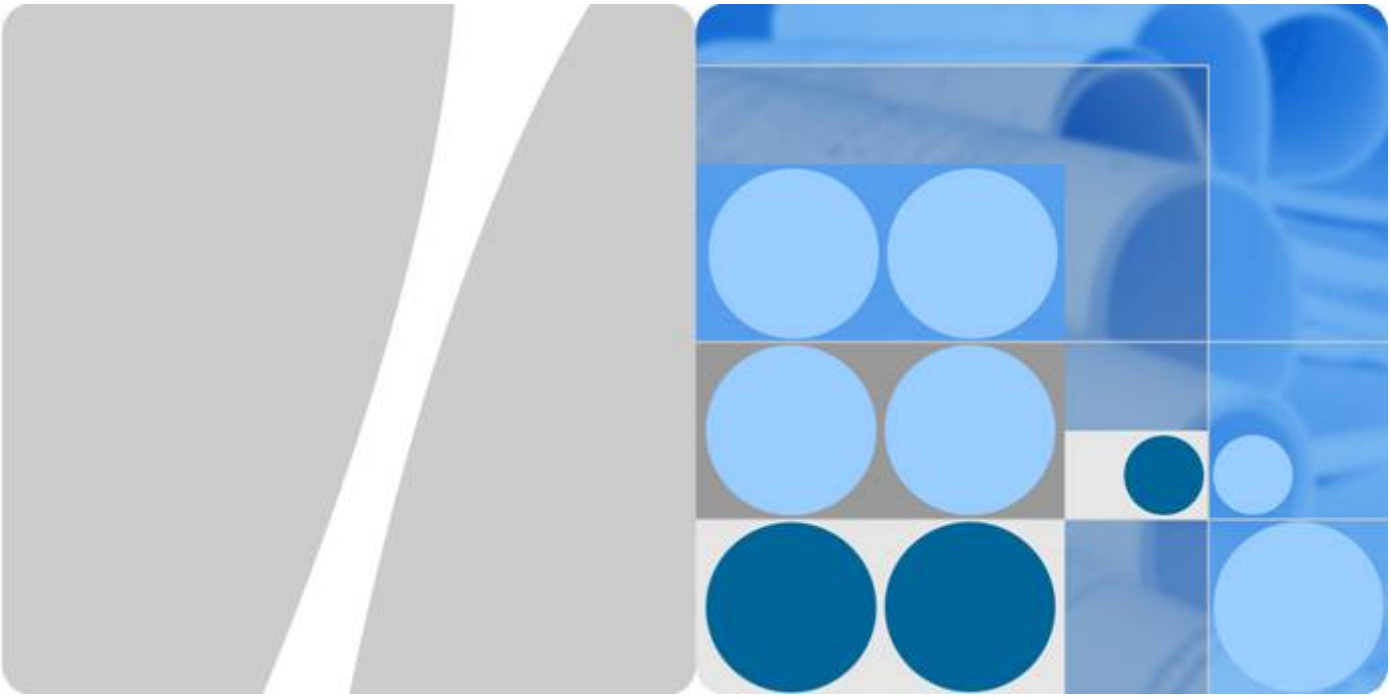


Huawei AR2200 Series Enterprise Routers

V200R002C00

Configuration Guide - WAN

Issue 02

Date 2012-03-30

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Email: support@huawei.com

About This Document

Intended Audience

This document describes WAN features on the AR2200 and provides configuration procedures and configuration examples.

This document is intended for:

- Data configuration engineers
- Commissioning engineers
- Network monitoring engineers
- System maintenance engineers

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
DANGER	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.
WARNING	Indicates a hazard with a medium or low level of risk, which if not avoided, could result in minor or moderate injury.
CAUTION	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
TIP	Indicates a tip that may help you solve a problem or save time.
NOTE	Provides additional information to emphasize or supplement important points of the main text.

Command Conventions

The command conventions that may be found in this document are defined as follows.

Convention	Description
Boldface	The keywords of a command line are in **boldface**.
Italic	Command arguments are in *italics*.
[ ]	Items (keywords or arguments) in brackets [ ] are optional.
{ x | y | ... }	Optional items are grouped in braces and separated by vertical bars. One item is selected.
[x | y | ...]	Optional items are grouped in brackets and separated by vertical bars. One item is selected or no item is selected.
{ x | y | ... }*	Optional items are grouped in braces and separated by vertical bars. A minimum of one item or a maximum of all items can be selected.
[x | y | ...]*	Optional items are grouped in brackets and separated by vertical bars. Several items or no item can be selected.
&<1-n>	The parameter before the & sign can be repeated 1 to n times.
#	A line starting with the # sign is comments.

Interface Numbering Conventions

Interface numbers used in this manual are examples. In device configuration, use the existing interface numbers on devices.

Change History

Changes between document issues are cumulative. Therefore, the latest document version contains all updates made to previous versions.

Changes in Issue 02 (2012-03-30)

Based on issue 01 (2011-12-30), the document is updated as follows:

The following information is modified:

- **4.4.2 Configuring a Dialer Interface**

Changes in Issue 01 (2011-12-30)

Initial commercial release.

Contents

1 ATM Configuration

About This Chapter

The Asynchronous Transfer Mode (ATM) is a cell transmission standard defined by the International Telecommunication Union - Telecommunication Standardization Sector (ITU-T). ATM organizes digital data into 53-byte cells and then transmits, multiplexes, or switches the cells. ATM transmits cells in fixed length (53 bytes), provides connection-oriented services, and simplifies the transmission process.

This section describes how to maintain ATM. Detailed operations include clearing statistics on an ATM interface.

1.8 Configuration Examples

This section provides several examples for configuring ATM. These configuration examples explain the networking requirements, configuration roadmap, data preparation, configuration procedure, and configuration files.

1.1 Introduction to ATM

ATM was specified as the transmission and switching mode for the Broadband Integrated Services Digital Network (B-ISDN) by the ITU-T in June 1992. Due to its high flexibility and support for multi-media services, ATM is a key technique for broadband communications.

ATM organizes digital data into 53-byte cells and then transmits, multiplexes, or switches the cells. An ATM cell consists of 53 bytes. The first 5 bytes is the cell header that contains the routing and priority information. The remaining 48 bytes are payloads.

ATM is connection-oriented. Each VC is identified by a Virtual Path Identifier (VPI) and a Virtual Channel Identifier (VCI). One pair of VPI/VCI values is useful only on a link segment between ATM nodes. If a connection is broken, the relevant VPI/VCI values are released.

ITU-T B-ISDN I.610 defines the Operation, Administration and Maintenance (OAM) functions on ATM networks. The OAM functions are divided into five levels: F1 (regenerator section level), F2 (digital section level), F3 (transmission path level), F4 (virtual path level), and F5 (virtual channel level). Two types of operating flows, F4 and F5, are defined for the ATM layer.

- F4 flows are OAM cell flows in Virtual Path Connect (VPC), providing VP-level operation management and maintenance.
- F5 flows are OAM cell flows in Virtual Channel Connect (VCC), providing VC-level operation management and maintenance.

After OAM is enabled for F4 and F5 flows, specific OAM cells are inserted into user cell flows. OAM and user cells are transmitted along the same physical channels and share the bandwidth.

F4 and F5 flows support four types of OAM cells, namely, fault management, performance management, activation-deactivation, and system management.

1.2 ATM Features Supported by the AR2200

The Asymmetric Digital Subscriber Line (ADSL) and G.Single-pair High Speed Digital Subscriber Line (G.SHDSL) interfaces are interfaces of the AR2200 and support the Asynchronous Transfer Mode (ATM).

An ADSL interface or a G.SHDSL interface working in ATM mode on the AR2200 provides ATM features. For details on how to configure ADSL and G.SHDSL interfaces, see ADSL Interface Configuration and G.SHDSL Interface Configuration in the *Huawei AR2200 Series Enterprise Routers Configuration Guide - Interface Management*.

An ADSL interface or a G.SHDSL interface working in ATM mode supports the following ATM features:

- Permanent virtual circuit (PVC) and PVC group
- IPoA, IPoEoA, PPPoA, and PPPoEoA that enable IP and PPP packets to be transmitted over ATM links
- PVC service type setting
- Virtual path (VP) policing

The AR2200 provides the ATM Operation Administration and Maintenance (OAM) function to monitor PVC link connectivity.

1.3 Configuring an ATM PVC Group

You can configure a PVC group to allow PVCs destined for the same IP address to forward data at the same time. Configuring a PVC group fully utilizes bandwidth resources and improves reliability of important services.

1.3.1 Establishing the Configuration Task

Before creating a PVC group and configuring PVC service mapping, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task quickly and accurately.

Applicable Environment

PVC service mapping allows different PVCs to transmit IP packets with different priorities between two nodes.

You configure a PVC group so that, when IP packets are transmitted over an ATM network, IP packets with different priorities are transmitted between two nodes along different PVCs.

Pre-configuration Tasks

Before creating a PVC group and configuring PVC service mapping, complete the following tasks:

- Configuring physical attributes for ATM interfaces on the router
- Configuring IP addresses and masks for ATM interfaces and sub-interfaces
- Creating PVCs and configuring their application mode

Data Preparation

To create a PVC group and configure PVC service mapping, you need the following data.

No.	Data
1	Number of an ATM interface or a sub-interface
2	IP address and mask of the ATM interface or sub-interface
3	PVC name (optional) and VPI/VCI values for the PVC group
4	Name (optional) and VPI/VCI values for each PVC in the PVC group
5	Lowest and highest priorities of IP packets transmitted along PVCs in the PVC group

1.3.2 Creating a PVC Group

This section describes how to create a PVC group.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface atm interface-number[.subinterface ]
```

The ATM interface or sub-interface view is displayed.

Step 3 Run:

```
pvc { pvc-name [ vpi/vci ] | vpi/vci }
```

A PVC is created and the PVC view is displayed.

NOTE

If the status of a PVC is unstable, and the local end of the PVC needs to know the status change of the remote end, the OAM F5 loopback function must be enabled on the local end.

The virtual path identifier (VPI)/virtual channel identifier (VCI) values configured for the primary and secondary ATM PVCs in an ATM PVC group must be the same on the local and remote ends. The IP precedence value configured for each ATM PVC must also be the same on the local and remote ends. If ATM PVCs on the local and remote ends are configured with different IP precedence values, services provided by the ATM PVC group will be interrupted.

Step 4 Run:

```
quit
```

The ATM interface or sub-interface view is displayed.

Step 5 Run:

```
pvc-group { pvc-name [ vpi/vci ] | vpi/vci }
```

A PVC group is created and the PVC group view is displayed.

The PVC name or VPI/VCI values must be available for creating a PVC group or entering the view of a PVC group.

----End

1.3.3 Mapping IP Precedence Values to Separate ATM PVCs in an ATM PVC Group

PVCs in a group can be configured to transmit IP packets with different precedence values. PVCs transmitting IP packets with high precedence values preferentially use bandwidth resources.

Prerequisites

PVCs with specified precedence values have been configured.

Context

After IP precedence values or DiffServ Code Point (DSCP) values are mapped to PVCs, IP packets with different precedence values are transmitted along different PVCs. In this manner, IP packets with different precedence values are transmitted separately.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface atm interface-number[.subinterface ]
```

The ATM interface or sub-interface view is displayed.

Step 3 Run:

```
pvc-group { pvc-name [ vpi/vci ] | vpi/vci }
```

The PVC group view is displayed.

IP precedence values can only be mapped to PVCs transmitting IPoA packets.

Step 4 Run either of the following commands as required:

- To map specified precedence values of IP packets to a PVC, run:
  ```
  ip precedence { pvc-name [ vpi/vci ] | vpi/vci } { min [ max ] | default }
  ```
- To map specified DSCP values of IP packets to a PVC, run:
  ```
  ip dscp { pvc-name [ vpi/vci ] | vpi/vci } { min [ max ] | default }
  ```

NOTE

PVC service mapping does not change the precedence values of IP packets transmitted along PVCs in a PVC group. To change precedence values for IP packets, configure certain tags carried in IP packets. For details, see the *Huawei AR2200 Series Enterprise Routers Configuration Guide - QoS*.

----End

1.3.4 Checking the Configuration

After a PVC group is created and PVC service mapping is configured, you can view information about the PVC group and PVCs in the group.

Prerequisites

The configurations of a PVC group and PVC service mapping are complete.

Procedure

- Run the **display atm pvc-info** [**interface atm** *interface-number* [**pvc** { *pvc-name* [*vpi/vci*] | *vpi/vci* }]] command to check information about PVCs.
- Run the **display atm pvc-group** [**interface atm** *interface-number* [**pvc** { *pvc-name* [*vpi/vci*] | *vpi/vci* }]] command to check information about a PVC group.

----End

Example

Run the **display atm pvc-info** command. The command output shows PVC status and ATM interface status.

```
<Huawei> display atm pvc-info
Atm2/0/0, VPI: 0, VCI: 35, Name: ipoa, INDEX: 2
  AAL5 Encaps: SNAP, Protocol: IP
```

```
  Service-type:UBR
  input pkts: 0, input bytes: 0, input pkt errors: 0
  output pkts: 0, output bytes: 0, output pkt errors: 0
  Interface State: DOWN, PVC State: DOWN
```

Run the **display atm pvc-group** command. The command output shows information about a PVC group, including the VPI/VCI values, PVC name, and group status.

```
<Huawei> display atm pvc-group
PVC-GROUP-NAME    VPI/VCI    STATE ENCAP PROTOCOL INTERFACE
aaa                 3/35     Down  SNAP  None     Atm1/0/0(DOWN)
```

1.4 Configuring ATM Links to Transmit Different Protocol Packets

This section describes how to configure IPoA, IPoEoA, PPPoA, PPPoEoA and ATM transparent bridging.

1.4.1 Establishing the Configuration Task

Before configuring ATM links to transmit different protocol packets, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task quickly and accurately.

Applicable Environment

Currently, ATM links can transmit packets of the following protocols:

- IPoA

  By configuring IPoA mapping on PVCs, you can enable a device to encapsulate IP packets into ATM cells and transmit them over ATM networks. This allows AAL5 to transmit IP protocol packets.

- IPoEoA

  By configuring IPoEoA mapping on PVCs, you can enable PVCs associated with the same Virtual Ethernet (VE) interface to communicate at Layer 2. This allows AAL5 to transmit IPoE protocol packets.

- PPPoA

  By configuring PPPoA mapping on PVCs, you can enable a device to encapsulate PPP packets into ATM cells and transmit them over ATM networks. This allows AAL5 to transmit PPP protocol packets.

- PPPoEoA

  By configuring PPPoEoA mapping on PVCs, you can enable a device to encapsulate PPPoE packets into ATM cells and transmit them over ATM networks. This allows AAL5 to transmit PPPoE protocol packets.

Pre-configuration Tasks

Before configuring ATM links to transmit different protocol packets, complete the following tasks:

- Powering on the router and ensuring that the router detects no error during self-check

- Creating PVCs
- Performing basic configuration of transparent bridging

Data Preparation

To configure ATM links to transmit different protocol packets, you need the following data.

No.	Data
1	Number of an ATM interface or a sub-interface
2	IP address and mask of the ATM interface or sub-interface
3	Name and VPI/VCI values of each PVC
4	AAL5 encapsulation type
5	Number of a VE interface
6	Virtual template number
7	IP address and mask of the virtual template

1.4.2 Configuring IPoA Mapping on PVCs

IPoA mapping on PVCs enables a device to encapsulate IP packets into ATM cells and transmit them over ATM networks.

Prerequisites

Before creating PVCs and configuring IPoA mapping on PVCs, complete the following configurations:

- Configuring physical attributes for ATM interfaces on the router

Context

Configure IPoA mapping on PVCs to allow AAL5 to transmit IP protocol packets.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface atm interface-number[.subinterface ]
```

The ATM interface or sub-interface view is displayed.

Step 3 Run:

```
pvc { pvc-name [ vpi/vci ] | vpi/vci }
```

A PVC is created and the PVC view is displayed.

NOTE

- The VCI values 3 and 4 are reserved.
- The VPI and VCI values cannot be both 0s.

Step 4 Run:

```
encapsulation aal5snap
```

The AAL5 encapsulation type is specified for the PVC.

The AAL5 encapsulation type can be **aal5snap** or **aal5mux**. The default value is **aal5snap**.

If **aal5mux** is configured as the AAL5 encapsulation type, InARP cannot be enabled. If InARP has been enabled, disable InARP before setting the AAL5 encapsulation type to **aal5mux** for PVCs.

Step 5 Run:

```
map ip { ip-address | default | inarp [ minutes ] } [ broadcast ]
```

IPoA mapping is configured.

NOTE

One IP address cannot be mapped to multiple ATM interfaces or sub-interfaces on the same device as this interrupts traffic forwarding.

If the PVC needs to transmit broadcast IP packets, **broadcast** must be configured.

CAUTION

The IP address specified in this command must be the IP address of the peer interface. Otherwise, data cannot be correctly forwarded.

----End

1.4.3 Configuring IPoEoA Mapping on PVCs

IPoEoA mapping on PVCs allows AAL5 to transmit IPoE protocol packets.

Prerequisites

Before creating PVCs and configuring IPoEoA mapping on PVCs, complete the following configurations:

- Configuring physical attributes for ATM interfaces on the router
- Creating a VE interface and configuring an IP address and a mask for the interface

Context

IPoEoA mapping on PVCs enables PVCs associated with the same VE interface to communicate at Layer 2.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface virtual-ethernet interface-number
```

A VE interface is created and the VE interface view is displayed.

Step 3 Run:

```
quit
```

The system view is displayed.

Step 4 Run:

```
interface atm interface-number [.subinterface ]
```

The ATM interface or sub-interface view is displayed.

Step 5 Run:

```
pvc { pvc-name [ vpi/vci ] | vpi/vci }
```

A PVC is created and the PVC view is displayed.

Step 6 Run:

```
encapsulation aal5-encap
```

The AAL5 encapsulation type is specified for the PVC.

The AAL5 encapsulation type can be **aal5snap** or **aal5mux**. The default value is **aal5snap**.

Step 7 Run:

```
map bridge virtual-ethernet interface-number
```

IPoEoA mapping is configured.

----End

1.4.4 Configuring PPPoA Mapping on PVCs in Permanent Online Mode

PPPoA mapping on PVCs enables a device to encapsulate PPP packets into ATM cells and transmit them over ATM networks.

Context

Configuring PPPoA mapping on PVCs allows AAL5 to transmit PPP protocol packets.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface virtual-template vt-number
```

A VT interface is created and the VT interface view is displayed.

Step 3 Configure the IP address of the VT interface.

- Configure the IPv4 address of the VT interface.
  - Assign an IP address to the VT interface.

    Run:

    ```
    ip address ip-address { mask | mask-length }
    ```

    An IP address is assigned to the VT interface.
  - Configure the VT interface to obtain an IP address from the remote end.

    Run:

    ```
    ip address ppp-negotiate
    ```

    The VT interface is configured to obtain an IP address from the remote end.
- Configure the IPv6 address of the VT interface.

  Run:

  ```
  ipv6 address { ipv6-address prefix-length | ipv6-address/prefix-length }
  ```

  An IPv6 address is assigned to the VT interface.

  NOTE

  Before assigning an IPv6 address to an interface, run the **ipv6** command in the system view to enable IPv6 packet forwarding and run the **ipv6 enable** command on the interface to enable IPv6.

Step 4 Run:

```
quit
```

The system view is displayed.

Step 5 Run:

```
interface atm interface-number[.subinterface ]
```

The ATM interface or sub-interface view is displayed.

Step 6 Run:

```
pvc { pvc-name [ vpi/vci ] | vpi/vci }
```

A PVC is created and the PVC view is displayed.

Step 7 Run:

```
encapsulation aal5-encap
```

The AAL5 encapsulation type is specified for the PVC.

The AAL5 encapsulation type can be **aal5snap** or **aal5mux**. The default value is **aal5snap**.

Step 8 Run:

```
map ppp virtual-template vt-number
```

PPPoA mapping is configured on the PVC.

----End

1.4.5 Configuring PPPoA Mapping on a PVC Using On-demand Dialing

PPPoA mapping on a PVC enables the router to encapsulate PPP packets into ATM cells and transmit them over an ATM network. To reduce traffic, configure PPPoA mapping using on-demand dialing.

Context

Configure PPPoA mapping on a PVC using the following methods:

- Permanent online
- On-demand dialing

In on-demand dialing mode, a PVC is terminated after it becomes idle for a period of time and is re-established when traffic needs to be transmitted. In permanent online mode, a PVC is always functioning after it is configured. Using a PVC in on-demand rather than permanent online dialing mode reduces traffic.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Configure a dialer interface. Refer to **4.4.2 Configuring a Dialer Interface** in **4 PPPoE Configuration**.

Step 3 Run:

```
dialer timer idle seconds
```

The maximum link idle time is set.

By default, the maximum link idle time is 120 seconds.

The configured link idle time determines the maximum idle time of a PPPoA connection established in on-demand dialing mode. A PPPoA connection is terminated when the maximum link idle time expires.

This command affects only new calls but not the established calls.

Step 4 Run:

```
quit
```

Return to the system view.

Step 5 Run:

```
interface atm interface-number[.subinterface ]
```

The ATM interface or sub-interface view is displayed.

Step 6 Run:

```
pvc { pvc-name [ vpi/vci ] | vpi/vci }
```

A PVC is created and the PVC view is displayed.

Step 7 Run:

```
encapsulation aal5-encap
```

The AAL5 encapsulation type is set for the PVC.

The AAL5 encapsulation type of a PVC can be **aal5snap** or **aal5mux**. By default, the AAL5 encapsulation type is **aal5snap**.

Step 8 Run:

```
map ppp dialer number
```

PPPoEoA mapping is configured on the PVC.

----End

1.4.6 Configuring PPPoEoA Mapping on a PVC

PPPoEoA mapping on a PVC enables the AR2200 to encapsulate PPPoE packets into ATM cells and transmit them over an ATM network.

Context

After PPPoEoA mapping is configured on a PVC, PPPoE packets can be transmitted over ATM Adaptation Layer 5 (AAL5).

PPPoEoA uses the client/server model. A PPPoEoA client sends a connection request to the PPPoEoA server. After the client and server complete negotiation, the server provides access control and authentication functions.

The AR2200 functions as a PPPoEoA client.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Configure a dialer interface. Refer to **4.4.2 Configuring a Dialer Interface** in **4 PPPoE Configuration**.

Step 3 Run:

```
interface virtual-ethernet interface-number
```

A VE interface is created and the VE interface view is displayed.

Step 4 Run:

```
pppoe-client dial-bundle-number number [ on-demand ] [ no-hostuniq ]
```

A PPPoE session is created and the dialer bundle is specified for the session.

Step 5 Run:

```
quit
```

Return to the system view.

Step 6 Run:

```
interface atm interface-number[.subinterface ]
```

The ATM interface view or ATM sub-interface view is displayed.

Step 7 Run:

```
pvc { pvc-name [ vpi/vci ] | vpi/vci }
```

A PVC is created and the PVC view is displayed.

Step 8 Run:

```
map bridge virtual-ethernet interface-number
```

PPPoEoA mapping is configured on the PVC.

----End

1.4.7 Configuring ATM Transparent Bridging

ATM transparent bridging allows devices on two Ethernet networks to communicate with each other through ATM links.

Context

If devices on two Ethernet networks need to communicate with each other through ATM links, the specified PVCs must be enabled to send and receive bridge packets carrying Ethernet packets.

NOTE

On an ATM interface, only one PVC is allowed to send and receive bridge packets. If a PVC is deleted, the configuration (sending and receiving bridge packets) of the PVC will also be automatically deleted.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface atm interface-number[.subinterface ]
```

The ATM interface or sub-interface view is displayed.

Step 3 Run:

```
pvc { pvc-name [ vpi/vci ] | vpi/vci }
```

A PVC is created and the PVC view is displayed.

NOTE

- The VCI values 3 and 4 are reserved.
- The VPI and VCI values cannot be both 0s.
- The PVC occupied by PVC-Group can't be configured.

Step 4 Run:

```
map bridge broadcast
```

The PVC is configured to send and receive bridge packets.

NOTE

The bridge must be enabled before **map bridge broadcast** command.

----End

1.4.8 Checking the Configuration

After configuring ATM links to transmit different protocol packets, you can view configurations and status of ATM interfaces or sub-interfaces, information about PVCs and PVC mapping, and status and statistics of VE interfaces.

Prerequisites

The configurations of ATM links to transmit different protocol packets are complete.

Procedure

- Run the **display atm pvc-info** [**interface atm** *interface-number* [**pvc** { *pvc-name* [*vpi*/*vci*] | *vpi*/*vci* }]] command to check information about PVCs.
- Run the **display atm map-info** [**interface atm** *interface-number* [**pvc** { *pvc-name* [*vpi*/*vci*] | *vpi*/*vci* }]] command to check information about PVC mapping.
- Run the **display interface virtual-ethernet** [*interface-number*] command to check status and statistics of VE interfaces.

----End

Example

Run the **display atm pvc-info** command. The command output shows PVC status and ATM interface status.

```
<Huawei> display atm pvc-info
Atm2/0/0, VPI: 0, VCI: 35, Name: ipoa, INDEX: 2
  AAL5 Encaps: SNAP, Protocol: IP
  Service-type:UBR
  input pkts: 0, input bytes: 0, input pkt errors: 0
  output pkts: 0, output bytes: 0, output pkt errors: 0
  Interface State: DOWN, PVC State: DOWN
```

After PVC mapping is successfully configured, the VE interface goes Up.

```
<Huawei> display interface virtual-ethernet 0/0/1
Virtual-Ethernet0/0/1 current state : UP
Line protocol current state : UP
Description:HUAWEI, AR Series, Virtual-Ethernet0/0/1 Interface
Route Port, The Maximum Transmit Unit is 1500
Internet Address is 10.1.1.1/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-fc7a-9e15
Current system time: 2010-10-10 14:39:45
  Input bandwidth utilization  : 5.00%
  Output bandwidth utilization : 6.00%
```

1.5 Configuring the Service Type of PVC

This section describes how to configure the service type, OAM F5 loopback, and VP policing for a PVC.

1.5.1 Establishing the Configuration Task

Before configuring TOS, OAM and VP values for a PVC, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task quickly and accurately.

Applicable Environment

In the practical networking, to configure the service type and the related parameters of a PVC (including the PVCs in the PVC-Group), you must configure service cbr, vbr or ubr of PVC.

Configure VP parameters to implement VP policing on ATM interfaces.

Pre-configuration Tasks

Before configuring the service types or OAM parameters of a PVC, complete the following tasks:

- Configuring physical attributes for the ATM interface
- Configuring an IP address and mask for the ATM interface or sub-interface
- Creating a PVC and configuring application modes

Before configuring the parameters of VP policing of ATM interface, complete the following tasks:

- Configuring the physical attributes for the ATM interface of a router
- Configuring the IP address and mask of the sub-interface

Data Preparation

To configure the service type of PVC, you need the following data.

No.	Data
1	Number of the ATM interface or sub-interface
2	IP address and mask of the ATM interface or sub-interface
3	PVC name, network VPI and VCI
4	cbr: Peak rate of outputting ATM cells, variation range of cell delays
5	vbr: Peak rate of outputting ATM cells, maintainable rate and maximum burst size
6	vbr-rt: Peak rate of outputting ATM cells, maintainable rate and maximum burst size

To configure VP policing, you need the following data.

No.	Data
1	Number of the ATM sub-interface
2	IP address and mask of the ATM interface
3	ATM network VPI
4	VP traffic

1.5.2 Configuring the Service Type of a PVC

The ATM layer provides the following types of services: Specified Bit Rate (SBR) services, Unspecified Bit Rate (UBR) services, Real-Time Variable Bit Rate (VBR-rt) services, and Non-Real-Time Variable Bit Rate (VBR-nrt) services.

Context

The PVC service type cannot be configured for a G.SHDSL interface working in ATM mode.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface atm interface-number[.subinterface ]
```

The ATM interface or the sub-interface view is displayed.

Step 3 Run:

```
pvc { pvc-name [ vpi/vci ] | vpi/vci }
```

A PVC is created and the PVC view is displayed.

Step 4 Choose the following steps to configure the service type of the PVC and related rate parameters.

By default, the service type is UBR after a PVC is created.

- Run the **service cbr** *output-pcr* command to set the service type to Constant Bit Rate (CBR)
- Run the **service ubr** command to set the service type to Unspecified Bit Rate (UBR).
- Run the **service vbr-nrt** *output-pcr output-scr output-mbs* command to set the service type to Variable Bit Rate-Non Real Time (VBR-NRT).
- Run the **service vbr-rt** *output-pcr output-scr output-mbs* command to set the service type to Variable Bit Rate-Real Time (VBR-RT)

----End

1.5.3 Configuring VP Policing

By configuring VP policing, you can set the normal volume of traffic on a VP.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface atm interface-number
```

The ATM interface is displayed.

Step 3 Run:

```
pvp limit vpi peak-rate
```

The parameters of VP policing are configured.

NOTE

If an ATM interface that has sub-interfaces is configured with VP policing, the VP policing is valid for all the PVCs with the same VPI.

----End

1.5.4 Checking the Configuration

After service type of PVC and the OAM and VP parameters are configured for a PVC, you can view the configuration and status of the ATM interface or its sub-interface, PVC information.

Prerequisites

The configurations of the service type of PVC and the OAM and VP parameters are complete.

Procedure

- Run the **display atm pvc-info** [**interface atm** *interface-number* [**pvc** { *pvc-name* [*vpi*/*vci*] | *vpi*/*vci* }]] command to check information about the PVC.

----End

1.6 Configuring ATM OAM

OAM can detect faults, locate faults, and evaluate network performance without interrupting services. OAM provides network information by encapsulating OAM cells in standard format into user cell flows.

1.6.1 Establishing the Configuration Task

Before configuring ATM OAM, you need to familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task quickly and accurately.

Applicable Environment

On an ATM network, to detect faults without interrupting services, configure ATM OAM.

ITU-T I.610 defines the following OAM levels on the ATM network:

- F1: regenerator section level
- F2: digital section level
- F3: transmission path level
- F4: virtual path level
- F5: virtual channel level

The AR2200 transmits OAM flows F5.

NOTE

G.SHDSL interfaces working in ATM mode support ATM OAM features, whereas ADSL interfaces do not support ATM OAM features.

Pre-configuration Tasks

Before configuring ATM OAM, complete the following tasks:

- Configuring physical attributes for the ATM interface on the router
- Configuring an IP address and a mask for the ATM interface
- Configuring an ATM PVC

Data Preparation

To configure ATM OAM, you need the following data.

No.	Data
1	● PVC where OAM F5 loopback cell transmission and retransmission detection are enabled ● Number of OAM F5 loopback cells ● Interval at which OAM F5 loopback cells are sent during retransmission detection before the PVC status changes
2	PVC and direction where CC is enabled
3	● PVC where AIS/RDI cell detection is enabled ● AIS/RDI cell detection parameters
4	● Number of the interface on which connectivity of the ATM link needs to be detected ● Connectivity test parameters

1.6.2 Configuring OAM F5 Loopback

OAM F5 loopback cells detect connectivity on the ATM network.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface atm interface-number [.subinterface-number ]
```

The ATM interface or sub-interface view is displayed.

Step 3 Run:

```
pvc { pvc-name [ vpi/vci ] | vpi/vci }
```

The PVC view is displayed.

Step 4 Run:

```
oam loopback [ up up-count down down-count retry-frequency retry-frequency ]
```

OAM F5 loopback cell transmission and retransmission detection are enabled.

By default, the AR2200 does not send OAM F5 loopback cells, but the AR2200 must respond to the received OAM F5 loopback cells.

After OAM F5 loopback cell transmission and retransmission detection are enabled, the PVC status changes only when a certain number of OAM F5 loopback cells are received. For example, when the AR2200 receives consecutive OAM F5 loopback cells of a number specified by *up-count*, the PVC becomes Up. When the AR2200 does not receive consecutive OAM F5 loopback cells of a number specified by *down-count*, the PVC becomes Down. *retry-frequency* specifies the interval at which OAM F5 loopback cells are sent.

----End

1.6.3 Configuring OAM CC

Connectivity check (CC) enables the AR2200 to periodically insert CC cells into cell flows. If CC cells are transmitted successfully, connectivity is normal.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface atm interface-number [.subinterface-number ]
```

The ATM interface or sub-interface view is displayed.

Step 3 Run:

```
pvc { pvc-name [ vpi/vci ] | vpi/vci }
```

The PVC view is displayed.

Step 4 Run:

```
oam cc end-to-end { both | sink | source }
```

OAM CC is enabled.

By default, OAM CC is disabled.

NOTE

When you configure CC, if **source** or **both** is configured on one end, **sink** or **both** must be configured on the other end.

----End

1.6.4 Configuring AIS/RDI Cell Detection

An AIS cell is sent to notify the downstream device that the upstream device is faulty. An RDI cell is sent to notify the upstream device that the downstream device is unreachable.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface atm interface-number [.subinterface-number ]
```

The ATM interface or sub-interface view is displayed.

Step 3 Run:

```
pvc { pvc-name [ vpi/vci ] | vpi/vci }
```

The PVC view is displayed.

Step 4 Run:

```
oam ais-rdi [ up up-count down down-count ]
```

AIS/RDI cell detection is enabled.

By default, AIS or RDI detection is enabled.

After AIS or RDI cell detection is enabled, if the AR2200 receives AIS/RDI cells of a number specified by *down-count*, the PVC becomes Down. If the AR2200 does not receive AIS/RDI cells in the consecutive interval specified by *up-count*, the PVC becomes Up.

----End

1.6.5 Detecting Connectivity of an ATM Link

The AR2200 can send OAM cells on a PVC of a specified ATM interface to determine connectivity of the ATM link. If no ATM response message is received within the timeout interval, packets are lost on the ATM link because the ATM link is unreachable or busy.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface atm interface-number [.subinterface-number ]
```

The ATM interface or sub-interface view is displayed.

Step 3 Run:

```
oamping pvc { pvc-name | vpi/vci } [ number timeout ]
```

Connectivity of an ATM link on a specified ATM interface is detected.

