp
Device2(config-if-virtual-template1)#ip unnumber loopback0
Device2(config-if-virtual-template1)#exit
```

Enable the VPDN function and configure the VPDN group.

```
Device2(config)#vpdn enable
Device2(config)#vpdn-group 1
```

```
Device2(config-vpdn)#accept-dialin
Device2(config-vpdn-acc-in)#protocol l2tp
Device2(config-vpdn-acc-in)#virtual-template 1
Device2(config-vpdn-acc-in)#exit
```

Configure only to accept the L2TP connection request of the LAC with hostname GGSNCD01 (optional).

```
Device2(config-vpdn)#terminate-from hostname GGSNCD01
```

Configure the L2TP tunnel authentication password. The password should be the same as the L2TP password provided by the carrier.

```
Device2(config-vpdn)#l2tp tunnel password admin
```

View the L2TP tunnel setup status on Device2.

```
Device2#show vpdn detail
L2TP MaxTun 6000, MaxSes 6000:
tunnel free num: 5999
TUNNELS:
LocID  LocName     RemID  RemName   RemAddr        Vpdn     Port   Sess   State
78     Router      78     GGSNCD01  115.169.201.159  1      1701   1      ESTAB
session free num: 1999
SESSIONS:
LocID  TunID  RemID  IfName         User          SysId  Imsi/calling-noState
30     78     386    virtual-access2  test1@jsyh.vpdn.sc  -  460110500000920
ESTAB

L2TP total Tunnel and Session Information. Tunnel 1  Session 1
```

After dialing successfully, the 4G interface of Device1 can get the IP address and the protocol is up.

```
Device1#show  interface fastcellular 1/0
Fastcellular1/0:
    line protocol is up
    Flags: (0xc208063) BROADCAST MULTICAST ARP RUNNING
    Type: ETHERNET_CSMACD
    Internet address: 64.19.245.249/30
    Broadcast address: 64.19.245.251
    Metric: 0, MTU: 1500, BW: 100000 Kbps, DLY: 100 usec, VRF: global
    Reliability 255/255, Txload 1/255, Rxload 1/255
    Ethernet address is 001f.ceb8.d858
    Last clearing of "show interface" counters never
```

```
input peak rate 596 bits/sec,  1 hour 58 minutes 8 seconds ago
output peak rate 715 bits/sec,  1 hour 58 minutes 8 seconds ago
5 minutes input rate 0 bit/sec, 0 packet/sec
5 minutes output rate 0 bit/sec, 0 packet/sec
618 packets received; 1807 packets sent
4 multicast packets received
29 multicast packets sent
0 input errors; 0 output errors
0 collisions; 0 dropped
Unknown protocol 0
Rate:  auto Duplex:  auto
rxframes 618, rx bytes 52160, rx arps 21
txframes 1807, tx bytes 308654, tx arps 25
rx errors 0, tx errors 0
```

On Device1, ping the address of the virtual interface virtual-access2 on Device2 and view whether the ping can succeed.

```
Device1#ping 64.19.245.250

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 64.19.245.250 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 316/502/1066 ms.
```

Device1 can ping the address of the virtual interface virtual- access2 of Device 2.

Step 5: Configure the 4G interface to associate with Track.

#On Device1, configure the ICMP-echo entity to detect the network connectivity from Device1 to Device2 and add the entity to the entity group. Schedule the RTP group 1.

```
Device1(config)#rtr enable
Device1(config)#rtr 1 icmpecho
Device1(config-rtr-icmpecho)#set 64.19.245.250 5 70 2 12
Device1(config-rtr-icmpecho)#exit
Device1(config)#rtr group 1
Device1(config-rtr-group)#member 1
Device1(config-rtr-group)#exit
Device1(config)#rtr schedule 1 group 1 start now ageout 100 life forever
```

Create Track to associate with SLA.

```
Device1(config)#track 1
```

```
Device1(config-track)#rtr 1
Device1(config-track)#exit
```

Associate Track1 on the 4G interface.

```
Device1(config)# interface  fastcellular1/0
Device1(config-if-fastcellular1/0)#dialer track id 1
```

Note:

- For the SLA configuration, refer to the SLA chapter of the configuration manual.

Step 6: Check the result.

When the link status between Device1 and Device2 is normal, view that the track status is up on Device1.

```
Device1#show  track object
track 1
status = up
entnum = 1
logic operator AND
        Object Type     Status  Refcnt                  instruction
------------------------  --------  ------  ---------------------------------
------
             rtr       up     1  rtr 1
   ------------------------------------------------------------------------
-----------
           module  priority  caller
------------------------- -------- ------
          NDISDDR      20  0xd56b88
   ------------------------------------------------------------------------
-----------
```

#On Device1, view that the 4G interface status is UP and can get the IP address.

```
Device1#show  interface fastcellular 1/0
Fastcellular1/0:
   line protocol is up
   Flags: (0xc208063) BROADCAST MULTICAST ARP RUNNING
   Type: ETHERNET_CSMACD
   Internet address: 64.19.245.249/30
   Broadcast address: 64.19.245.251
   Metric: 0, MTU: 1500, BW: 100000 Kbps, DLY: 100 usec, VRF: global
```

```
Reliability 255/255, Txload 1/255, Rxload 1/255
Ethernet address is 001f.ceb8.d858
Last clearing of "show interface" counters never
input peak rate 596 bits/sec,  1 hour 58 minutes 8 seconds ago
output peak rate 715 bits/sec,  1 hour 58 minutes 8 seconds ago
5 minutes input rate 0 bit/sec, 0 packet/sec
5 minutes output rate 0 bit/sec, 0 packet/sec
618 packets received; 1807 packets sent
4 multicast packets received
29 multicast packets sent
0 input errors; 0 output errors
0 collisions; 0 dropped
Unknown protocol 0
Rate:  auto Duplex:  auto
rxframes 618, rx bytes 52160, rx arps 21
txframes 1807, tx bytes 308654, tx arps 25
rx errors 0, tx errors 0
```

When the link status between Device1 and Device2 is not normal, view that the track status is down on Device1. Here, make the 4G interface down and re-dial.

8.3.3. 4G IP APN Typical Configuration Example

Network Requirements

- Device1 is connected to the specified private network environment via the APN.
- 4G router Device1 and Device2 use the IPSEC extended authentication to set up the IPsec tunnel, protecting the data between the PC1 network and Network-Center.
- IPsec proposed security protocol adopts ESP, IKE proposal and IPsec proposal encryption algorithm adopts 3DES; authentication algorithm adopts SHA1.
- Set up BFD echo multi-hop session between device1 and device2; detect the 4G link status between device1 and device2.

Network Topology

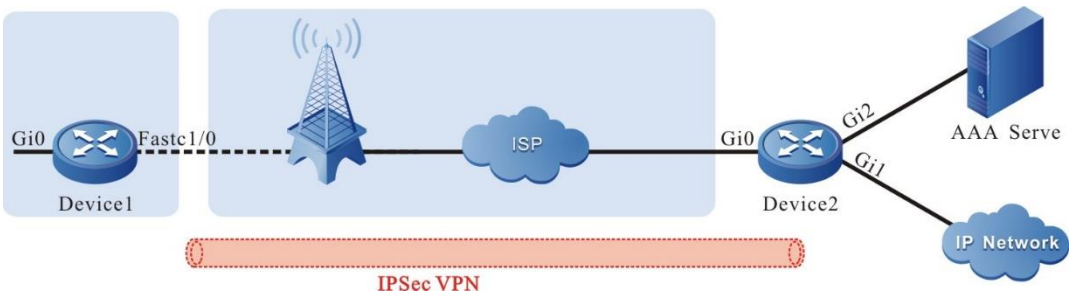

Figure 8-4 4G IP APN typical networking

Device	Interface	IP address	Device	Interface	IP address
Device1	Gi0	172.16.2.1/24	AAA Server		130.255.12.28/24
Device2	Gi0	125.71.215.223/24			
	Gi1	26.1.1.1/24			
	Gi2	130.255.100.29/24			

Configuration Steps

Step 1: Configure the IP address and route of the interface (omitted).

Step 2: Configure the 4G interface.

#Configure Device1; configure 4G interface fastcellular1/0 as auto dialing mode and get IP address via DHCP automatically.