----End

1.6.6 Checking the Configuration

After ATM OAM is configured, you can check the configuration.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface atm interface-number [. subinterface-number ]
```

The ATM interface or sub-interface view is displayed.

Step 3 Run:

```
display this
```

The connectivity test result on the ATM link and relevant parameters are displayed.

----End

1.7 Maintaining ATM Configuration

This section describes how to maintain ATM. Detailed operations include clearing statistics on an ATM interface.

1.7.1 Clearing the ATM Interface Statistics

You can run the reset commands to clear interface statistics before recollecting traffic statistics on the interface.

Context

CAUTION

The statistics data cannot be restored after you clear it. Confirm the action before you use the command.

To reset the interface statistics of the Network Management System (NMS) or that displayed by running the **display interface** command, run the following commands in the user view.

NOTE

For more information about the display of interface statistics in the NMS, see related NMS manuals.

Procedure

Step 1 Run the **reset counters interface** [**atm** [*interface-number*]] command to clear the interface statistics displayed by running the **display interface** command.

Step 2 Run the **reset counters if-mib interface** [**atm** [*interface-number*]] command to clear the interface statistics in the NMS.

Step 3 Run the **reset atm interface** [**atm** *interface-number*] command to clear the ATM interface statistics.

----End

1.8 Configuration Examples

This section provides several examples for configuring ATM. These configuration examples explain the networking requirements, configuration roadmap, data preparation, configuration procedure, and configuration files.

1.8.1 Example for Configuring IPoA

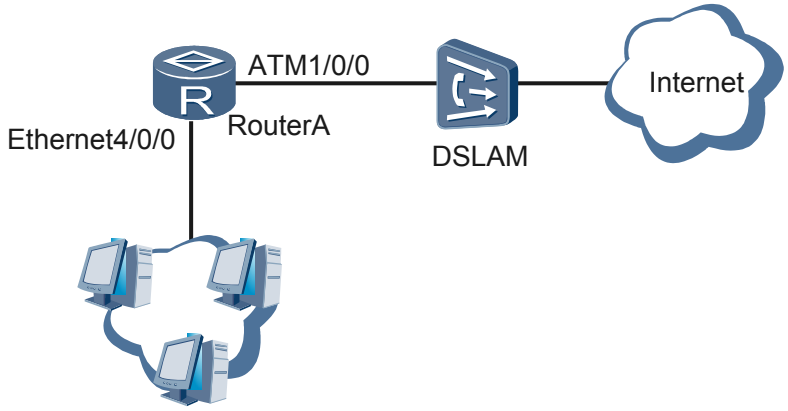
This section describes how to configure IPoA on the AR2200.

Networking Requirements

In IPoA application, IP packets are transmitted on an ATM network. The ATM network provides the data link layer to transmit data between IP hosts on the same network. IP packets are encapsulated in ATM cells. As the bearer network of IP services, the ATM network ensures network performance and provides QoS guarantee for IP services.

As shown in **Figure 1-1**, users on an enterprise network connect to a Layer 2 Ethernet interface of RouterA (an AR2200), which functions as the gateway on the enterprise network. A DSLAM connects the ADSL interface of RouterA to the Internet. IPoA application needs to be implemented.

Figure 1-1 Networking diagram of IPoA application



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the LAN side so that users on the enterprise network can connect to RouterA through the Layer 2 Ethernet interface.
2. Configure the WAN side so that RouterA can use the ADSL interface to communicate with the DSLAM.

Data Preparation

To complete the configuration, you need the following data:

- On the LAN side:
  - VLAN ID allowed by the Ethernet interface: 200
  - IP address of the VLANIF interface corresponding to the allowed VLAN ID: 22.0.0.1/24
- On the WAN side:
  - IP address of the ADSL interface: 23.0.0.1/24
  - PVC name: ipoa
  - PVC number: 0/35
  - IPoA mapping on the PVC (remote IP address 23.0.0.2/24)

Procedure

Step 1 Configure RouterA.

Configure the LAN side.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface ethernet 4/0/0
[RouterA-Ethernet4/0/0] port link-type trunk
[RouterA-Ethernet4/0/0] port trunk allow-pass vlan 200
[RouterA-Ethernet4/0/0] undo port trunk allow-pass vlan 1
[RouterA-Ethernet4/0/0] quit
[RouterA] vlan 200
[RouterA-vlan200] quit
[RouterA] interface vlanif 200
[RouterA-Vlanif200] ip address 22.0.0.1 255.255.255.0
[RouterA-Vlanif200] quit
```

Create a PVC and configure IPoA mapping on the PVC.

```
[RouterA] interface atm 1/0/0
[RouterA-Atm1/0/0] ip address 23.0.0.1 255.255.255.0
[RouterA-Atm1/0/0] pvc ipoa 0/35
[RouterA-atm-pvc-Atm1/0/0-0/35-ipoa] map ip 23.0.0.2
[RouterA-atm-pvc-Atm1/0/0-0/35-ipoa] quit
[RouterA-Atm1/0/0] quit
```

Step 2 Configure the DSLAM.

See the DSLAM documentation.

Step 3 Verify the configuration.

After the configuration is complete, RouterA can ping the remote IP address 23.0.0.2/24.

```
[RouterA] ping 23.0.0.2
PING 23.0.0.2: 56  data bytes, press CTRL_C to break
    Reply from 23.0.0.2: bytes=56 Sequence=1 ttl=255 time=2 ms
    Reply from 23.0.0.2: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 23.0.0.2: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 23.0.0.2: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 23.0.0.2: bytes=56 Sequence=5 ttl=255 time=1 ms
  --- 23.0.0.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
```

```
0.00% packet loss
round-trip min/avg/max = 1/1/2 ms
```

----End

Configuration Files

- Configuration file of RouterA

```
#
 sysname RouterA
#
 interface Atm1/0/0
  ip address 23.0.0.1 255.255.255.0
  pvc ipoa 0/35
   map ip 23.0.0.2
#
interface
Ethernet4/0/0
 port link-type
trunk
 undo port trunk allow-pass vlan
1
 port trunk allow-pass vlan
200
#
 vlan batch 200
#
interface
Vlanif200
 ip address 22.0.0.1
255.255.255.0
#
return
```

1.8.2 Example for Configuring IPoEoA

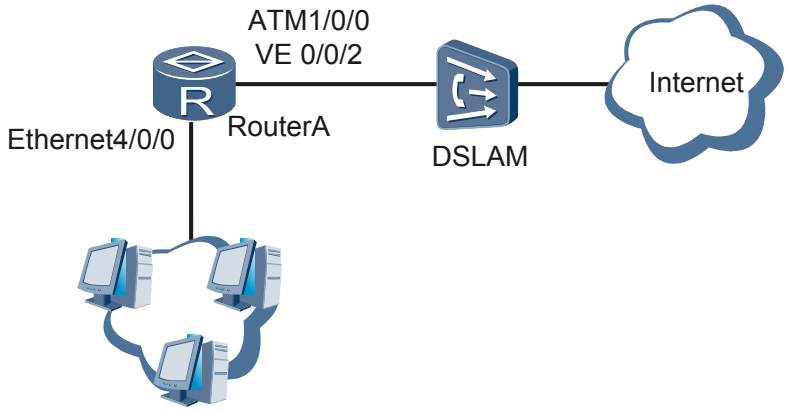
This section describes how to configure IPoEoA on the AR2200.

Networking Requirements

In IPoEoA application, IP packets are encapsulated in Ethernet frames and Ethernet frames are encapsulated in ATM cells.

As shown in **Figure 1-2**, users on an enterprise network connect to a Layer 2 Ethernet interface of RouterA (an AR2200), which functions as the gateway on the enterprise network. A DSLAM connects the ADSL interface of RouterA to the Internet. Before IP packets are sent out from the ADSL interface of RouterA, they are encapsulated in Ethernet frames on a VE interface. The Ethernet frames are then transmitted over an ATM network.

Figure 1-2 Networking diagram of IPoEoA application



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the LAN side so that users on the enterprise network can connect to RouterA through the Layer 2 Ethernet interface.
2. Configure the WAN side so that RouterA can use the ADSL interface to communicate with the DSLAM.

Data Preparation

To complete the configuration, you need the following data:

- On the LAN side:
  - VLAN ID allowed by the Ethernet interface: 200
  - IP address of the VLANIF interface corresponding to the allowed VLAN ID: 22.0.0.1/24
- On the WAN side:
  - IP address of the VE interface: 26.0.0.1/24
  - PVC name: ipoeoa
  - PVC number: 25/45
  - IPoEoA mapping on the PVC

Procedure

Step 1 Configure RouterA.

Configure the LAN side.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface ethernet 4/0/0
[RouterA-Ethernet4/0/0] port link-type trunk
[RouterA-Ethernet4/0/0] port trunk allow-pass vlan 200
[RouterA-Ethernet4/0/0] undo port trunk allow-pass vlan 1
[RouterA-Ethernet4/0/0] quit
[RouterA] vlan 200
```

```
[RouterA-vlan200] quit
[RouterA] interface vlanif 200
[RouterA-Vlanif200] ip address 22.0.0.1 255.255.255.0
[RouterA-Vlanif200] quit
```

Configure the WAN side.

```
[RouterA] interface virtual-ethernet 0/0/2
[RouterA-Virtual-Ethernet0/0/2] ip address 26.0.0.1 255.255.255.0
[RouterA-Virtual-Ethernet0/0/2] quit
[RouterA] interface atm 1/0/0
[RouterA-Atm1/0/0] ip address 23.0.0.1 255.255.255.0
[RouterA-Atm1/0/0] pvc ipoeoa 25/45
[RouterA-atm-pvc-Atm1/0/0-25/45-ipoeoa] map bridge virtual-ethernet 0/0/2
[RouterA-atm-pvc-Atm1/0/0-25/45-ipoeoa] quit
[RouterA-Atm1/0/0] quit
```

Step 2 Configure the DSLAM.

See the DSLAM documentation.

Step 3 Verify the configuration.

After the configuration is complete, RouterA can ping the upstream device. Assume that the IP address of the upstream device connected to the DSLAM is 26.0.0.2.

```
[RouterA] ping 26.0.0.2
PING 26.0.0.2: 56  data bytes, press CTRL_C to break
    Reply from 26.0.0.2: bytes=56 Sequence=1 ttl=255 time=2 ms
    Reply from 26.0.0.2: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 26.0.0.2: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 26.0.0.2: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 26.0.0.2: bytes=56 Sequence=5 ttl=255 time=1 ms
  --- 26.0.0.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/2 ms
```

----End

Configuration Files

- Configuration file of RouterA

```
#
 sysname RouterA
#
 interface Virtual-Ethernet0/0/2
  ip address 26.0.0.1 255.255.255.0
#
 interface Atm1/0/0
  ip address 23.0.0.1 255.255.255.0
  pvc ipoeoa 25/45
   map bridge Virtual-Ethernet 0/0/2
#
interface
Ethernet4/0/0
 port link-type
trunk
 undo port trunk allow-pass vlan
1
 port trunk allow-pass vlan
200
#
 vlan batch 200
#
interface
Vlanif200
```

```
 ip address 22.0.0.1
255.255.255.0
#
return
```

1.8.3 Example for Configuring Permanent Online PPPoA

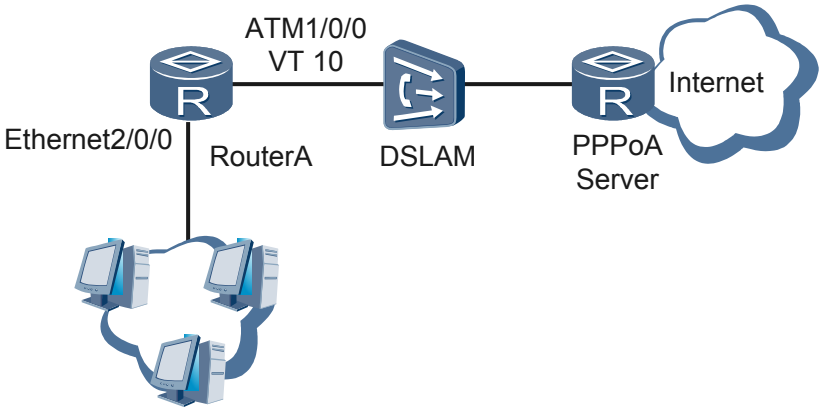
This section describes how to configure PPPoA on the AR2200.

Networking Requirements

In PPPoA application, PPP packets are encapsulated in ATM cells, and IP packets and other protocol packets are encapsulated in PPP packets. PPPoA packet transmission is controlled by the PPP protocol, which is flexible and supports a variety of applications.

As shown in **Figure 1-3**, users on an enterprise network connect to a Layer 3 Ethernet interface of RouterA (an AR2200), which functions as the gateway on the enterprise network. A DSLAM connects the ADSL interface of RouterA to the Internet. IP packets sent from the enterprise network are encapsulated in PPP packets and forwarded by the ADSL interface to the Internet.

Figure 1-3 Networking diagram of PPPoA application



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the LAN side so that users on the enterprise network can connect to RouterA through the Layer 3 Ethernet interface.
2. Configure the WAN side so that IP packets sent from the enterprise network are encapsulated in PPP packets and RouterA can use the ADSL interface to communicate with the DSLAM.

Data Preparation

To complete the configuration, you need the following data:

- On the LAN side:
  - IP address of the Layer 3 Ethernet interface: 22.0.0.1/24

- On the WAN side:
  - PPPoA client: RouterA
  - Virtual template (VT) interface ID: 10
  - IP address of the VT interface: negotiated
  - Authentication mode: PAP authentication (user name **pppoa**; password **huawei**)
  - PVC name: pppoa
  - PVC number: 35/53
  - PPPoA mapping on the PVC

Procedure

Step 1 Configure RouterA.

Configure the LAN side.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface ethernet 2/0/0
[RouterA-Ethernet2/0/0] ip address 22.0.0.1 255.255.255.0
[RouterA-Ethernet2/0/0] quit
```

Configure the WAN side.

```
[RouterA] interface virtual-template 10
[RouterA-Virtual-Template10] ppp pap local-user pppoa password simple huawei
[RouterA-Virtual-Template10] ip address ppp-negotiate
[RouterA-Virtual-Template10] quit
[RouterA] interface atm 1/0/0
[RouterA-Atm1/0/0] pvc pppoa 35/53
[RouterA-atm-pvc-Atm1/0/0-35/53-pppoa] map ppp virtual-template 10
[RouterA-atm-pvc-Atm1/0/0-35/53-pppoa] quit
[RouterA-Atm1/0/0] quit
```

Step 2 Configure the DSLAM.

See the DSLAM documentation.

Step 3 Configure the PPPoA server.

Assign IP address 23.0.0.2 to the PPPoA server and configure the PPPoA server to assign IP address 23.0.0.1 to the PPPoA client (RouterA). Set the authentication mode to PAP authentication, and set the user name and password to be the same as those configured on RouterA.

Step 4 Verify the configuration.

- Run the **display interface virtual-template** command to check whether the VT interface on RouterA has been assigned the correct IP address.

  ```
  [RouterA] display interface virtual-template 10
  ```

  The following information indicates that the VT interface has been assigned the correct IP address.

  ```
  Internet Address is negotiated, 23.0.0.1/32
  ```

- Run the **display virtual-access** command to view the PPP negotiation status of the virtual access interface created using the VT.

  ```
  [RouterA] display virtual-access
  ```

  The following information indicates that PPP negotiation is successful on the virtual access interface.

  ```
  LCP opened, IPCP opened
  ```

- RouterA can ping the PPPoA server.

```
[RouterA] ping 23.0.0.2
PING 23.0.0.2: 56  data bytes, press CTRL_C to break
    Reply from 23.0.0.2: bytes=56 Sequence=1 ttl=255 time=2 ms
    Reply from 23.0.0.2: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 23.0.0.2: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 23.0.0.2: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 23.0.0.2: bytes=56 Sequence=5 ttl=255 time=1 ms
  --- 23.0.0.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/2 ms
```

----End

Configuration Files

- Configuration file of RouterA

```
#
 sysname RouterA
#
 interface Virtual-Template10
  ppp pap local-user pppoa password simple huawei
  ip address ppp-negotiate
#
 interface Atm1/0/0
  pvc pppoa 35/53
   map ppp Virtual-Template10
#
 interface
Ethernet2/0/0
  ip address 22.0.0.1
255.255.255.0
#
return
```

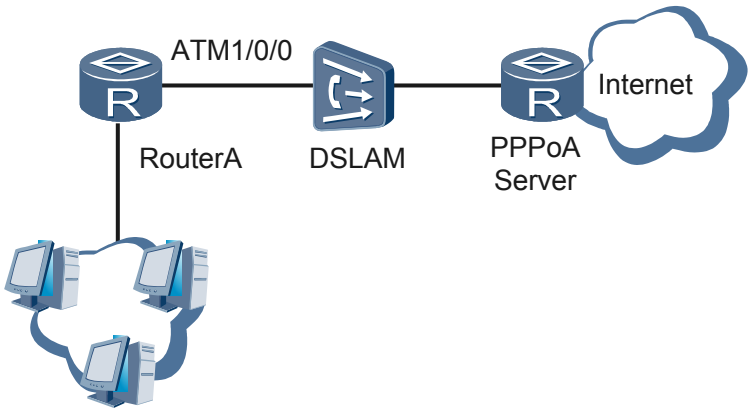
1.8.4 Example for Configuring PPPoA in On-demand Dialing Mode

This section describes how to configure the AR2200 as a PPPoA client working in on-demand dialing mode.

Networking Requirements

As shown in **Figure 1-4**, all users on an enterprise network use the IP address of an Ethernet interface on RouterA (an AR2200) as the gateway address. RouterA uses an ADSL interface to connect to a DSLAM and functions as a PPPoA client to communicate with the PPPoA server. The PPPoA server performs CHAP authentication. After the link between the PPPoA client and PPPoA server becomes idle for a period of time, the PPPoA client is automatically disconnected and then connected again when traffic needs to be transmitted.

Figure 1-4 Networking diagram of PPPoA application



Configuration Roadmap

The configuration roadmap is as follows:

- Configure a dialer interface.
- Configure an ATM interface.
- Configure a static route from the local end to the PPPoA server.

Data Preparation

To complete the configuration, you need the following data:

- Dialer interface: dial rule number 10 (allowing all IP packets to pass through), dialer interface number 1, dial user name u1, dialer access group number 10, dialer interface IP address to be allocated by the server, CHAP user name usera, CHAP password huawei in plain text, maximum link idle time 90 seconds, and interface buffer queue length 8
- ATM interface: ATM interface number, PVC name pppoa, PVC number 2/40, and on-demand PPPoA mapping on the PVC
- Static route: destination address 21.0.0.2, 24-bit mask length, and outbound interface Dialer 1

Procedure

Step 1 Configure RouterA.

Configure a dialer interface.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] dialer-rule
[RouterA-dialer-rule] dialer-rule 10 ip permit
[RouterA-dialer-rule] quit
[RouterA] interface dialer 1
[RouterA-Dialer1] dialer user u1
[RouterA-Dialer1] dialer-group 10
[RouterA-Dialer1] dialer bundle 12
[RouterA-Dialer1] ip address ppp-negotiate
[RouterA-Dialer1] link-protocol ppp
[RouterA-Dialer1] ppp chap user usera
[RouterA-Dialer1] ppp chap password simple huawei
```

```
[RouterA-Dialer1] dialer timer idle 90
INFO:  The configuration will become effective after link reset.
[RouterA-Dialer1] dialer queue-length 8
[RouterA-Dialer1] quit
```

Configure an ATM interface.

```
[RouterA] interface atm 1/0/0
[RouterA-Atm1/0/0] pvc pppoa 2/40
[RouterA-atm-pvc-Atm1/0/0-2/40-pppoa] map ppp dialer 1
[RouterA-atm-pvc-Atm1/0/0-2/40-pppoa] quit
[RouterA-Atm1/0/0] quit
```

Configure a static route from the local end to the PPPoA server.

```
[RouterA] ip route-static 21.0.0.0 24 dialer 1
```

Step 2 Configure the DSLAM.

See the DSLAM documentation.

Step 3 Configure the PPPoA server.

Assign IP address 21.0.0.2 to the PPPoA server and configure the PPPoA server to assign IP address 21.0.0.1 to the PPPoA client (AR2200A). Set the authentication mode to CHAP authentication, and set the user name and password to be the same as those configured on AR2200A.

Step 4 Verify the configuration.

- Run the **display interface dialer** command to check whether the dialer interface on RouterA has been assigned a correct IP address.

  ```
  [RouterA] display interface dialer 1
  ```

  The following information indicates that the dialer interface has been assigned a correct IP address.

  ```
  Internet Address is negotiated, 21.0.0.1/24
  ```

- Run the **display virtual-access** command to view the PPP negotiation status of the virtual access interface created using the dialer interface.

  ```
  [RouterA] display virtual-access
  ```

  The following information indicates that PPP negotiation is successful on the virtual access interface.

  ```
  LCP opened, IPCP opened
  ```

- RouterA can ping the PPPoEoA server.

  ```
  [RouterA] ping 21.0.0.2
  PING 23.0.0.2: 56  data bytes, press CTRL_C to break
      Reply from 23.0.0.2: bytes=56 Sequence=1 ttl=255 time=2 ms
      Reply from 23.0.0.2: bytes=56 Sequence=2 ttl=255 time=1 ms
      Reply from 23.0.0.2: bytes=56 Sequence=3 ttl=255 time=1 ms
      Reply from 23.0.0.2: bytes=56 Sequence=4 ttl=255 time=1 ms
      Reply from 23.0.0.2: bytes=56 Sequence=5 ttl=255 time=1 ms
    --- 23.0.0.2 ping statistics ---
      5 packet(s) transmitted
      5 packet(s) received
      0.00% packet loss
      round-trip min/avg/max = 1/1/2 ms
  ```

----End

Configuration Files

- Configuration file of RouterA

  ```
  #
   sysname RouterA
  #
  ```

```
dialer-rule
 dialer-rule 10 ip permit
#
interface
Dialer1
 link-protocol
ppp
 ppp chap user
usera
 ppp chap password simple
huawei
 ip address ppp-
negotiate
 dialer user
u1
 dialer bundle
12
 dialer timer idle 90
 dialer queue-length
8
 dialer-group 10
#
 interface Atm1/0/0
  pvc pppoa 2/40
   map ppp Dialer1
#
 ip route-static 21.0.0.0 255.255.255.0 Dialer1
#
return
```

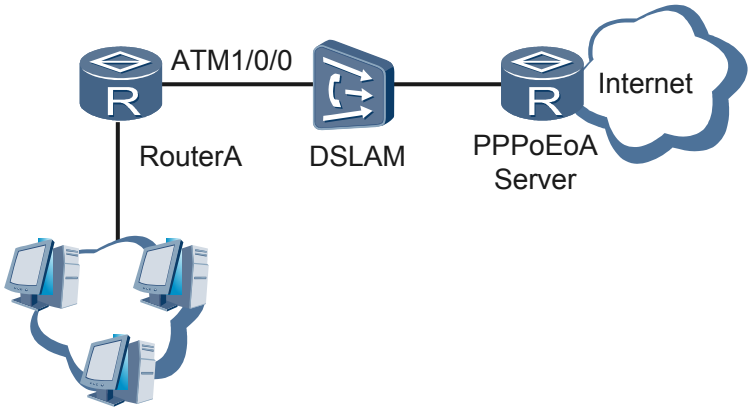
1.8.5 Example for Configuring a PPPoEoA Client

This section describes how to configure the AR2200 as a PPPoEoA client.

Networking Requirements

As shown in **Figure 1-5**, all users on an enterprise network use the IP address of an Ethernet interface on RouterA (an AR2200) as the gateway address. RouterA uses an ADSL interface to connect to a DSLAM and functions as a PPPoEoA client to communicate with the PPPoEoA server. The PPPoEoA server performs CHAP authentication.

Figure 1-5 Networking diagram of PPPoEoA application



Configuration Roadmap

The configuration roadmap is as follows:

- Configure a dialer interface.
- Configure a VE interface.
- Configure an ATM interface and configure PPPoEoA mapping on the ATM interface.
- Configure a static route from the local end to the PPPoEoA server.

Data Preparation

To complete the configuration, you need the following data:

- Dialer interface: interface number, IP address, dialer ACL number, and dialer group number
- VE interface: interface number and dialer bundle number
- ATM interface: PVC name, PVC number, and PPPoEoA mapping on the PVC
- Static route: destination address, mask, and outbound interface

Procedure

Step 1 Configure RouterA.

Configure a dialer interface.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] dialer-rule
[RouterA-dialer-rule] dialer-rule 10 ip permit
[RouterA-dialer-rule] quit
[RouterA] interface dialer 1
[RouterA-Dialer1] dialer user u1
[RouterA-Dialer1] dialer-group 10
[RouterA-Dialer1] dialer bundle 12
[RouterA-Dialer1] ip address ppp-negotiate
[RouterA-Dialer1] link-protocol ppp
[RouterA-Dialer1] ppp chap user usera
[RouterA-Dialer1] ppp chap password simple huawei
[RouterA-Dialer1] quit
```

Configure a VE interface.

```
[RouterA] interface virtual-ethernet 0/0/0
[RouterA-Virtual-Ethernet0/0/0] pppoe-client dial-bundle-number 12
[RouterA-Virtual-Ethernet0/0/0] quit
```

Configure an ATM interface.

```
[RouterA] interface atm 1/0/0
[RouterA-Atm1/0/0] pvc pppoeoa 2/45
[RouterA-atm-pvc-Atm1/0/0-2/45-pppoeoa] map bridge virtual-ethernet 0/0/0
[RouterA-atm-pvc-Atm1/0/0-2/45-pppoeoa] quit
[RouterA-Atm1/0/0] quit
```

Configure a static route.

```
[RouterA] ip route-static 23.0.0.0 24 dialer 1
```

Step 2 Configure the DSLAM.

See the DSLAM documentation.

Step 3 Configure the PPPoEoA server.

Assign IP address 23.0.0.2 to the PPPoEoA server and configure the PPPoEoA server to assign IP address 23.0.0.1 to the PPPoEoA client (RouterA). Set the authentication mode to CHAP authentication, and set the user name and password to be the same as those configured on the RouterA.

Step 4 Verify the configuration.

- Run the **display interface dialer** command to check whether the dialer interface on RouterA has been assigned the correct IP address.

```
[RouterA] display interface dialer 1
```

  The following information indicates that the dialer interface has been assigned the correct IP address.

```
Internet Address is negotiated, 23.0.0.1/32
```

- Run the **display virtual-access** command to view the PPP negotiation status of the virtual access interface created using the dialer interface.

```
[RouterA] display virtual-access
```

  The following information indicates that PPP negotiation is successful on the virtual access interface.

```
LCP opened, IPCP opened
```

- RouterA can ping the PPPoEoA server.

```
[RouterA] ping 23.0.0.2
PING 23.0.0.2: 56  data bytes, press CTRL_C to break
    Reply from 23.0.0.2: bytes=56 Sequence=1 ttl=255 time=2 ms
    Reply from 23.0.0.2: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 23.0.0.2: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 23.0.0.2: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 23.0.0.2: bytes=56 Sequence=5 ttl=255 time=1 ms
  --- 23.0.0.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/2 ms
```

----End

Configuration Files

- Configuration file of RouterA

```
#
 sysname RouterA
#
dialer-rule
 dialer-rule 10 ip permit
#
interface
Dialer1
 link-protocol
ppp
 ppp chap user usera
 ppp chap password simple
huawei
 dialer user
u1
 dialer-group 10
 dialer bundle 12
 ip address ppp-negotiate
#
 interface Virtual-Ethernet0/0/0
  pppoe-client dial-bundle-number 12
#
 interface Atm1/0/0
  pvc pppoeoa 2/45
   map bridge Virtual-Ethernet0/0/0
```

```
#
ip route-static 23.0.0.0 255.255.255.0 Dialer1
return
```

2 FR Configuration

About This Chapter

Frame Relay (FR) is a fast packet switching technology that exchanges data units at the data link layer. Enabled with FR, devices communicate with each other through virtual circuits (VCs).

This section describes how to maintain FR. Detailed operations include clearing FR statistics and enabling FR alarms.

2.10 Configuration Examples

This section provides several examples for configuring FR. These configuration examples explain the networking requirements, configuration roadmap, data preparation, configuration procedure, and configuration files.

2.1 Introduction to FR

FR allows user devices such as routers and hosts to exchange data on an FR network.

Conventional wide area networks (WANs) use X.25, FR, and Asynchronous Transfer Mode (ATM) protocols. Any of these protocols transmits data from one local area network (LAN) over a WAN to another LAN. As terminals become intelligent and the quality of physical links improves, the functions of error control and flow control for data at the data link layer on X.25 networks are no longer required. In addition, limited bandwidth resources on X.25 networks cannot meet requirements of users for services. Due to expensive ATM-capable devices and complicated compatibility, ATM networks are unsuitable for large-scale deployment. Although the bandwidth provided by FR networks is lower than the bandwidth provided by ATM networks, FR networks boast of low delays and costs, and thereby are preferentially used to upgrade X.25 networks.

The Statistical Division Multiplexing (SDM) technique is used to bear multiple types of upper-layer packets on FR networks. If a single FR link cannot provide sufficient bandwidth, and multiple FR physical links exist between devices, you can bundle these FR physical links into a Multilink Frame Relay (MFR) link to increase bandwidth.

DLCI

A DLCI identifies a VC. Currently, a DLCI can identify only a permanent virtual circuit (PVC). The DLCI is not globally unique and applies only to the local and directly-connected interfaces. The same DLCI values on different physical interfaces of an FR network do not indicate the same PVC.

The FR address mapping function associates the protocol address of a peer device with the FR address (DLCI value) of the local device. This helps upper-layer protocols locate a remote device based on the protocol address of the remote device. For example, in the case of IPoFR, when the system sends an IP packet, the system searches the routing table for the next hop address for the packet, and then searches the FR address mapping table for the DLCI value corresponding to the next hop address.

DTE, DCE, UNI, and NNI

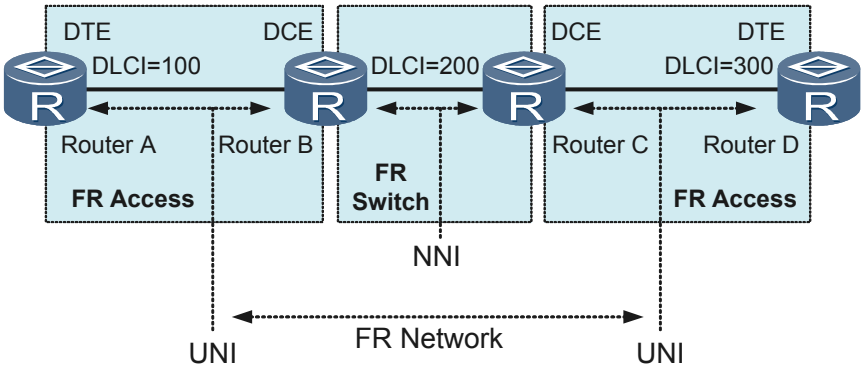
FR networks allow devices to exchange data. Devices and interfaces on FR networks play one of the following roles:

- DTE: data terminal equipment
- DCE: data communication equipment, providing access services for DTE devices
- UNI: user-network interface, interconnecting a DTE device and a DCE device
- NNI: network-network interface, interconnecting DCE devices

An FR network can be a public network, a private network of an enterprise, or a network formed by directly connected devices.

On the FR network shown in **Figure 2-1**, two DTE devices Router A and Router D at the access layer are connected over the switch layer formed by two DCE devices, Router B and Router C. DTE and DCE devices are connected through UNIs, which must be configured with the same DLCI. UNIs are applicable to only the FR access scenario. A PVC is established between the two DTE devices, and each PVC segment can be configured with a different DLCI.

Figure 2-1 Roles of devices and interfaces on FR networks



NOTE

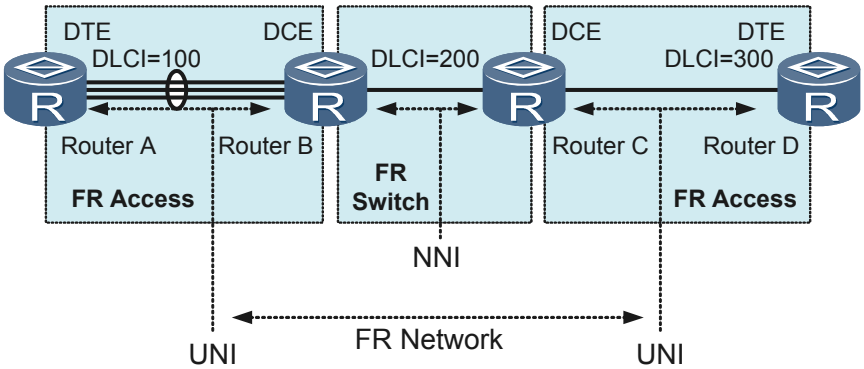
The AR2200 functions as a DTE or DCE. When functioning as a DCE, the AR2200 only provides UNIs for FR termination.

MFR

The MFR feature introduces functionality based on the Frame Relay Forum Multilink Frame Relay UNI/NNI Implementation Agreement (FRF.16). This feature provides a cost-effective way to increase bandwidth for particular applications. MFR is supported by UNIs and NNIs on FR networks.

On the network shown in **Figure 2-2**, Router A and Router B are directly connected through three FR physical links. By creating a logical MFR interface, you can bundle these physical links into a logical MFR link to provide higher bandwidth and transmit data at a higher speed.

Figure 2-2 MFR networking diagram



2.2 FR Features Supported by the AR2200

The AR2200 functions as a DTE or DCE. When functioning as a DCE, the AR2200 only provides UNIs for FR termination.

FR-Supporting Interfaces on the AR2200

The FR features can be configured on the following interfaces: synchronous serial interface, E1-F interface, T1-F interface, BRI interface, CPOS sub-channel interface, CE1/PRI interface, and CT1/PRI interface.

FR Features and Usage Scenarios

Table 2-1 lists FR features that the AR2200 supports. Deploy the features in appropriate scenarios to enhance FR network performance.

Table 2-1 Description of features and scenarios that the AR2200 supports

FR Feature	Description	Usage Scenario
MFR	The MFR feature introduces functionality based on FRF.16. This feature provides a cost-effective way to increase bandwidth for particular applications. MFR is supported by UNIs and NNIs on FR networks.	If bandwidth provided by currently used devices cannot meet users' requirements, configure MFR to increase bandwidth.
PVC group	Configuring a PVC group allows PVCs with the same destination address to forward packets at the same time. Packets with different priorities will be transmitted along separate PVCs.	A PVC group can be configured in either of the following scenarios: ● Multiple PVCs are destined for the same address. ● Different services are required to be transmitted along different PVCs. A PVC group fully uses existing bandwidth resources and improves reliability for important services.
LMI	The LMI protocol exchanges status information to maintain FR link and PVC status.	LMI maintains PVC status.
InARP	The InARP protocol obtains the protocol address of the device on the remote end of each VC.	● To improve stability and security of an FR network, disable InARP and configure the static address mapping function. ● To improve maintainability of an FR network, enable InARP and configure the dynamic address mapping function.
FR over ISDN	Frame Relay over Integrated Services Digital Network (FRoISDN) allows FR data transmission over ISDN B channel. With FRoISDN, data from access devices is sent to an aggregation device. The aggregation device then sends the data to the core network.	Generally, FR leased lines are used as physical links on FR networks. The cost of leasing FR lines is relatively high. Using an FRoISDN scheme decreases the number of leased FR lines required, reducing enterprise expenditures.
FRF.9	FRF.9 compresses FR packets. This function compresses data and InARP packets, not LMI packets.	This function helps increase bandwidth on links of low-speed devices and reduce network load.
FRF.20	FRF.20 compresses FR IP headers.	

FR Features and Usage Scenarios that the AR2200 Supports

As an SDM protocol, FR is able to transmit multiple types of upper-layer protocol packets. Table 2-2 shows mappings between FR features and usage scenarios. After a usage scenario is determined, only allowed FR features can be configured. Otherwise, the configuration will fail.

Table 2-2 Mappings between FR features and usage scenarios that the AR2200 supports

Usage Scenario that the AR2200 Supports	IPoFR	IPoMFR	PPP/ MPoFR	PPPoMFR	BridgeoFR
PVC group	Yes	No	No	No	No
LMI	Yes	Yes	Yes	Yes	Yes
InARP	Yes	Yes	No	No	No

NOTE

Yes indicates that the usage scenario supports the FR feature. No indicates that the usage scenario does not support the FR feature.

Usage scenarios for BridgeoFR are not provided in this chapter. For the detailed configuration procedure, see Transparent Bridging Configuration.

2.3 Configuring IPoFR Through a Single Link

FR can bear IP services. With FR, IP devices can establish an end-to-end (E2E) connection over an FR network.

Currently, IP networks are widely deployed. FR can bear IP services. With FR, IP devices can establish an end-to-end (E2E) connection over an FR network. If two IP devices need to communicate with each other over an FR network, you must configure Internet Protocol over Frame Relay (IPoFR).

2.3.1 Establishing the Configuration Task

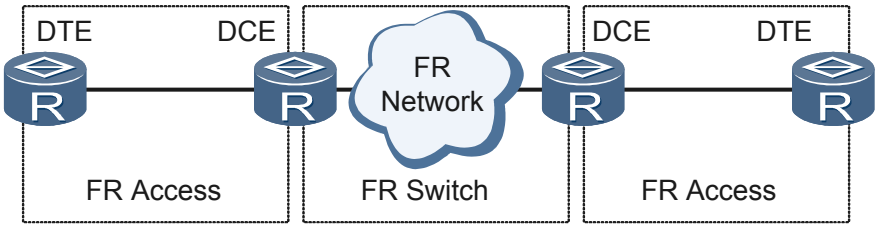
Before configuring IPoFR, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration.

Applicable Environment

The Internet and IP network technologies are simple and flexible and therefore rapidly developed. If IP services travel across an FR network, devices on the FR network must be able to bear IP packets. The SDM feature enables FR to bear IP packets. Currently, IPoFR is preferentially used in the construction of IP broadband networks.

As shown in **Figure 2-3**, if FR is deployed on the user side, configure FR access; if FR is deployed on the network side, configure FR switching. The AR2200 does not support FR switching.

Figure 2-3 Networking diagram for IPoFR



- FR access

  In this scenario, network devices provide access services for user devices, receiving IP packets from users.

  FR allows user devices such as routers, bridges, and hosts to exchange data on an FR network. User devices are DTE devices. Network devices are DCE devices.

- FR switching

  In this scenario, DCE devices exchange and forward IP packets at the data link layer through PVCs.

IPoFR supports PVC groups. Among the PVCs destined for the same IP address, only one forwards data. Configure a PVC group to allow PVCs destined for the same IP address to forward data at the same time. Configuring a PVC group provides an optimal use of bandwidth resources and improved reliability of important services.

For details about configurations, see **Configuring an FR PVC Group**.

As a cost-effective solution provided for FR users, FR compression saves network bandwidth resources, reduces network loads, and improves transmission efficiency. For detailed configurations, see **Configuring FR Compression**.

Pre-configuration Tasks

Before configuring IPoMFR, complete the following task:

- Configuring physical attributes for FR interfaces

Data Preparation

To complete the configuration, you need the following data.

No.	Data
1	● Number, IP address, and data link connection identifier (DLCI) value of each FR interface or sub-interface ● IP address mapped to the DLCI value of each MFR interface and mask of the IP address
2	(Optional) PVC group name, DLCI value, priority levels/values of IP packets transmitted along PVCs in the PVC group

No.	Data
3	(Optional) DLCI value, number of RTP or TCP compression sessions

2.3.2 Configuring Basic IPoFR Functions

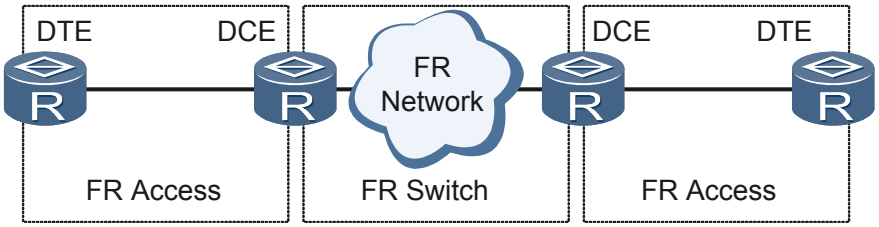
Configuring basic IPoFR functions allows FR links to transmit IP packets.

Context

Packets transmitted on an IP network carry IP addresses. When IP packets enter an FR network, FR devices must be able to forward the packets to the destination. FR devices, however, use DLCI values to identify VCs. To forward IP packets, FR devices must have mappings between DLCI values and destination IP addresses.

On the network shown in **Figure 2-4**, IP packets are transmitted over an FR network that is a public network, a private network of an enterprise, or a network comprising devices directly connected through leased lines.

Figure 2-4 Networking diagram for IPoFR



FR can be deployed on the user side (FR access). In this scenario, if InARP is enabled, you do not need to configure mappings between DLCI values and destination IP addresses. If InARP is disabled, you must configure static or dynamic mappings between DLCI values and destination IP addresses. Choose a static or dynamic mapping as follows.

- Static address mappings improve stability and security of FR networks.

  If a peer device does not support InARP or the InARP function for IPoFR packets, configure address mappings by manually specifying a next hop address for each DLCI.

  For the detailed configuration procedure, see **Configuring static address mappings for FR access between DTE and DCE**.

- Dynamic address mappings improve network maintainability.

  InARP determines the next hop address for each DLCI.

  By default, the dynamic address mapping function is enabled on every physical interface. If the peer device does not support the dynamic address mapping function, disable this function on the local device.

  For the detailed configuration procedure, see **Configuring the dynamic address mapping function for FR access between DTE and DCE**.

NOTE

Unless otherwise specified, configure both ends of an FR link.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The FR interface view is displayed.

Step 3 Run:

```
link-protocol fr [ ietf | nonstandard ]
```

The FR encapsulation format is set.

The **link-protocol fr** command configures FR as the data link layer protocol for the interface. There are two FR encapsulation formats:

- **ietf**: is used if both ends use the encapsulation format defined in RFC 1490.
- **nonstandard**: is used if both ends do not use the encapsulation format defined in RFC 1490.

By default, the FR encapsulation format is IETF.

Two connected Interfaces send packets only in locally set formats. If the interfaces can recognize both formats, they can receive packets in both formats even though they are configured with different FR encapsulation formats. If one device cannot automatically recognize both formats, you must configure both devices with the same FR encapsulation format.

Step 4 Configure FR address mappings.

The FR address mapping function associates the protocol address of a peer device with the FR address (DLCI value) of the local device. This helps upper-layer protocols of the local device locate the peer device based on the protocol address of the peer device.

Choose one of the following configurations according to the FR applicable scenarios and mapping modes described in "Context":

- Configuring static address mappings for FR access between DTE and DCE
  1. Configure the FR interface type.
     a. Perform the following operations on the DTE device:
        1) Run the **fr interface-type dte** command to set the FR interface type to DTE.
        2) Run the **ip address** *ip-address* { *mask* | *mask-length* } [**sub**] command to assign an IP address to the interface.
        3) (Optional) Run the **fr dlci** *dlci* command to set a DLCI value for the FR link.
        4) Run the **quit** command to exit from the DLCI view.
        5) Run the **fr map ip** { *ip-address* [*mask*] | **default** } *dlci-number* [[**ietf** | **nonstandard**] [**broadcast**]] command to configure a mapping between the local DLCI value and the IP address of the peer device.

           This command cannot be used on point-to-point (P2P) sub-interfaces. Choose either **ietf** or **nonstandard** the same as the configured FR encapsulation format.
     b. Perform the following operations on the DCE device:

1) Run the **fr interface-type dce** command to set the FR interface type to DCE.
2) Run the **ip address** *ip-address* { *mask* | *mask-length* } [**sub**] command to assign an IP address to the interface.
3) Run the **fr dlci** *dlci* command to set a DLCI value for the FR link.
4) Run the **quit** command to exit from the DLCI view.
5) Run the **fr map ip** { *ip-address* [*mask*] | **default** } *dlci-number* [[**ietf** | **nonstandard**] [**broadcast**]] command to configure a mapping between the local DLCI value and the IP address of the peer device.

   This command cannot be used on point-to-point (P2P) sub-interfaces. Choose either **ietf** or **nonstandard** the same as the configured FR encapsulation format.

- Configuring the dynamic address mapping function for FR access between DTE and DCE

1. Perform the following operations on the DTE device:
   a. Run the **fr interface-type dte** command to set the FR interface type to DTE.

      This step can be skipped if the **link-protocol fr** command has been used on an FR interface, which allows the DTE interface type to take effect by default.
   b. Run the **ip address** *ip-address* { *mask* | *mask-length* } [**sub**] command to assign an IP address to the interface.
   c. (Optional) Run the **fr inarp** [**ip** [*dlci-number*]] command to enable the dynamic address mapping function.

      This command applies only to FR interfaces not sub-interfaces. After you run this command, InARP automatically determines the next hop address based on the local DLCI value.
2. Perform the following operations on the DCE device:
   a. Run the **fr interface-type dce** command to set the FR interface type to DCE.
   b. Run the **ip address** *ip-address* { *mask* | *mask-length* } [**sub**] command to assign an IP address to the interface.
   c. Run the **fr dlci** *dlci* command to set a DLCI value for the FR link.
   d. Run the **quit** command to exit from the DLCI view.
   e. (Optional) Run the **fr inarp** [**ip** [*dlci-number*]] command to enable the dynamic address mapping function.

      This command applies only to FR interfaces not sub-interfaces. After you run this command, InARP automatically determines the next hop address based on the local DLCI value.

Step 5 Run:

```
fr lmi type { ansi | nonstandard | q933a }
```

The FR LMI protocol type is configured.

By default, the LMI protocol type of an FR interface is **q933a**.

The LMI module manages PVCs, including adding and deleting PVCs, and detecting PVC status and integrity of PVC links. Currently, three standard LMI protocol types are supported:

- **ansi**: is used if both ends use the encapsulation format defined in ANSI T1.617.
- **nonstandard**: can be used if the peer end is a Cisco device.
- **q933a**: is used if both ends use the encapsulation format defined in Q933A.

The two DCE devices must be configured with the same FR LMI protocol type. Otherwise, they cannot communicate with each other.

----End

2.3.3 (Optional) Configuring an FR PVC Group

Configure a PVC group to allow PVCs destined for the same IP address to forward data at the same time. Configuring a PVC group provides an optimal use of bandwidth resources and improved reliability of important services.

Context

On a conventional FR network, only one PVC forwards packets even though multiple PVCs have been configured with the same destination address. If this PVC becomes unavailable, another PVC will be used to forward packets. This results in low bandwidth usage and a failure in providing sufficient bandwidth for packets with high priorities.

Configuring a PVC group allows PVCs with the same destination address to forward packets at the same time. Packets with different priorities will be transmitted along separate PVCs. If IP packets are transmitted along FR PVCs in a PVC group, map the Type of Service (ToS) fields of IP packets to FR PVCs so that IP packets with different priorities are transmitted along separate PVCs. In addition, each PVC in the group can be configured with a different QoS policy for transmitting a specific type of services.

NOTE

Unless otherwise specified, configure both ends of an FR link.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The FR interface view is displayed.

Step 3 Run:

```
fr pvc-group pvc-group-name
```

A PVC group is created and the PVC group view is displayed.

Step 4 Run:

```
fr dlci dlci
```

A PVC is added to the PVC group.

A maximum of eight PVCs can be added to one PVC group.

NOTE

The PVC link configured in the interface view cannot be added to the PVC group. The PVC link in a PVC group cannot be configured in the interface view.

Step 5 Configure packets with different priorities to be transmitted along separate PVCs in an FR PVC group.

PVCs in a group can be configured to transmit IP packets with different priorities. PVCs transmitting IP packets with high priorities preferentially use bandwidth resources. After IP Precedence values or DiffServ Code Point (DSCP) values are mapped to PVCs, IP packets with different priorities are transmitted along different PVCs. In this manner, services with different priorities are transmitted separately.

- To map IP Precedence values to PVCs in a PVC group, run the **fr ip precedence** *dlci-number* { *min* [*max*] | **default** } command.

  An IP Precedence value uses 3 bits of the ToS field in an IP packet, ranging from 0 to 7. The greater the value, the higher the priority.

- To map DSCP values to PVCs in a PVC group, run the **fr ip dscp** *dlci-number* { *min* [*max*] | **default** } command.

  A DSCP value uses 6 bits of the ToS field, ranging from 0 to 63. The greater the value, the higher the priority.

IP Precedence or DSCP values can be mapped to only PVCs in the PVC group. The *min* value must be less than or equal to the *max* value. If the PVC associated with a specific priority value is Down, IP packets with this priority value will be transmitted along the default PVC. If the default PVC is also Down, the packets will be transmitted along a PVC that has been associated with a smaller priority value. The following configurations are recommended:

- Map priority values of unicast packets to PVCs so that unicast packets are transmitted along separate PVCs based on their priority values.
- Configure IS-IS, multicast, and broadcast packets to be transmitted along the PVC associated with the IP Precedence value of 63.

NOTE

Before mapping priorities of IP packets to PVCs, ensure that the PVCs have been created.

If a specific IP Precedence value is not mapped to a PVC in a group, the entire group will become unavailable.

Mapping priorities of IP packets to PVCs in a PVC group does not change the priorities of IP packets. To change priorities of IP packets, see the *Huawei AR2200 Series Enterprise Routers Configuration Guide - QoS*.

----End

2.3.4 (Optional) Configuring FR Compression

Compressing FR packets reduces bandwidth consumption and network load, and improves data transmission efficiency on FR networks.

Context

FR compression can be classified into two modes: payload compression and IP header compression. Their differences are as follows:

- IP header compression complies with the FRF.20 protocol and includes RTP and TCP header compression.
- Payload compression complies with the FRF.9 protocol and compresses unnumbered frames, including FR compression status negotiation, FR compression packet synchronization, FR compression, and FR decompression. The STAC algorithm (ANSI X3.241-1994) is used in FR compression calculation.

As shown in **Table 2-3**, select either of the compression modes or both of them based on different types of interfaces.

Table 2-3 Compression functions that FR interfaces support

	FR Interface	P2P FR Sub-interface	P2MP FR Sub-interface
FR IP header compression	Supported	Supported	Supported
FR payload compression	Supported	Supported	Supported

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Configure FR compression

Select either of compression modes or both of them according to actual scenarios and bandwidth requirements.

- Configure IP header compression on an FR interface or an FR sub-interface.
  1. Perform either of the following configurations based on different types of interfaces:
     - If the interface is an FR interface, run:

       interface *interface-type interface-number*

       The FR interface view is displayed.
     - If the interface is an FR sub-interface, run:

       interface *interface-type interface-number.subnumber*

       The FR sub-interface view is displayed.
  2. Run:

     fr compression iphc

     IP header compression is enabled on an FR interface.
- Configure IP header compression on a P2MP FR sub-interface.
  1. Run:

     interface *interface-type interface-number.subnumber* **p2mp**

     The P2MP FR sub-interface view is displayed.
  2. Run:

     fr map ip { *destination-address* [*mask*] | **default** } *dlci-number* [[**ietf** | **nonstandard**] [**broadcast**]] [**compression** { **frf9** | **iphc rtp-connections** *rtp-connections-number* [**tcp-connections** *tcp-connections-number*] }

     IP header compression is enabled on the P2MP FR sub-interface.
- Configure payload compression on an FR interface or a P2MP FR sub-interface.
  1. Perform either of the following configurations based on different types of interfaces:
     - If the interface is an FR interface, run:

       interface *interface-type interface-number*

       The FR interface view is displayed.

- If the interface is a P2MP FR sub-interface, run:

  interface *interface-number.subnumber* **p2mp**

  The P2MP FR sub-interface view is displayed.

2. Run:

   fr map ip { *destination-address* [*mask*] | **default** } *dlci-number* [[**ietf** | **nonstandard**] [**broadcast**]] [**compression** { **frf9** | **iphc rtp-connections** *rtp-connections-number* [**tcp-connections** *tcp-connections-number*] }

   A mapping is created between the local DLCI value and the destination IP address and FRF.9 compression is enabled for the PVC indicated by the DLCI.

   This command can be used only on FR interfaces or P2MP FR sub-interfaces, and the FR encapsulation format of these interfaces must be IETF. If the encapsulation format is nonstandard and this command with **compression** is run to enable FRF.9 compression, the system displays a message indicating that this encapsulation format does not support FRF.9 compression.

- Configure payload compression on a P2P FR sub-interface.

  1. Run:

     interface interface-type *interface-number.subnumber* **p2p**

     A P2P FR sub-interface is created, and the FR sub-interface view is displayed.

  2. Run:

     fr compression frf9

     FRF.9 compression is enabled.

  This command can be configured only on P2P FR sub-interfaces, and the encapsulation format of the interfaces must be IETF. If the encapsulation format is nonstandard and this command with **compression** is run to enable FRF.9 compression, the system displays a message indicating that this encapsulation format does not support FRF.9 compression.

----End

2.3.5 Checking the Configuration

After IPoFR is successfully configured, you can view FR configurations.

Prerequisites

All IPoFR configurations are complete.

Procedure

- Run the **display fr interface** [*interface-type interface-number*[*.subnumber*]] command to check the FR protocol status and information about FR interfaces.
- Run the **display fr map-info** [**interface** *interface-type interface-number*[*.subnumber*]] command to check the mappings between protocol addresses and FR addresses.
- Run the **display fr map-info** [**interface** *interface-type interface-number*] command to check FR InARP statistics.
- Run the **display interface brief** command to check the interface status and brief information about the configured interface.
- Run the **display fr pvc-group** [[*pvc-group-name* [**verbose**]] **interface** *interface-type interface-number*[*.subnumber*]] command to check information about a specified PVC group or all PVC groups.

- Run the **display fr compression iphc** command to check IP header compression information on FR interfaces.
- Run the **display fr compression frf9** command to check statistics about FRF.9 STAC compression.

----End

Example

Run the **display fr interface** [*interface-type interface-number*[*.subnumber*]] command to view the FR protocol status and information about FR interfaces.

```
<Huawei> display fr interface MFR0/0/1, DCE, physical up, protocol up Serial2/0/0,
DTE, physical down, protocol down
```

Run the **display fr map-info** [**interface** *interface-type interface-number*[*.subnumber*]] command to view the mappings between protocol addresses and FR addresses.

```
<Huawei> display fr map-info Map Statistics for interface MFR0/0/1 (DCE) DLCI =
100, IP 2.2.2.2, MFR0/0/1 create time = 2010/12/02 19:54:23, status = ACTIVE
encapsulation = ietf, vlink = 4
```

Run the **display fr inarp-info** command to view FR InARP statistics.

```
<Huawei> display fr inarp-info Frame relay InverseARP statistics for interface
MFR0/0/0 (DTE) In ARP request  Out ARP reply  Out ARP request  In ARP reply
5               5               5               5 Frame relay InverseARP statistics
for interface Serial1/0/0:0 (DTE) In ARP request  Out ARP reply  Out ARP request
In ARP reply 0               0              0                0
```

Run the **display interface brief** command to view the interface status and brief information about the configured interface.

```
<Huawei> display interface brief | begin MFR PHY: Physical *down: administratively
down (l): loopback (s): spoofing (b): BFD down (d): Dampening Suppressed InUti/
OutUti: input utility/output utility Interface                   PHY   Protocol
InUti OutUti   inErrors  outErrors MFR0/0/1                   up    up       0.04%
0.04%          0          0 Pos0/0/0                  up    up       0.03%
0.03%          0          0 NULL0                       up    up(s)        0%
0%          0          0 Serial1/0/0                 *down down        0%
0%          0          0
```

Run the **display fr pvc-group** command to view information about a specific PVC group or all PVC groups.

```
<Huawei> display fr pvc-group PVC-GROUP-name    State     TosType     INARP
Interface        Type PhyStatus abc               Inactive  PRECEDENCE  Enable
Serial1/0/0      DTE  Down def               Inactive  PRECEDENCE  Enable
Serial1/0/0      DTE  Down
```

Run the **display fr compression iphc** command to view information about IP header compression on FR interfaces.

```
<Huawei> display fr compression iphc
Serial1/0/0:0 -DLCI:22
  RTP header compression information:
    Compression:
        RtpTotal      :               0 , RtpCompressed :               0
        RtpLongSearch :               0 , RtpMiss       :               0
        RtpSavedbytes :               0 , RtpSentBytes  :               0
    Decompression:
        RtpTotal      :               0 , RtpCompressed :               0
        RtpError      :               0
    Compression-connections: 256 , Decompression-connections: 256

  Information of TCP header compression:
    Compression:
        TcpTotal      :            9230 , TcpCompressed :            9229
        TcpLongSearch :               0 , TcpMiss       :               1
        TcpSavedbytes :          304557 , TcpSentBytes  :          452303
    Decompression:
```

```
      TcpTotal      :               0 , TcpCompressed :               0
      TcpError      :               0
  Compression-connections: 256 , Decompression-connections: 256
```

Run the **display fr compression frf9** command to view statistics about FRF.9 compression.

```
<Huawei> display fr compression frf9
  Serial1/0/0:0   -DLCI = 22
  sent:
    CompressedPackets  = 10103,  UnCompressedPackets  = 0
    CompressedOctets    = 337695,  OriginalOctets    = 838549
  receive:
    CompressedPackets  = 10101,  UnCompressedPackets  = 0
    CompressedOctets    = 60681,  UnCompressedOctets     = 0
    NotDroppedCompressedPackets = 10101, NotDroppedUnCompressedPackets = 0
    DeCompressedPackets = 10101, DeCompressedOctets = 838383
```

2.4 Configuring IPoMFR

FR can bear IP services. With MFR, IP devices can establish an E2E connection over an FR network. IPoMFR bundles multiple physical links (including channelized serial interfaces) to provide higher bandwidth.

As IP networks are widely deployed, if two IP devices need to communicate with each other over an FR network, configure IPoFR.

2.4.1 Establishing the Configuration Task

Before configuring IPoMFR, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task quickly and efficiently.

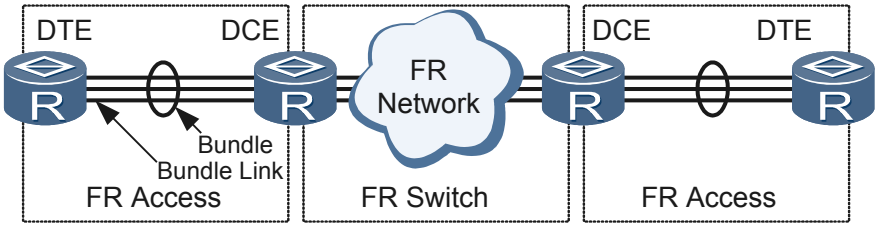
Applicable Environment

If IP services need to be transmitted through an FR network, devices on the FR network must be able to bear IP packets. The SDM feature enables FR to bear IP packets. Currently, IPoMFR is preferentially used in the construction of IP broadband networks.

Generally, FR physical links work at the same rate as that supported by E1 or T1 links. As IP services are rapidly developed, FR networks cannot provide sufficient bandwidth for IP services. Upgrading the existing FR devices requires huge investments and extensive technical supports. If the existing FR devices are connected through multiple FR physical links, configure MFR on UNIs and NNIs to increase bandwidth without changing the network topology.

As shown in **Figure 2-5**, an MFR link is called a bundle, and physical member links are called bundle links. The bandwidth of an MFR link is the sum of its member links' bandwidth. IP packets can be transmitted over a public MFR network, a private MFR network of an enterprise, or an MFR network comprising devices directly connected through leased lines.

Figure 2-5 Networking diagram for IPoMFR



MFR can be deployed on the user side (MFR access) and on the network side (MFR switching):

- MFR access (between DTE and DCE)

  In this scenario, network devices provide access services for user devices, receiving IP packets from users.

  MFR allows user devices such as routers, bridges, and hosts to exchange data on an FR network. User devices are DTE devices. Network devices are DCE devices.

- MFR switching (between DCEs)

  In this scenario, DCE devices exchange and forward IP packets at the data link layer through PVCs.

The AR2200 does not support MFR switching.

As a cost-effective solution provided for FR users, FR compression saves network bandwidth resources, reduces network loads, and improves transmission efficiency. For detailed configurations, see **Configuring FR Compression**.

Pre-configuration Tasks

Before configuring IPoMFR, complete the following task:

- Configuring physical attributes for FR interfaces

Data Preparation

To complete the configuration, you need the following data.

No.	Data
1	Number, IP address, and DLCI value of each MFR interface; IP address mapped to the DLCI value of each MFR interface and mask of the IP address
2	Number of each FR interface or sub-interface
3	(Optional) DLCI of each MFR member link, interval at which Hello packets are sent, waiting time before a Hello packet is retransmitted, number of Hello packet retransmissions, and maximum fragment size as well as DLCI, maximum fragment size, and slide window size of the MFR link

2.4.2 Creating and Configuring an MFR Interface

You can configure logical MFR interfaces to allow IP packets to travel over an FR network through MFR links.

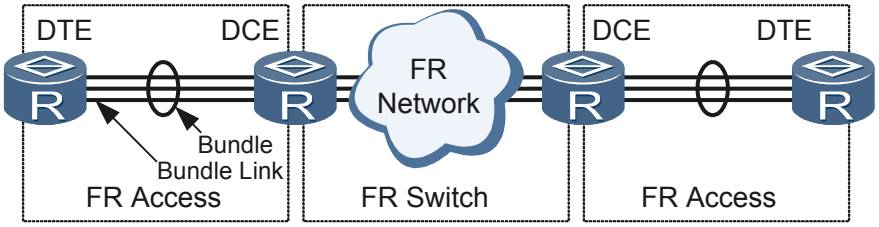
Context

Packets transmitted on an IP network carry IP addresses. When IP packets enter an FR network, FR devices must be able to forward the packets to the destination. FR devices, however, use DLCI values to identify VCs. To forward IP packets, FR devices must have mappings between DLCI values and destination IP addresses.

To allow IP packets to travel through an MFR link, configure mappings between the DLCI value of the MFR interface and destination IP addresses.

As shown in **Figure 2-6**, MFR can be deployed on the user side (MFR access) and on the network side (MFR switching):

Figure 2-6 Networking diagram for IPoMFR



The AR2200 does not support MFR switching.

MFR can be deployed on the user side (MFR access). In this scenario, if InARP is enabled for the dynamic address mapping function, you do not need to configure mappings between DLCI values and destination IP addresses. If InARP is disabled, you must configure static or dynamic mappings between DLCI values and destination IP addresses. Choose a static or dynamic mapping as follows.

- Static address mappings improve stability and security of FR networks.

  You must manually specify the next hop address for each DLCI and ensure that InARP is disabled. If the peer device does not support InARP or the InARP function for IPoFR packets, you must configure address mappings manually.

  If DTE and DCE devices are directly connected through leased lines, the devices must be configured with the same DLCI value.

  For the detailed configuration procedure, see **Configuring static address mappings for MFR access between DTE and DCE**.

- Dynamic address mappings improve network maintainability.

  InARP determines the next hop address for each DLCI.

  By default, the dynamic address mapping function is enabled on every physical interface. If the peer device does not support the dynamic address mapping function, disable this function on the local device.

  For the detailed configuration procedure, see **Configuring the dynamic address mapping function for MFR access between DTE and DCE**.

NOTE

Unless otherwise specified, configure both ends of an FR link.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface mfr interface-number[.subnumber | p2p ] ]
```

An MFR interface is created and the MFR interface view is displayed.

To create an MFR sub-interface on a P2MP link, run the **interface mfr** *interface-number.subnumber* **p2mp** command.

Step 3 Run:

```
ip address ip-address { mask | mask-length } [ sub ]
```

An IP address is configured for the MFR interface.

Step 4 Configure MFR address mappings.

The MFR address mapping function associates the protocol address of a peer device with the FR address (DLCI value) of the local device. This helps upper-layer protocols of the local device locate the peer device based on the protocol address of the peer device.

Choose one of the following configurations according to FR applicable scenarios and mapping modes described in "Context":

- Configuring static address mappings for MFR access between DTE and DCE
  1. Perform the following operations on the DTE device:
     a. (Optional) Run the **fr interface-type dte** command to set the MFR interface type to DTE.

        This step is optional because the default MFR interface type is DTE.
     b. Run the **fr dlci** *dlci* command to set a DLCI value for the MFR interface.
     c. Run the **quit** command to exit from the DLCI view.
     d. Run the **fr map ip** { *ip-address* [*mask*] | **default** } *dlci-number* [[**ietf** | **nonstandard**] [**broadcast**]] command to configure a mapping between the local DLCI value and the IP address of a peer device.

        This command cannot be used on P2P sub-interfaces. Choose either **ietf** or **nonstandard** so that this value is the same as that of the configured FR encapsulation format.
  2. Perform the following operations on the DCE device:
     a. Run the **fr interface-type dce** command to set the MFR interface type to DCE.
     b. Run the **fr dlci** *dlci* command to set a DLCI value for the MFR interface.
     c. Run the **quit** command to exit from the DLCI view.
     d. Run the **fr map ip** { *ip-address* [*mask*] | **default** } *dlci-number* [[**ietf** | **nonstandard**] [**broadcast**]] command to configure a mapping between the local DLCI value and the IP address of a peer device.

        This command cannot be used on P2P sub-interfaces. Choose either **ietf** or **nonstandard** so that this value is the same as that of the configured FR encapsulation format.
- Configuring the dynamic address mapping function for MFR access between DTE and DCE
  1. Perform the following operations on the DTE device:
     a. Run the **fr interface-type dte** command to set the MFR interface type to DTE.

        This step is optional because the default MFR interface type is DTE.
     b. Run the **fr inarp** [**ip** [*dlci-number*]] command to enable the dynamic address mapping function.

This command applies only to MFR interfaces not sub-interfaces. After you run this command, InARP automatically determines the next hop address based on the local DLCI value.

2. Perform the following operations on the DCE device:
   a. Run the **fr interface-type dce** command to set the MFR interface type to DCE.
   b. Run the **fr inarp** [**ip** [*dlci-number*]] command to enable the dynamic address mapping function.

      This command applies only to MFR interfaces not sub-interfaces. After you run this command, InARP automatically determines the next hop address based on the local DLCI value.

----End

2.4.3 Adding Physical Interfaces to an MFR Interface

MFR is a cost-effective solution provided for FR users. MFR bundles multiple physical interfaces on a device to provide higher bandwidth for users without increasing investments on network devices.

Context

An MFR link is called a bundle, and physical member links are called bundle links. The bandwidth of an MFR link is the bandwidth sum of its member links. An MFR interface represents a bundle, and a bundle can contain multiple bundle links, each of which corresponds to a physical interface. A bundle manages its bundle links. Bundle links are visible at the physical layer, and bundle links are visible at the data link layer.

The function and configuration of an MFR interface are the same as those of an ordinary FR interface. After a physical interface is added to an MFR interface, the original physical layer and data link layer parameters of the physical interface are replaced by the parameters of the MFR interface.

The status of every physical interface added to an MFR interface determines the status of the MFR interface. As long as one physical interface of the MFR interface is available, the MFR interface is available for upper-layer FR applications. If all physical interfaces of the MFR interface are unavailable, the MFR interface is unavailable for upper-layer FR applications. An MFR interface is a logical interface working at the data link layer, and its member interfaces are physical interfaces working at the physical layer.

NOTE

Unless otherwise specified, configure both ends of an FR link.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The FR interface view is displayed.

Step 3 Run:

```
link-protocol fr mfr interface-number
```

The FR interface is added to a specified MFR interface.

A maximum of 128 physical interfaces can be added to an MFR interface.

----End

2.4.4 (Optional) Configuring Parameters for an MFR Link and Its Member Links

Configuring interface identifiers, parameters for packets detecting link status, and the maximum MFR fragment size and slide window size improves MFR maintainability and performance.

Context

After configuring basic MFR functions, configure the following functions to improve MFR maintainability:

- To identify an MFR interface and its member interfaces, you can change identifiers of the interfaces.

  For the detailed configuration procedure, see **Configure interface identifiers**.
- After an MFR link is configured, the two ends of the link must keep informed of the other's MFR PVC status. This prevents packet forwarding failures if one end fails. MFR sends packets to detect link status to ensure reliable PVC status. Modify packet parameters according to network conditions.

  For the detailed configuration procedure, see **Configure parameters for packets detecting link status**.

You can configure the maximum fragment size and slide window size for low-speed links working at rates lower than 768 kbit/s to improve MFR performance:

- If a large packet is transmitted through only one member link, other member links are idle. As a result, the MFR link works inefficiently. Set the maximum MFR fragment size to reduce transmission delays and improve transmission efficiency of the MFR link.

  The maximum MFR fragment size is determined by the member interface working at the lowest speed. For example, if T1 interfaces are bundled on one end and 64 kbit/s interfaces are bundled on the other end, both devices are configured with the maximum MFR fragment size based on the remote interfaces. For details about fragmentation, see **Table 2-4**.

Table 2-4 Recommended fragmentation for less than 10 ms link transmission delays

Lowest Link Rate (in kbps)	Recommended Maximum Fragment Size (in bytes)
56	70
64	80
128	160
256	320
512	640

Lowest Link Rate (in kbps)	Recommended Maximum Fragment Size (in bytes)
768	1000
1536	1600

For the detailed configuration procedure, see **Configure the maximum MFR fragment size**.

- After an MFR link is configured, the two ends of the link must keep informed of the other's MFR PVC status. This prevents packet forwarding failures if one end fails. MFR sends packets to detect link status to ensure reliable PVC status. Modify packet parameters according to network conditions.

  For the detailed configuration procedure, see **Configure the MFR slide window size**.

NOTE

Unless otherwise specified, configure both ends of an FR link.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Configure interface identifiers.

- Configure an identifier for an FR interface.
  1. Run the **interface** *interface-type interface-number* command to enter the interface view.
  2. Run the **mfr link-name** *name* command to configure an MFR LID for an FR link.

     The default MFR LID is the name of the physical interface.
  3. Run the **quit** command to exit from the FR interface view.
- Configure an identifier for an MFR interface.
  1. Run the **interface mfr** *interface-number* command to enter the view of an MFR interface.

     Only MFR interfaces can be configured with interface identifiers.
  2. Run the **mfr bundle-name** *name* command to configure an MFR BID for the MFR link.

     The default MFR BID format is MFR plus the number of the MFR interface.

     The **mfr bundle-name** command applies only to MFR interfaces not MFR sub-interfaces.
  3. Run the **quit** command to exit from the MFR interface view.

Step 3 Configure parameters for packets detecting link status.

1. Run the **interface** *interface-type interface-number* command to enter the view of an FR interface.
2. Run the **mfr timer hello** *seconds* command to set an interval at which Hello packets are sent on the FR link.

By default, a Hello packet is sent every 10 seconds on the FR link.

3. Run the **mfr timer ack** *seconds* command to set the timeout period for ACK packets on the FR link.

   By default, an FR link waits a maximum of 4 seconds for an ACK packet.

4. Run the **mfr retry** *number* command to set the number of attempts to resend a Hello packet on the FR link.

   By default, a Hello packet can be resent twice on an FR link.

5. Run the **quit** command to exit from the FR interface view.

The two ends of a link perform the following operations to maintain the link status:

1. The sender sends a Hello packet to the receiver through the MFR link. The interval at which Hello packets are sent can be specified using the **mfr timer hello** *hello-interval* command.
2. There are two possible results as the sender does or does not receive an ACK packet:
   - The sender receives an ACK packet before the timeout period expires, and the MFR link is successfully established. The timeout period for a Hello packet can be specified using the **mfr timer ack** *ack-timeout* command.
   - The sender does not receive any ACK packet before the timeout period expires, and the MFR link fails to be established. The sender will send a Hello packet again, expecting to receive an ACK packet. The maximum times for resending a Hello packet can be specified using the **mfr retry** *retry-number* command.

If the sender does not receive an ACK packet after a maximum number of Hello packets are sent, the system considers that the data link layer protocol of the FR link fails.

Step 4 Configure the maximum MFR fragment size.

Configure the maximum MFR fragment size on an MFR interface.

1. Run the **interface mfr** *interface-number* command to enter the view of an MFR interface.
2. Run the **mfr fragment** command to enable MFR fragmentation.

   By default, MFR fragmentation is disabled.

3. Run the **mfr fragment-size** *bytes* command to set the maximum fragment size allowed by the MFR link.

   Configuring the same maximum fragment size for both ends of an MFR link is recommended to maximize efficiency.

   By default, the maximum fragment size is 300 bytes.

4. Run the **quit** command to exit from the MFR interface view.

Step 5 Configure the MFR slide window size.

1. Run the **interface mfr** *interface-number* command to enter the view of an MFR interface.
2. Run the **mfr window-size** *number* command to set the MFR slide window size.

   The MFR slide window size indicates the maximum number of fragments that the slide window contains when an MFR interface reassembles fragments using the slide window algorithm. By configuring the slide window size, you can restrict the volume of traffic transmitted on the network to improve network performance.

NOTE

- The slide window size determines the speed at which fragments are reassembled. Find the trade-off between the number of MFR member links and the slide window size. The default slide window size is recommended.
- By default, the slide window size is equal to the number of physical interfaces bundled into the MFR interface.

----End

2.4.5 (Optional) Configuring an FR PVC Group

Among the PVCs destined for the same IP address, only one forwards data. Configure a PVC group to allow PVCs destined for the same IP address to forward data at the same time. Configuring a PVC group provides an optimal use of bandwidth resources and improved reliability of important services.

Context

On a conventional FR network, only one PVC forwards packets even though multiple PVCs have been configured with the same destination address. If this PVC becomes unavailable, another PVC will be used to forward packets. This results in low bandwidth usage and a failure in providing sufficient bandwidth for packets with high priorities.

Configuring a PVC group allows PVCs with the same destination address to forward packets at the same time. Packets with different priorities will be transmitted along separate PVCs. If IP packets need to be transmitted along FR PVCs in a PVC group, map the ToS fields of IP packets to FR PVCs so that IP packets with different priorities are transmitted along separate PVCs. In addition, each PVC in the group can be configured with a different QoS policy for transmitting a specific type of services.

NOTE

Unless otherwise specified, configure both ends of an FR link.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
fr pvc-group pvc-group-name
```

A PVC group is created and the PVC group view is displayed.