```
Device1#configure terminal
Device1(config)#interface  fastcellular1/0
Device1(config-if-fastcellular1/0)#dialer mode auto
Device1(config-if-fastcellular1/0)#ip address dhcp
Device1(config-if-fastcellular1/0)#dialer config apn cdmptx.sc
Device1(config-if-fastcellular1/0)#exit
```

Note:

- The 4G private network can be connected via the APN and domain name. The specific mode depends on the carrier. In the example, use the APN mode to access.

Step 3: Configure AAA.

#Configure Device2; use Radius to authenticate; the authentication list and accounting list are named as 4g; configure the Radius server address, authentication port, statistics port, and Radius server password.

```
Device2#configure terminal
Device2(config)#aaa new-model
Device2(config)#aaa authentication xauth 4g radius
Device2(config)#aaa accounting network 4g wait-start radius
Device2(config)#radius-server host 130.255.12.28 auth-port 1812 acct-port 1813
priority 0 key 0 a
```

Step 4: Configure the IKE and IPsec proposal.

#Configure the IKE proposal ikepro on Device1, use the encryption algorithm 3DES and authentication algorithm SHA1; configure the IPsec proposal ippro, use ESP security protocol, use the encryption algorithm 3DES and authentication algorithm SHA1.

```
Device1(config)#crypto ike proposal ikepro
Device1(config-ike-prop)#encryption 3des
Device1(config-ike-prop)#exit
Device1(config)#crypto ipsec proposal ippro
Device1(config-ipsec-prop)#esp 3des sha1
Device1(config-ipsec-prop)#exit
```

#Configure the pre-share key on Device1 as admin and permit all peers to use the key.

```
Device1(config)#crypto ike key admin any
```

#Configure the IKE proposal ikepro on Device2, use the encryption algorithm 3DES and authentication algorithm SHA1; configure the IPsec proposal ippro, use the ESP security protocol, use the encryption algorithm 3DES and authentication algorithm SHA1.

```
Device2(config)#crypto ike proposal ikepro
Device2(config-ike-prop)#encryption 3des
Device2(config-ike-prop)#exit
Device2(config)#crypto ipsec proposal ippro
Device2(config-ipsec-prop)#esp 3des sha1
Device2(config-ipsec-prop)#exit
```

#Configure the pre-share key on Device2 as admin and permit all peers to use the key.

Step 5: Configure the IKE ID alias.

```
Device2(config)#crypto  ike key admin any
```

#Configure the IKE ID alias as 4g on Device2, apply the extended authentication list 4g, specify the extended authentication IMSI attribute and optional attribute, and apply the accounting list 4g.

```
Device2(config)#crypto ike id alias 4g
Device2(config)#authentication 4g authen_imsi optional
Device2(config)#accounting  4g
```

Step 6: Configure the IPsec tunnel.

#Configure the tunnel tun on Device1 to initiate the negotiation with the identity of the extended authentication client, use the 4G interface fastcellular1/0 as the local address of the tunnel, configure the peer address of the tunnel as 125.71.215.223, configure the authentication mode as the pre-share key authentication, IKE proposal uses ikepro, the IPsec proposal uses ippro, configure the extended authentication client user name as a and password as a, and enable auto initiating negotiation. On the AAA server, it is necessary to configure the IKE extended authentication user name, password, and IMSI information.

Note:

- The IMSI value of the AAA server is consistent with the IMSI value of the 4G interface.

```
Device1(config)#crypto tunnel tun
Device1(config-tunnel)#local interface fastcellular1/0
Device1(config-tunnel)#peer address 125.71.215.223
Device1(config-tunnel)#set authentication preshared
Device1(config-tunnel)#set ike proposal ikepro
Device1(config-tunnel)#set ipsec proposal ippro
Device1(config-tunnel)#set xauth-client user-name a password a
Device1(config-tunnel)#set auto-up
Device1(config-tunnel)#exit
```

#On Device2, configure the tunnel, use the address of the interface Gi0 125.71.215.223 as the local address of the tunnel, configure the peer address of the tunnel as any, the IKE proposal uses ikepro, the IPsec proposal uses ippro, and set the peer ID alias as 4g.

```
Device2(config)#crypto tunnel tun
Device2(config-tunnel)#local address 125.71.215.223
Device2(config-tunnel)#peer any
Device2(config-tunnel)#set ike proposal ikepro
Device2(config-tunnel)#set ipsec proposal ippro
Device2(config-tunnel)#set peer-id alias 4g
Device2(config-tunnel)#exit
```

Step 7: Configure the IPsec security policy.

#Configure Device1, configure the security policy policy1, protect the IP communication from network 172.16.2.0/24 to network 26.1.1.0/24, and associate the tunnel tun.

```
Device1(config)#crypto policy policy1
Device1(config-policy)#flow 172.16.2.0 255.255.255.0 26.1.1.0 255.255.255.0 ip tunnel tun
Device1(config-policy)#exit
```

#Configure Device2, configure the security policy policy1, protect the IP communication of any network, and associate the tunnel tun.

```
Device2(config)#crypto policy policy1
Device2(config-policy)#flow any any ip tunnel tunnel bypass
Device2(config-policy)#exit
```

Step 8: Configure BFD.

#Configure Device1, configure BFD on the 4G interface fastcellular1/0, the remote IP address is 125.71.215.223, and the local IP address of the BFD is got from the 4G interface dynamically.

```
Device1(config)#interface fastcellular1/0
Device1 (config-if-fastcellular1/0)#dialer bfd remote-ip 125.71.215.223
Device1 (config-if-fastcellular1/0)#exit
```

#Configure Device2, and enable BFD on gigabitethernet 0.

```
Device2(config)#interface gigabitethernet0
Device2(config-if-gigabitethernet0)#bfd echo multihop local-ip 125.71.215.223
Device2(config-if-gigabitethernet0)#exit
```

Step 9: Check the result.

#View the interface information of the 4G interface fastcellular1/0 on Device1.

```
Device1#show interface  fastcellular1/0
fastcellular1/0:
    line protocol is up
    Flags: (0xc208063) BROADCAST MULTICAST ARP RUNNING
    Type: ETHERNET_CSMACD
    Internet address: 10.230.33.13/30
    Broadcast address: 10.230.33.15
    Metric: 0, MTU: 1500, BW: 1000000 Kbps, DLY: 100 usec, VRF: global
    Reliability 255/255, Txload 1/255, Rxload 1/255
    Ethernet address is 001f.cedf.e997
    Last clearing of "show interface" counters never
    input peak rate 545 bits/sec,  0 hour 8 minutes 10 seconds ago
    output peak rate 4028 bits/sec,  0 hour 1 minute 20 seconds ago
    5 minutes input rate 0 bit/sec, 0 packet/sec
    5 minutes output rate 2000 bits/sec, 3 packets/sec
    43 packets received; 1749 packets sent
    6 multicast packets received
    16 multicast packets sent
    0 input errors; 0 output errors
    0 collisions; 0 dropped
    Unknown protocol 0
    Rate:  auto Duplex:  auto
    rxframes 43, rx bytes 4842, rx arps 3
    txframes 1736, tx bytes 158030, tx arps 9
```

```
rx errors 0, tx errors 0
```

#View the BFD session information on Device1.

```
Device1#show bfd session
OurAddr         NeighAddr         LD/RD      State      Holddown      interface
10.230.33.13    125.71.215.223    4/4        UP         90000         fastcellular3/0
```

#View the BFD session information on Device2.

```
Device2#show bfd session
OurAddr         NeighAddr         LD/RD      State      Holddown      interface
125.71.215.223  0.0.0.0           4/4        DOWN       0             gigabitethernet0
```

Note:

- Currently, BFD only detects the lower-end device, so the upper Device2 session status is always DOWN.

#View the IPsec tunnel information on Device1.