Step 3 Run:

```
fr dlci dlci
```

A PVC is added to the PVC group.

A maximum of eight PVCs can be added to one PVC group.

Step 4 Configure packets with different priorities to be transmitted along separate PVCs in an FR PVC group.

PVCs in a group can be configured to transmit IP packets with different priorities. PVCs transmitting IP packets with high priorities preferentially use bandwidth resources. After IP

Precedence values or DSCP values are mapped to PVCs, IP packets with different priorities are transmitted along different PVCs. In this manner, services with different priorities are transmitted separately.

- To map specified IP Precedence values of IP packets to a PVC, run:
  fr ip precedence *dlci-number* { *min* [*max*] | **default** }

  An IP Precedence value uses 3 bits of the ToS field in an IP packet, ranging from 0 to 7. The greater the value, the higher the priority.
- To map specified DSCP values of IP packets to a PVC, run:
  fr ip dscp *dlci-number* { *min* [*max*] | **default** }

  A DSCP value uses 6 bits of the ToS field, ranging from 0 to 63. The greater the value, the higher the priority.

IP Precedence or DSCP values can be mapped to only PVCs in the PVC group. The *min* value must be less than or equal to the *max* value. If the PVC associated with a specific priority value is Down, IP packets with this priority value will be transmitted along the default PVC. If the default PVC is also Down, the packets will be transmitted along a PVC that has been associated with a smaller priority value. The following configurations are recommended:

- Map priority values of unicast packets to PVCs so that unicast packets are transmitted along separate PVCs based on their priority values.
- Configure IS-IS, multicast, and broadcast packets to be transmitted along the PVC associated with the IP Precedence value of 63.

NOTE

Before mapping priorities of IP packets to PVCs, ensure that the PVCs have been created.

If a specific IP Precedence value is not mapped to a PVC in a group, the entire group will become unavailable.

Mapping priorities of IP packets to PVCs in a PVC group does not change the priorities of IP packets. To change priorities of IP packets, see the *Huawei AR2200 Series Enterprise Routers Configuration Guide - QoS*.

----End

2.4.6 (Optional) Configuring FR Compression

Compressing FR packets reduces bandwidth consumption and network load, and improves data transmission efficiency on FR networks.

Context

FR compression can be classified into two modes: payload compression and header compression. Their differences are as follows:

- IP header compression complies with the FRF.20 protocol and includes RTP and TCP header compression.
- Payload compression complies with the FRF.9 protocol and compresses unnumbered frames, including FR compression status negotiation, FR compression packet synchronization, FR compression, and FR decompression. The STAC algorithm (ANSI X3.241-1994) is used in FR compression calculation.

As shown in **Table 2-5**, select either of the compression modes or both of them based on different types of interfaces.

Table 2-5 Compression functions that FR interfaces support

	MFR Interface	P2P MFR Sub-interface	P2MP MFR Sub-interface
FR IP header compression	Supported	Supported	Supported
FR payload compression Not recommended	Supported	Supported	Supported

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Configure FR compression

Select either of compression modes or both of them according to actual scenarios and bandwidth requirements.

- Configure IP header compression on an MFR interface or a P2P MFR sub-interface.
  1. Run:
     ```
     interface mfr interface-number
     ```
     The MRF interface or the P2P MFR sub-interface view is displayed.
  2. Run:
     ```
     fr compression iphc
     ```
     IP header compression is enabled on the MFR interface or the P2P MFR sub-interface.
- Configure IP header compression on a P2MP MFR sub-interface.
  1. Run:
     ```
     interface mfr interface-number.subnumber p2mp
     ```
     The P2MP MFR sub-interface view is displayed.
  2. Run:
     ```
     fr map ip { destination-address [ mask ] | default } dlci-number [ [ ietf |
     nonstandard ] [ broadcast ] ] [ compression { frf9 | iphc rtp-connections
     rtp-connections-number [ tcp-connections tcp-connections-number ] }
     ```
     IP header compression is enabled on the P2MP MFR sub-interface.
- Configure payload compression on a P2MP MFR sub-interface.
  1. Run:
     ```
     interface mfr interface-number.subnumber p2mp
     ```
     The P2MP MFR sub-interface view is displayed.
  2. Run:
     ```
     fr map ip { destination-address [ mask ] | default } dlci-number [ [ ietf |
     nonstandard ] [ broadcast ] ] [ compression { frf9 | iphc rtp-connections
     rtp-connections-number [ tcp-connections tcp-connections-number ] }
     ```
     A mapping between the local DLCI value and the destination IP address is created and FRF.9 compression is enabled for the PVC indicated by the DLCI.

This command can be used only on FR interfaces or P2MP FR sub-interfaces, and the FR encapsulation format of these interfaces must be IETF. If the encapsulation format is nonstandard and this command with **compression** is run to enable FRF.9 compression, the system displays a message indicating that this encapsulation format does not support FRF.9 compression.

- Configure payload compression for an MFR interface.
  1. Run:

     ```
     interface mfr interface-number
     ```

     The MFR interface view is displayed.
  2. Run:

     ```
     fr map ip { destination-address [ mask ] | default } dlci-number [ [ ietf |
     nonstandard ] [ broadcast ] ] [ compression { frf9 | iphc rtp-connections
     rtp-connections-number [ tcp-connections tcp-connections-number ] }
     ```

     FRF.9 compression is enabled on the MFR interface.
- Configure payload header compression for a P2P MFR sub-interfaces.
  1. Run:

     ```
     interface mfr interface-number
     ```

     The P2P MFR sub-interface view is displayed.
  2. Run:

     ```
     fr compression frf9
     ```

     FRF.9 compression is enabled on the P2P MFR sub-interface.

  This command can be used only on P2P FR sub-interfaces, and the encapsulation format of the interfaces must be IETF. If the encapsulation format is nonstandard and this command with **compression** is run to enable FRF.9 compression, the system displays a message indicating that this encapsulation format does not support FRF.9 compression.

----End

2.4.7 Checking the Configuration

After IPoMFR is successfully configured, you can view MFR configurations.

Prerequisites

All IPoMFR configurations are complete.

Procedure

- Run the **display fr interface** [*interface-type interface-number*[.*subnumber*]] command to check the FR protocol status and information about FR interfaces.
- Run the **display fr map-info** [**interface** *interface-type interface-number*[.*subnumber*]] command, you can check the mappings between protocol addresses and FR addresses.
- Run the **display fr inarp-info** [**interface** *interface-type interface-number*] command to check FR Inverse ARP statistics.
- Run the **display interface brief** command to check the interface status and brief information about the configured interface.
- Run the **display interface mfr** [*interface-number*] command to check the status and configurations of the MFR interface.

- Run the **display fr compression iphc** command to check IP header compression information on FR interfaces.
- Run the **display fr compression frf9** command to check statistics about FRF.9 STAC compression.

----End

Example

Run the **display fr interface** [*interface-type interface-number*[*.subnumber*]] command to view the FR protocol status and information about FR interfaces.

```
<Huawei> display fr interface MFR0/0/1, DCE, physical up, protocol up Serial2/0/0,
DTE, physical down, protocol down
```

Run the **display fr map-info** [**interface** *interface-type interface-number*[*.subnumber*]] command to view the mappings between protocol addresses and FR addresses.

```
<Huawei> display fr map-info Map Statistics for interface MFR0/0/1 (DCE) DLCI =
100, IP 2.2.2.2, MFR0/0/1 create time = 2010/12/02 19:54:23, status = ACTIVE
encapsulation = ietf, vlink = 4
```

Run the **display fr inarp-info** command to view FR Inverse ARP statistics.

```
<Huawei> display fr inarp-info Frame relay InverseARP statistics for interface
MFR0/0/0 (DTE) In ARP request  Out ARP reply  Out ARP request  In ARP reply
5               5               5               5 Frame relay InverseARP statistics
for interface Serial1/0/0:0 (DTE) In ARP request  Out ARP reply  Out ARP request
In ARP reply 0               0              0                0
```

Run the **display interface brief** command to view the interface status and brief information about the configured interface.

```
<Huawei> display interface brief | begin MFR PHY: Physical *down: administratively
down (l): loopback (s): spoofing (b): BFD down (d): Dampening Suppressed InUti/
OutUti: input utility/output utility Interface                   PHY   Protocol
InUti OutUti   inErrors  outErrors MFR0/0/1                   up    up       0.04%
0.04%          0          0 NULL0                       up    up(s)       0%
0%          0          0 Serial1/0/0                 *down down        0%
0%          0          0
```

Run the **display interface mfr** command to view information about the configured MFR interface. The system does not display the default description of an interface by default.

```
<Huawei> display interface MFR MFR0/0/1 current state : UP Line protocol current
state : UP Description:HUAWEI, AR Series, MFR0/0/1 Interface Route Port,The Maximum
Transmit Unit is 1500, Hold timer is 10(sec) Internet Address is 1.1.1.1/24 Link
layer protocol is FR IETF LMI DLCI is 0, LMI type is ANSI, frame relay DCE LMI
status enquiry received 0, LMI status sent 0 LMI status enquiry timeout 0, LMI
message discarded 0 Physical is MFR, baudrate: 0 bps Current system time:
2010-12-02 19:56:43-08:00 Last 300 seconds input rate 11 bytes/sec, 1 packets/sec
Last 300 seconds output rate 20 bytes/sec, 1 packets/sec Realtime 0 seconds input
rate 0 bytes/sec, 0 packets/sec Realtime 0 seconds output rate 0 bytes/sec, 0
packets/sec 1 packets input, 30 bytes, 0 drops 1 packets output, 25 bytes, 0 drops
Input bandwidth utilization  : 12.00% Output bandwidth utilization :
15.00%
```

Run the **display fr compression iphc** command to view IP header compression information on FR interfaces.

```
<Huawei> display fr compression iphc
Serial1/0/0:0 -DLCI:22
  RTP header compression information:
    Compression:
        RtpTotal      :               0 , RtpCompressed :               0
        RtpLongSearch :               0 , RtpMiss       :               0
        RtpSavedbytes :               0 , RtpSentBytes  :               0
    Decompression:
        RtpTotal      :               0 , RtpCompressed :               0
        RtpError      :               0
    Compression-connections: 256 , Decompression-connections: 256
```

```
  Information of TCP header compression:
    Compression:
        TcpTotal      :            9230 , TcpCompressed :            9229
        TcpLongSearch :               0 , TcpMiss       :               1
        TcpSavedbytes :          304557 , TcpSentBytes  :          452303
    Decompression:
        TcpTotal      :               0 , TcpCompressed :               0
        TcpError      :               0
    Compression-connections: 256 , Decompression-connections: 256
```

Run the **display fr compression frf9** command to view statistics about FRF.9 STAC compression.

```
<Huawei> display fr compression frf9
  Serial1/0/0:0   -DLCI = 22
  sent:
    CompressedPackets  = 10103,  UnCompressedPackets  = 0
    CompressedOctets    = 337695,  OriginalOctets    = 838549
  receive:
    CompressedPackets  = 10101,  UnCompressedPackets  = 0
    CompressedOctets    = 60681,  UnCompressedOctets     = 0
    NotDroppedCompressedPackets = 10101, NotDroppedUnCompressedPackets = 0
    DeCompressedPackets = 10101, DeCompressedOctets = 838383
```

2.5 Configuring PPPoFR Through a Single Link

FR can bear PPP/MP services. With FR, devices can establish an E2E PPP/MP connection over an FR network.

FR does not provide authentication functions, and therefore cannot guarantee that only valid users access enterprise networks. The Point-to-Point Protocol (PPP) provides effective authentication functions. By configuring PPPoFR, you can use the Link Control Protocol (LCP) and Network Control Protocol (NCP) of PPP to authenticate users accessing FR networks.

2.5.1 Establishing the Configuration Task

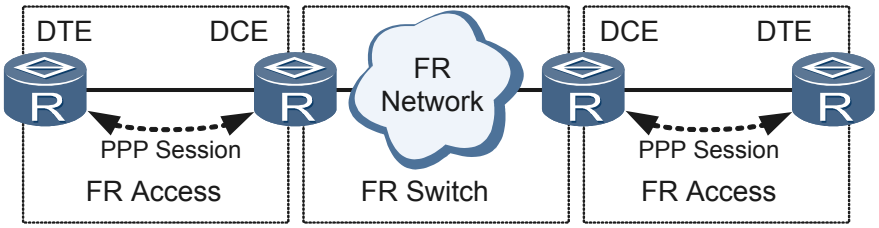
Before configuring PPPoFR, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task quickly and efficiently.

Applicable Environment

FR simplifies frame encapsulation. It features lower communication delays and higher network throughput, compared to other data link layer protocols. FR, however, does not provide authentication functions, and cannot guarantee that only valid users accessing enterprise networks. PPP is a data link layer protocol used to transmit network layer packets on P2P links. It provides effective authentication functions and is extensible. Configuring PPPoFR allows devices to check validity of login users, ensuring FR network security.

On the network shown in **Figure 2-7**, DTE devices such as routers, bridges, and hosts at the FR access layer provide access services for users. DCE devices provide access services for DTE devices. By configuring PPPoFR, you can connect users to DCE devices of an enterprise to protect the enterprise network against malicious attacks.

Figure 2-7 Networking diagram for FR user authentication and access



To increase bandwidth, bundle PPP links on an FR network into a logical MP link. This scheme is called MPoFR. MP is configured based on PPPoFR. For the detailed MP configuration procedure, see **3.6 Configuring MP**.

Pre-configuration Tasks

Before configuring PPPoFR, complete the following tasks:

- Configuring physical attributes for FR interfaces
- Configuring VT interfaces

Data Preparation

To configure PPPoFR, you need the following data.

No.	Data
1	Number, IP address, and DLCI value of each FR interface or sub-interface; IP address mapped to the DLCI value of each MFR interface and mask of the IP address

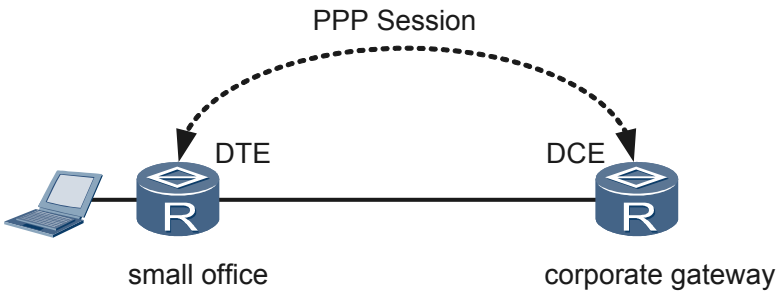
2.5.2 Configuring PPPoFR

Configuring PPPoFR allows PPP services to be transmitted over an FR network.

Context

On the network shown in **Figure 2-8**, a DTE device maps a PVC to a PPP link to establish a PPPoFR link. This allows PPP packets to be transmitted along the FR PVC. PPP packets can be transmitted over a public FR network, a private FR network of an enterprise, or an FR network comprising devices directly connected through leased lines.

Figure 2-8 Networking diagram for PPPoFR



NOTE

Unless otherwise specified, configure both ends of an FR link.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The FR interface view is displayed.

Step 3 Run:

```
link-protocol fr [ ietf | nonstandard ]
```

The FR encapsulation format is set.

The **link-protocol fr** command configures FR as the data link layer protocol for the interface. There are two FR encapsulation formats:

- **ietf**: is used if both ends use the encapsulation format defined in RFC 1490.
- **nonstandard**: is used if both ends do not use the encapsulation format defined in RFC 1490.

By default, the FR encapsulation format is IETF.

Two connected Interfaces send packets only in locally set formats. If the interfaces can recognize both formats, they can receive packets in both formats even though they are configured with different FR encapsulation formats. If one device cannot automatically recognize both formats, you must configure both devices with the same FR encapsulation format.

When using the **link-protocol fr** command, note that if the FR encapsulation format configured for an interface is changed, the system deletes all FR configurations on this interface. You will need to reconfigure FR for this interface.

Step 4 Configure the FR interface type.

Run either of the following commands as needed:

- To set the FR interface type to DTE, run:
  ```
  fr interface-type dte
  ```
  After FR is configured on an interface, the interface functions as a DTE interface by default. This step is optional.
- To set the FR interface type to DCE, run:
  ```
  fr interface-type dce
  ```

Step 5 Run:

```
ip address ip-address { mask | mask-length } [ sub ]
```

An IP address is assigned to the FR interface.

Step 6 Run:

```
fr dlci dlci
```

The DLCI is configured for the interface.

Step 7 Run:

```
quit
```

Exit from the DLCI view.

Step 8 Run:

```
fr map ppp interface interface-type interface-number dlci-number
```

An FR PVC is mapped to a PPP link.

Step 9 Run:

```
fr lmi type { ansi | nonstandard | q933a }
```

The FR LMI protocol type is configured.

By default, the LMI protocol type of an FR interface is **q933a**.

The LMI module manages PVCs, including adding PVCs, deleting PVCs, and detecting PVC status and integrity of PVC links. Currently, three standard LMI protocol types are supported:

- **ansi**: is used if both ends use the encapsulation format defined in ANSI T1.617.
- **nonstandard**: can be used if the peer end is a Cisco device.
- **q933a**: is used if both ends use the encapsulation format defined in Q933A.

The two DCE devices must be configured with the same FR LMI protocol type. Otherwise, they cannot communicate with each other.

----End

2.5.3 Checking the Configuration

After PPPoFR is successfully configured, you can view FR configurations.

Prerequisites

All PPPoFR configurations are complete.

Procedure

- Run the **display fr interface** [*interface-type interface-number*[*.subnumber*]] command to check the FR protocol status and information about FR interfaces.
- Run the **display fr map-info** [**interface** *interface-type interface-number*[*.subnumber*]] command to check mappings between protocol addresses and DLCI values.

----End

Example

Run the **display fr interface** [*interface-type interface-number*[*.subnumber*]] command to view the FR protocol status and information about FR interfaces.

```
<Huawei> display fr interface
MFR0/0/1, DCE, physical up, protocol up
Serial2/0/0, DTE, physical down, protocol down
```

Run the **display fr map-info** [**interface** *interface-type interface-number*[*.subnumber*]] command to view mappings between protocol addresses and DLCI values.

```
<Huawei> display fr map-info
Map Statistics for interface MFR0/0/1 (DCE)
  DLCI = 100, PPP over FR Virtual-Template10, MFR0/0/1
    create time = 2010/12/02 19:54:23, status = ACTIVE
    encapsulation = ietf, vlink = 4
```

2.6 Configuring PPPoMFR

FR can bear PPP services. With MFR, devices can establish an E2E PPP connection through MFR links over an FR network. PPPoMFR bundles multiple physical links (including links connected to channelized serial interfaces) to provide higher bandwidth.

MPoFR is an extension to PPPoFR. MPoFR allows MP fragments to be transmitted along FR PVCs.

2.6.1 Establishing the Configuration Task

Before configuring PPPoMFR, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task quickly and efficiently.

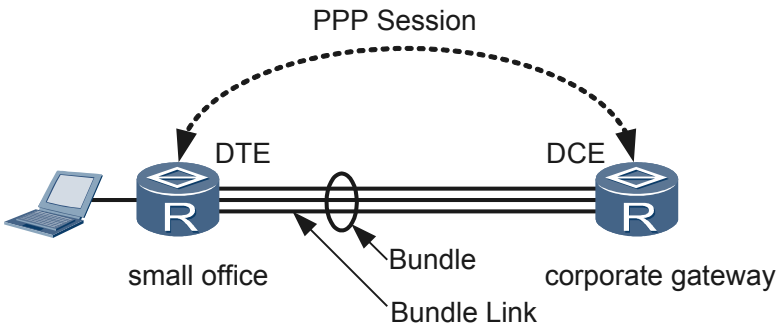
Applicable Environment

FR simplifies frame encapsulation. It features lower communication delays and higher network throughput, compared to other data link layer protocols. FR does not provide authentication functions, and therefore cannot guarantee that only valid users access enterprise networks. PPP is a data link layer protocol used to transmit network layer packets on P2P links. It provides effective authentication functions and is extensible. Configuring PPPoFR allows devices to check validity of login users, ensuring FR network security.

In most cases, a physical FR link works at the same rate as that supported by an E1 or a T1 link, which cannot provide sufficient bandwidth for upper-layer services. Upgrading the existing FR devices requires huge investments and complicated technical supports. If existing FR devices are connected through multiple FR physical links, configure MFR on UNIs and NNIs to increase bandwidth without changing the network topology.

As shown in **Figure 2-9**, an MFR link is called a bundle, and physical member links are called bundle links. The bandwidth of an MFR link is the bandwidth sum of its member links. PPP packets can be transmitted over a public FR network, a private FR network of an enterprise, or an FR network comprising devices directly connected through leased lines.

Figure 2-9 Networking diagram for FR user authentication and access



Pre-configuration Tasks

Before configuring PPPoMFR, complete the following tasks:

- Configuring physical attributes for FR interfaces
- Configuring VT interfaces

Data Preparation

To configure PPPoMFR, you need the following data.

No.	Data
1	Number, IP address, and DLCI value of each MFR interface; IP address mapped to the DLCI value of each MFR interface and mask of the IP address
2	Number of each FR interface or sub-interface
3	(Optional) DLCI of each MFR member link, interval at which Hello packets are sent, waiting time before a Hello packet is retransmitted, number of Hello packet retransmissions, and maximum fragment size as well as DLCI, maximum fragment size, and slide window size of the MFR link

2.6.2 Creating and Configuring an MFR Interface

You can configure logical MFR interfaces to allow PPP packets to travel over an FR network through MFR links.

Context

When an FR network bears PPP services, FR devices must be able to forward PPP packets to destinations. FR devices use DLCI values to identify VCs. To transmit PPP services, FR devices must be configured with mappings between DLCI values and upper-layer protocol addresses of their peer devices.

To allow PPP packets to travel through an MFR link, configure mappings between the DLCI value of the MFR interface and destination IP addresses.

NOTE

Unless otherwise specified, configure both ends of an FR link.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface mfr interface-number[.subnumber [ p2mp | p2p ] ]
```

An MFR interface is created and the MFR interface view is displayed.

To create an MFR sub-interface on a P2MP link, run the **interface mfr** *interface-number.subnumber* **p2mp** command.

Step 3 Run:

```
ip address ip-address { mask | mask-length } [ sub ]
```

An IP address is configured for the MFR interface.

Step 4 Configure static address mappings for MFR access between DTE and DCE.

The MFR address mapping function associates the protocol address of a peer device with the FR address (DLCI value) of the local device. This helps upper-layer protocols of the local device locate the peer device based on the protocol address of the peer device.

1. Configure the MFR interface type.

   Perform the following operations on DTE and DCE devices:

   - On a DTE device, run the **fr interface-type dte** command to set the MFR interface type to DTE.

     This step can be skipped if the **link-protocol fr** command has been used on an MFR interface, which allows the DTE interface type to take effect by default.
   - On a DCE device, run the **fr interface-type dce** command to set the MFR interface type to DCE.
2. Run the **fr dlci** *dlci* command to set a DLCI value for the MFR interface.
3. Run the **quit** command to exit from the DLCI view.
4. Run the **fr map ppp interface** *interface-type interface-number dlci-number* command to map an MFR link to a PPP link.

----End

2.6.3 Adding Physical Interfaces to an MFR Interface

MFR is a cost-effective solution provided for FR users. MFR bundles multiple physical interfaces on a device to provide higher bandwidth for users without increasing investments on network devices.

Context

An MFR link is called a bundle, and physical member links are called bundle links. The bandwidth of an MFR link is the bandwidth sum of its member links. An MFR interface represents a bundle, and a bundle can contain multiple bundle links, each of which corresponds to a physical interface. A bundle manages its bundle links. Bundle links are visible at the physical layer, and bundle links are visible at the data link layer.

The function and configuration of an MFR interface are the same as those of an ordinary FR interface. After a physical interface is added to an MFR interface, the original physical layer and data link layer parameters of the physical interface are replaced by the parameters of the MFR interface.

The status of every physical interface added to an MFR interface determines the status of the MFR interface. As long as one physical interface of the MFR interface is available, the MFR interface is available for upper-layer FR applications. If all physical interfaces of the MFR interface are unavailable, the MFR interface is unavailable for upper-layer FR applications. An MFR interface is a logical interface working at the data link layer, and its member interfaces are physical interfaces working at the physical layer.

NOTE

Unless otherwise specified, configure both ends of an FR link.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The FR interface view is displayed.

Step 3 Run:

```
link-protocol fr mfr interface-number
```

The FR interface is added to a specified MFR interface.

A maximum of 128 physical interfaces can be added to an MFR interface.

----End

2.6.4 (Optional) Configuring Parameters for an MFR Link and Its Member Links

Configuring interface identifiers, parameters for packets detecting link status, and the maximum MFR fragment size and slide window size improves MFR maintainability and performance.

Context

After configuring basic MFR functions, configure the following functions to improve MFR maintainability:

- To identify an MFR interface and its member interfaces, you can change identifiers of the interfaces.

  For the detailed configuration procedure, see **Configure interface identifiers**.

- After an MFR link is configured, the two ends of the link must keep informed of the other's MFR PVC status. This prevents packet forwarding failures if one end fails. MFR sends packets to detect link status to ensure reliable PVC status. Modify packet parameters according to network conditions.

  For the detailed configuration procedure, see **Configure parameters for packets detecting link status**.

You can configure the maximum fragment size and slide window size for low-speed links working at rates lower than 768 kbit/s to improve MFR performance:

- If a large packet is transmitted through only one member link, other member links are idle. As a result, the MFR link works inefficiently. Set the maximum MFR fragment size to reduce transmission delays and improve transmission efficiency of the MFR link.

  The maximum MFR fragment size is determined by the member interface working at the lowest speed. For example, if T1 interfaces are bundled on one end and 64 kbit/s interfaces are bundled on the other end, both devices are configured with the maximum MFR fragment size based on the remote interfaces. For details about fragmentation, see **Table 2-6**.

Table 2-6 Recommended fragmentation for less than 10 ms link transmission delays

Lowest Link Rate (in kbps)	Recommended Maximum Fragment Size (in bytes)
56	70
64	80
128	160
256	320
512	640
768	1000
1536	1600

For the detailed configuration procedure, see **Configure the maximum MFR fragment size**.

- After an MFR link is configured, the two ends of the link must keep informed of the other's MFR PVC status. This prevents packet forwarding failures if one end fails. MFR sends packets to detect link status to ensure reliable PVC status. Modify packet parameters according to network conditions.

  For the detailed configuration procedure, see **Configure the MFR slide window size**.

NOTE

Unless otherwise specified, configure both ends of an FR link.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Configure interface identifiers.

- Configure an identifier for an FR interface.
  1. Run the **interface** *interface-type interface-number* command to enter the interface view.
  2. Run the **mfr link-name** *name* command to configure an MFR LID for an FR link.

     The default MFR LID is the name of the physical interface.
  3. Run the **quit** command to exit from the FR interface view.
- Configure an identifier for an MFR interface.
  1. Run the **interface mfr** *interface-number* command to enter the view of an MFR interface.

     Only MFR interfaces can be configured with interface identifiers.
  2. Run the **mfr bundle-name** *name* command to configure an MFR BID for the MFR link.

     The default MFR BID format is MFR plus the number of the MFR interface.

The **mfr bundle-name** command applies only to MFR interfaces not MFR sub-interfaces.

3. Run the **quit** command to exit from the MFR interface view.

Step 3 Configure parameters for packets detecting link status.

1. Run the **interface** *interface-type interface-number* command to enter the view of an FR interface.
2. Run the **mfr timer hello** *seconds* command to set an interval at which Hello packets are sent on the FR link.

   By default, a Hello packet is sent every 10 seconds on the FR link.
3. Run the **mfr timer ack** *seconds* command to set the timeout period for ACK packets on the FR link.

   By default, an FR link waits a maximum of 4 seconds for an ACK packet.
4. Run the **mfr retry** *number* command to set the number of attempts to resend a Hello packet on the FR link.

   By default, a Hello packet can be resent twice on an FR link.
5. Run the **quit** command to exit from the FR interface view.

The two ends of a link perform the following operations to maintain the link status:

1. The sender sends a Hello packet to the receiver through the MFR link. The interval at which Hello packets are sent can be specified using the **mfr timer hello** *hello-interval* command.
2. There are two possible results as the sender does or does not receive an ACK packet:
   - The sender receives an ACK packet before the timeout period expires, and the MFR link is successfully established. The timeout period for a Hello packet can be specified using the **mfr timer ack** *ack-timeout* command.
   - The sender does not receive any ACK packet before the timeout period expires, and the MFR link fails to be established. The sender will send a Hello packet again, expecting to receive an ACK packet. The maximum times for resending a Hello packet can be specified using the **mfr retry** *retry-number* command.

If the sender does not receive an ACK packet after a maximum number of Hello packets are sent, the system considers that the data link layer protocol of the FR link fails.

Step 4 Configure the maximum MFR fragment size.

Configure the maximum MFR fragment size on an MFR interface.

1. Run the **interface mfr** *interface-number* command to enter the view of an MFR interface.
2. Run the **mfr fragment** command to enable MFR fragmentation.

   By default, MFR fragmentation is disabled.
3. Run the **mfr fragment-size** *bytes* command to set the maximum fragment size allowed by the MFR link.

   Configuring the same maximum fragment size for both ends of an MFR link is recommended to maximize efficiency.

   By default, the maximum fragment size is 300 bytes.
4. Run the **quit** command to exit from the MFR interface view.

Step 5 Configure the MFR slide window size.

1. Run the **interface mfr** *interface-number* command to enter the view of an MFR interface.

2. Run the **mfr window-size** *number* command to set the MFR slide window size.

   The MFR slide window size indicates the maximum number of fragments that the slide window contains when an MFR interface reassembles fragments using the slide window algorithm. By configuring the slide window size, you can restrict the volume of traffic transmitted on the network to improve network performance.

NOTE

- The slide window size determines the speed at which fragments are reassembled. Find the trade-off between the number of MFR member links and the slide window size. The default slide window size is recommended.
- By default, the slide window size is equal to the number of physical interfaces bundled into the MFR interface.

----End

2.6.5 Checking the Configuration

After PPPoMFR is successfully configured, you can view MFR configurations.

Prerequisites

All PPPoMFR configurations are complete.

Procedure

- Run the **display fr interface** [*interface-type interface-number*[.*subnumber*]] command to check the FR protocol status and information about MFR interfaces.
- Run the **display fr map-info** [**interface** *interface-type interface-number*[.*subnumber*]] command to check mappings between protocol addresses and DLCI values.
- Run the **display interface brief** command to view the status and configuration of interfaces.
- Run the **display interface mfr** [*interface-number*] command to check status and configurations of the MFR interface.

----End

Example

Run the **display fr interface** [*interface-type interface-number*[.*subnumber*]] command to view the FR protocol status and information about MFR interfaces.