```
Device1#show crypto  ike sa
sa-id   negotiation-state    localaddr       peeraddr        peer-identity
 2128    STATE_XAUTH_C2      10.230.33.13    125.71.215.223  125.71.215.223
 2129    STATE_QUICK_I2      10.230.33.13    125.71.215.223  125.71.215.223
Device1#show crypto  ipsec sa
policy name : policy1
 f (src, dst, protocol, src port, dst port) :  172.16.2.0/24  26.1.1.0/24  ip  any  any
 local tunnel endpoint : 10.230.33.13 remote tunnel endpoint : 125.71.215.223
 the pairs of ESP ipsec sa : id : 2129, algorithm : 3DES HMAC-SHA1-96
  inbound esp ipsec sa :  spi : 0x262f3048(640626760)  crypto m_context(s_context) :
0x9e44e60 / 0x137cd368
     current input 10 packets, 0 kbytes
     encapsulation mode : UDP-Encapsulation-Tunnel
     replay protection : ON
     remaining lifetime (seconds/kbytes) : 28696/4294967295
     uptime is 0 hour 1 minute 44 second
  outbound esp ipsec sa :  spi : 0xd1e04f22(3521138466)  crypto
m_context(s_context) : 0x137cd230 / 0x137cd1c8
     current output 10 packets, 0 kbytes
     encapsulation mode : UDP-Encapsulation-Tunnel
     replay protection : ON
     remaining lifetime (seconds/kbytes) : 28696/4294967295
     uptime is 0 hour 1 minute 44 second
```

```
total sa and sa group is 1
```

#View the Ipsec tunnel information on Device2.

```
Device2#show crypto  ike sa
sa-id    negotiation-state     localaddr       peeraddr        peer-identity
 67155    STATE_XAUTH_S3       125.71.215.223   223.104.9.12     a(a)
 67156    STATE_QUICK_R2       125.71.215.223   223.104.9.12     a
Device2#show crypto  ipsec sa tunnel tun
policy name : subflow-1610618814, the parent policy name : policy1
 f (src, dst, protocol, src port, dst port) :  26.1.1.0/24  172.16.2.0/24  ip  any  any
 local tunnel endpoint : 125.71.215.223 remote tunnel endpoint : 223.104.9.12
 the pairs of ESP ipsec sa : id : 67156, algorithm : 3DES HMAC-SHA1-96
  inbound esp ipsec sa :  spi : 0xd1e04f22(3521138466)  crypto m_context(s_context) :
0xa6f4ab8 / 0x18b80d90
     current input 10 packets, 0 kbytes
     encapsulation mode : UDP-Encapsulation-Tunnel
     replay protection : ON
     remaining lifetime (seconds/kbytes) : 28643/4294967295
     uptime is 0 hour 2 minute 37 second
  outbound esp ipsec sa :  spi : 0x262f3048(640626760)  crypto
m_context(s_context) : 0x19c0fc58 / 0x2031a298
     current output 10 packets, 0 kbytes
     encapsulation mode : UDP-Encapsulation-Tunnel
     replay protection : ON
     remaining lifetime (seconds/kbytes) : 28643/4294967295
     uptime is 0 hour 2 minute 37 second

total sa and sa group is 1
```

#You can see that Device1 and Device2 set up the IPsec extended authentication tunnel successfully.

#PC1 and data center can ping each other via the Ipsec tunnel.

#After the line between Device1 and Device2 fails, BFD can detect the fault fast and trigger re-initiating dialing after the 4G interface is down.

8.3.4. Dual-4G Signal Switching

Network Requirements

- The device has two 4G card interfaces, that is, fastcellular 1/0 and fastcellular 2/0.

- There is the SIM card on two 4G board cards, which can be connected to the network.
- On the device, configure the signal switching parameter. According to the signal strength, switch the interface, and the route is switched synchronously.

Configuration Steps

Step 1: Configure the routes of the two 4G interfaces on the device.

```
Device1(config)#ip route 0.0.0.0 0.0.0.0 fastcellular 1/0
Device1(config)#ip route 0.0.0.0 0.0.0.0 fastcellular 2/0 100
```

Step 2: Configure adding fastcellular1/0 of the device to the dual-4G switching group 1.

```
Device1#configure terminal
Device1(config)# cellular signal-switch group 1 add interface fastcellular1/0
```

Step 3: Configure adding fastcellular2/0 of the device to the dual-4G switching group 1.

```
Device1#configure terminal
Device1(config)# cellular signal-switch group 1 add interface fastcellular2/0
```

Note:

- Signal switching depends on the quality of the signal, but the signal cannot truly reflect the link situation. When the signal is good, the link is not always smooth; when the signal is poor, the link is not necessarily congested, so to a certain extent, it is not necessarily reliable to decide whether to switch according to the signal quality.
- In order to prevent business interruption and dialup fluctuations caused by signal instability, do not switch if the interface with poor signal has been allocated and the signal strength value of the interface is >=9.

8.3.5. Configure 4G IPV6 Public Network

Network Requirements

- Device accesses the IPv6 public network via the 4G interface.

Network Topology

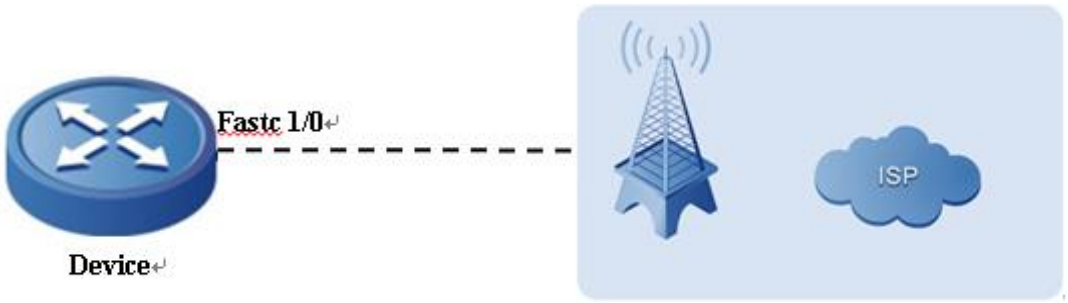

Figure 8-5 Networking of configuring the 4G IPv6 public network

Configuration Steps

Step 1 : Configure the 4G interface.

#Configure Device.

```
Device(config)# interface fastcellular1/0
Device(config-if-fastcellular1)# dialer config ipfamily ipv6
Device(config-if-fastcellular1)# dialer mode auto
Device(config-if-fastcellular1)# ipv6 enable
Device(config-if-fastcellular1)# ipv6 address autoconfig
Device(config-if-fastcellular1)#exit
```

Step 2: Configure the default route on Device, and the egress interface is fastcellular 1/0.

#Configure Device.

```
Device(config)# ipv6 route 0::0/0 fastcellular 1/0
```

Step 3: Check the result.

#After dialing successfully, view the IPv6 address that the fastcellular 1/0 interface of Device can get.

```
Device# show ipv6 interface fastcellular 1/0
fastcellular1/0 is up
  VRF: global
  IPv6 is enable, link-local address is fe80::201:7aff:fe5e:714b
  Global unicast address(es):
    2409:894c:c00:7784:201:7aff:fe5e:714b, subnet is 2409:894c:c00:7784::/64
[EUI/CAL/PRE]
  Joined group address(es):
    ff02::1:ff00:0
    ff02::2
    ff02::1
    ff02::1:ff5e:714b
  ND control flags: 0x3
  MTU is 1500 bytes, Link MTU is 1500 bytes
  ICMP redirects are enabled
  ICMP unreachables are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND config flags is 0x0
  ND MaxRtrAdvInterval is 600
```

```
ND MinRtrAdvInterval is 198
ND AdvDefaultLifetime is 1800
```

Step 4: Check the DNS server address of the IPv6 public network that can ping.

#After dialing successfully, view the DNS server address of the IPv6 public network that the fastcellular 1 interface of Device can ping.