```
<Huawei> display fr interface
MFR0/0/1, DCE, physical up, protocol up
Serial2/0/0, DTE, physical down, protocol down
```

Run the **display fr map-info** [**interface** *interface-type interface-number*[.*subnumber*]] command to view mappings between protocol addresses and DLCI values.

```
<Huawei> display fr map-info
Map Statistics for interface MFR0/0/0 (DCE)
  DLCI = 30, PPP over FR Virtual-Template10, MFR0/0/0
    create time = 2010/12/27 20:50:57, status = ACTIVE
    encapsulation = ietf, vlink = 0
```

Run the **display interface brief** command. The command output shows brief information about the status and configuration of interfaces.

```
<Huawei> display interface brief | begin MFR
PHY: Physical
*down: administratively down
(l): loopback
```

```
(s): spoofing
(b): BFD down
(d): Dampening Suppressed
InUti/OutUti: input utility/output utility
Interface                   PHY   Protocol InUti OutUti   inErrors  outErrors
MFR0/0/1                   up    up       0.04%  0.04%          0          0
NULL0                        up    up(s)       0%     0%          0          0
Serial1/0/0                  *down down        0%     0%          0          0
```

Run the **display interface mfr** command. The command output shows the configurations of an MFR interface. By default, the system does not display the default description of an interface.

```
<Huawei> display interface MFR
MFR0/0/1 current state : UP
Line protocol current state : UP
Description:HUAWEI, AR Series, MFR0/0/1 Interface
Route Port,The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet Address is 1.1.1.1/24
Link layer protocol is FR IETF
  LMI DLCI is 0, LMI type is ANSI, frame relay DCE
  LMI status enquiry received 0, LMI status sent 0
  LMI status enquiry timeout 0, LMI message discarded 0
Physical is MFR, baudrate: 0 bps
Current system time: 2010-12-02 19:56:43-08:00
    Last 300 seconds input rate 11 bytes/sec, 1 packets/sec
    Last 300 seconds output rate 20 bytes/sec, 1 packets/sec
    Realtime 0 seconds input rate 0 bytes/sec, 0 packets/sec
    Realtime 0 seconds output rate 0 bytes/sec, 0 packets/sec
    1 packets input, 30 bytes, 0 drops
    1 packets output, 25 bytes, 0 drops
    Input bandwidth utilization  : 12.00%
    Output bandwidth utilization : 15.00%
```

2.7 Configuring FRoIP

FRoIP allows FR services to be transmitted over an IP network.

2.7.1 Establishing the Configuration Task

Before configuring FRoIP, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration.

Applicable Environment

A device must be enabled with the FR switching function when the device functions as an FR switch or needs to implement data exchange on an FR network.

The FR switching function can be implemented on the router in the following modes:

- FR switching routes: After the outbound interface and the outbound DLCI value are specified on an interface, a route is created to forward packets on the interface.
- FR switching PVCs: A route is created on two interfaces of a device to forward packets to implement the FR switching function.

Pre-configuration Tasks

Before configuring FR switching function, complete the following tasks:

- Configuring physical attributes of Serial or MFR interfaces
- Configuring basic functions of FR DTE/DCE devices

NOTE

Only a serial or an MFR interface can be specified as the inbound interface, and only a tunnel interface can be specified as the outbound interface.

The type of an interface enabled with FR switching must be configured as DCE by running the **fr interface-type** command. Otherwise, FR switching does not take effect.

Data Preparation

To complete the configuration, you need the following data.

No.	Data
1	FR interface number of the router, the IP address of peer interface, the local and remote DLCI values, and the name of a PVC used for FR switching

2.7.2 Configuring Basic FRoIP Functions

FR switching routes or FR switching PVCs can be used to implement FRoIP.

Context

FR switching routes and FR switching PVCs have the same usage scenario except that the FR switching function can be disabled only by deleting FR configurations, whereas the PVC switching function can be enabled or disabled for a specific PVC.

Procedure

Step 1 On the router, run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
fr switching
```

The FR switching function is enabled.

Step 3 Configure the FR switching function.

- FR switching routes:
  - Select one of interface views based on actual scenarios and network requirements.
    - Run:

      ```
      interface interface-type interface-number
      ```

      The FR Serial interface view is displayed.
    - Run:

      ```
      interface mfr interface-number
      ```

      The MFR interface view is displayed.
  - Run:

    ```
    fr dlci-switch in-dlci interface interface-type interface-number dlci out-dlci
    ```

Static routes used for FR switching are created on the inbound interface.

- FR switching PVCs.
  - Run:

    fr switch *name* [**interface** *interface-type in-interface-number* **dlci** *in-dlci* **interface** *interface-type out-interface-number* **dlci** *out-dlci*]

    A PVC used for FR switching is configured.

    After the switching PVC is configured, running the **shutdown** or **undo shutdown** command in the FR switching view can add or delete the corresponding route to or from the routing table.

    NOTE

    A PVC configured with the static mapping between the DLCI and FR address cannot be configured with FR switching.

----End

2.7.3 Checking the Configuration

After FRoIP is successfully configured, you can view information about FR switching routes and FR switching PVCs.

Prerequisites

The FRoIP configurations are completed.

Procedure

- Run the **display fr dlci-switch** [**interface** *interface-type interface-number*] command to check information about the configured FR switching routes.
- Run the **display fr switch-table** [**name** *pvc-name*] command to check information about the configured FR switching PVCs.

----End

Example

Run the **display fr dlci-switch** command to check information about FR switching routes.

```
<Huawei> display fr dlci-switch
Frame relay switch statistics for board 0
Status   Interface(DLCI)    ---------->   Interface(DLCI)
Inactive Serial1/0/0(110)                Tunnel0/0/1(220)
Active   Tunnel0/0/1(220)                Serial1/0/0(110)
```

Run the **display fr switch-table** command to check statistics about FR switching PVCs.

```
<Huawei> display fr switch-table
Total PVC switch records:1
PVC-Name                      Status   Interface(DLCI) <-----> Interface(DLCI)
pvc1                          Active   Serial1/0/0(300)        Tunnel0/0/2(500)
```

2.8 FR QoS Configuration

On a Frame Relay (FR) interface, use the common QoS mechanism to provide traffic policing, traffic shaping, congestion management, and congestion avoidance for users. Besides the common QoS mechanism, an FR network also has its QoS mechanism.

2.8.1 Establishing the Configuration Task

Before configuring FR QoS, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task quickly and accurately.

Applicable Environment

In addition to the common QoS mechanism, an FR network has its own QoS mechanism, which provides functions such as FR traffic shaping, Discard Eligibility (DE) rule list, and FR queue management. FR QoS can provide QoS services for both interfaces and each virtual circuit (VC) on the interfaces, whereas common QoS can provide QoS services only for interfaces. Compared to common QoS, FR QoS provides services more flexibly.

The configuration roadmap is as follows:

1. Create and configure an FR class and set FR QoS parameters in the FR class, including the traffic shaping parameters, queue type, and fragment size.
2. Associate the FR interface or FR VC with the FR class.

After the preceding configurations, FR QoS parameters are applied to the FR interface or FR VC.

Pre-configuration Tasks

Before configuring FR QoS, complete the following task:

- Setting parameters on an FR interface, for example, IP address, link layer protocol, and data link connection identifier (DLCI)

Data Preparation

To configure FR QoS, you need the following data.

No.	Data
1	Name of the FR class and number of the FR interface or FR VC associated with the FR class
2	Number of the FR interface enabled with traffic shaping and traffic shaping parameters including the committed burst size (CBS), committed information rate (CIR), allowed CIR, and traffic shaping adaptation parameters
3	Number of the DE rule list, parameters of the interface-based/IP-based DE rule list, and numbers of the FR interface and FR VC to which the DE rule list is applied
4	Number of the FR interface where the queue type needs to be set to PVC priority queuing (PVC PQ), length of each PVC PQ queue, and name of the FR class
5	Fragment size

2.8.2 Configuring an FR Class

Before configuring FR QoS, create an FR class and set QoS parameters in the FR class. Then associate the FR class with an FR VC.

Context

When an FR VC provides QoS services, it prefers the FR class associated with the FR VC. If the FR VC is not bound to any FR class, it uses the FR class associated with the FR interface or sub-interface where the FR VC is established.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
fr class name
```

An FR class is created and the FR class view is displayed.

By default, no FR class is created.

NOTE

You can set different parameters for FR QoS including FR traffic shaping and FR queue management in the FR class view.

Step 3 Run:

```
apply policy policy-name { inbound | outbound }
```

A traffic policy is applied in the FR class view.

The traffic policy to be applied has been created using the **traffic policy** command. For details, see Traffic Policy Configuration in the *Huawei AR2200 Series Enterprise Routers Configuration Guide - QoS*.

NOTE

On the AR2200, you can apply a traffic policy to an FR class or FR interface:

- A traffic policy that contains class-based queue (CBQ) can only be applied to an FR interface.
- A traffic policy that does not contain CBQ can be applied to either an FR class or an FR interface. You are advised to apply a traffic policy to an FR class.

FR class does not support traffic policy nesting.

Step 4 Run:

```
quit
```

Return to the system view.

Step 5 Associate the FR class with an FR interface or an FR VC.

NOTE

An FR class can be associated with an FR interface or an FR VC, or both an FR interface and an FR VC. After an FR class is associated with an FR interface, QoS parameters in the FR class are applied to all VCs on the interface.

- To associate the FR class with an FR interface, perform the following steps:
  1. Run:
     interface *interface-type interface-number*
     The FR interface or sub-interface view is displayed.
  2. Run:
     fr-class *class-name*
     The FR class is associated with the FR interface or sub-interface.
  3. Run:
     quit
     Return to the system view.
- To associate the FR class with an FR VC, perform the following steps:
  1. Run:
     interface *interface-type interface-number*
     The FR interface or sub-interface view is displayed.
  2. Run:
     fr dlci *dlci*
     The FR VC view is displayed.
  3. Run:
     fr-class *class-name*
     The FR class is associated with the FR VC.
  4. Run:
     quit
     Return to the system view.

----End

2.8.3 Configuring FR Traffic Shaping

FR traffic shaping is applied to an outbound interface to control outgoing packets. Generally, FR traffic shaping is applied to the Data Terminal Equipment (DTE) side on an FR network.

Context

FR traffic shaping limits the rate of outgoing packets and burst packets from an FR VC so that these packets are sent out at an even rate.

FR traffic shaping uses the following parameters:

- CBS: indicates the volume of traffic that an FR network is committed to transmit within the interval specified as Tc. When network congestion occurs, the FR network can successfully transmit this volume of traffic.
- CIR: indicates the minimum transmission rate that a VC is committed to provide. Users can send data at the CIR even when network congestion occurs.
- Allowed CIR: indicates the transmission rate that an FR network can provide in normal situations. When the network is not congested, users can send data at the allowed CIR.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The FR interface view is displayed.

Step 3 Run:

```
fr traffic-shaping
```

FR traffic shaping is enabled.

Step 4 Run:

```
quit
```

Return to the system view.

Step 5 Run:

```
fr class name
```

An FR class is created and the FR class view is displayed.

By default, no FR class is created.

Step 6 Run:

```
cbs outbound committed-burst-size
```

The CBS is set on an FR VC in the outbound direction.

By default, the CBS of FR VCs is 1500 bytes.

Step 7 Run:

```
cir allow outbound committed-information-rate
```

The allowed CIR is set on an FR VC.

By default, the allowed CIR of FR VCs is 56 kbit/s.

Step 8 Run:

```
cir committed-information-rate
```

The CIR is set on an FR VC.

By default, the CIR of FR VCs is 56 kbit/s.

The allowed CIR set by step 7 cannot be greater than the CIR set by step 8.

Step 9 Run:

```
traffic-shaping adaptation { becn percentage | interface-congestion number }
```

Traffic shaping adaptation is enabled.

By default, traffic shaping adaptation is enabled in FR traffic shaping. Traffic is adjusted based on the backward explicit congestion notification (BECN) bit by 25% of the transmission rate.

Step 10 Run:

```
quit
```

Return to the system view.

Step 11 Associate the FR class with an FR interface or an FR VC.

NOTE

An FR class can be associated with an FR interface or an FR VC, or both an FR interface and an FR VC. After an FR class is associated with an FR interface, QoS parameters in the FR class are applied to all VCs on the interface.

- To associate the FR class with an FR interface, perform the following steps:
  1. Run:
     interface *interface-type interface-number*
     The FR interface or sub-interface view is displayed.
  2. Run:
     fr-class *class-name*
     The FR class is associated with the FR interface or sub-interface.
  3. Run:
     quit
     Return to the system view.
- To associate the FR class with an FR VC, perform the following steps:
  1. Run:
     interface *interface-type interface-number*
     The FR interface or sub-interface view is displayed.
  2. Run:
     fr dlci *dlci*
     The FR VC view is displayed.
  3. Run:
     fr-class *class-name*
     The FR class is associated with the FR VC.
  4. Run:
     quit
     Return to the system view.

----End

2.8.4 Configuring an FR DE Rule List

The AR2200 supports interface- and IP-based FR Discard Eligibility (DE) rule lists.

Context

If a Discard Eligibility (DE) rule list is applied to an FR VC, and packets transmitted over the VC match rules in the DE rule list, the DE bit of the packets is set to 1.

On an FR network, packets with the DE value 1 are discarded first when congestion occurs. The DE bit is set to 1 in the following situations:

- After an interface-based DE rule list is configured, a router sets the DE bit of packets received from a specified interface to 1 before forwarding them as FR packets.

- After an IP-based DE rule list is configured, a router identifies the IP packets to be marked based on the configured DE rules and sets the DE bit of these packets to 1 before forwarding them as FR packets.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Configure a DE rule list.

- To configure an interface-based DE rule list, run:

  ```
  fr del list-number inbound-interface interface-type interface-number
  ```

  By default, no interface-based DE rule list is created.

- To configure an IP-based DE rule list, run:

  ```
  fr del list-number protocol ip [ fragments | acl acl-number | less-than bytes
  | greater-than bytes | source-port { tcp ports | udp ports } | destination-
  port { tcp ports | udp ports } ]
  ```

  By default, no IP-based DE rule list is created.

Step 3 Run:

```
interface interface-type interface-number
```

The FR interface or sub-interface view is displayed.

Step 4 Run:

```
fr de del list-number dlci dlci-number
```

The DE rule list is applied to a specified FR VC.

By default, no DE rule list is applied to an FR VC.

----End

2.8.5 Configuring FR Queue Management

PVC Priority Queuing (PQ) can be applied only to FR interfaces.

Context

On an FR interface, you can configure the following queues provided by the common QoS mechanism:

- Priority Queuing (PQ)
- Weighted Fair Queue (WFQ)
- Class-based Queuing (CBQ)
- PQ+WFQ

After FR traffic shaping is enabled on an FR interface, the queue type can only be First In First Out (FIFO) or PVC PQ.

PVC PQ supports four types of queue priorities: top, middle, normal, and bottom, which are listed in descending order of priority. Packets are sent based on their queue priorities. Packets in the top-priority queue are sent first, then packets in the middle-priority queue, then packets

in the normal-priority queue, and finally packets in the bottom-priority queue. Each FR VC has its PVC PQ queue priority. Packets sent out from the VC can only enter the corresponding PVC PQ queue.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The FR interface view is displayed.

Step 3 Run:

```
fr pvc-pq [ top-limit middle-limit normal-limit bottom-limit ]
```

The queue type on the FR interface is set to PVC PQ and the queue length is set.

By default, the queue type of an FR interface is FIFO.

Step 4 Run:

```
quit
```

Return to the system view.

Step 5 Run:

```
fr class name
```

The FR class view is displayed.

Step 6 Run:

```
pvc-pq { top | middle | normal | bottom }
```

A PVC PQ queue is specified for packets transmitted over FR VCs.

By default, packets transmitted over FR VCs are placed into the normal-priority queue of PVC PQ.

Step 7 Run:

```
quit
```

Return to the system view.

Step 8 Associate the FR class with an FR interface or an FR VC.

NOTE

An FR class can be associated with an FR interface or an FR VC, or both an FR interface and an FR VC. After an FR class is associated with an FR interface, QoS parameters in the FR class are applied to all VCs on the interface.

- To associate the FR class with an FR interface, perform the following steps:
  1. Run:

     ```
     interface interface-type interface-number
     ```

     The FR interface or sub-interface view is displayed.
  2. Run:

```
fr-class class-name
```

The FR class is associated with the FR interface or sub-interface.

3. Run:

```
quit
```

Return to the system view.

- To associate the FR class with an FR VC, perform the following steps:
  1. Run:

```
interface interface-type interface-number
```

The FR interface or sub-interface view is displayed.

  2. Run:

```
fr dlci dlci
```

The FR VC view is displayed.

  3. Run:

```
fr-class class-name
```

The FR class is associated with the FR VC.

  4. Run:

```
quit
```

Return to the system view.

----End

2.8.6 Configuring FR Fragmentation

FR fragmentation shortens the transmission delay caused by large data packets on a low-speed FR link.

Context

When voice and data packets are sent simultaneously, bandwidth is occupied by large data packets for long periods of time. Consequently, voice packets are delayed or discarded, and the voice quality deteriorates. FR fragmentation minimizes the voice delay and ensures real-time voice transmission. FR fragmentation breaks up a large data packet into several smaller data packets. Voice packets and the smaller data packets are sent alternately to ensure that voice packets are processed in a timely manner. This shortens the voice delay.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
fr class name
```

The FR class view is displayed.

Step 3 Run:

```
fragment [ fragment-size ]
```

FR fragmentation is enabled on an FR VC.

By default, FR fragmentation is disabled on an FR VC.

Step 4 Run:

```
quit
```

Return to the system view.

Step 5 Associate the FR class with an FR interface or an FR VC.

NOTE

An FR class can be associated with an FR interface or an FR VC, or both an FR interface and an FR VC. After an FR class is associated with an FR interface, QoS parameters in the FR class are applied to all VCs on the interface.

- To associate the FR class with an FR interface, perform the following steps:
  1. Run:
     interface *interface-type interface-number*
     The FR interface or sub-interface view is displayed.
  2. Run:
     fr-class *class-name*
     The FR class is associated with the FR interface or sub-interface.
  3. Run:
     quit
     Return to the system view.
- To associate the FR class with an FR VC, perform the following steps:
  1. Run:
     interface *interface-type interface-number*
     The FR interface or sub-interface view is displayed.
  2. Run:
     fr dlci *dlci*
     The FR VC view is displayed.
  3. Run:
     fr-class *class-name*
     The FR class is associated with the FR VC.
  4. Run:
     quit
     Return to the system view.

----End

2.8.7 Checking the Configuration

After FR QoS is configured, you can view the configuration.

Procedure

Step 1 Run:

```
display fr class
```

The FR class configuration is displayed.

Step 2 Run:

```
display fr del
```

Detailed information about the DE rule list is displayed.

Step 3 In the FR interface view, run:

```
display this
```

The configuration of the FR interface is displayed.

----End

2.9 Maintaining FR

This section describes how to maintain FR. Detailed operations include clearing FR statistics and enabling FR alarms.

2.9.1 Clearing Statistics on FR Interfaces and Dynamic Address Mapping Entries

You can clear statistics on FR interfaces and dynamic address mapping entries before recollecting statistics.

Context

Before collecting traffic statistics on an interface for a specified period, clear the existing traffic statistics on this interface.

Procedure

- Run the **reset counters interface** [*interface-type* [*interface-number*]] command to clear statistics on FR interfaces.

  The **reset counters interface** command clears statistics about sent and received packets on an interface, displayed in the last part of the **display interface** command output. Therefore, exercise caution when using this command.
- Run the **reset fr inarp** command to clear dynamic address mapping entries.

CAUTION

Running the **reset fr inarp** command to clear dynamic address mapping entries may change the network topology and invalidates existing dynamic address mappings.

----End

2.10 Configuration Examples

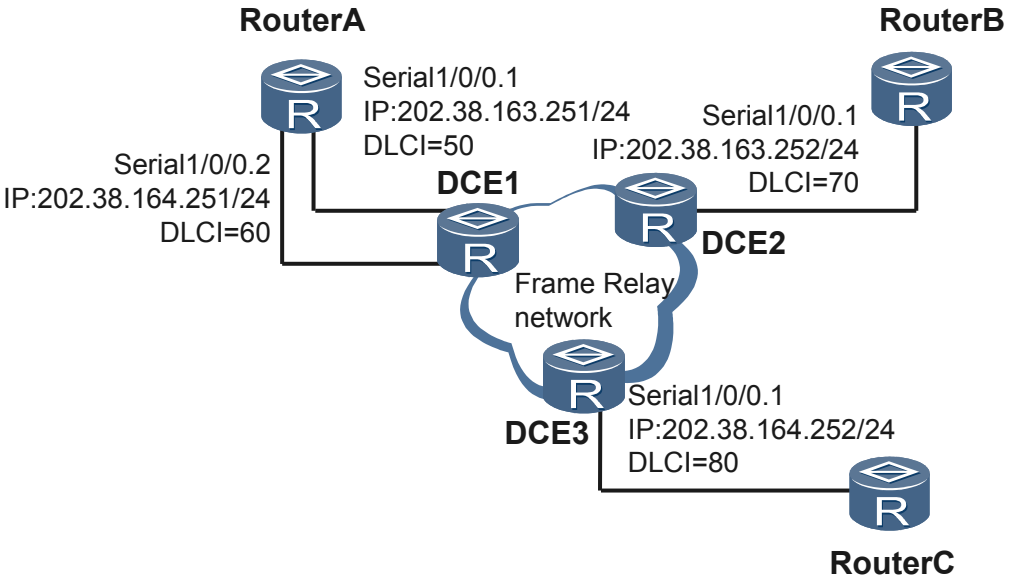
This section provides several examples for configuring FR. These configuration examples explain the networking requirements, configuration roadmap, data preparation, configuration procedure, and configuration files.

2.10.1 Example for Configuring IPoFR (Single Link)

Networking Requirements

On the FR network, RouterA, RouterB, and RouterC function as DTEs to transmit IP packets. A public FR network connects local area networks (LANs).

Figure 2-10 Example for configuring IPoFR (single link)



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure FR as the link-layer protocol on the router.
2. Set the operation mode of the interface connecting the router to the public FR network.
3. Configure the virtual circuit ID for each network segment.
4. Configure address mapping for each sub-interface.

Data Preparation

To complete the configuration, you need the following data:

- IP address of each interface and virtual circuit ID of each network segment
- DTE mode of the interface on the router that functions as a user device

Procedure

Step 1 Configure routerRouterA.

Configure FR as the link-layer protocol on the interface.

```
<Huawei> system-view
[Huawei] sysname RouterA
```

```
[RouterA] interface serial 1/0/0
[RouterA-Serial1/0/0] link-protocol fr
Warning: The encapsulation protocol of the link will be changed. Continue? [Y/N]
:y
[RouterA-Serial1/0/0] fr interface-type dte
[RouterA-Serial1/0/0] quit
```

Configure static address mapping.

```
[RouterA] interface serial 1/0/0.1
[RouterA-Serial1/0/0.1] fr dlci 50
[RouterA-fr-dlci-Serial1/0/0.1-50] quit
[RouterA-Serial1/0/0.1] ip address 202.38.163.251 24
[RouterA-Serial1/0/0.1] fr map ip 202.38.163.252 50
[RouterA-Serial1/0/0.1] quit
[RouterA] interface serial 1/0/0.2
[RouterA-Serial1/0/0.2] fr dlci 60
[RouterA-fr-dlci-Serial1/0/0.2-60] quit
[RouterA-Serial1/0/0.2] ip address 202.38.164.251 24
[RouterA-Serial1/0/0.2] fr map ip 202.38.164.252 60
[RouterA-Serial1/0/0.2] quit
```

Step 2 Configure routerRouterB.

Configure FR as the link-layer protocol on the interface.

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] interface serial 1/0/0
[RouterB-Serial1/0/0] link-protocol fr
Warning: The encapsulation protocol of the link will be changed. Continue? [Y/N]
:y
[RouterB-Serial1/0/0] fr interface-type dte
[RouterB-Serial1/0/0] quit
```

Configure static address mapping.

```
[RouterB] interface serial 1/0/0.1
[RouterB-Serial1/0/0.1] fr dlci 70
[RouterB-fr-dlci-Serial1/0/0.1-70] quit
[RouterB-Serial1/0/0.1] ip address 202.38.163.252 24
[RouterB-Serial1/0/0.1] fr map ip 202.38.163.251 70
[RouterB-Serial1/0/0.1] quit
```

Step 3 Configure routerRouterC.

Configure FR as the link-layer protocol on the interface.

```
<Huawei> system-view
[Huawei] sysname RouterC
[RouterC] interface serial 1/0/0
[RouterC-Serial1/0/0] link-protocol fr
Warning: The encapsulation protocol of the link will be changed. Continue? [Y/N]
:y
[RouterC-Serial1/0/0] fr interface-type dte
[RouterC-Serial1/0/0] quit
```

Configure static address mapping.

```
[RouterC] interface serial 1/0/0.1
[RouterC-Serial1/0/0.1] fr dlci 80
[RouterC-fr-dlci-Serial1/0/0.1-80] quit
[RouterC-Serial1/0/0.1] ip address 202.38.164.252 24
[RouterC-Serial1/0/0.1] fr map ip 202.38.164.251 80
[RouterC-Serial1/0/0.1] quit
```

Step 4 Verify the configuration.

RouterA can ping the interface of RouterB.

```
[RouterA] ping 202.38.164.252
  PING 202.38.164.252: 56  data bytes, press CTRL_C to break
    Reply from 202.38.164.252: bytes=56 Sequence=1 ttl=255 time=14 ms
    Reply from 202.38.164.252: bytes=56 Sequence=2 ttl=255 time=9 ms
    Reply from 202.38.164.252: bytes=56 Sequence=3 ttl=255 time=9 ms
    Reply from 202.38.164.252: bytes=56 Sequence=4 ttl=255 time=9 ms
    Reply from 202.38.164.252: bytes=56 Sequence=5 ttl=255 time=9 ms
  --- 202.38.164.252 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 9/10/14 ms
```

RouterB can ping the interface of RouterA. RouterA and RouterC can ping each other.

----End

Configuration Files

- Configuration file of RouterA

```
#
 sysname RouterA
#
interface
Serial1/0/0
 link-protocol fr
#
interface Serial1/0/0.1
 fr map ip 202.38.163.252 50
 fr dlci 50
 ip address 202.38.163.251 255.255.255.0
#
interface Serial1/0/0.2
 fr map ip 202.38.164.252 60
 fr dlci 60
 ip address 202.38.164.251 255.255.255.0
#
return
```

- Configuration file of RouterB

```
#
 sysname RouterB
#
interface
Serial1/0/0
 link-protocol fr
#
interface Serial1/0/0.1
 fr map ip 202.38.163.251 70
 fr dlci 70
 ip address 202.38.163.252 255.255.255.0
#
return
```

- Configuration file of RouterC

```
#
 sysname RouterC
#
interface
Serial1/0/0
 link-protocol fr
#
interface Serial1/0/0.1
 fr map ip 202.38.164.251 80
 fr dlci 80
 ip address 202.38.164.252 255.255.255.0
```

```
#
return
```

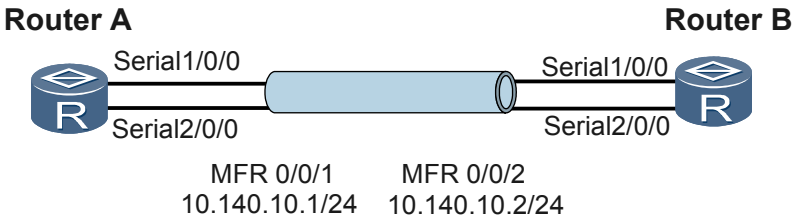
2.10.2 Example for Configuring MFR

This example shows how to configure MFR to provide higher bandwidth in typical networking.

Networking Requirements

As shown in **Figure 2-11**, Router A and Router B are directly connected through Serial 1/0/0 and Serial 2/0/0. The FR protocol is used to bundle the two serial ports for broader bandwidth.

Figure 2-11 Networking diagram of MFR bundle configuration



Configuration Roadmap

The configuration roadmap is as follows:

1. Create the MFR interface.
2. Bind the corresponding interfaces into the MFR interface.
3. Configure the working mode and the IP address of each interface.
4. Configure the VC number of the network segment.

Data Preparation

To configure MFR, you need the following data:

- IP address of the MFR interface on Router A
- IP address of the MFR interface on Router B
- VC number

Procedure

Step 1 Configure Router A.

Create and configure MFR 0/0/1.

```
<Huawei> system-view
[Huawei] sysname Router A
[Router A] interface mfr 0/0/1
[Router A-MFR0/0/1] ip address 10.140.10.1 255.255.255.0
[Router A-MFR0/0/1] fr interface-type dte
[Router A-MFR0/0/1] fr dlci 100
[Router A-MFR0/0/1-100] quit
[Router A-MFR0/0/1] fr map ip 10.140.10.2 100
[Router A-MFR0/0/1] quit
```

Bind Serial 1/0/0 and Serial 2/0/0 into MFR 0/0/1.

```
[Router A] interface serial 1/0/0
[Router A-Serial1/0/0] link-protocol fr mfr 0/0/1
[Router A-Serial1/0/0] quit
[Router A] interface serial 2/0/0
[Router A-Serial2/0/0] link-protocol fr mfr 0/0/1
[Router A-Serial2/0/0] quit
```

Step 2 Configure Router B.

Create and configure MFR 0/0/2.

```
<Huawei> system-view
[Huawei] sysname Router B
[Router B] interface mfr 0/0/2
[Router B-MFR0/0/2] ip address 10.140.10.2 255.255.255.0
[Router B-MFR0/0/2] fr interface-type dce
[Router B-MFR0/0/2] fr dlci 100
[Router B-fr-dlci-MFR0/0/2-100] quit
[Router B-MFR0/0/2] fr map ip 10.140.10.1 100
[Router B-fr-dlci-MFR0/0/2-100] quit
[Router B-MFR0/0/2] quit
```

Bind Serial 1/0/0 and Serial 2/0/0 into MFR 0/0/2.

```
[Router B] interface serial 1/0/0
[Router B-Serial1/0/0] link-protocol fr mfr 0/0/2
[Router B-Serial1/0/0] quit
[Router B] interface serial 2/0/0
[Router B-Serial2/0/0] link-protocol fr mfr 0/0/2
[Router B-Serial2/0/0] quit
```

Step 3 Check the configuration.

On Router A, ping the interface on Router B.

```
[Router A] ping 10.140.10.2
  PING 10.140.10.2: 56  data bytes, press CTRL_C to break
    Reply from 10.140.10.2: bytes=56 Sequence=1 ttl=255 time=14 ms
    Reply from 10.140.10.2: bytes=56 Sequence=2 ttl=255 time=9 ms
    Reply from 10.140.10.2: bytes=56 Sequence=3 ttl=255 time=9 ms
    Reply from 10.140.10.2: bytes=56 Sequence=4 ttl=255 time=9 ms
    Reply from 10.140.10.2: bytes=56 Sequence=5 ttl=255 time=9 ms
  --- 10.140.10.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 9/10/14 ms
```

----End

Configuration Files

- Configuration file of Router A

```
#
 sysname Router A
#
interface Serial1/0/0
 link-protocol fr MFR0/0/1
#
interface Serial2/0/0
 link-protocol fr MFR0/0/1
#
interface MFR0/0/1
 fr dlci 100
 fr map ip 10.140.10.2 100
```

```
 ip address 10.140.10.1 255.255.255.0
#
return
```

- Configuration file of Router B

```
#
 sysname Router B
#
interface Serial1/0/0
 link-protocol fr MFR0/0/2
#
interface Serial2/0/0
 link-protocol fr MFR0/0/2
#
interface MFR0/0/2
 fr interface-type dce
 fr dlci 100
 fr map ip 10.140.10.1 100
 ip address 10.140.10.2 255.255.255.0
#
return
```

2.10.3 Example for Configuring PPPoFR

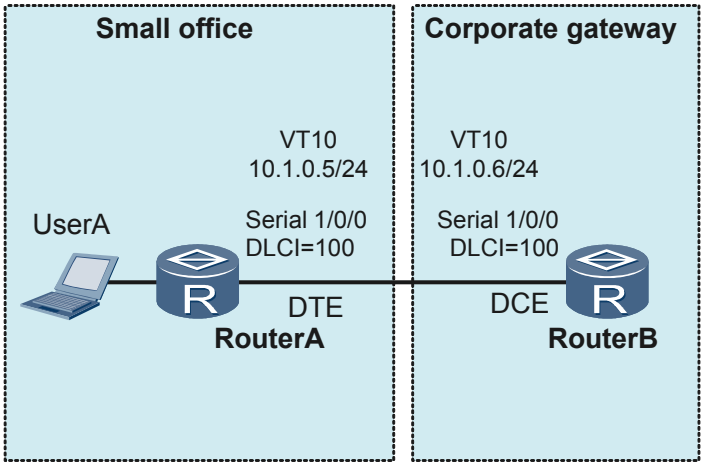
This example describes how to configure PPPoFR to allow PPP packets to be transmitted along FR PVCs in typical networking.

Networking Requirements

On the network shown in **Figure 2-12**, user A is connected to the corporate gateway Router B through Router A. Router A and Router B are connected through FR leased lines.

As FR does not provide authentication functions, Router B cannot authenticate the identities of login users. PPP provides effective authentication functions and is extensible. By configuring PPPoFR, you can add user A to the local user list of Router B for unidirectional Password Authentication Protocol (PAP) authentication of PPP packets. If authentication succeeds, PPP packets are transmitted over the FR network using an E2E PPP session.

Figure 2-12 Networking diagram for configuring PPPoFR



In this example, two routers are interconnected using serial interfaces. The interface on Router A works in FR DTE mode. The interface on Router B works in FR DCE mode.

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure user names and passwords that Router A sends to Router B.
2. Configure Router B to authenticate users in PAP mode.
3. Configure PPPoFR.

Data Preparation

To complete the configuration, you need the following data:

- User name and password of user A
- DLCI value of each interface

Procedure

Step 1 Configure user names and passwords that Router A sends to Router B.

Configure user name and password of user A.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface virtual-template 10
[RouterA-Virtual-Template10] ip address 10.1.0.5 255.255.255.0
[RouterA-Virtual-Template10] ppp pap local-user usera password simple huawei
[RouterA-Virtual-Template10] quit
```

Step 2 Configure Router B to authenticate users in PAP mode.