```
Device(config)# ping 240c::6666

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 240c::6666 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 149/355/1134 ms.
```

8.3.6. Configure L2TPv3 over L2TPv2

Network Requirements

- Device1 is the client of 4G network site, LAC is the operator device, Device2 is the LNS and connected with ISP network, and Network-Center is the data center.
- Device1 dials in the operator through 4G, and the LAC of the operator establishes L2TPv2 with Device2.
- Device1 and Device2 use the interface IP address of L2TPv2 tunnel to establish the connection of L2TPv3, and reference the L2TPv3 connection on the port of each endpoint router connecting to PC.
- Configure the IP address of the same network segment on PC, and you can perform L2 communication.

Network Topology

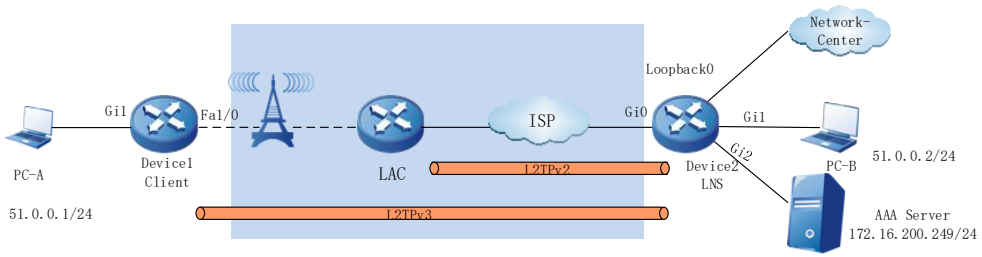

Figure 8-6 Networking of configuring L2TP V3 OVER L2TP V2

Device	Interface	IP address	Device	Interface	IP address
Device2	Gi0	192.168.208.75/24	Device2	Loopback0	100.1.1.1/32
	Gi2	172.16.200.165/24			

Configuration Steps

Step 1: Configure the IP address of the interface. (omitted)

Step 2: Configure the 4G dialing interface.

#Configure Device1, configure 4G interface fastcellular1/0 as auto dialing mode, configure special line APN, user name and password, and automatically obtain IP address through DHCP.

```
Device1(config)# interface fastcellular 1/0
Device1(config-if-fastcellular1)# dialer config apn whmptxgs.oth.oth.hbapn
Device1(config-if-fastcellular1)# dialer config username
test@whmptxgs.oth.oth.hbapn password 0 123456
Device1(config-if-fastcellular1)# dialer mode auto
Device1(config-if-fastcellular1)# ip address dhcp
Device1(config-if-fastcellular1)#exit
```

Step 3: Configure Device2 as AAA client.

#Configure Device2.

Configure the name of authentication and authorization list as PPP, and configure the address, authentication port, statistics port, and radius server password of radius server (Refer to the AAA section of the configuration manual)

```
Device2#configure terminal
Device2(config)#aaa server group radius ppp
Device2(config-sg-radius-ppp)# server 172.16.200.249 auth-port 1812 acct-port 1813
key a
Device2(config-sg-radius-ppp)# exit
Device2(config)#domain ppp
Device2(config-isp-ppp)# aaa authentication ppp radius-group ppp
Device2(config-isp-ppp)# aaa authorization ppp radius-group ppp
Device2(config-isp-ppp)# aaa accounting ppp start-stop radius-group ppp
Device2(config-isp-ppp)# exit
```

Step 4: Configure LNS.

#Configure Device2.

Configure the virtual template virtual-template0, and use AAA authentication and authorization list l2tp.

```
Device2(config)#interface virtual-template 0
Device2(config-if-virtual-template0)#encapsulation ppp
Device2(config-if-virtual-template0)# ppp authentication chap pap ppp
Device2(config-if-virtual-template0)# ppp authorization ppp
Device2(config-if-virtual-template0)# ip unnumbered loopback0
Device2(config-if-virtual-template0)#exit
```

Enable VPDN, create VPDN group Ins, configure as accept dial-in request mode, apply the L2TP protocol, and borrow virtual-template0. Configure the shared key of LAC and LNS as admin.

```
Device2(config)#vpdn enable
Device2(config)#vpdn-group lns
Device2(config-vpdn)#accept-dialin
Device2(config-vpdn-acc-in)#protocol l2tp
Device2(config-vpdn-acc-in)#virtual-template 0
Device2(config-vpdn-acc-in)#exit
Device2(config-vpdn)#local name lns
Device2(config-vpdn)#l2tp tunnel password 0 admin
Device2(config-vpdn)#exit
```

Note:

- If not needing to perform the tunnel authentication with LAC, execute the **no l2tp tunnel authentication** command on LNS to disable authentication.

Step 5: Check the result.

#View the fastcellular1/0 interface information of Device1.

```
Device1#show  interface  fastcellular1/0
Fastcellular1/0:
    line protocol is up
    Flags: (0xc208063) BROADCAST MULTICAST ARP RUNNING
    Type: ETHERNET_CSMACD
    Internet address: 70.0.0.15/27
    Broadcast address: 70.0.0.31
    Metric: 0, MTU: 1500, BW: 100000 Kbps, DLY: 100 usec, VRF: global
    Reliability 255/255, Txload 1/255, Rxload 1/255
    Ethernet address is 001f.ce5e.714d
    Last clearing of "show interface" counters never
    input peak rate 1136780 bits/sec,  2 days 22 hours ago
    output peak rate 1136804 bits/sec,  2 days 22 hours ago
    5 minutes input rate 0 bit/sec, 0 packet/sec, bandwidth utilization 0.00%
    5 minutes output rate 3000 bits/sec, 4 packets/sec, bandwidth utilization 0.00%
    4674215 packets received; 5193301 packets sent
    292110403 bytes received; 345063002 bytes sent
    0 multicast packets received
    302 multicast packets sent
    3 input errors; 0 output errors
    0 collisions; 0 dropped
    Unknown protocol 0
    Rate:  auto Duplex:  auto
```

```
rxframes 4674218, rx bytes 292110757, rx arps 0
txframes 5193173, tx bytes 345050317, tx arps 272
rx errors 0, tx errors 0
```

You can see that the 4G interface dials successfully, and the negotiated IP address is 70.0.0.15.

#On Device2, view the L2TP information.

```
Device2#show vpdn detail

L2tp MaxTun 3000, MaxSes 3000:

tunnel free num: 2999
TUNNELS:
    LOCAL-ID REM-ID   LOCAL-NAME          REM-NAME          VPDN-GROUP
PORT   SES-CNT  STATE       REM-ADDR
    74       32087    Router              VPDN-BANK-L2TP      1              1701   1
ESTABLISHED  192.168.247.9

session free num: 2999
SESSIONS:
    LOCAL-ID REM-ID  TUN-ID  IF-NAME          SYSTEMID          IMSI/CALLING-
NUM       STATE
    67       3665     74       virtual-access1       --------              8613164629736
ESTABLISHED

L2tp total Tunnel and Session Information. Tunnel 1  Session 1
```

It can be observed that the L2TPv2 tunnel is successfully established between LAC and Device2.

#The virtual template0 interface address of Device2 can be pinged on Device1.

```
Device1# ping 100.1.1.1


Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 100.1.1.1 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 52/57/65 ms.
```

Step 6: Configure L2TPv3.

#Configure Device1.

Configure the pseudo wire template l2tpv3-1, encapsulate the protocol type L2TPv3, and borrow fastcellular1. Configure L2TPv3 on the interface of gigabitethernet1, and use l2tpv3-1 to establish L2TPv3 dynamic session with device2.

```
Device1 (config)#pseudowire-class l2tpv3-1
Device1 (config-pw-class)#encapsulation l2tpv3
Device1 (config-pw-class)#protocol l2tpv3
Device1 (config-pw-class)#ip local interface fastcellular1
Device1 (config-pw-class)#exit
Device1 (config)#interface gigabitethernet 1
Device1 (config-if-gigabitethernet1)#xconnect 100.1.1.1 370 pw-class l2tpv3-1
Device1 (config-if-gigabitethernet1)#exit
```

#Configure Device2.

Configure the pseudo wire template l2tpv3-1, encapsulate the protocol type L2TPv3, and borrow loopback0. Configure L2TPv3 on the interface of gigabitethernet1, and use l2tpv3-1 to establish L2TPv3 dynamic session with Device1.

```
Device 2(config)#pseudowire-class l2tpv3-1
Device 2(config-pw-class)#encapsulation l2tpv3
Device 2(config-pw-class)#protocol l2tpv3
Device 2(config-pw-class)#ip local interface loopback0
Device 2(config-pw-class)#exit
Device 2(config)#interface gigabitethernet 1
Device 2(config-if-gigabitethernet1)#xconnect 70.0.0.15 370 pw-class l2tpv3-1
Device 2(config-if-gigabitethernet1)#exit
```

Note:

- The VCIDs at the two sides of the L2TPv3 session must be consistent. Otherwise, you cannot establish the dynamic session.

Step 7: : Check the result.

#View the L2TPv3 tunnel information of Device1.