Add user name and password of user A to the local user list of Router B.

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] aaa
[RouterB-aaa] local-user usera password simple huawei
[RouterB-aaa] local-user usera service-type ppp
[RouterB-aaa] quit
```

Configure Router B to authenticate user A in PAP mode.

```
[RouterB] interface virtual-template 10
[RouterB-Virtual-Template10] ip address 10.1.0.6 255.255.255.0
[RouterB-Virtual-Template10] ppp authentication-mode pap
[RouterB-Virtual-Template10] quit
```

Step 3 Configure PPPoFR.

Configure Router A.

```
[RouterA] interface Serial 1/0/0
[RouterA-Serial1/0/0] link-protocol fr
Warning: The encapsulation protocol of the link will be changed. Continue? [Y/N]
:y
[RouterA-Serial1/0/0] fr interface-type dte
[RouterA-Serial1/0/0] fr dlci 100
[RouterA-fr-dlci-Serial1/0/0-100] quit
[RouterA-fr-dlci-Serial1/0/0-100] fr map ppp interface Virtual-Template 10 100
```

Configure Router B.

```
[RouterB] interface Serial 1/0/0
[RouterB-Serial1/0/0] link-protocol fr
```

```
Warning: The encapsulation protocol of the link will be changed. Continue? [Y/N]
:y
[RouterB-Serial1/0/0] fr interface-type dce
[RouterB-Serial1/0/0] fr dlci 100
[RouterB-fr-dlci-Serial1/0/0-100] quit
[RouterB-fr-dlci-Serial1/0/0-100] fr map ppp interface Virtual-Template 10 100
```

Step 4 Verify the configuration.

Check the status of the virtual access interface on Router B.

```
[RouterB] display virtual-access vt 10
Virtual-Template10:0 current state : UP
Line protocol current state : UP
Last line protocol up time : 2011-05-12 11:55:06
Description:HUAWEI, AR Series, Virtual-Template10:0 Interface
Route Port,The Maximum Transmit Unit is 1500
Link layer protocol is PPP
LCP opened, IPCP opened
Physical is PPPOFR
Current system time: 2011-05-12 14:40:09
    Last 300 seconds input rate 16 bits/sec, 0 packets/sec
    Last 300 seconds output rate 16 bits/sec, 0 packets/sec
    Realtime 0 seconds input rate 0 bits/sec, 0 packets/sec
    Realtime 0 seconds output rate 0 bits/sec, 0 packets/sec
    Input: 1991 packets,20325 bytes
           0 unicast,0 broadcast,0 multicast
    Output:1992 packets,20376 bytes
           0 unicast,0 broadcast,0 multicast
    Input bandwidth utilization  : 0.03%
    Output bandwidth utilization : 0.03%
```

Check FR address mapping information on Router B. The displayed information shows that the FR interface has learned the DLCI value of the peer interface using the dynamic address mapping function. The two interfaces can communicate with each other.

```
[RouterB] display fr map-info interface Serial 1/0/0
Map Statistics for interface Serial1/0/0 (DCE)
  DLCI = 100, PPP over FR Virtual-Template10, Serial1/0/0
    create time = 2011/05/12 11:54:58, status = ACTIVE
    encapsulation = ietf, vlink = 0
```

----End

Configuration Files

- Configuration file of Router A

```
#
 sysname RouterA
#
interface Virtual-Template10
 ip address 10.1.0.5 255.255.255.0
 ppp pap local-user usera password simple huawei
#
interface Serial1/0/0
 link-protocol fr
 fr dlci 100
 fr map ppp interface Virtual-Template10 100
#
return
```

- Configuration file of Router B

```
#
 sysname RouterB
#
aaa
 local-user usera password simple huawei
 local-user usera service-type ppp
#
```

```
interface Virtual-Template10
 ip address 10.1.0.6 255.255.255.0
 ppp authentication-mode pap
#
interface Serial1/0/0
 link-protocol fr
 fr interface-type dce
 fr dlci 100
 fr map ppp interface Virtual-Template10 100
#
return
```

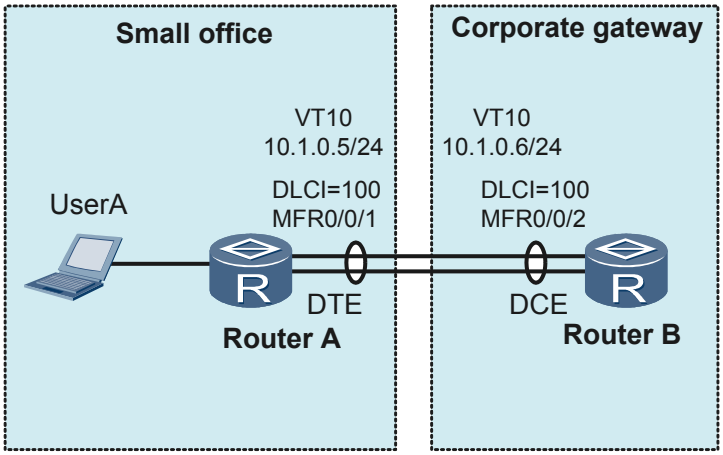
2.10.4 Example for Configuring PPPoMFR

This example describes how to configure PPPoMFR to allow PPP packets to be transmitted along MFR links in typical networking.

Networking Requirements

On the network shown in **Figure 2-13**, UserA is connected to the corporate gateway Router B through Router A. Router A and Router B are connected through serial interfaces. Service data is saved on Router B to reduce expenditures. UserA must access Router B to obtain service data at the rate of 3 Mbit/s to ensure working efficiency.

Figure 2-13 Networking diagram for configuring PPPoMFR



The following solution can meet the networking requirements:

- Router A and Router B are connected through FR leased lines. As FR does not provide authentication functions, Router B cannot authenticate the identities of login users. PPP provides effective authentication functions and is extensible. By configuring PPPoFR, you can add UserA to the local user list of Router B for unidirectional PAP authentication of PPP packets. If authentication succeeds, PPP packets are transmitted over the FR network using an E2E PPP session.
- A single serial link provides the bandwidth of 2.048 Mbit/s, which cannot meet the 3 Mbit/s bandwidth requirement. To provide 3 Mbit/s bandwidth, bundle the two links between Router A and Router B into an MFR link. In addition, static address mappings can be configured for MFR interfaces to improve MFR link stability and security.

Configuration Roadmap

The configuration roadmap is as follows:

1. Create and configure an MFR interface on each device.
2. Add physical interfaces to each MFR interface.
3. Configure user names and passwords that Router A sends to Router B.
4. Configure Router B to authenticate users in PAP mode.
5. Configure PPPoMFR.

Data Preparation

To complete the configuration, you need the following data:

- Name and IP address of each MFR interface
- DLCI value of each MFR interface
- User name and password of UserA

Procedure

Step 1 Create and configure an MFR interface on each device.

Configure Router A.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface mfr 0/0/1
[RouterA-MFR0/0/1] fr interface-type dte
[RouterA-MFR0/0/1] fr dlci 100
[RouterA-MFR0/0/1-100] quit
[RouterA-MFR0/0/1] quit
```

Configure Router B.

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] interface mfr 0/0/2
[RouterB-MFR0/0/2] link-protocol fr
Warning: The encapsulation protocol of the link will be changed. Continue? [Y/N]
:y
[RouterB-MFR0/0/2] fr interface-type dce
[RouterB-MFR0/0/2] fr dlci 100
[RouterB-MFR0/0/2-100] quit
[RouterB-MFR0/0/2] quit
```

Step 2 Add physical interfaces to an MFR interface.

Configure Router A.

```
[RouterA] interface serial 1/0/0
[RouterA-Serial1/0/0] link-protocol fr mfr 0/0/1
[RouterA-Serial1/0/0] quit
[RouterA] interface serial 2/0/0
[RouterA-Serial2/0/0] link-protocol fr mfr 0/0/1
[RouterA-Serial2/0/0] quit
```

Configure Router B.

```
[RouterB] interface serial 1/0/0
[RouterB-Serial1/0/0] link-protocol fr mfr 0/0/2
[RouterB-Serial1/0/0] quit
[RouterB] interface serial 2/0/0
[RouterB-Serial2/0/0] link-protocol fr mfr 0/0/2
[RouterB-Serial2/0/0] quit
```

Step 3 Configure user names and passwords that Router A sends to Router B.

```
[RouterA] interface Virtual-Template 10
[RouterA-Virtual-Template10] ip address 10.1.0.5 255.255.255.0
[RouterA-Virtual-Template10] ppp pap local-user usera password simple huawei
[RouterA-Virtual-Template10] quit
```

Step 4 Configure Router B to authenticate users in PAP mode.

Add user name and password of UserA to the local user list of Router B.

```
[RouterB] aaa
[RouterB-aaa] local-user usera password simple huawei
[RouterB-aaa] local-user usera service-type ppp
[RouterB-aaa] quit
```

Configure Router B to authenticate UserA in PAP mode.

```
[RouterB] interface Virtual-Template 10
[RouterB-Virtual-Template10] ip address 10.1.0.6 255.255.255.0
[RouterB-Virtual-Template10] ppp authentication-mode pap
[RouterB-Virtual-Template10] quit
```

Step 5 Configure PPPoFR.

Configure Router A.

```
[RouterA] interface mfr 0/0/1
[RouterA-MFR0/0/1] fr map ppp interface Virtual-Template 10 100
```

Configure Router B.

```
[RouterB] interface mfr 0/0/2
[RouterB-MFR0/0/2] fr map ppp interface Virtual-Template 10 100
```

Step 6 Verify the configuration.

Check the status of the virtual access interface on Router B.

```
[RouterB] display virtual-access vt 10
Virtual-Template10:1 current state : UP
Line protocol current state : UP
Last line protocol up time : 2011-05-12 15:10:34
Description:HUAWEI, AR Series, Virtual-Template10:1 Interface
Route Port,The Maximum Transmit Unit is 1500
Link layer protocol is PPP
LCP opened, IPCP opened
Physical is PPPOFR
Current system time: 2011-05-12 15:27:24
    Last 300 seconds input rate 24 bits/sec, 0 packets/sec
    Last 300 seconds output rate 24 bits/sec, 0 packets/sec
    Realtime 0 seconds input rate 0 bits/sec, 0 packets/sec
    Realtime 0 seconds output rate 0 bits/sec, 0 packets/sec
    Input: 212 packets,2529 bytes
           0 unicast,0 broadcast,0 multicast
    Output:213 packets,2580 bytes
           0 unicast,0 broadcast,0 multicast
    Input bandwidth utilization  : 0.04%
    Output bandwidth utilization : 0.04%
```

Check FR address mapping information on Router B. The displayed information shows that the FR interface has learned the DLCI value of the peer interface using the dynamic address mapping function. The two interfaces can communicate with each other.

```
[RouterB] display fr map-info interface mfr 0/0/2
Map Statistics for interface MFR0/0/2 (DCE)
  DLCI = 100, PPP over FR Virtual-Template10, MFR0/0/2
    create time = 2011/05/12 15:00:29, status = ACTIVE
    encapsulation = ietf, vlink = 0
```

----End

Configuration Files

- Configuration file of Router A

```
#
 sysname RouterA
#
interface Virtual-Template10
 ip address 10.1.0.5 255.255.255.0
 ppp pap local-user usera password simple huawei
#
interface Serial1/0/0
 link-protocol fr MFR0/0/1
#
interface Serial2/0/0
 link-protocol fr MFR0/0/1
#
interface MFR0/0/1
 fr dlci 100
 fr map ppp interface Virtual-Template10 100
#
return
```

- Configuration file of Router B

```
#
 sysname RouterB
#
aaa
 local-user usera password simple huawei
 local-user usera service-type ppp
#
interface Virtual-Template10
 ip address 10.1.0.6 255.255.255.0
 ppp authentication-mode pap
#
interface Serial1/0/0
 link-protocol fr MFR0/0/2
#
interface Serial2/0/0
 link-protocol fr MFR0/0/2
#
interface MFR0/0/2
 fr interface-type dce
 fr dlci 100
 fr map ppp interface Virtual-Template10 100
#
return
```

2.10.5 Example for Configuring MPoFR

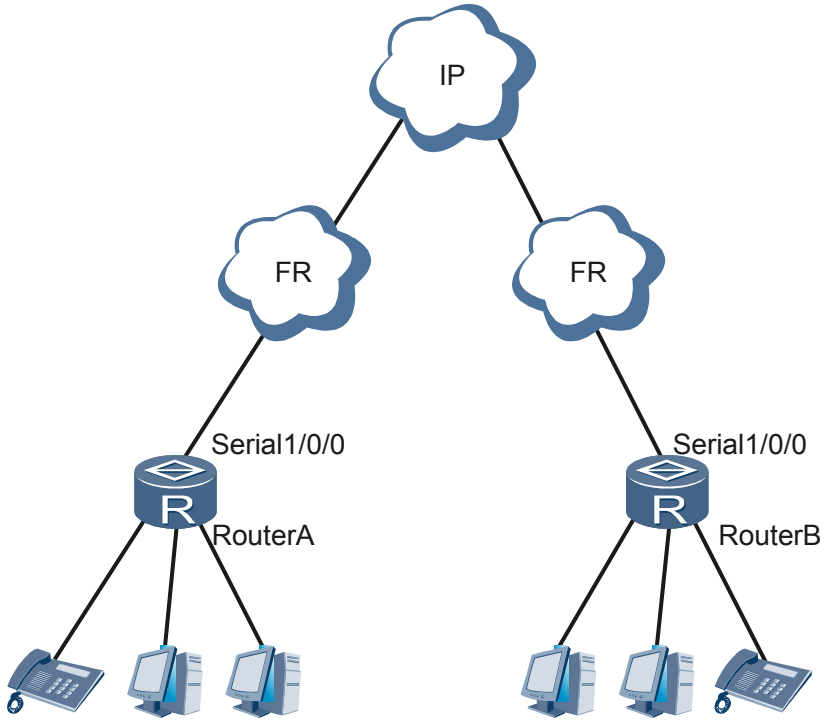
This section describes how to configure MPoFR on the AR2200.

Networking Requirements

As shown in **Figure 2-14**, branches A and B use RouterA and RouterB as their respective gateways. RouterA and RouterB connect to the IP core network through an FR link.

Branches A and B exchange voice and data services between each other. To ensure the voice service quality, data packets are fragmented to reduce the voice packet delay and jitter. In this example, MPoFR is used, and data packets are fragmented using the MP technique so that both voice packets and fragmented data packets can be transmitted over the FR link.

Figure 2-14 Networking diagram of MPoFR configuration



Configuration Roadmap

The configuration roadmap is as follows:

- On the LAN side: Connect PCs in an enterprise to RouterA through a Layer 2 Ethernet interface, and connect phones in the enterprise to RouterA through an FXS interface.
- On the WAN side: Connect RouterA to the FR network through a serial interface and configure an FR virtual circuit to transmit different types of data.

Data Preparation

To complete the configuration, you need the following data:

- On the LAN side: interface number, interface parameters, and dialup parameters
- On the WAN side:
  - On the MP link: virtual template interface number, virtual template interface address (IP address assigned by the remote end), CIR 100 kbit/s, CBS 100000 bytes, and maximum fragment delay 20 ms
  - On the MP member link: virtual template interface number
  - On the virtual circuit: virtual circuit number and member link number mapping the virtual circuit

Procedure

Step 1 Configure RouterA.

Configure LAN-side interfaces.

To connect PCs in an enterprise to RouterA through a Layer 2 Ethernet interface, configure a VLAN and a VLANIF interface. For details, see the *Huawei AR2200 Series Enterprise Routers Configuration Guide - LAN*.

To connect phones in the enterprise to RouterA through an FXS interface, configure an FXS interface, a SIP AG interface, and a SIP AG user. For details, see the *Huawei AR2200 Series Enterprise Routers Configuration Guide - Voice*.

Configure WAN-side interfaces.

- Configure an MP link.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface virtual-template 3
[RouterA-Virtual-Template3] ppp mp lfi
[RouterA-Virtual-Template3] ip address ppp-negotiate
[RouterA-Virtual-Template3] qos gts cir 100 cbs 100000
[RouterA-Virtual-Template3] ppp mp lfi delay-per-frag 20
[RouterA-Virtual-Template3] quit
```

- Configure MP member links.

```
[RouterA] interface virtual-template 1
[RouterA-Virtual-Template1] ppp mp virtual-template 3
[RouterA-Virtual-Template1] quit
[RouterA] interface virtual-template 2
[RouterA-Virtual-Template2] ppp mp virtual-template 3
[RouterA-Virtual-Template2] quit
```

- Map member links to virtual links on interfaces.

```
[RouterA] interface serial 1/0/0
[RouterA-Serial1/0/0] link-protocol fr
Warning: The encapsulation protocol of the link will be changed. Continue? [Y/
N]
:y
[RouterA-Serial1/0/0] fr dlci 100
[RouterA-fr-dlci-Serial1/0/0-100] quit
[RouterA-Serial1/0/0] fr map ppp interface Virtual-Template 1 100
[RouterA-Serial1/0/0] fr dlci 200
[RouterA-fr-dlci-Serial1/0/0-200] quit
[RouterA-Serial1/0/0] fr map ppp interface Virtual-Template 2 200
[RouterA-Serial1/0/0] quit
```

Step 2 Configure RouterB.

The configuration of RouterB is similar to that of RouterA, and is not mentioned here.

----End

Configuration Files

- Configuration file of RouterA

```
#
 sysname RouterA
#
 interface Virtual-Template3
  ppp mp
lfi
  ppp mp lfi delay-per-frag
20
  ip address ppp-
negotiate
  qos gts cir 100 cbs 100000
#
 interface Virtual-Template1
```

```
  ppp mp Virtual-Template 3
#
 interface Virtual-Template2
  ppp mp Virtual-Template 3
#
 interface Serial1/0/0
  link-protocol fr
  fr dlci 100
  fr dlci 200
  fr map ppp interface Virtual-Template1 100
  fr map ppp interface Virtual-Template2 200
#
return
```

- Configuration file of RouterB

```
#
 sysname RouterB
#
 interface Virtual-Template3
  ppp mp lfi
  ppp mp lfi delay-per-frag 20
  ip address ppp-negotiate
  qos gts cir 100 cbs 100000

#
 interface Virtual-Template1
  ppp mp Virtual-Template 3
#
 interface Virtual-Template2
  ppp mp Virtual-Template 3
#
 interface Serial1/0/0
  link-protocol fr
  fr dlci 100
  fr dlci 200
  fr map ppp interface Virtual-Template1 100
  fr map ppp interface Virtual-Template2 200
#
return
```

2.10.6 Example for Configuring FRoIP

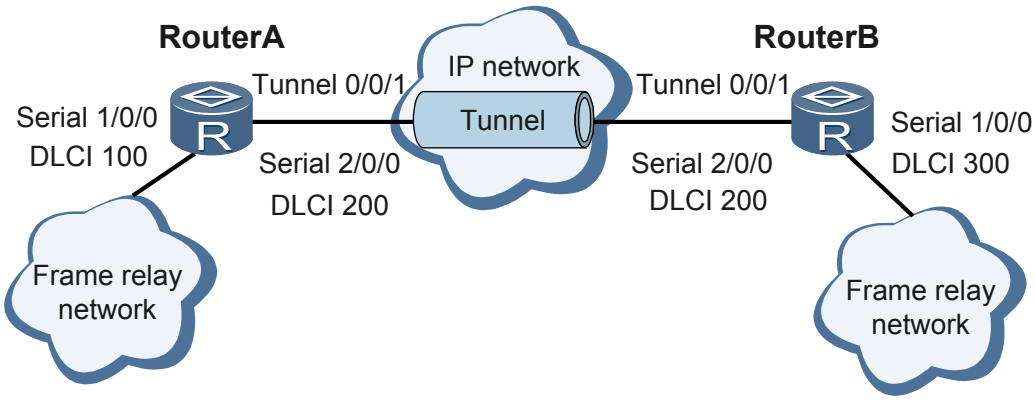
This example shows how to connect two FR networks through an IP network.

Networking Requirements

In real world situations, devices on IP networks need to transmit FR packets. FRoIP can be used to transmit FR packets through IP networks. In an FRoIP scenario, GRE tunnels are set up between two ends of an FR network. FR packets are transmitted along the GRE tunnels. Tunnel interfaces are used to implement FR switching and FR packets can be transmitted over an IP network.

As shown in **Figure 2-15**, two FR networks are connected through routerRouter A and Router B. Router A and Router B are configured with FRoIP to connect two FR networks through an IP network.

Figure 2-15 Networking for FRoIP Configurations



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the link layer protocol to FR.
2. Enable FR switching on Router A and Router B globally.
3. Configure interface types, IP addresses and DLCI values of a network segment.
4. Configure tunnel interfaces.
5. Configure FRoIP.

Data Preparation

To complete the configuration, you need the following data:

- DLCI value of each interface
- IP address of serial 2/0/0 on Router A
- IP address of serial 2/0/0 on Router B

Procedure

Step 1 Configure Router A.

Enable FR switching on router.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] fr switching
```

Configure an FR interface Serial 1/0/0.

```
[RouterA] interface serial 1/0/0
[RouterA-Serial1/0/0] link-protocol fr
[RouterA-Serial1/0/0] fr interface-type dce
[RouterA-Serial1/0/0] quit
```

Configure an IP address for Serial 2/0/0.

```
[RouterA] interface serial 2/0/0
[RouterA-Serial2/0/0] ip address 10.120.20.1 255.255.255.0
[RouterA-Serial2/0/0] quit
```

Configure a tunnel interface.

```
[RouterA] interface tunnel 0/0/1
[RouterA-Tunnel0/0/1] tunnel-protocol gre
[RouterA-Tunnel0/0/1] ip address 10.120.21.5 24
[RouterA-Tunnel0/0/1] source 10.120.20.1
[RouterA-Tunnel0/0/1] destination 10.120.20.2
[RouterA-Tunnel0/0/1] quit
```

Configure FRoIP.

```
[RouterA] interface serial 1/0/0
[RouterA-Serial1/0/0] fr dlci-switch 100 interface tunnel 0/0/1 dlci 200
[RouterA-Serial1/0/0] quit
```

Step 2 Configure Router B.

Enable FR switching on router.

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] fr switching
```

Configure an FR interface Serial 1/0/0.

```
[RouterB] interface serial 1/0/0
[RouterB-Serial1/0/0] link-protocol fr
[RouterB-Serial1/0/0] fr interface-type dce
[RouterB-Serial1/0/0] quit
```

Configure an IP address for Serial 2/0/0

```
[RouterB] interface serial 2/0/0
[RouterB-Serial2/0/0] ip address 10.120.20.2 255.255.255.0
[RouterB-Serial2/0/0] quit
```

Configure a tunnel interface.

```
[RouterB] interface tunnel 0/0/1
[RouterB-Tunnel0/0/1] tunnel-protocol gre
[RouterB-Tunnel0/0/1] ip address 10.120.21.3 24
[RouterB-Tunnel0/0/1] source 10.120.20.2
[RouterB-Tunnel0/0/1] destination 10.120.20.1
[RouterB-Tunnel0/0/1] quit
```

Configure FRoIP.

```
[RouterB] interface serial 1/0/0
[RouterB-Serial1/0/0] fr dlci-switch 300 interface tunnel 0/0/1 dlci 200
[RouterB-Serial1/0/0] quit
```

Step 3 Verify the configuration.

View the FR switching status on routerRouter B. The FR switching status on Router B is Active.

```
[RouterB] display fr dlci-switch
Frame relay switch statistics for board 1
Status   Interface(DLCI)    ---------->   Interface(DLCI)
Active   Serial1/0/0(300)                   Tunnel0/0/1(200)
Active   Tunnel0/0/1(200)                   Serial1/0/0(300)
```

Similarly, you can view FR switching inforamtion of Router A.

----End

Configuration Files

- Configuration file of RouterA

```
#
 sysname RouterA
#
fr switching
#
interface Serial1/0/0
 link-protocol fr
 fr interface-type dce
 fr dlci-switch 100 interface Tunnel0/0/1 dlci 200
#
interface Serial2/0/0
 link-protocol ppp
 ip address 10.120.20.1 255.255.255.0
#
interface Tunnel0/0/1
 ip address 10.120.21.5 255.255.255.0
 tunnel-protocol gre
 source 10.120.20.1
 destination 10.120.20.2
#
return
```

- Configuration file of RouterB

```
#
 sysname RouterB
#
fr switching
#
interface Serial1/0/0
 link-protocol fr
 fr interface-type dce
 fr dlci-switch 300 interface Tunnel0/0/1 dlci 200
#
interface Serial2/0/0
 link-protocol ppp
 ip address 10.120.20.2 255.255.255.0
#
interface Tunnel0/0/1
 ip address 10.120.21.3 255.255.255.0
 tunnel-protocol gre
 source 10.120.20.2
 destination 10.120.20.1
#
return
```

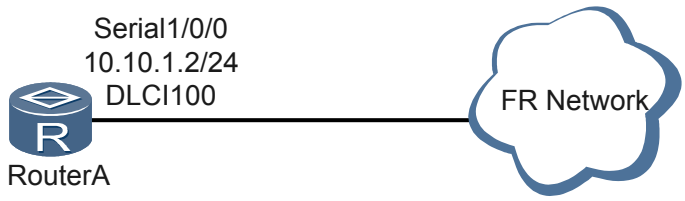
2.10.7 Example for Configuring FR Traffic Shaping

This section provides an example for configuring FR traffic shaping on the AR2200.

Networking Requirements

As shown in **Figure 2-16**, RouterA is connected to the FR network through a serial interface. Data services such as email and IP phone services are often transmitted between RouterA and the FR network. RouterA does not require high bandwidth. The requirements are as follows: The CIR should be set to 64 kbit/s; the allowed CIR should be set to 96 kbit/s; the traffic shaping adaptation percentage should be 20% based on the BECN bit.

Figure 2-16 Networking diagram of FR traffic shaping configuration



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure FR traffic shaping on an FR interface.
2. Create an FR class and set traffic shaping parameters in the FR class.
3. Create an FR VC and associate the FR VC with the FR class.

Data Preparation

To complete the configuration, you need to plan the following data:

- FR interface number Serial1/0/0 and IP address 10.10.1.2/24
- FR class name **huawei**, CIR 64 kbit/s, allowed CIR 96 kbit/s, and traffic shaping adaptation percentage 20%
- FR VC number 100

Procedure

Step 1 Configure an FR interface.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface serial 1/0/0
[RouterA-serial1/0/0] link-protocol fr
Warning: The encapsulation protocol of the link will be changed. Continue? [Y/N]
:y
[RouterA-serial1/0/0] ip address 10.10.1.2 24
[RouterA-serial1/0/0] fr traffic-shaping
[RouterA-serial1/0/0] quit
```

Step 2 Create and configure an FR class.

```
[RouterA] fr class huawei
[RouterA-fr-class-huawei] cir allow outbound 96
[RouterA-fr-class-huawei] cir 64
[RouterA-fr-class-huawei] traffic-shaping adaptation becn 20
[RouterA-fr-class-huawei] quit
```

Step 3 Create an FR VC and associate the FR VC with the FR class **huawei**.

```
[RouterA] interface serial 1/0/0
[RouterA-serial1/0/0] fr dlci 100
[RouterA-fr-dlci-Serial1/0/0-100] fr-class huawei
```

Step 4 Verify the configuration.

NOTE

Ensure that the configuration on the FR network is complete.

Run the **display this** command to view the configuration of the FR interface.

Run the **display fr class** command to view the configuration of FR class.

```
[Router]display fr class huawei
fr class huawei
 General Traffic Shape Info:
  CIR allow outbound 96(Kbps), CIR 64(Kbps), CBS outbound 1500(byte)
 Traffic Shaping Adaptation Info:
  traffic-shaping adaptation becn 20(percentage)
 PVC-PQ Queue Info:
  pvc-pq normal
```

The command output shows that the CIR is 64 kbit/s and the allowed CIR is 96 kbit/s on Serial1/0/0 in the outbound direction, and RouterA adjusts the transmission rate of packets by 20% based on the BECN bit.

----End

Configuration Files

Configuration file of RouterA

```
#
sysname RouterA
#
fr class huawei
 cir allow outbound 96
 cir 64
 traffic-shaping adaptation becn 20
#
interface Serial1/0/0
 link-protocol fr
 fr traffic-shaping
 fr dlci 100
   fr-class huawei
 ip address 10.10.1.2 255.255.255.0
#
return
```

2.10.8 Example for Configuring FR Fragmentation

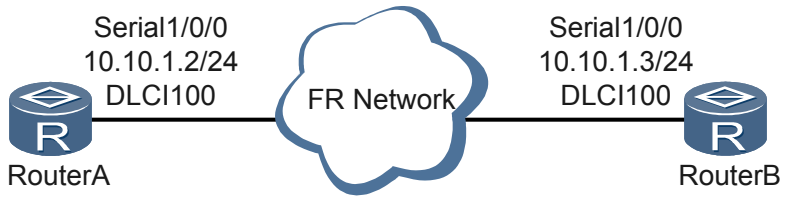
This section provides an example for configuring FR fragmentation on the AR2200.

Networking Requirements

As shown in **Figure 2-17**, RouterA is connected to RouterB across the FR network. Voice and data services are transmitted between RouterA and RouterB. To ensure that voice services are processed in real time, fragment packets transmitted over the FR network.

RouterA and RouterB are AR2200s.

Figure 2-17 Networking diagram of FR fragmentation configuration



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure FR interfaces, assign IP addresses to the FR interfaces, and configure the link protocol of the FR interfaces as FR.
2. Create and configure FR classes, enable FR fragmentation, and configure the fragment size.

3. Create FR VCs and associate the FR VCs with FR classes.

Data Preparation

To complete the configuration, you need to plan the following data:

On RouterA:

- FR interface number Serial1/0/0 and IP address 10.10.1.2/24
- FR class name **huawei** and fragment size 128 bytes
- FR VC number 100

On RouterB:

- FR interface number Serial1/0/0 and IP address 10.10.1.3/24
- FR class name **huawei** and fragment size 128 bytes
- FR VC number 100

Procedure

Step 1 Configure RouterA.

Configure an FR interface.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface serial 1/0/0
[RouterA-serial1/0/0] link-protocol fr
Warning: The encapsulation protocol of the link will be changed. Continue? [Y/N]
:y
[RouterA-serial1/0/0] ip address 10.10.1.2 24
[RouterA-serial1/0/0] quit
```

Create an FR class and set the fragment size to 128 bytes in the FR class.

```
[RouterA] fr class huawei
[RouterA-fr-class-huawei] fragment 128
[RouterA-fr-class-huawei] quit
```

Create an FR VC and associate the FR VC with the FR class **huawei**.

```
[RouterA] interface serial 1/0/0
[RouterA-serial1/0/0] fr dlci 100
[RouterA-fr-dlci-Serial1/0/0-100] fr-class huawei
```

Step 2 Configure RouterB.

The configuration of RouterB is similar to that of RouterA, and is not mentioned here.

Step 3 Verify the configuration.

NOTE

Ensure that the configuration on the FR network is complete.

Run the **display this** command to view the configuration of the FR interface.

Run the **display fr class** command to view the configuration of FR class.

```
[Router]display fr class huawei
fr class huawei
 General Traffic Shape Info:
  CIR allow outbound 56(Kbps), CIR 56(Kbps), CBS outbound 1500(byte)
 Fragment Size Info:
```

```
  fragment 128(byte)
 Traffic Shaping Adaptation Info:
  traffic-shaping adaptation becn 25(percentage)
 PVC-PQ Queue Info:
  pvc-pq normal
```

After FR fragmentation is configured, packets with more than 128 bytes are fragmented.

----End

Configuration Files

Configuration file of RouterA

```
#
sysname RouterA
#
fr class huawei
 fragment 128
#
interface Serial1/0/0
 link-protocol fr
 fr dlci 100
   fr-class huawei
 ip address 10.10.1.2 255.255.255.0
#
return
```

Configuration file of RouterB

```
#
sysname RouterB
#
fr class huawei
 fragment 128
#
interface Serial1/0/0
 link-protocol fr
 fr dlci 100
   fr-class huawei
 ip address 10.10.1.3 255.255.255.0
#
return
```

3 PPP and MP Configuration

About This Chapter

The Point-to-Point Protocol (PPP) is used at the data link layer of the Open System Interconnection (OSI) model, and at the link layer of the TCP/IP protocol suite. PPP encapsulates and transmits network layer packets over P2P links. Multilink PPP (MP) is a technique that bundles multiple PPP links to increase bandwidth.

3.1 PPP and MP Overview

This section describes concepts of PPP and MP.

Introduction to PPP

A P2P connection is a simple form of Wide Area Network (WAN) connections. Link layer protocols of a P2P connection include PPP and the High-level Data Link Control protocol (HDLC). PPP supports both the synchronous transfer mode (STM) and asynchronous transfer mode (ATM), whereas HDLC supports only STM.

PPP is used at the data link layer of the OSI model for point-to-point data transmission over full-duplex synchronous and asynchronous links. PPP is widely used because it provides user authentication, supports synchronous and asynchronous communication, and is easy to extend.

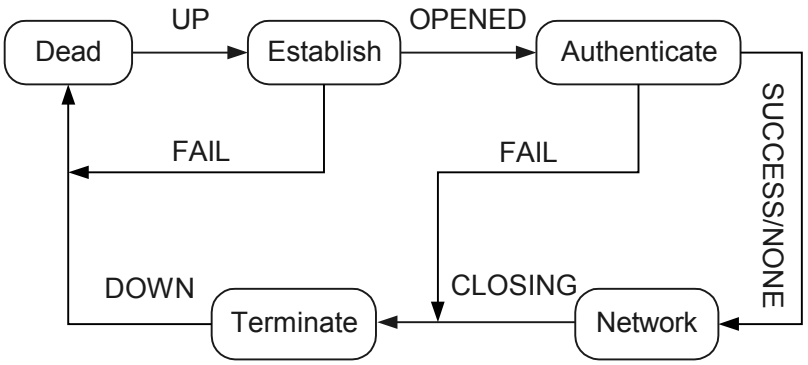
A suite of protocols is defined for PPP, including:

- Link Control Protocol (LCP) used to establish, monitor, and tear down data links
- Network Control Protocol (NCP) used to negotiate the format and type of packets transmitted on data links
- Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) used for network security authentication

PPP Operation Process

Figure 3-1 shows the PPP operation process.

Figure 3-1 PPP operation flowchart



The PPP operation process is as follows:

1. PPP starts and ends with the Dead phase. Two communicating devices stay in the Dead phase for a very short period and then enter the Establish phase after detecting that the physical connection status is Up.
2. In the Establish phase, the devices perform LCP negotiation to negotiate the following items: the working mode such as single-link PPP (SP) and MP, maximum receive unit (MRU), authentication mode, magic number, and asynchronous character mapping. If LCP

negotiation succeeds, LCP enters the Opened state, indicating that the lower-layer link has been established.

3. If authentication is configured, the two devices enter the Authenticate phase and perform CHAP or PAP authentication. If no authentication is configured, the two devices enter the Network phase.
4. In the Authenticate phase, if the authentication fails, the two devices enter the Terminate phase to tear down the link. At this time, LCP goes Down. If the authentication succeeds, the two devices enter the Network phase. LCP remains Opened, whereas the NCP status changes from Initial to Starting.
5. In the Network phase, the two devices perform NCP negotiation, which includes the Internet Protocol Control Protocol (IPCP) negotiation and Multiprotocol Label Switching Control Protocol (MPLSCP) negotiation. In IPCP negotiation, the two devices negotiate IP addresses of their interfaces. In NCP negotiation, the two devices select a network layer protocol. After the negotiation succeeds (that is, the NCP negotiation status is Opened), packets of the network layer protocol can be sent over the PPP link. For example, after IPCP negotiation succeeds, IP packets can be sent over the PPP link.
6. After LCP negotiation and NCP negotiation succeeds, packets can be sent over the PPP link. During the operation of PPP, the two devices enter the Terminate phase if the PPP connection is interrupted, the physical link is disconnected, PPP authentication fails, or the negotiation timeout period expires.
7. In the Terminate phase, if all resources are released, the two devices enter the Dead phase.

Introduction to MP

MP is a technique that bundles multiple PPP links to increase bandwidth. It can be used on the low-speed interfaces that support PPP, such as serial interfaces.

MP allows packets to be fragmented. Fragmented packets are sent to the same destination over multiple PPP links.

MP negotiation involves LCP negotiation and NCP negotiation:

- LCP negotiation: During LCP negotiation, devices on both ends negotiate LCP parameters and check whether they both work in MP mode. If they work in different working modes, LCP negotiation fails.
- NCP negotiation: Devices on both ends perform NCP negotiation using NCP parameters (such as IP addresses) of the MP-Group interface or virtual template interface but not NCP parameters of physical interfaces.

If NCP negotiation succeeds, an MP link can be established.

3.2 PPP and MP Features Supported by the AR2200

This section describes the PPP and MP features supported by the AR2200.

PPP Features

On the AR2200, PPP can be configured on the synchronous serial interface, CE1/PRI interface, CT1/PRI interface, ISDN BRI interface, E1-F interface, T1-F interface, Cellular interface, asynchronous serial interface, CPOS sub-channel interface, dialer interfaces, and virtual template interfaces to provide the following functions:

- PAP authentication and CHAP authentication
- Configuration of some negotiation attributes, including the negotiation timeout period, IP address, and DNS server address

PPP can be used with other technologies to provide PPPoX services. PPPoX services supported by the AR2200 include PPP over Ethernet (PPPoE), PPP over ATM (PPPoA), PPP over Ethernet over ATM (PPPoEoA), PPP over frame relay (PPPoFR), and PPP over Integrated Services Digital Network (PPPoISDN).

For the configuration of PPPoE, see **4 PPPoE Configuration**. For the configuration of PPPoA and PPPoEoA, see **1 ATM Configuration**. For the configuration of PPPoFR, see **2 FR Configuration**. For the configuration of PPPoISDN, see **5 ISDN Configuration**

MP Features

On the AR2200, multiple PPP links can be bundled into an MP link to increase link bandwidth.

The AR2200 allows you to configure MP binding using the following interfaces:

- Virtual template interface

  You can use a virtual template interface to configure MP binding of the following types:

  - MP direct binding: This MP binding is implemented by binding one or more interfaces to a virtual template interface.
  - MP authentication binding: The system searches for a virtual template interface based on the authenticated remote user name. Links of the authenticated remote users are bound to form an MP link.
- MP-Group interface

  An MP-Group interface is the dedicated interface in MP. The MP binding is implemented by binding one or more interfaces to an MP-Group interface.

The AR2200 supports MP fragmentation and reassembly, the minimum length of outgoing packets to be fragmented, Link Fragmentation and Interleaving (LFI), and the maximum delay of an LFI fragment.

MP can be used with other technologies to provide services such as MP over FR (MPoFR) and MP over ISDN (MPoISDN).

3.3 Configuring PPP

You can configure the PPP authentication mode and PPP negotiation parameters. Configure these parameters on the interface whose link layer protocol is PPP.

3.3.1 Establishing the Configuration Task

Before configuring PPP, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task quickly and accurately.

Applicable Environment

PPP is a link layer protocol that transmits network layer packets over P2P links. PPP is widely used because it provides user authentication, supports synchronous and asynchronous communication, and is easy to extend.

By default, an interface runs PPP at the link layer, and PPP authentication is not performed. If PPP authentication does not need to be performed, this configuration task is not required.

Pre-configuration Tasks

None.

Data Preparation

To configure PPP, you need the following data.

No.	Data
1	Number of the interface to be configured with PPP
2	(Optional) PPP authentication mode and user name and password required for PPP authentication
3	(Optional) Timeout period of PPP negotiation, and IP address, IP address pool, or DNS server address specified for the remote device

3.3.2 Configuring PPP as the Link Layer Protocol of an Interface

This section describes how to configure PPP as the link layer protocol of an interface.

Context

Serial interfaces, ISDN BRI interfaces, E1-F interfaces, T1-F interfaces, dialer interfaces, and virtual template interfaces can be configured with PPP.

NOTE

Serial interfaces include synchronous serial interfaces created using CE1/PRI interfaces and CT1/PRI interfaces.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
link-protocol ppp
```

PPP is configured as the link layer protocol of the interface.

By default, the link layer protocol of an interface is PPP.

Step 4 Assign an IP address to the interface.

- Run:

  ip address *ip-address* { *mask* | *mask-length* }

  An IPv4 address is assigned to the interface.

- Run:

  ipv6 address { *ipv6-address prefix-length* | *ipv6-address/prefix-length* }

  An IPv6 address is assigned to the interface.

  NOTE

  Before assigning an IPv6 address to an interface, run the **ipv6** command in the system view to enable IPv6 packet forwarding and run the **ipv6 enable** command on the interface to enable IPv6.

----End

3.3.3 (Optional) Configuring PPP Authentication

Two PPP authentication modes are available: PAP authentication and CHAP authentication. The two authentication modes are applicable to different scenarios. Select the authentication mode as required.

Context

On a PPP link, the local device authenticates the remote device to improve security. Two PPP authentication modes are available:

- PAP: It is a two-way handshake authentication protocol and transmits passwords in plain text.
- CHAP: It is a three-way handshake authentication protocol and transmits passwords in cipher text.

CHAP authentication provides higher security than PAP authentication. Therefore, CHAP authentication is usually used.

If PPP authentication is configured on one end of a link, it must also be configured on the other end. For the configuration scenario and procedure of PPP authentication, see **3.4 Configuring PPP Authentication**.

3.3.4 (Optional) Setting PPP Negotiation Parameters

PPP negotiation parameters include the negotiation timeout period, IP address, and DNS server address.

Context

PPP negotiation parameters are optional. For the configuration scenario and procedure of PPP negotiation parameters, see **3.5 Setting PPP IPv4 Negotiation Parameters**.

3.3.5 Checking the Configuration

After PPP is configured, you can check whether PPP configuration is correct, including the PPP authentication mode and PPP negotiation parameters.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **interface** *interface-type interface-number* command to enter the interface view.

Step 3 Run the **display this** command to check the interface configuration, including the PPP authentication mode and PPP negotiation parameters.

----End

3.4 Configuring PPP Authentication

Two PPP authentication modes are available: PAP authentication and CHAP authentication.

3.4.1 Establishing the Configuration Task

Before configuring PPP authentication, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task quickly and accurately.

Applicable Environment

Table 3-1 lists characteristics and usage scenarios of PAP authentication and CHAP authentication.

Table 3-1 PPP authentication

Authentication Mode	Characteristic	Usage Scenario
PAP authentication	PAP is a two-way handshake authentication protocol and transmits passwords in plain text. Passwords are sent over links in plain text. After a PPP link is established, the authenticated device repeatedly sends the user name and password until the authentication finishes. Malicious attacks, therefore, cannot be prevented.	PAP authentication is used on networks that do not require high security.
CHAP authentication	CHAP is a three-way handshake authentication protocol and transmits passwords in cipher text. In CHAP authentication, passwords are encrypted using the Message Digest 5 (MD5) algorithm and then sent over links. This prevents attacks.	CHAP authentication ensures network security and therefore is widely used.

PPP authentication involves the authenticating device and authenticated device. The AR2200 can function as either the authenticating device or the authenticated device. When two AR2200s are connected, bidirectional authentication can be performed between them:

- In unidirectional PAP authentication, the following configurations are required:
  - When the AR2200 functions as the authenticating device, configure it to authenticate the remote device in PAP mode.
  - When the AR2200 functions as the authenticated device, configure it to be authenticated by the remote device in PAP mode.
- In unidirectional CHAP authentication, the following configurations are required:
  - When the AR2200 functions as the authenticating device, configure it to authenticate the remote device in CHAP mode.
  - When the AR2200 functions as the authenticated device, configure it to be authenticated by the remote device in CHAP mode.

Pre-configuration Tasks

Before configuring PPP authentication, complete the following task:

- Configuring PPP as the link layer protocol of the interface

Data Preparation

To configure PPP authentication, you need the following data.

No.	Data
1	Authentication mode and authentication domain of the authenticating device, and remote user name, password, and service type for local authentication
2	User name and password of the authenticated device for PPP authentication

3.4.2 Configuring the AR2200 to Authenticate the Remote Device in PAP Mode

When the PPP authentication mode is PAP authentication and the AR2200 functions as the authenticating device, configure the AR2200 to authenticate the remote device in PAP mode.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
ppp authentication-mode pap [ [ call-in ] domain domain-name ]
```

The PPP authentication mode is set to PAP authentication.

By default, PPP authentication is not performed.

If the **call-in** parameter is specified, the AR2200 authenticates users only when these users call in.

If the **domain** parameter is not specified or the configured domain name is not defined on the AR2200, the domain name contained in the remote user name is used as the authentication domain first. If the remote user name does not contain any domain name, the default domain is used as the authentication domain.

Step 4 Run:

```
quit
```

Return to the system view.

Step 5 Configure an authentication domain and user information.

The following describes only how to configure AAA local authentication. For the configuration of AAA remote authentication, see AAA Configuration in the *Huawei AR2200 Series Enterprise Routers Configuration Guide - Security*.

1. Run:

   ```
   aaa
   ```

   The AAA view is displayed.

2. Run:

   ```
   authentication-scheme authentication-scheme-name
   ```

   An authentication scheme is created and the authentication scheme view is displayed.

   By default, the AR2200 has an authentication scheme named **default**, which can only be deleted but cannot be modified.

3. Run:

   ```
   authentication-mode local
   ```

   The authentication mode is set to local authentication.

   By default, the authentication mode is local authentication.

4. Run:

   ```
   quit
   ```

   Return to the AAA view.

5. Run:

   ```
   domain domain-name
   ```

   A domain is created and the domain view is displayed.

   The AR2200 has two default domains named **default** and **default_admin**. Domain **default** is used for common access users. Domain **default_admin** is used for administrators.

6. Run:

   ```
   authentication-scheme authentication-scheme-name
   ```

   The authentication scheme is configured for the domain.

   By default, the authentication scheme named **default** is used for the domain.

The authentication scheme name specified in this command must be the same as that specified in **Step 5.2**.

7. Run:

```
quit
```

Return to the AAA view.

8. Run:

```
local-user user-name password { cipher | simple } password
```

The user name and password are configured for local users.

The user name and password configured by this command must be the same as those configured on the authenticated device.

9. Run:

```
local-user user-name service-type ppp
```

The service type PPP is configured for local users.

----End

3.4.3 Configuring the AR2200 to Be Authenticated by the Remote Device in PAP Mode

When the PPP authentication mode is PAP authentication and the AR2200 functions as the authenticated device, configure the AR2200 to be authenticated in PAP mode.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
ppp pap local-user username password { cipher | simple } password
```

The user name and password sent from the local device to the remote device in PAP authentication are configured.

By default, the local device sends a request to the remote device without the user name and password in PAP authentication.

----End

3.4.4 Configuring the AR2200 to Authenticate the Remote Device in CHAP Mode

When the PPP authentication mode is CHAP authentication and the AR2200 functions as the authenticating device, configure the AR2200 to authenticate the remote device in CHAP mode.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
ppp authentication-mode chap [ [ call-in ] domain domain-name ]
```

The PPP authentication mode is set to CHAP authentication.

By default, PPP authentication is not performed.

If the **call-in** parameter is specified, the AR2200 authenticates users only when these users call in.

If the **domain** parameter is not specified or the configured domain name is not defined on the AR2200, the domain name contained in the remote user name is used as the authentication domain first. If the remote user name does not contain any domain name, the default domain is used as the authentication domain.

Step 4 Run:

```
quit
```

Return to the system view.

Step 5 Configure an authentication domain and user information.

The following describes only how to configure AAA local authentication. For the configuration of AAA remote authentication, see AAA Configuration in the *Huawei AR2200 Series Enterprise Routers Configuration Guide - Security*.

1. Run:

   ```
   aaa
   ```

   The AAA view is displayed.

2. Run:

   ```
   authentication-scheme authentication-scheme-name
   ```

   An authentication scheme is created and the authentication scheme view is displayed.

   By default, the AR2200 has an authentication scheme named **default**, which can only be deleted but cannot be modified.

3. Run:

   ```
   authentication-mode local
   ```

   The authentication mode is set to local authentication.

   By default, the authentication mode is local authentication.

4. Run:

   ```
   quit
   ```

   Return to the AAA view.

5. Run:
   domain *domain-name*

   A domain is created and the domain view is displayed.

   The AR2200 has two default domains named **default** and **default_admin**. Domain **default** is used for common access users. Domain **default_admin** is used for administrators.
6. Run:
   authentication-scheme *authentication-scheme-name*

   The authentication scheme is configured for the domain.

   By default, the authentication scheme named **default** is used for the domain.

   The authentication scheme name specified in this command must be the same as that specified in **Step 5.2**.
7. Run:
   quit

   Return to the AAA view.
8. Run:
   local-user *user-name* **password** { **cipher** | **simple** } *password*

   The user name and password are configured for local users.

   The user name and password configured by this command must be the same as those configured on the authenticated device.
9. Run:
   local-user *user-name* **service-type ppp**

   The service type PPP is configured for local users.

----End

3.4.5 Configuring the AR2200 to Be Authenticated by the Remote Device in CHAP Mode

When the PPP authentication mode is CHAP authentication and the AR2200 functions as the authenticated device, configure the AR2200 to be authenticated in CHAP mode.

Procedure

Step 1 Run:
system-view

The system view is displayed.

Step 2 Run:
interface *interface-type interface-number*

The interface view is displayed.

Step 3 Run:
ppp chap user *username*

The user name for CHAP authentication is configured.

Step 4 Run:

```
ppp chap password { cipher | simple } password
```

The password for CHAP authentication is configured.

----End

3.4.6 Checking the Configuration

After PPP authentication is configured, you can check whether the configuration is correct, including the PPP authentication mode, authentication user name, and authentication password.

Procedure

- Check the configuration of the authenticating device.
  1. Run the **system-view** command to enter the system view.
  2. Run the **interface** *interface-type interface-number* command to enter the view of the PPP-enabled interface.
  3. Run the **display this** command to check the PPP authentication mode of the interface.
  4. Run the **display local-user** command to check the local user configuration.
- Check the configuration of the authenticated device.

  To check the configuration of the authenticated device, you only need to check whether the user name and password for CHAP or PAP authentication are configured correctly on the interface configured with PPP authentication.

  1. Run the **system-view** command to enter the system view.
  2. Run the **interface** *interface-type interface-number* command to enter the view of the PPP-enabled interface.
  3. Run the **display this** command to check the user name and password configured for PPP authentication.

----End

3.5 Setting PPP IPv4 Negotiation Parameters

On the AR2200, you can set PPP negotiation parameters including the negotiation timeout period, IP address, and DNS server address.

3.5.1 Establishing the Configuration Task

Before setting PPP negotiation parameters, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task quickly and accurately.

Applicable Environment

To establish a PPP link, devices on both ends need to perform negotiations such as LCP negotiation and NCP negotiation. Some parameters can be set for these negotiations. On the

AR2200, you can set PPP negotiation parameters including the negotiation timeout period, IP address, and DNS server address.

Pre-configuration Tasks

Before setting PPP negotiation parameters, complete the following task:

- Configuring PPP as the link layer protocol of the interface on which you need to set PPP negotiation parameters

Data Preparation

To set PPP negotiation parameters, you need the following data.

No.	Data
1	Negotiation timeout period
2	IP address or IP address pool specified for the remote device
3	DNS server address specified for the remote device

3.5.2 Setting the Negotiation Timeout Period

In PPP negotiation, if the local end does not receive any response from the remote end within the specified timeout period, it resends a packet.

Context

If the negotiation timeout period is too long, link transmission efficiency decreases. If the negotiation timeout period is too short, unnecessary packet retransmission occurs, increasing the link load. Therefore, the negotiation timeout period must be set properly.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
ppp timer negotiate seconds
```

The negotiation timeout period is set.

By default, the timeout period of PPP negotiation is 3 seconds.

----End

3.5.3 Configuring IP Address Negotiation

The IP address negotiation function allows PPP access users to obtain IP addresses from servers.

Context

IP address negotiation can be configured in the following scenarios:

- The AR2200 functions as a client.

  If the local interface runs PPP at the link layer but is not assigned an IP address, and the remote device has IP addresses, you can configure IP address negotiation on the local interface so that it can obtain an IP address from the remote device. For example, when the client accesses the Internet through an Internet Server Provider (ISP) network, it can obtain an IP address from the ISP.
- The AR2200 functions as a server.

  If the remote interface runs PPP at the link layer, you can configure the AR2200 to assign an IP address to the remote interface.

Procedure

- Configuring the AR2200 as a client
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     interface *interface-type interface-number*

     The interface view is displayed.
  3. Run:
     ip address ppp-negotiate

     IP address negotiation is configured on the interface.

     By default, IP address negotiation is not configured on an interface.
- Configuring the AR2200 as a server
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     interface *interface-type interface-number*

     The interface view is displayed.
  3. Run:
     remote address { *ip-address* | **pool** *pool-name* }

     An IP address or an IP address pool is configured for the client.

     By default, the AR2200 does not assign IP addresses to clients.
  4. Run:
     quit

Return to the system view.

5. (Optional) Configure a global address pool.

   When the **pool** parameter is specified in step 3, this step is required.

   - Run:
     ```
     ip pool ip-pool-name
     ```
     A global address pool is created and the global address pool view is displayed.
   - Run:
     ```
     network ip-address [ mask { mask | mask-length } ]
     ```
     The IP address range of the global address pool is set.
   - Run:
     ```
     gateway-list ip-address &<1-8>
     ```
     The egress gateway address is configured for the global address pool.
   - Run:
     ```
     quit
     ```
     Return to the system view.

----End

3.5.4 Configuring DNS Server Address Negotiation

During IP address negotiation, the AR2200 negotiates the DNS server address with the remote device.

Context

When a host connects to the AR2200 using PPP, the AR2200 must specify a DNS server address for the host so that the host can access the Internet using a domain name. When the AR2200 connects to an access server using PPP, the AR2200 must be configured to accept the DNS server address specified by the access server.

NOTE

If an AR2200 is configured to specify DNS server address for hosts, it cannot accept the DNS server addresses delivered by other devices.

Procedure

- Configuring the AR2200 to accept the DNS server address specified by the remote device
  1. Run:
     ```
     system-view
     ```
     The system view is displayed.
  2. Run:
     ```
     interface interface-type interface-number
     ```
     The interface view is displayed.
  3. Run the following commands as required:
     - Run:
       ```
       ppp ipcp dns request
       ```
       The AR2200 is configured to request a DNS server address from the remote device.

By default, the AR2200 is disabled from requesting a DNS server address from the remote device.

- Run:

  ppp ipcp dns admit-any

  The AR2200 is configured to accept the DNS server address specified by the remote device.

  By default, the AR2200 cannot obtain the DNS server address specified by the remote device.

- Configuring the AR2200 to specify a DNS server address for the remote device

  1. Run:

     system-view

     The system view is displayed.

  2. Run:

     interface *interface-type interface-number*

     The interface view is displayed.

  3. Run:

     ppp ipcp dns *primary-dns-address* [*secondary-dns-address*]

     The AR2200 is configured to specify a DNS server address for the remote device.

     By default, the AR2200 does not specify any DNS server address for the remote device.

----End

3.5.5 Checking the Configuration

After PPP negotiation parameters are set, you can check whether the configuration is correct, including the negotiation timeout period, status of IP address negotiation, and status of DNS server address negotiation.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **interface** *interface-type interface-number* command to enter the interface view.

Step 3 Run the **display this** command to check PPP negotiation parameters.

----End

3.6 Configuring MP

A Multi-Link PPP (MP) group is created by binding multiple Point-to-Point Protocol (PPP) links and is applied to PPP interfaces.

3.6.1 Establishing the Configuration Task

Before configuring MP, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This helps you complete the configuration task quickly and accurately.

Applicable Environment

To increase link bandwidth, you can bind multiple PPP links to an MP link.

Large packets require a longer transmission period of time and occupy a link for a long time. If subsequent packets such as voice packets need to be forwarded in real time, there may be a delay and user experience is low. To solve the problem, fragment packets and place fragments of small packets and large packets to the queue. To fragment and reassemble packets, enable LFI.

Table 3-2 lists the MP binding types.

Table 3-2 MP binding types

Type	Subtype	Characteristic	Limitation
MP binding using a virtual template interface	MP direct binding	This MP binding is implemented by binding one or more interfaces to a virtual template interface.	One interface can be configured with only one binding type: direct binding or authentication binding.
	MP authentication binding	The system searches for a virtual template interface based on the authenticated remote user name. Links of the authenticated remote users are bound to form an MP link. This method is flexible but the configuration is complex.	
MP binding using an MP-Group interface	MP binding using an MP-Group interface	An MP-Group interface is dedicated to MP application. This MP binding is implemented by binding one or more interfaces to an MP-Group interface. The configuration is simple. It is widely used on networks.	-

Pre-configuration Tasks

Before configuring MP, complete the following task:

- Configuring PPP as the link layer protocol on the MP interface

Data Preparation

To configure MP, you need the following data.

No.	Data
1	Number of the physical interface, and IP address and number of the virtual template interface used for MP direct binding
2	Number of the physical interface, IP address and number of the virtual template interface, user name for authentication, and PPP authentication parameters for MP authentication binding
3	Number of the physical interface, and IP address and number of the MP-Group interface for MP binding
4	(Optional) Minimum length of outgoing MP packets to be fragmented, maximum delay of an LFI fragment, and maximum number of links in an MP link

3.6.2 Configuring MP Direct Binding by Using a Virtual Template Interface

MP binding is implemented by binding one or more interfaces to a virtual template interface.

Context

In this mode, you can choose to configure PPP authentication.

- If PPP authentication is configured, interface binding takes effect only after the interfaces are authenticated.
- If PPP authentication is not configured, interface binding takes effect only after the LCP status of the interfaces becomes Up.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface virtual-template vt-number
```

A virtual template interface is created and the virtual template interface view is displayed.

Step 3 Run:

```
ip address ip-address { mask | mask-length }
```

An IP address is allocated to the virtual template interface.

Step 4 (Optional) Run:

```
ppp mp binding-mode { authentication | descriptor | both }
```

The MP binding mode is configured.

By default, MP binding is performed based on the remote user name and remote endpoint discriminator. That is, the MP binding mode is **both**.

NOTE

The local and remote devices must have the same MP binding mode; otherwise, errors occur in MP negotiation.

If the MP binding mode is **descriptor**, you can configure an endpoint discriminator for the remote device. If the remote device is an AR2200, run the **ppp mp endpoint** command to configure an endpoint discriminator.

Step 5 Run:

```
quit
```

Return to the system view.

Step 6 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 7 Run:

```
ppp mp virtual-template vt-number
```

The interface is bound to the created virtual template.

Step 8 (Optional) Configure authentication as required. For details on how to configure authentication, see **3.4 Configuring PPP Authentication**.

Repeat steps 6 to 8 to bind multiple interfaces to the virtual template interface.

Step 9 Run:

```
shutdown
```

and

```
undo shutdown
```

/

```
restart
```

The interface is restarted.

TIP

To ensure that all the interfaces are bound to the MP successfully by PPP re-negotiation, restart all the interfaces after configuration.

----End

3.6.3 Configuring MP Authentication Binding by Using a Virtual Template Interface

This MP binding is implemented by associating the user name of the remote device with a virtual template interface. The user name of the remote device is obtained in authentication.

Context

The AR2200 searches for a virtual template interface based on the authenticated remote user name. Interfaces connected to users with the same user name are bound to the same virtual template interface. This MP binding mode requires PPP authentication. MP binding takes effect only after the interfaces are authenticated.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface virtual-template vt-number
```

A virtual template interface is created and the virtual template interface view is displayed.

Step 3 Run:

```
ip address ip-address { mask | mask-length }
```

An IP address is allocated to the virtual template interface.

Step 4 (Optional) Run:

```
ppp mp binding-mode { authentication | descriptor | both }
```

The MP binding mode is configured.

By default, MP binding is performed based on the remote user name and remote endpoint discriminator. That is, the MP binding mode is **both**.

NOTE

The local and remote devices must have the same MP binding mode; otherwise, errors occur in MP negotiation.

If the MP binding mode is **descriptor**, you can configure an endpoint discriminator for the remote device. If the remote device is an AR2200, run the **ppp mp endpoint** command to configure an endpoint discriminator.

Step 5 Run:

```
quit
```

Return to the system view.

Step 6 Run:

```
ppp mp user username bind virtual-template vt-number
```

The user name of the remote device is associated with the virtual template interface.

Step 7 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 8 Run:

```
ppp mp
```

The PPP interface is configured to work in MP mode.

By default, an interface works in PPP mode.

Step 9 Configure bidirectional PPP authentication. For details, see **3.4 Configuring PPP Authentication**.

Repeat steps 7 and 9 to bind multiple interfaces to the virtual template interface.

Step 10 Run:

shutdown
and
undo shutdown
/
restart

The interface is restarted.

TIP
To ensure that all the interfaces are bound to the MP successfully by PPP re-negotiation, restart all the interfaces after configuration.

----End

3.6.4 Configuring MP Binding by Using an MP Group Interface

This MP binding is implemented by binding one or more interfaces to an MP-Group interface.

Context

An MP-Group interface is the dedicated interface in MP. The MP binding is implemented by binding one or more interfaces to an MP-Group interface.

Procedure

Step 1 Run:
system-view

The system view is displayed.

Step 2 Run:
interface mp-group *number*

An MP-Group interface is created and the MP-Group interface view is displayed.

Step 3 Run:
ip address *ip-address { mask | mask-length }*

An IP address is allocated to the MP-Group interface.

Step 4 Run:
quit

Return to the system view.

Step 5 Run:
interface *interface-type interface-number*

The interface view is displayed.

Step 6 Run:
ppp mp mp-group *number*

The interface is bound to the MP-Group interface so that the interface works in MP mode.

The value of *number* must be the same as the value of *number* in step 2.

Repeat steps 5 to 6 to bind multiple interfaces to the MP-Group interface.

Step 7 (Optional) Configure authentication as required. For details on how to configure authentication, see **3.4 Configuring PPP Authentication**.

Repeat steps 5 to 7 to bind multiple interfaces to the MP-Group interface.

Step 8 Run:

```
shutdown
```

and

```
undo shutdown
```

/

```
restart
```

The interface is restarted.

TIP

To ensure that all the interfaces are bound to the MP successfully by PPP re-negotiation, restart all the interfaces after configuration.

----End

3.6.5 (Optional) Configuring MP Fragmentation and Maximum Number of Links in an MP Group

Optional MP parameters include the minimum length of outgoing MP packets to be fragmented and the maximum number of links in an MP link.

Context

After the minimum length of outgoing MP packets to be fragmented is set, only the outgoing MP packets whose length is greater than the minimum length are fragmented.

If the number of links in an MP link reaches the maximum value, new available PPP links cannot join the MP link.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Configuring MP fragmentation.

- Run:

  ```
  ppp mp min-fragment size
  ```

  The minimum length of outgoing MP packets to be fragmented is set.

  By default, the minimum length of outgoing MP packets to be fragmented is 500 bytes.

- Run:

  ```
  ppp mp lfi
  ```

  The Link Fragmentation and Interleaving (LFI) is enabled.

  By default, LFI is disabled on an interface.

  After LFI is enabled, the minimum length of outgoing MP packets to be fragmented (set using the **ppp mp min-fragment** command) becomes invalid. The LFI fragment size is

determined by the maximum delay of an LFI fragment and interface committed information rate (CIR), in bytes. The formula for calculating the LFI fragment size is as follows:

LFI fragment size = (maximum fragment delay x interface CIR)/8

The maximum fragment delay is set using the **ppp mp lfi delay-per-frag** command, and the interface CIR is set using the **qos gts** command.

Step 4 Run:

```
ppp mp max-bind max-bind-number
```

The maximum number of links in an MP link is set.

By default, the maximum number of links in an MP link is 16.

NOTE

To make this command take effect, ensure that there is no member link in the MP group.

Step 5 Run:

```
shutdown
```

and

```
undo shutdown
```

/

```
restart
```

The interface is restarted.

If the interface is a virtual template interface, its physical interface needs to be restarted.

----End

3.6.6 Checking the Configuration

After the MP configuration is complete, you can view the MP binding information and the statistics on links in an MP link. You can also view the MP configuration on an interface.

Context

The MP configuration on the peer device must be complete before you check the configuration.

Procedure

Step 1 Run the **display ppp mp** [**interface** *interface-type interface-number*] command to view the MP binding information and the statistics on links in an MP link.

Step 2 Run the **display ppp mp** [**interface** *interface-type interface-number*] command to view the MP configuration on the interface.

- Run the **display interface virtual-template** [*vt-number*] command to view the specified virtual template interface status if MP binding is configured using a virtual template interface.
- Run the **display interface mp-group** [*number*] command to view the specified MP-Group interface status if MP binding is configured using an MP-Group interface.

----End

Example

Run the **display ppp mp interface virtual-template** *vt-number* command to view MP binding information.

```
<Huawei> display ppp mp interface virtual-template 1
Template is Virtual-Template1
 Bundle 10cd6d925ac6, 2 members, slot 0, Master link is Virtual-Template1:0
  0 lost fragments, 0 reordered, 0 unassigned, 0 interleaved,
 sequence 0/0 rcvd/sent
 The bundled sub channels are:
      Serial1/0/0
      Serial1/0/1
```

The preceding information indicates that Serial1/0/0 and Serial1/0/1 are bound to the virtual template interface **virtual-template 1**.

Run the **display interface virtual-template** *vt-number* command to view information about the virtual template interface.

```
<Huawei> display interface virtual-template 1
Virtual-Template1 current state : UP
Line protocol current state : UP (spoofing)
Description:HUAWEI, AR Series, Virtual-Template1 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 10.10.10.10/24
Link layer protocol is PPP
LCP initial, MP opened
Physical is None, baudrate is 64000 bps
Current system time: 2011-02-09 13:15:26
    Last 300 seconds input rate 0 bits/sec, 0 packets/sec
    Last 300 seconds output rate 0 bits/sec, 0 packets/sec
    Realtime 19 seconds input rate 0 bits/sec, 0 packets/sec
    Realtime 19 seconds output rate 56 bits/sec, 0 packets/sec
    Input: 8 packets,112 bytes
           0 unicast,0 broadcast,0 multicast
           0 errors,0 unknownprotocol
    Output:53 packets,6232 bytes
           0 unicast,0 broadcast,0 multicast
           0 errors
    Input bandwidth utilization  : 0%
    Output bandwidth utilization : 0%
```

You can view the interface status, IP address, and LCP and MP negotiation.

3.7 Configuration Examples

This section describes the networking requirements, configuration roadmap, and data preparation for typical PPP applications and provides the configuration file.

Context

NOTE

When an AR2200 directly connects to another device through a PPP link, and interfaces on both ends of the PPP link are on the same segment segment, setting the mask length of IP addresses of the two interfaces to 30 bits is recommended. This prevents packets from being repeatedly transmitted on the PPP link.

3.7.1 Example for Establishing a PPP Connection by Using PAP Authentication

This section provides an example to illustrate how to establish a PPP connection between AR2200s using PAP authentication.

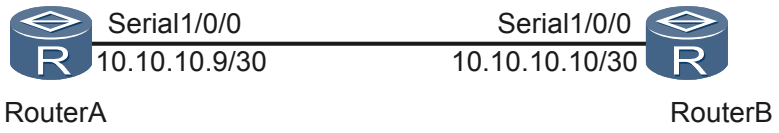
Networking Requirements

In PAP authentication, passwords are sent over links in plain text. After a PPP link is established, the authenticated device repeatedly sends the user name and password until the authentication

finishes. This mode cannot ensure high security, so it is used on networks that do not require high security.

As shown in **Figure 3-2**, RouterA and RouterB establish a PPP connection using PAP authentication. RouterA authenticates RouterB in PAP mode, and local authentication is used. RouterB does not authenticate RouterA.

Figure 3-2 Network diagram of PAP authentication



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure RouterA as the authenticating device.
2. Configure RouterB as the authenticated device.

Data Preparation

To complete the configuration, you need the following data:

- On RouterA: link layer protocol of the interface, PPP authentication mode, local user name, password, service type, and authentication domain
- On RouterB: link layer protocol of the interface, authentication user name, and authentication password

Procedure

Step 1 Configure RouterA.

Assign an IP address to Serial1/0/0 and configure PPP as the link layer protocol of Serial1/0/0.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface serial 1/0/0
[RouterA-serial1/0/0] link-protocol ppp
[RouterA-serial1/0/0] ip address 10.10.10.9 30
```

Set the PPP authentication mode to PAP authentication and specify an authentication domain named **system**.

```
[RouterA-serial1/0/0] ppp authentication-mode pap domain system
[RouterA-serial1/0/0] quit
```

Configure a local user and specify the authentication domain for the local user.

```
[RouterA] aaa
[RouterA-aaa] authentication-scheme system_a
[RouterA-aaa-authen-system_a] authentication-mode local
[RouterA-aaa-authen-system_a] quit
[RouterA-aaa] domain system
[RouterA-aaa-domain-system] authentication-scheme system_a
[RouterA-aaa-domain-system] quit
```

```
[RouterA-aaa] local-user user1@system password simple huawei
[RouterA-aaa] local-user user1@system service-type ppp
[RouterA-aaa] quit
```

Step 2 Configure RouterB.