```
Device1# show l2tun detail
L2TPv3 established Tunnel 1. established Session 1
L2TPv3 total Tunnel and Session Information. Tunnel 1  Session 1

 TUNNELS:
    LocID  LocName      RemID       RemName      RemAddr      Port   Sess
State
    1     client       96          Device2      100.1.1.1    0      1      ESTAB
 SESSIONS:
```

```
LocID   RemID       TunID       State   Type    Vcid        Interface
1121    1108        1           ESTAB   dynamic 1           gigabitethernet1
```

You can see that the L2TPv3 tunnel is set up between Device1 and Device2 successfully.

#View the L2TPv3 session information of Device1.

```
Device1# show l2tun session
L2TPv3 established Tunnel 1. established Session 1
L2TPv3 total Tunnel and Session Information. Tunnel 1  Session 1

Session id 1121 is up, tunnel id 1  *
Call serial number is 233444622
Remote tunnel name is Device2
    Internet address is 100.1.1.1
Local tunnel name is client
    Internet Address is 70.0.0.15
    Session is L2TP signaled
    Session state is established, time since change 00:03:08
        0 Packets sent, 0 Packets received
        0 Bytes sent, 0 Bytes received
    Session vcid is 1
    Session Layer 2 circuit, type is Ethernet-Tagged-Mode, name is
gigabitethernet1
    Circuit state is UP
        Remote session id is 1108, remote tunnel id 96
    DF bit off
    Vrf index 0
    Session cookie information:
    FS cached header information:
        encap size = 24 bytes
        45000000 00000000 ff730000 4600000f 64010101
        00000454
        decap size = 24 bytes
        forward IF = 59
```

It can be observed that L2TPv3 dynamic session is successfully established between Device1 and Device2.

Note:

- The viewing method of device2 is the same as that of device1, and the viewing process is omitted.

#You can ping PC-B on PC-A.

```
C:\windows\system32>ping 51.0.0.2
```

9. LOOPBACK INTERFACE

9.1. Overview

Loopback interface, also called local loopback interface, is one logical virtual interface realized by software. The interface is not affected by the physical status. As long as not disabling manually, its status is always enabled. In the dynamical routing protocol, such as OSPF, you can select the IP address of loopback interface as Router ID. For the packets sent to the loopback interface, the device regards that the packets are sent to itself, so it does not forward the packets.

9.2. Loopback Interface Function Configuration

Table 9-1 Function configuration list of loopback interface

Configuration Task	
Configure the loopback interface	Configure loopback interface

9.3. Configure Loopback Interface

Configuration Condition

None

Configure Basic Functions of Loopback Interface

Table 9-2 Configure basic functions of the loopback interface

Step	**Command**	**Description**
Enter the global configuration mode	**configure terminal**	-
Create the loopback interface	**interface loopback** *unit –number*	Mandatory By default, the loopback interface is not created

10. NULL INTERFACE

10.1. Overview

Null interface is one logical interface realized by software. Any packet sent to null interface is dropped. The dynamic routing protocol, such as OSPF, generates the auto-summarized route. The egress interface points to null interface and can avoid route loop effectively. Null0 interface is created by the device by default and the user cannot disable or delete it.

10.2. Null Interface Function Configuration

Table 10-1 Function configuration list of Null interface

Configuration Task	
Configure the basic functions of Null interface	Configure the basic functions of Null interface

10.2.1. Configure Null Interface

Configuration Condition

None

Configure Basic Functions of Null Interface

Table 10-2 Configure basic functions of Null interface

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the null interface configuration mode	**interface null 0**	Mandatory
Configure prohibiting sending the error packet of ICMP unreachable	**no ip unreachables**	Optional By default, prohibit sending the error packet of ICMP unreachable.

Note:

- Null interface just supports configuring permitting or prohibiting sending the error packet of ICMP unreachable.
- The packet reaching Null interface is dropped and do not send the error of ICMP unreachable by default.

11. TUNNEL INTERFACE

11.1. Overview

Tunnel is the technology of using one network protocol to transmit another network protocol. It includes the process of encapsulating, transmitting, and de-encapsulating data. The path passed by the encapsulated packet when being transmitted in the network is called tunnel. Tunnel is one virtual point-to-point connection. The devices at the two sides of the tunnel are called tunnel endpoints and they are responsible for encapsulating and de-encapsulating packets.

Tunnel interface is one logical interface realized by software, providing the transmission link for the point-to-point mode.

11.2. Tunnel Interface Function Configuration

Table 11-1 Function configuration list of tunnel interface

Configuration Task	
Configure the basic functions of the tunnel interface	Configure the basic functions of the tunnel interface

11.2.1. Configure Tunnel Interface

Configuration Condition

None

Configure Basic Functions of Tunnel Interface

Table 11-2 Configure basic functions of tunnel interface

Step	**Command**	**Description**
Enter the global configuration mode	**configure terminal**	-
Create tunnel interface and enter its configuration mode	**interface tunnel** *tunnel-unit*	Mandatory By default, the tunnel interface is not created on the device.
Configure work mode of tunnel interface	**tunnel mode** {**[dvpn mgre | udp]**} **gre** { **ip** | **mpls traffic-eng** }	Optional By default, the work mode of the tunnel interface is GRE over IPv4.

Step	Command	Description
Configure TOS of tunnel interface	**tunnel tos** *tos-value*	Optional By default, the tunnel interface is not configured with TOS.
Configure TTL of tunnel interface	**tunnel ttl** *ttl-value*	Optional By default, the TTL value of the tunnel interface is 255.
Configure the MTU value of the Tunnel interface	**mtu** *size* **ipv6 mtu** *size*	Optional By default, the MTU value on the tunnel interface varies with the mode.
Configure the Tunnel interface to encapsulate vrf	**tunnel encapsulation-vrf** *vrf-name*	Optional By default, the Tunnel interface is not encapsulated with vrf.

Note:

- On the Tunnel interface, encapsulate vrf. When the tunnel source interface is not configure, use the vrf as the vrf of the interface to which the destination address belongs and the vrf used by encapsulating the packet. If the tunnel source interface is configured, use the vrf of the tunnel source interface. The logic of configuring vrf on the tunnel interface is the same as other common physical interface, not related with the encapsulated vrf logic of the packet.
- On the Tunnel interface, support configuring the MTU value. After configuration, it takes precedence. If MTU is not configured, link with the MTU of the egress interface of the tunnel. The tunnel interface can also be configured with IPv6 MTU. After configuration, it takes precedence. If not configured, it depends on the configured MTU of the tunnel interface. If MTU is not configured for tunnel interface, the tunnel IPv6 MTU is calculated automatically with the same logic as IPv4 MTU.
- The TOS configured on tunnel interface is used to fill the TOS field in the outer IPv4 packet header during encapsulation. If the TOS value is not configured on tunnel interface, use the TOS value in the inner IPv4 packet header.
- The TTL value configured on tunnel interface is used to fill the TTL field in the outer IPv4 packet header during encapsulation.
- Two or more tunnels with the same tunnel mode, source address and destination address cannot be configured on the same device at the same time.

11.2.2. Tunnel Interface Monitoring and Maintaining

Table 11-3 tunnel interface monitoring and maintaining

Command	Description
clear tunnel statistic	Clear the packet statistics information of the tunnel interface
show tunnel statistic	Display the packet statistics information of the tunnel interface

12. SYNCHRONOUS/ASYNCHRONOUS SERIAL INTERFACE

12.1. Overview

Generally, a conductor or voltage fluctuation on the cable is used to transmit data among data communication devices. During the communication, if multiple channels transmit a byte, this is called parallel communication. Conversely, if data is transmitted on the channel bit by bit, this is called serial communication.

In the parallel communication, data bits of one character are transmitted over different channels. Therefore, the data is transmitted in high speed. When eighth data bits are transmitted in the parallel communication, at least eight data channels and one common channel are required and sometimes control channels such as status channel and response channel are required. This is expensive and inconvenient for long-distance transmission. In the serial communication, only two channels are required. It is cost effective for long-distance transmission. However, the serial communication can only transmit one bit every time, resulting in slow transmission speed. However, with the improvement of the communication signal frequency, the slow transmission speed problem has solved. The serial communication is generally applied to synchronous and asynchronous serial interface communication.

The synchronous/asynchronous serial interface is a slow WAN interface, able to encapsulate WAN protocols such as HDLC and PPP. It is divided into synchronization serial interface and asynchronism serial interface.

12.1.1. Synchronous Serial Interface

In the channel, the amplitude and pulse width are used to specify the data pulse signal. The receiving end samples the received signal by a certain clock serial number. Therefore, timing is an important factor to correctly receive and transmit data.

Synchronous/Asynchronous serial interface is called the synchronous serial interface when it works in the synchronous mode and it adopts the synchronous transmission mode. In the synchronous transmission, characters are transmitted in frame groups. Some special synchronous characters, placed at the start part of each frame, are a special bit group. It informs the receiving end that a frame is reached and triggers the synchronous clock to start to transmit or receive data. The receiving end starts to receive data when it correctly receives the synchronous characters. The synchronous serial interface obtains the timing signal in the following method: The timing information is contained in the data flow and the synchronous serial interface requires that the timing signal must be easy to be extracted from the data flow. In this way, no special signal channel is required to transmit the clock. The synchronous serial interface determines whether a clock needs to be configured based on the device work mode and works at the DTE (Data Terminal Equipment) or DCE (Data Circuit-terminating Equipment) end. The clock is provided by the DCE end.

12.1.2. Asynchronous Serial Interface

Synchronous/Asynchronous serial interface is called the asynchronous serial interface when it works in the asynchronous mode and it adopts the asynchronous transmission mode. The asynchronous communication has a low requirement for the hardware, which is easy and simple for transmitting and receiving data randomly. In the asynchronous transmission, the start bit and end bit are added for the character to spate the character. Because the synchronization is created for every character, that is, each character will be added extra two bits (start bit and end bit), the transmission rate is low. The asynchronous serial interface needs the clock to ensure normal data receiving. Compared with the synchronous clock of the synchronous serial interface, the

asynchronous serial interface must configure the same clock rate for devices on both ends. Otherwise, normal communication cannot be achieved.

12.2. Synchronous/Asynchronous Serial Interface Function Configuration

Table 12-1 Function configuration list of synchronous/asynchronous serial interface

Configuration Task	
Configure the synchronous/asynchronous serial interface work mode	Configure the synchronous/asynchronous serial interface work mode
Configure the synchronous serial interface	Configure the synchronous/asynchronous serial interface clock rate
	Configure the synchronous serial interface line coding
	Configure the synchronous serial interface idle transmission character
	Configure the synchronous serial interface clock rate
	Configure the CRC check mode of the synchronous serial interface data frame
Configure the asynchronous serial interface	Configure the asynchronous serial interface clock rate
	Configure the asynchronous serial interface data bit length
	Configure the asynchronous serial interface end bit length
	Configure the asynchronous serial interface flow control mode
	Configure the asynchronous serial interface verification mode

Configuration Task	
Configure the data transmitting and receiving condition of the synchronous/asynchronous serial interface	Configure the synchronous/asynchronous serial interface data receiving and transmitting condition

12.2.1. Configure Synchronous/Asynchronous Serial Interface Work mode

The synchronous/asynchronous serial interface works in the synchronous mode or the asynchronous mode.

Configuration Condition

None

Configure the synchronous/asynchronous Serial Interface Work Mode

Table 12-2Configure the synchronous/asynchronous serial interface work mode

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the synchronous/asynchronous serial interface work mode	**physical-layer** { **async** | **sync** }	Optional By default, the synchronous/asynchronous serial interface works in the sync mode.

12.2.2. Configure Synchronous Serial Interface

Configuration Condition

Before configuring the synchronous serial interface, first complete the following task:

- The interface works in the synchronous mode.

Configure Synchronous Serial Interface Clock Rate

During the data transmission, both frame synchronization and clock synchronization must be ensured. Packet loss may occur when the clock is not synchronized. Therefore, to ensure clock synchronization, a unified clock must be used. One end is configured with an internal clock and the other end is configured with a line clock. Thus, a unified clock is ensured on the line. You are advised to avoid configuring clocks at both ends of the device. Otherwise, interfaces may be unable for communications due to clock chaos. Generally, the clock is configured at the DCE. When the DTE is operating, the device does not need to be configured with a clock. It transmits and receives data via the clock provided by the DCE. When the DCE is operating, the device

needs to be configured with a clock. It transmits and receives data by the clock configured by itself. The DCE also provides the clock for other devices. The V.35 or V.24 mode determines the highest clock rate configured. The V.35 or V.24 mode is determined by the connected cable.

The synchronous serial interface clock rate needs to be configured under interfaces.

Table 12-3 Configure the synchronous serial interface clock rate

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the synchronous serial interface clock rate	**clock rate** *rate-value*	Mandatory By default, the clock rate is not configured Value range: 1200, 2400, 4800, 9600, 19200, 38400, 56000, 64000, 72000, 125000, 128000, 148000, 250000, 500000, 800000, 1000000, 1300000, 2000000

Note:

- Run the **show interface** command to view whether the interface works in the DCE or DTE mode.
- When the synchronous serial interface of the device works in the DCE mode, a clock rate needs to be configured. The device also provides external clock for other devices.
- When the synchronous serial interface of the device works in the DTE mode, it obtains the clock form the DCE.
- In the V.24 mode, the clock rate of the interface can reach a maximum of 128 kbit/s.
- In the V.35mode, the clock rate of the interface can reach a maximum of 2 Mbit/s.

Configure Synchronous Serial Interface Line Coding

The E1 receiving and transmitting directions are independent without interfering each other. Because the clock is extracted from the line signal, no independent clock line is needed. The line coding usually uses NRZI and NRZ.

The synchronous serial interface line coding needs to be configured under interfaces.

Table 12-4 Configure the synchronous serial interface line coding

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the synchronous serial interface line coding	**nrzi-encoding**	Optional By default, the line coding method is NRZ.

Note:

- By default, the NRZ coding method is adopted and no configuration command is configured. You can only run the **no nrzi-encoding** command to restore to the NRZ coding method.
- The synchronous serial interface of both ends of the device must be configured with the same line coding method. Otherwise, the interface cannot communicate normally.

Configure Synchronous Serial Interface Idle Transmission Character

This section mainly describes the characters transmitted over the line when the synchronous serial interface is idle.

The idle transmission character of the synchronous serial interface must be configured under interfaces.

Table 12-5 Configure the synchronous serial interface idle transmission character

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the idle transmission character of the synchronous serial interface	**idle-character** { **flags** | **marks** }	Optional By default, the idle transmission character is **flags**.

Note:

- When the idle transmission character is set to flags, the transmission character on the line is 7E character actually.

- When the idle transmission character is set to marks, the transmission character on the line is FF character actually.

Configure Synchronous Serial Interface Clock Rotation

Because of the long line and fast clock, the clock may be delayed for more than half period and less than one period. This results in that the packet cannot be received and transmitted normally. At this time, the following command can be configured to rotate the clock to adjust the clock for half period.

Table 12-6Configure the synchronous serial interface clock rotation

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the synchronous serial interface clock rotation	**clock invert** { **rxclk | txclk** }	Mandatory By default, the clock rotations not configured.

Note:

- The clock frequency of different devices may be different and the clock rotation needs to be configured.

Configure CRC Check Mode of Synchronous Serial Interface Data Frame

PPP and HDLC are the protocols supported by synchronous serial interface. After each data frame, CRC can be used to check the data frame. This command can configure the CRC check mode of the data frame.

Table 12-7 Configure the CRC check mode of the synchronous serial interface data frame

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the CRC check mode of the data frame	**crc** { **32** | **16** }	Mandatory By default, the CRC check length of the synchronous serial interface is 16 bits (2Bytes).

12.2.3. Configure Asynchronous Serial Interface

Configuration Condition

Before configuring the asynchronous serial interface, first complete the following task:

- The interface works in the asynchronous mode.

Configure Asynchronous Serial Interface Clock Rate

The clock rate of the asynchronous serial interface can reach a maximum of 115200 kbit/s. The both devices must be configured with the same clock rate for normal communications.

The asynchronous serial interface clock rate must be configured under devices.

Table 12-7 Configure the asynchronous serial interface clock rate

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the clock rate for the asynchronous serial interface	**speed** *speed-value*	Optional By default, the clock rate is 9600 bit/s. Value range: 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200

Configure Asynchronous Serial Interface Data Bit Length

Configure the bit number occupied by data when a character is transmitted over the line. By default, a character data occupies 8 bits.

The data bit length of the asynchronous data bit must be configured under interfaces.

Table 12-8 Configure asynchronous serial interface data bit length

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure asynchronous serial interface data bit length	**databits** { **5 | 6 | 7 | 8** }	Mandatory By default, the data bit length is 8 bits.

Note:

- After the 5, 6, and 7 bits are configured, exceptions may occur to the communication unless the corresponding data bits are sent by the interface.
- When the data bit configured by the interface is 5, the stop bit length of the interface must be configured to 2 at first. Because the ASCII code is 7 bits, at least 7 bits must be configured during the transmission.

Configure Asynchronous Serial Interface Stop Bit Length

Configuring the data bit number occupied by the stop bit when a character is transmitted over the line. By default, 1 bit is occupied.

The stop bit length of the asynchronous serial interface must be configured under interfaces.

Table 12-9 Configure the asynchronous serial interface stop bit length

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the stop bit length of the asynchronous serial interface	**stopbits** { **1 | 2** }	Optional By default, the stop bit length is 1 bit.

Configure Asynchronous Serial Interface Flow Control Mode

The flow control is used to avoid the phenomenon that packet loss occurs when sending devices due to different device receiving speed. The flow control mode is divided into hardware flow control and software flow control.

The software flow control indicates that the receiving end informs the sending end to send or not send data using special characters.

The hardware flow control indicates the receiving end uses the hardware control signal line on the interface to inform the sending end to send or not send data. Compared with the software flow control, the sending end of the hardware flow control does not need to insert the flow control character in the data flow. The receiving end does not need to check whether the flow control character is received.

Generally, the hardware flow control has a higher transmission rate than the software flow control. When the control signal line is incomplete, the software flow control is adopted.

The flow control mode of the asynchronous serial interface must be configured under interfaces.

Table 12-10 Configure the flow control mode of the asynchronous serial interface

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the flow control mode for the asynchronous serial interface	**flow-control** { **none | hardware | software [***timeout-vlule***]**}	Mandatory By default, the flow control mode is not configured. Hardware flow control and software flow control need to set the flow control timeout, and the default value is 65535.

Configure Asynchronous Serial Interface Verification Mode

The verification ensures the data correctness. The verification is divided into **odd**, **mark**, **even**, and **spac**. When the parity bit is any odd number, it is called **odd**. When all the parity bits are 1, it is called **mark**. When the parity bit is any even number, it is called **even**. When all the parity bits are 0, it is called **space**.

The verification mode of the asynchronous serial interface must be configured under interfaces.

Table 12-11 Configure the asynchronous serial interface verification mode

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the verification mode for the asynchronous interface	**parity** { **even | mark | none | odd | space** }	Mandatory By default, the verification mode is not configured.

12.2.4. Configure Synchronous/Asynchronous Serial Interface Data Receiving and Transmitting Condition

Configuration Condition

Before the data receiving and transmitting condition of the synchronous/asynchronous serial interface, first complete the following task:

- The interface works in the synchronous mode or the asynchronous mode.

Configure the Synchronous/Asynchronous Serial Interface Data Receiving and Transmitting Condition

The synchronous/asynchronous serial interface follows the RS-232-C standard, but the RS-232-C standard has many signal lines, commonly data signal line and control signal line.

DSR (Data Set Ready) signal line: When the interface is up, the data communication terminal is ready for use.

DTR (Data Terminal Ready) signal line: When the interface is up, the data communication terminal is ready for use.

The preceding two signals are valid immediately when powering on. This only indicates that the device is available, instead of indicating that the device is ready for communications. Whether the communication is available is determined by the following control signal.

RTS (Request To Send) signal line: It indicates that signal is sent to the communication device to make the signal up when the DCT requests to send data to the DCE, that is, when the terminal begins to send data. It controls whether the communication terminal will enter the sending status.

CTS (Clear To Send) signal line: It indicates the response signal to the RTS when the DCE is ready to receive the data sent by the DTE. When the communication terminal is ready to receive the data sent by the terminal, the signal is up and the terminal is informed to send data.

DCD (Data Carrier Detection) signal line: It indicates that the DCE is connected to the communication link and informs that the DTE is ready to receive data.

Generally, when all control signal line are valid, the interfaces can communicate normally. When the control signal line is incomplete, you can run the following command to change the

condition for receiving and transmitting data to enable normal communications of synchronous/asynchronous serial interface.

The condition for receiving and transmitting data of the synchronous/asynchronous serial interface must be configured under interfaces.

Table 12-12 Configure the synchronous/asynchronous serial interface data receiving and transmitting condition

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the condition for receiving and transmitting data of the synchronous/asynchronous serial interface	**tx-on** { **cts | dcd | dcd-dsr | dsr** }	Optional By default, the condition for receiving and transmitting data is **dcd-dsr**.

12.2.5. Synchronous/Asynchronous Serial Interface Monitoring and Maintaining

Table 12-13 Synchronous/Asynchronous serial interface monitoring and maintaining

Command	Description
show interface *interface-name*	View the interface information

12.3. Typical Configuration Example of Synchronous/Asynchronous Serial Interface

12.3.1. Configure Interconnection in Synchronous Serial Mode

Network Requirements

- Device1 connects to Device2 via the synchronous/asynchronous serial interface. Data communicates in the synchronous serial mode.
- Device1 acts as the DTE and Device2 acts as the DCE.

Network Topology

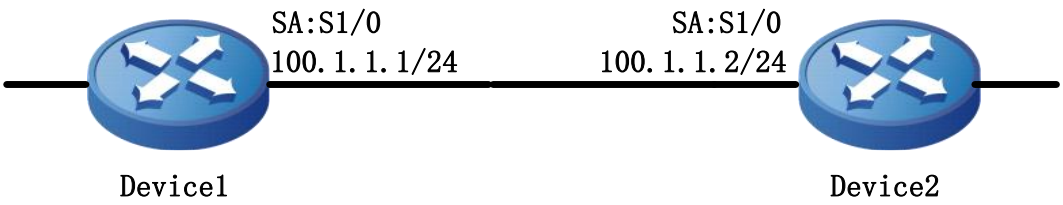

Figure 12-1Networking of interconnection in the synchronous serial mode

Configuration Steps

Step 1: Configure the interface in the synchronous serial mode. Configure the IP address on the interface and encapsulate the protocol.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#interface serial 1/0
Device1(config-if-serial1/0)#ip address 100.1.1.1 255.255.255.0
Device1(config-if-serial1/0)#encapsulation ppp
Device1(config-if-serial1/0)#exit
Device1(config)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#interface serial 1/0
Device2(config-if-serial1/0)#ip address 100.1.1.2 255.255.255.0
Device2(config-if-serial1/0)#encapsulation ppp
Device2(config-if-serial1/0)#exit
```

Step 2: Configure the Interface clock rate.

#Configure Device2.

```
Device2(config)#interface serial 1/0
Device2(config-if-serial1/0)#clock rate 2000000
Device2(config)#exit
```

When the clock rate for the interface is configured, the device works in the DCE mode.

Step 3: Check the result.

#View the serial interface status on Device1.

```
Device1#show interface serial 1/0
serial1/0:
```

```
line protocol is up
Flags: (0x80080f1) POINT-TO-POINT MULTICAST RUNNING
Type: PPP
Internet address: 100.1.1.1/24
Destination Internet address: 100.1.1.2
Metric: 0, MTU: 1500, BW: 2000 Kbps, DLY: 20000 usec, VRF: global
Reliability 255/255, Txload 1/255, Rxload 1/255
Last clearing of "show interface" counters never
input peak rate 52 bits/sec,  0 hour 0 minute 40 seconds ago
output peak rate 52 bits/sec,  0 hour 0 minute 40 seconds ago
5 minutes input rate 0 bit/sec, 0 packet/sec
5 minutes output rate 0 bit/sec, 0 packet/sec
27 packets received; 67 packets sent
0 multicast packets received
0 multicast packets sent
0 input errors; 0 output errors
0 collisions; 0 dropped
 LCP:OPENED
 IPCP:OPENED
 encap-type: simply PPP
   rxFrames: 27, rxChars: 346
   txFrames: 26, txChars: 320
   rxNoOctet: 0, rxAbtErrs: 0, rxCrcErrs: 0
   rxOverrun: 0, rxLenErrs: 0, txUnderrun: 0
   idle flag, encode NRZ
    You insert DTE line,V35 model
   DCD=up  DSR=up  DTR=up  RTS=up  CTS=up  TxC=up
```

#View the serial interface status on Device2.

```
Device2#show interface serial 1/0
serial1/0:
    line protocol is up
    Flags: (0x80080f1) POINT-TO-POINT MULTICAST RUNNING
    Type: PPP
    Internet address: 100.1.1.2/24
    Destination Internet address: 100.1.1.1
    Metric: 0, MTU: 1500, BW: 2000 Kbps, DLY: 20000 usec, VRF: global
    Reliability 255/255, Txload 1/255, Rxload 1/255
```

```
Last clearing of "show interface" counters is 0 hour 0 minute 0 second ago
input rate 0 bit/sec, 0 packet/sec, bandwidth utilization 0.00%
output rate 0 bit/sec, 0 packet/sec, bandwidth utilization 0.00%
1 packets received; 0 packets sent
72 bytes received; 0 bytes sent
1 multicast packets received
0 multicast packets sent
0 input errors; 0 output errors
0 collisions; 0 dropped
 LCP:OPENED
 IPCP:OPENED
 encap-type: simply PPP
  rxFrames: 0, rxChars: 0
  txFrames: 0, txChars: 0
  rxNoOctet: 0, rxAbtErrs: 0, rxCrcErrs: 0
  rxOverrun: 0, rxLenErrs: 0, txUnderrun: 0
  idle flag, encode NRZ
   You insert DCE line,V35 model
  DCD=up  DSR=up  DTR=up  RTS=up  CTS=up  TxC=up
  Rate = 2000000 bps
```

Run the **show interface** command on Device1, it can be observed that the status of the interface is up, able to obtaining the IP address of the peer device.

#Ping the IP address of the peer device on Device1. The IP address can be pinged through.

```
Device1#ping 100.1.1.2

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 100.1.1.2 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

Note:

- Whether the synchronous/asynchronous serial interface works in the V35 or V24 mode is determined by the connected cable on the interface card.
- Different work mode of the device has different cables connected on the interface. In the actual scenario, QTECH device works in the DTE mode. Use the DTE cable for physical connection.
- When configuring the clock rate, if the "Warning: The line is DTE, cannot set clock rate." message is displayed, it indicates that the interface can work in the DTE mode.

1.2.2. Configure Interconnection in Asynchronous Serial Mode

Network Requirements

- Device1 connects to Device2 via the synchronous/asynchronous serial interface. Data communicates in the asynchronous serial mode.

Network Topology

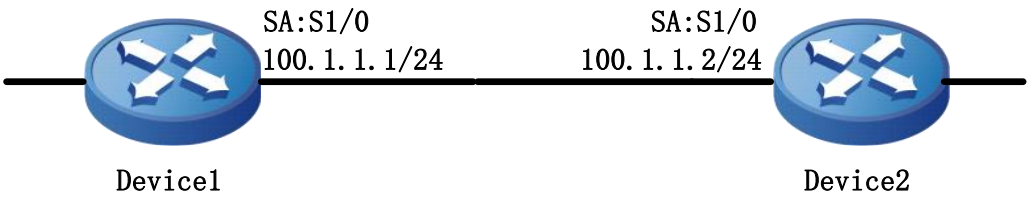

Figure 12-2 Networking of interconnection in the asynchronous serial mode

Configuration Steps

Step 1: Configure the interface in the asynchronous serial mode. Configure the IP address on the interface and encapsulate the protocol.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#interface serial 1/0
Device1(config-if-serial1/0)#physical-layer async
Device1(config-if-serial1/0)#ip address 100.1.1.1 255.255.255.0
Device1(config-if-serial1/0)#encapsulation ppp
Device1(config-if-serial1/0)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#interface serial 1/0
Device2(config-if-serial1/0)#physical-layer async
Device2(config-if-serial1/0)#ip address 100.1.1.2 255.255.255.0
Device2(config-if-serial1/0)#encapsulation ppp
Device2(config-if-serial1/0)#exit
```

Step 2: Configure the interface transmission rate.

#Configure Device1.

```
Device1(config)#interface serial 1/0
Device1(config-if-serial1/0)#speed 115200
Device1(config-if-serial1/0)#exit
Device1(config)#exit
```

#Configure Device2.

```
Device2(config)#interface serial 1/0
Device2(config-if-serial1/0)#speed 115200
Device2(config-if-serial1/0)#exit
Device2(config)#exit
```

Step 3: Check the result.

View the serial interface status on Device1.

```
Device1#show interface serial 1/0
serial1/0:
    line protocol is up
    Flags: (0xc0080f1) POINT-TO-POINT MULTICAST RUNNING
    Type: PPP
    Internet address: 100.1.1.1/24
    Destination Internet address: 100.1.1.2
    Metric: 0, MTU: 1500, BW: 116 Kbps, DLY: 20000 usec, VRF: global
    Reliability 255/255, Txload 1/255, Rxload 1/255
    Last clearing of "show interface" counters is 0 hour 0 minute 1 second ago
    input rate 0 bit/sec, 0 packet/sec, bandwidth utilization 0.00%
    output rate 0 bit/sec, 0 packet/sec, bandwidth utilization 0.00%
    0 packets received; 0 packets sent
    0 bytes received; 0 bytes sent
    0 multicast packets received
    0 multicast packets sent
    0 input errors; 0 output errors
    0 collisions; 0 dropped
     encap-type: simply PPP
     LCP:OPENED
     IPCP:OPENED   NDSPCP:INITIAL
      rxFrames: 0, rxChars: 0
      txFrames: 0,txChars: 0
      rxNoOctet: 0, rxAbtErrs: 0, rxCrcErrs: 0
      rxOverrun: 0, rxLenErrs: 0, txUnderrun: 0
      speed 115200, dataBits 8, stopBits 1
      parity none, flow-control none, tx-on dcd-dsr
       You insert DTE line,V35 model
      DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Run the **show interface** command on Device1, it can be observed that the status of the interface is up, able to obtaining the IP address of the peer device. The interface works in the asycnhronous mode.

#Ping the IP address of the peer device on Device1. The IP address can be pinged through.

```
Device1#ping 100.1.1.2
```

13. ОБЩАЯ ИНФОРМАЦИЯ

13.1. Замечания и предложения

Мы всегда стремимся улучшить нашу документацию и помочь вам работать лучше, поэтому мы хотим услышать вас. Мы всегда рады обратной связи, в особенности:

- ошибки в содержании, непонятные или противоречащие места в тексте;
- идеи по улучшению документации, чтобы находить информацию быстрее;
- неработающие ссылки и замечания к навигации по документу.

Если вы хотите написать нам по поводу данного документа, то используйте, пожалуйста, форму обратной связи на qtech.ru.

13.2. Гарантия и сервис

Процедура и необходимые действия по вопросам гарантии описаны на сайте QTECH в разделе «Поддержка» −> «Гарантийное обслуживание».

Ознакомиться с информацией по вопросам тестирования оборудования можно на сайте QTECH в разделе «Поддержка» −> «Взять оборудование на тест».

Вы можете написать напрямую в службу сервиса по электронной почте sc@qtech.ru.

13.3. Техническая поддержка

Если вам необходимо содействие в вопросах, касающихся нашего оборудования, то можете воспользоваться нашей автоматизированной системой запросов технического сервис-центра helpdesk.qtech.ru.

Телефон Технической поддержки +7 (495) 797-33-11 доб. 0