Assign an IP address to Serial1/0/0 and configure PPP as the link layer protocol of Serial1/0/0.

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] interface serial 1/0/0
[RouterB-serial1/0/0] link-protocol ppp
[RouterB-serial1/0/0] ip address 10.10.10.10 30
```

Configure the user name and password sent from RouterB to RouterA in PAP authentication.

```
[RouterB-serial1/0/0] ppp pap local-user user1@system password simple huawei
```

Step 3 Verify the configuration.

Run the **display interface serial 1/0/0** command to check the interface configuration. The command output shows that both the physical layer status and link layer status of the interface are Up and that both LCP and IPCP are in Opened state. This indicates that PPP negotiation succeeds and that RouterA and RouterB can ping each other successfully.

```
[Huawei] display interface serial 1/0/0
Serial1/0/0 current state : UP
Line protocol current state : UP
Last line protocol up time : 2011-03-25 11:35:10
Description:HUAWEI, AR Series, Serial1/0/0 Interface
Route Port,The Maximum Transmit Unit is 1500, Hold timer is 0(sec)
Internet Address is 10.10.10.9/30
Link layer protocol is PPP
LCP opened, IPCP opened
Last physical up time   : 2011-03-25 11:35:10
Last physical down time : 2011-03-25 11:35:01
Current system time: 2011-03-25 17:30:07
Physical layer is synchronous, Virtualbaudrate is 64000 bps
Interface is DTE, Cable type is V35, Clock mode is RC
Last 10 seconds input rate 7 bytes/sec 56 bits/sec 0 packets/sec
Last 10 seconds output rate 7 bytes/sec 56 bits/sec 0 packets/sec
Input: 7343762 packets, 463499285 bytes
  broadcasts:            0,  multicasts:            0
  errors:                0,  runts:                 0,  giants:                0
  CRC:                   0,  align errors:          0,  overruns:              0
  dribbles:              0,  aborts:                0,  no buffers:            0
  frame errors:          0
Output: 8940170 packets, 530215343 bytes
  errors:                0,  underruns:             0,  collisions:            0
  deferred:              0
DCD=UP DTR=UP DSR=UP RTS=UP CTS=UP

    Input bandwidth utilization  : 0.18%
    Output bandwidth utilization : 0.18%
```

----End

Configuration Files

Configuration file of RouterA

```
#
aaa
 authentication-scheme system_a
 domain system
  authentication-scheme system_a
 local-user user1@system password simple huawei
```

```
 local-user user1@system service-type ppp
#
interface Serial1/0/0
 link-protocol ppp
 ppp authentication-mode pap domain system
 ip address 10.10.10.9 255.255.255.252
#
return
```

Configuration file of RouterB

```
#
interface Serial1/0/0
 link-protocol ppp
 ppp pap local-user user1@system password simple huawei
 ip address 10.10.10.10 255.255.255.252
#
return
```

3.7.2 Example for Establishing a PPP Connection by Using CHAP Authentication

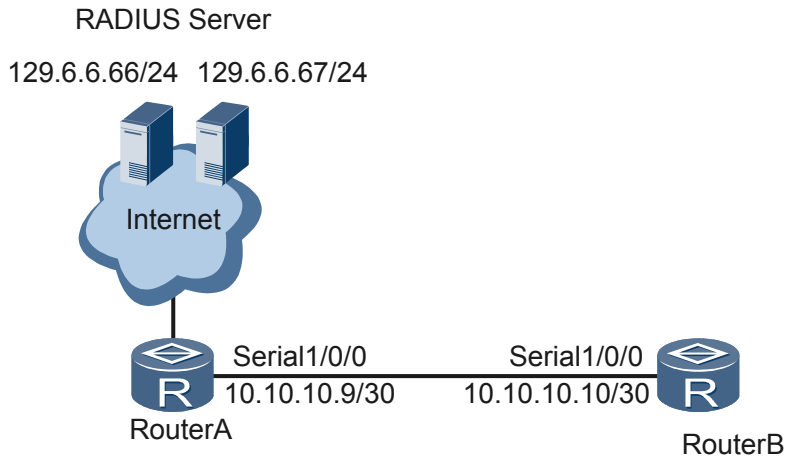
This section provides an example to illustrate how to establish a PPP connection between AR2200s using CHAP authentication.

Networking Requirements

CHAP is a three-way handshake authentication protocol. In CHAP authentication, the authenticated device sends only the user name to the authenticating device. Compared with PAP, CHAP features higher security because passwords are not transmitted. On networks requiring high security, you can establish a PPP connection using CHAP authentication.

As shown in **Figure 3-3**, RouterA authenticates RouterB in CHAP mode, and Remote Authentication Dial-In User Service (RADIUS) authentication is used. RouterB does not need to authenticate RouterA.

Figure 3-3 Network diagram of CHAP authentication



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure RouterA as the authenticating device.
2. Configure RouterB as the authenticated device.

Data Preparation

To complete the configuration, you need the following data:

- On RouterA: link layer protocol of the interface, PPP authentication mode, and RADIUS server parameters
- On RouterB: link layer protocol of the interface, authentication user name, and authentication password

Procedure

Step 1 Configure RouterA.

Assign an IP address to Serial1/0/0 and configure PPP as the link layer protocol of Serial1/0/0.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface serial 1/0/0
[RouterA-serial1/0/0] link-protocol ppp
[RouterA-serial1/0/0] ip address 10.10.10.9 30
```

Set the PPP authentication mode to PAP authentication and specify an authentication domain named **system**.

```
[RouterA-serial1/0/0] ppp authentication-mode chap domain system
[RouterA-serial1/0/0] quit
```

Configure RADIUS authentication.

1. Configure a RADIUS server template named **shiva**.

```
[RouterA] radius-server template shiva
[RouterA-radius-shiva] radius-server authentication 129.6.6.66 1812
[RouterA-radius-shiva] radius-server accounting 129.6.6.66 1813
[RouterA-radius-shiva] radius-server authentication 129.6.6.67 1812 secondary
[RouterA-radius-shiva] radius-server accounting 129.6.6.67 1813 secondary
[RouterA-radius-shiva] radius-server shared-key simple hello
[RouterA-radius-shiva] quit
```

2. Configure authentication and accounting schemes.

```
[RouterA] aaa
[RouterA-aaa] authentication-scheme 1
[RouterA-aaa-authen-1] authentication-mode radius
[RouterA-aaa-authen-1] quit
[RouterA-aaa] accounting-scheme 1
[RouterA-aaa-accounting-1] accounting-mode radius
[RouterA-aaa-accounting-1] quit
```

3. Configure a domain named **system** and apply authentication scheme 1, accounting scheme 1, and RADIUS server template **shiva** to the domain.

```
[RouterA-aaa] domain system
[RouterA-aaa-domain-system] authentication-scheme 1
[RouterA-aaa-domain-system] accounting-scheme 1
[RouterA-aaa-domain-system] radius-server shiva
```

NOTE

On the RADIUS server, you must configure the user name and password for RADIUS authentication. For details, see the documentation of the RADIUS server.

Step 2 Configure RouterB.

Assign an IP address to Serial1/0/0 and configure PPP as the link layer protocol of Serial1/0/0.

```
<Huawei> system-view
[Huawei] RouterB
[RouterB] interface serial 1/0/0
[RouterB-serial1/0/0] link-protocol ppp
[RouterB-serial1/0/0] ip address 10.10.10.10 30
```

Configure the user name and password sent from RouterB to RouterA in CHAP authentication.

```
[RouterB-serial1/0/0] ppp chap user user1@system
[RouterB-serial1/0/0] ppp chap password simple huawei
```

Step 3 Verify the configuration.

Run the **display interface serial 1/0/0** command to check the interface configuration. The command output shows that both the physical layer status and link layer status of the interface are Up and that both LCP and IPCP are in Opened state. This indicates that PPP negotiation succeeds and that RouterA and RouterB can ping each other successfully.

```
[Huawei] display interface serial 1/0/0
Serial1/0/0 current state : UP
Line protocol current state : UP
Last line protocol up time : 2011-03-25 11:35:10
Description:HUAWEI, AR Series, Serial1/0/0 Interface
Route Port,The Maximum Transmit Unit is 1500, Hold timer is 0(sec)
Internet Address is 10.10.10.9/30
Link layer protocol is PPP
LCP opened, IPCP opened
Last physical up time   : 2011-03-25 11:35:10
Last physical down time : 2011-03-25 11:35:01
Current system time: 2011-03-25 17:30:07
Physical layer is synchronous, Virtualbaudrate is 64000 bps
Interface is DTE, Cable type is V35, Clock mode is RC
Last 10 seconds input rate 7 bytes/sec 56 bits/sec 0 packets/sec
Last 10 seconds output rate 7 bytes/sec 56 bits/sec 0 packets/sec
Input: 7343762 packets, 463499285 bytes
  broadcasts:            0,  multicasts:            0
  errors:                0,  runts:                 0,  giants:                0
  CRC:                   0,  align errors:          0,  overruns:              0
  dribbles:              0,  aborts:                0,  no buffers:            0
  frame errors:          0
Output: 8940170 packets, 530215343 bytes
  errors:                0,  underruns:             0,  collisions:            0
  deferred:              0
DCD=UP DTR=UP DSR=UP RTS=UP CTS=UP

    Input bandwidth utilization  : 0.18%
    Output bandwidth utilization : 0.18%
```

----End

Configuration Files

Configuration file of RouterA

```
#
radius-server template shiva
 radius-server shared-key simple hello
 radius-server authentication 129.6.6.66 1812
 radius-server authentication 129.6.6.67 1812 secondary
 radius-server accounting 129.6.6.66 1813
 radius-server accounting 129.6.6.67 1813 secondary
#
aaa
 authentication-scheme 1
  authentication-mode radius
```

```
 accounting-scheme 1
  accounting-mode radius
 domain system
  authentication-scheme 1
  accounting-scheme 1
  radius-server  shiva
#
interface Serial1/0/0
 link-protocol ppp
 ppp authentication-mode chap domain system
 ip address 10.10.10.9 255.255.255.252
#
return
```

Configuration file of RouterB

```
#
interface Serial1/0/0
 link-protocol ppp
 ppp chap user user1@system
 ppp chap password simple huawei
 ip address 10.10.10.10 255.255.255.252
#
return
```

3.7.3 Example for Configuring MP Direct Binding by Using a Virtual Template Interface

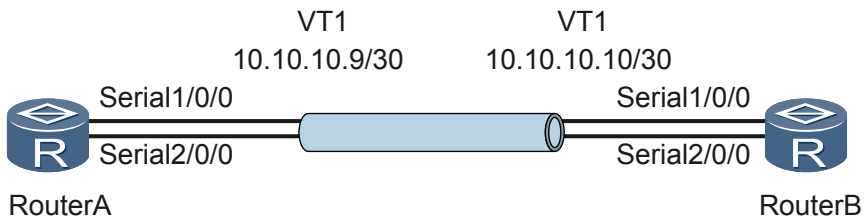
This section provides an example for configuring MP direct binding using a virtual template interface.

Networking Requirements

To increase link bandwidth, you can bind multiple PPP links to an MP link. Configuring MP direct binding using a virtual template interface is seldom used.

As shown in **Figure 3-4**, two pairs of serial interfaces on RouterA and RouterB are connected and are bound to a virtual template interface. Authentication is not performed.

Figure 3-4 Network diagram



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure virtual template interfaces.
2. Bind physical interfaces to virtual template interfaces so that the physical interfaces work in MP mode.

Data Preparation

To complete the configuration, you need the following data:

- Numbers of virtual template interfaces
- IP addresses of virtual template interfaces

Procedure

Step 1 Configure RouterA.

Create and configure a virtual template interface.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface virtual-template 1
[RouterA-Virtual-Template1] ip address 10.10.10.9 30
[RouterA-Virtual-Template1] quit
```

Bind Serial1/0/0 and Serial2/0/0 to the virtual template interface so that the physical interfaces work in MP mode.

```
[RouterA] interface Serial 1/0/0
[RouterA-Serial1/0/0] ppp mp virtual-template 1
[RouterA-Serial1/0/0] quit
[RouterA] interface Serial 2/0/0
[RouterA-Serial2/0/0] ppp mp virtual-template 1
[RouterA-Serial2/0/0] quit
```

Step 2 Configure RouterB.

Create and configure a virtual template interface.

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] interface virtual-template 1
[RouterB-Virtual-Template1] ip address 10.10.10.9 30
[RouterB-Virtual-Template1] quit
```

Bind Serial1/0/0 and Serial2/0/0 to the virtual template interface so that the physical interfaces work in MP mode.

```
[RouterB] interface Serial 1/0/0
[RouterB-Serial1/0/0] ppp mp virtual-template 1
[RouterB-Serial1/0/0] quit
[RouterB] interface Serial 2/0/0
[RouterB-Serial2/0/0] ppp mp virtual-template 1
[RouterB-Serial2/0/0] quit
```

Step 3 Verify the configuration.

Run the **display ppp mp** command on RouterA to view the MP binding information.

```
<RouterA> display ppp mp
Template is Virtual-Template1
 Bundle 10cd6d925ac6, 2 members, slot 0, Master link is Virtual-Template1:0
  0 lost fragments, 0 reordered, 0 unassigned, 0 interleaved,
 sequence 0/0 rcvd/sent
 The bundled sub channels are:
      Serial1/0/0
      Serial2/0/0
```

Bundle 10cd6d925ac6 indicates that the MP binding is implemented using a virtual template interface. **10cd6d925ac6** is the endpoint discriminator of the remote device. The MP link contains two links Serial1/0/0 and Serial2/0/0.

Run the **display virtual-access** command on RouterA to view the virtual access interface status.

```
<RouterA> display virtual-access
Virtual-Template1:0 current state : UP
Line protocol current state : UP
Last line protocol up time : 2011-02-09 09:56:31
Description:HUAWEI, AR Series, Virtual-Template1:0 Interface
Route Port,The Maximum Transmit Unit is 1500
Link layer protocol is PPP
LCP opened, MP opened, IPCP opened
Physical is MP
Current system time: 2011-02-09 09:59:16
    Last 300 seconds input rate 0 bits/sec, 0 packets/sec
    Last 300 seconds output rate 0 bits/sec, 0 packets/sec
    Realtime 0 seconds input rate 0 bits/sec, 0 packets/sec
    Realtime 0 seconds output rate 0 bits/sec, 0 packets/sec
    Input: 0 packets,0 bytes
           0 unicast,0 broadcast,0 multicast
           0 errors,0 unknownprotocol
    Output:0 packets,0 bytes
           0 unicast,0 broadcast,0 multicast
           0 errors
    Input bandwidth utilization  : 0.00%
    Output bandwidth utilization : 0.00%
```

You can obtain similar MP binding information on RouterB.

Ping RouterA on RouterB.

```
<RouterB> ping 10.10.10.9
PING 10.10.10.9: 56  data bytes, press CTRL_C to break
    Reply from 10.10.10.9: bytes=56 Sequence=1 ttl=255 time=40 ms
    Reply from 10.10.10.9: bytes=56 Sequence=2 ttl=255 time=50 ms
    Reply from 10.10.10.9: bytes=56 Sequence=3 ttl=255 time=50 ms
    Reply from 10.10.10.9: bytes=56 Sequence=4 ttl=255 time=50 ms
    Reply from 10.10.10.9: bytes=56 Sequence=5 ttl=255 time=50 ms

  --- 10.10.10.9 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 40/48/50 ms
```

RouterB can ping RouterA successfully.

----End

Configuration Files

Configuration file of RouterA

```
#
sysname RouterA
serial 1/0/0
 link-protocol ppp
 ppp mp Virtual-Template 1
#
serial 2/0/0
 link-protocol ppp
 ppp mp Virtual-Template 1
#
interface Virtual-Template1
 ip address 10.10.10.9 255.255.255.252
return
```

Configuration file of RouterB

```
#
sysname RouterB
serial 1/0/0
 link-protocol ppp
 ppp mp Virtual-Template 1
#
serial 2/0/0
 link-protocol ppp
 ppp mp Virtual-Template 1
#
interface Virtual-Template1
 ip address 10.10.10.9 255.255.255.252
return
```

3.7.4 Example for Configuring MP Authentication Binding by Using a Virtual Template Interface

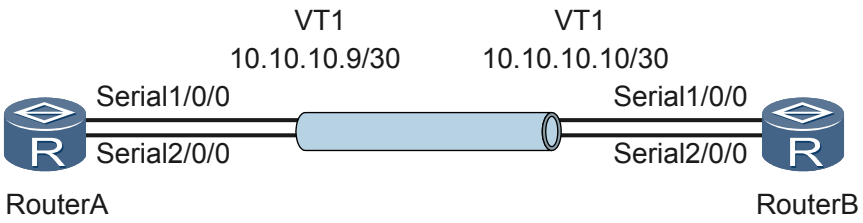
This section provides an example for configuring MP authentication binding using a virtual template interface.

Networking Requirements

To increase link bandwidth, you can bind multiple PPP links to an MP link. Virtual template interfaces can be used for MP authentication binding. This method is flexible but the configuration is complex.

As shown in **Figure 3-5**, two pairs of serial interfaces on RouterA and RouterB are connected and are bound to the virtual template interface; Challenge Handshake Authentication Protocol (CHAP) authentication is used. RouterA searches for a virtual template interface according to user name **UserB**, and RouterB searches for a virtual template interface according to user name **UserA**. CHAP user name **UserA** is configured for RouterA, and CHAP user name **UserB** is configured for RouterB. After bidirectional CHAP authentication succeeds, an MP link is established between RouterA and RouterB.

Figure 3-5 Network diagram



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure virtual template interfaces.
2. Bind user names of remote devices to virtual template interfaces.
3. Configure interfaces to work in MP mode and configure bidirectional CHAP authentication.
4. Restart the physical interfaces to make the configuration take effect.

Data Preparation

To complete the configuration, you need the following data:

- Numbers of virtual template interfaces
- IP addresses of virtual template interfaces
- User names of remote devices in authentication
- Bidirectional CHAP authentication parameters: authentication mode and local user of the authenticator or user name and password of the authenticated party

Procedure

Step 1 Configure RouterA.

Create and configure a virtual template interface.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface virtual-template 1
[RouterA-Virtual-Template1] ip address 10.10.10.9 30
[RouterA-Virtual-Template1] ppp mp binding-mode authentication
[RouterA-Virtual-Template1] quit
```

Bind the user name of the remote device to the virtual template interface **virtual-template 1**.

```
[RouterA] ppp mp user userb@system bind virtual-template 1
```

Configure Serial1/0/0 and Serial2/0/0 to work in MP mode and use CHAP authentication. Configure the local user if the device functions as the authenticator, or the user name and password for CHAP authentication if the device is used as the authenticated party.

```
[RouterA] aaa
[RouterA-aaa] local-user userb@system password simple userb
[RouterA-aaa] local-user userb@system service-type ppp
[RouterA-aaa] authentication-scheme system_a
[RouterA-aaa-authen-system_a] authentication-mode local
[RouterA-aaa-authen-system_a] quit
[RouterA-aaa] domain system
[RouterA-aaa-domain-system] authentication-scheme system_a
[RouterA-aaa-domain-system] quit
[RouterA-aaa] quit
[RouterA] interface Serial 1/0/0
[RouterA-Serial1/0/0] ppp authentication-mode chap domain system
[RouterA-Serial1/0/0] ppp chap user usera@system
[RouterA-Serial1/0/0] ppp chap password simple usera
[RouterA-Serial1/0/0] ppp mp
[RouterA-Serial1/0/0] quit
[RouterA] interface Serial 2/0/0
[RouterA-Serial2/0/0] ppp authentication-mode chap domain system
[RouterA-Serial2/0/0] ppp chap user usera@system
[RouterA-Serial2/0/0] ppp chap password simple usera
[RouterA-Serial2/0/0] ppp mp
[RouterA-Serial2/0/0] quit
```

Step 2 Configure RouterB.

Create and configure a virtual template interface.

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] interface virtual-template 1
[RouterB-Virtual-Template1] ip address 10.10.10.10 30
[RouterB-Virtual-Template1] ppp mp binding-mode authentication
[RouterB-Virtual-Template1] quit
```

Bind the user name of the remote device to the virtual template interface **virtual-template 1**.

```
[RouterB] ppp mp user usera bind virtual-template 1
```

Configure Serial1/0/0 and Serial2/0/0 to work in MP mode and use CHAP authentication. Configure the local user if the device functions as the authenticator, or the user name and password for CHAP authentication if the device is used as the authenticated party.

```
[RouterB] aaa
[RouterB-aaa] local-user usera@system password simple usera
[RouterB-aaa] local-user usera@system service-type ppp
[RouterB-aaa] authentication-scheme system_b
[RouterB-aaa-authen-system_b] authentication-mode local
[RouterB-aaa-authen-system_b] quit
[RouterB-aaa] domain system
[RouterB-aaa-domain-system] authentication-scheme system_b
[RouterB-aaa-domain-system] quit
[RouterB-aaa] quit
[RouterB] interface Serial 1/0/0
[RouterB-Serial1/0/0] ppp authentication-mode chap domain system
[RouterB-Serial1/0/0] ppp chap user userb@system
[RouterB-Serial1/0/0] ppp chap password simple userb
[RouterB-Serial1/0/0] ppp mp
[RouterB-Serial1/0/0] quit
[RouterB] interface Serial 2/0/0
[RouterB-Serial2/0/0] ppp authentication-mode chap domain system
[RouterB-Serial2/0/0] ppp chap user userb@system
[RouterB-Serial2/0/0] ppp chap password simple userb
[RouterB-Serial2/0/0] ppp mp
[RouterB-Serial2/0/0] quit
```

Step 3 Restart member interfaces on RouterA.

```
[RouterA] interface Serial 1/0/0
[RouterA-Serial1/0/0] shutdown
[RouterA-Serial1/0/0] undo shutdown
[RouterA-Serial1/0/0] quit
[RouterA] interface Serial 2/0/0
[RouterA-Serial2/0/0] shutdown
[RouterA-Serial2/0/0] undo shutdown
[RouterA-Serial2/0/0] quit
```

Step 4 Restart member interfaces on RouterB. Use the commands in step 3 to restart member interfaces.

NOTE

To make the configuration take effect, restart all the member interfaces after the configuration is complete.

Step 5 Verify the configuration.

Run the **display ppp mp** command on RouterA to view the MP binding information.

```
<RouterA> display ppp mp
Template is Virtual-Template1
 Bundle userb, 2 members, slot 0, Master link is Virtual-Template1:0
  0 lost fragments, 0 reordered, 0 unassigned, 0 interleaved,
 sequence 0/0 rcvd/sent
 The bundled sub channels are:
      Serial1/0/0
      Serial2/0/0
```

Bundle userb indicates that an MP is generated by binding the authenticated user name and the virtual template interface. The MP contains Serial1/0/0 and Serial2/0/0.

Run the **display virtual-access** command on RouterA to view the virtual access interface status.

```
<RouterA> display virtual-access
Virtual-Template1:0 current state : UP
```

```
Line protocol current state : UP
Last line protocol up time : 2011-02-09 09:56:31
Description:HUAWEI, AR Series, Virtual-Template1:0 Interface
Route Port,The Maximum Transmit Unit is 1500
Link layer protocol is PPP
LCP opened, MP opened, IPCP opened
Physical is MP
Current system time: 2011-02-09 09:59:16
    Last 300 seconds input rate 0 bits/sec, 0 packets/sec
    Last 300 seconds output rate 0 bits/sec, 0 packets/sec
    Realtime 0 seconds input rate 0 bits/sec, 0 packets/sec
    Realtime 0 seconds output rate 0 bits/sec, 0 packets/sec
    Input: 0 packets,0 bytes
           0 unicast,0 broadcast,0 multicast
           0 errors,0 unknownprotocol
    Output:0 packets,0 bytes
           0 unicast,0 broadcast,0 multicast
           0 errors
    Input bandwidth utilization  : 0.00%
    Output bandwidth utilization : 0.00%
```

You can obtain similar MP binding information on RouterB.

Ping RouterA on RouterB.

```
<RouterB> ping 10.10.10.9
PING 10.10.10.9: 56  data bytes, press CTRL_C to break
    Reply from 10.10.10.9: bytes=56 Sequence=1 ttl=255 time=50 ms
    Reply from 10.10.10.9: bytes=56 Sequence=2 ttl=255 time=50 ms
    Reply from 10.10.10.9: bytes=56 Sequence=3 ttl=255 time=50 ms
    Reply from 10.10.10.9: bytes=56 Sequence=4 ttl=255 time=50 ms
    Reply from 10.10.10.9: bytes=56 Sequence=5 ttl=255 time=50 ms

  --- 10.10.10.9 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 50/50/50 ms
```

RouterB can ping RouterA successfully.

----End

Configuration Files

Configuration file of RouterA

```
#
 sysname RouterA
 #
 ppp mp user userb bind Virtual-Template 1
#
aaa
  authentication-scheme system_a
 domain system
  authentication-scheme system_a
 local-user userb@system password simple userb
 local-user userb@system service-type ppp
#
interface Serial1/0/0
 link-protocol ppp
 ppp authentication-mode chap domain system
 ppp chap user user@system
 ppp chap password simple usera
 ppp mp
#
interface Serial2/0/0
 link-protocol ppp
```

```
 ppp authentication-mode chap domain system
 ppp chap user usera@system
 ppp chap password simple usera
 ppp mp
#
interface Virtual-Template1
 ppp mp binding-mode authentication
 ip address 10.10.10.9 255.255.255.252
#
return
```

Configuration file of RouterB

```
#
 sysname RouterB
 #
 ppp mp user usera bind Virtual-Template 1
#
aaa
 authentication-scheme system_b
 domain system
  authentication-scheme system_b
 local-user usera@system password simple usera
 local-user usera@system service-type ppp
#
interface Serial1/0/0
 link-protocol ppp
 ppp authentication-mode chap domain system
 ppp chap user userb@system
 ppp chap password simple userb
 ppp mp
#
interface Serial2/0/0
 link-protocol ppp
 ppp authentication-mode chap domain system
 ppp chap user userb@system
 ppp chap password simple userb
 ppp mp
#
interface Virtual-Template1
 ppp mp binding-mode authentication
 ip address 10.10.10.10 255.255.255.252
#
return
```

3.7.5 Example for Configuring MP Binding by Using an MP-Group Interface

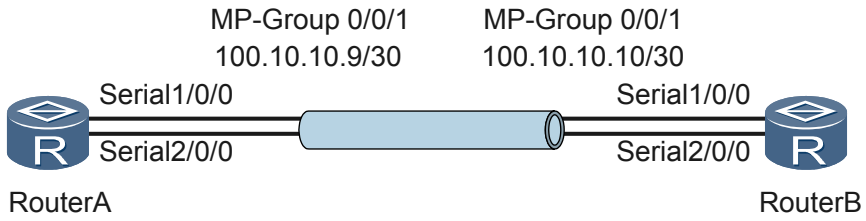
This section provides an example for configuring MP binding using an MP-Group interface.

Networking Requirements

To increase link bandwidth, you can bind multiple PPP links to an MP link. In this mode, PPP links in an MP link are fixed. The configuration is simple. It is widely used on networks.

As shown in **Figure 3-6**, two pairs of serial interfaces on RouterA and RouterB are connected and are bound to the MP-Group interface; CHAP authentication is used.

Figure 3-6 Network diagram



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure MP-Group interfaces.
2. Configure bidirectional CHAP authentication for the physical interfaces and add the physical interfaces to the MP-Group interface.
3. Restart the physical interfaces to make the configuration take effect.

Data Preparation

To complete the configuration, you need the following data:

- Numbers of MP-Group interfaces
- IP addresses of MP-Group interfaces
- Bidirectional CHAP authentication parameters: authentication mode and local user of the authenticator or user name and password of the authenticated party

Procedure

Step 1 Configure RouterA.

Create and configure an MP-Group interface.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface mp-group 0/0/1
[RouterA-Mp-group0/0/1] ip address 100.10.10.9 30
[RouterA-Mp-group0/0/1] quit
```

Add Serial1/0/0 and Serial2/0/0 to the MP-Group interface and use CHAP authentication. Configure the local user if the device functions as the authenticator, or the user name and password for CHAP authentication if the device is used as the authenticated party.

```
[RouterA] aaa
[RouterA-aaa] local-user userb password simple userb
[RouterA-aaa] local-user userb service-type ppp
[RouterA-aaa] authentication-scheme system_a
[RouterA-aaa-authen-system_a] authentication-mode local
[RouterA-aaa-authen-system_a] quit
[RouterA-aaa] domain system
[RouterA-aaa-domain-system] authentication-scheme system_a
[RouterA-aaa-domain-system] quit
[RouterA-aaa] quit
[RouterA] interface Serial 1/0/0
[RouterA-Serial1/0/0] ppp authentication-mode chap domain system
[RouterA-Serial1/0/0] ppp chap user usera
```

```
[RouterA-Serial1/0/0] ppp chap password simple usera
[RouterA-Serial1/0/0] ppp mp mp-group 0/0/1
[RouterA-Serial1/0/0] quit
[RouterA] interface Serial 2/0/0
[RouterA-Serial2/0/0] ppp authentication-mode chap domain system
[RouterA-Serial2/0/0] ppp chap user usera
[RouterA-Serial2/0/0] ppp chap password simple usera
[RouterA-Serial2/0/0] ppp mp mp-group 0/0/1
[RouterA-Serial2/0/0] quit
```

Step 2 Configure RouterB.

Create and configure an MP-Group interface.

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] interface mp-group 0/0/1
[RouterB-Mp-group0/0/1] ip address 100.10.10.10 30
[RouterB-Mp-group0/0/1] quit
```

Add Serial1/0/0 and Serial2/0/0 to the MP-Group interface and use CHAP authentication. Configure the local user if the device functions as the authenticator, or the user name and password for CHAP authentication if the device is used as the authenticated party.

```
[RouterB] aaa
[RouterB-aaa] local-user usera password simple usera
[RouterB-aaa] local-user usera service-type ppp
[RouterB-aaa] authentication-scheme system_b
[RouterB-aaa-authen-system_b] authentication-mode local
[RouterB-aaa-authen-system_b] quit
[RouterB-aaa] domain system
[RouterB-aaa-domain-system] authentication-scheme system_b
[RouterB-aaa-domain-system] quit
[RouterB-aaa] quit
[RouterB] interface Serial 1/0/0
[RouterB-Serial1/0/0] ppp authentication-mode chap domain system
[RouterB-Serial1/0/0] ppp chap user userb
[RouterB-Serial1/0/0] ppp chap password simple userb
[RouterB-Serial1/0/0] ppp mp mp-group 0/0/1
[RouterB-Serial1/0/0] quit
[RouterB] interface Serial 2/0/0
[RouterB-Serial2/0/0] ppp authentication-mode chap domain system
[RouterB-Serial2/0/0] ppp chap user userb
[RouterB-Serial2/0/0] ppp chap password simple userb
[RouterB-Serial2/0/0] ppp mp mp-group 0/0/1
[RouterB-Serial2/0/0] quit
```

Step 3 Restart member interfaces on RouterA.

```
[RouterA] interface Serial 1/0/0
[RouterA-Serial1/0/0] restart
[RouterA-Serial1/0/0] quit
[RouterA] interface Serial 2/0/0
[RouterA-Serial2/0/0] restart
[RouterA-Serial2/0/0] quit
```

Step 4 Restart member interfaces on RouterB. Use the commands in step 3 to restart member interfaces.

NOTE

To make the configuration take effect, restart all the member interfaces after the configuration is complete.

Step 5 Verify the configuration.

Run the **display ppp mp** command on RouterA to view the MP binding information.

```
<RouterA> display ppp mp interface Mp-group 0/0/1
Mp-group is Mp-group0/0/1
 ===========Sublinks status begin======
 Serial1/0/0 physical UP,protocol UP
```

```
 Serial2/0/0 physical UP,protocol UP
 ===========Sublinks status end========
 Bundle Multilink, 2 members, slot 0, Master link is Mp-group0/0/1
  0 lost fragments, 0 reordered, 0 unassigned, 0 interleaved,
 sequence 0/0 rcvd/sent
 The bundled sub channels are:
      Serial1/0/0
      Serial2/0/0
```

The command output provides the physical status and protocol status of member links, the number of member links, and member interfaces of the MP-Group interface.

Run the **display interface mp-group** command on RouterA to view the MP binding information.

```
<RouterA> display interface mp-group 0/0/1
Mp-group0/0/1 current state : UP
Line protocol current state : UP
Last line protocol up time : 2011-02-09 10:20:36
Description:HUAWEI, AR Series, Mp-group0/0/1 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 100.10.10.9/30
Link layer protocol is PPP
LCP opened, MP opened, IPCP opened
Physical is MP, baudrate is 64000 bps
Current system time: 2011-02-09 10:21:48
    Last 300 seconds input rate 0 bytes/sec, 0 packets/sec
    Last 300 seconds output rate 0 bytes/sec, 0 packets/sec
    Realtime 0 seconds input rate 0 bytes/sec, 0 packets/sec
    Realtime 0 seconds output rate 0 bytes/sec, 0 packets/sec
    6 packets input, 84 bytes, 0 drops
    6 packets output, 84 bytes, 0 drops
    Input bandwidth utilization  : 0.00%
    Output bandwidth utilization : 0.00%
```

As shown in the preceding information, the MP-Group interface is Up, the link layer protocol is PPP, and the status of LCP negotiation, MP negotiation, and IPCP negotiation is Opened.

You can obtain similar MP binding information on RouterB.

Ping RouterA on RouterB.

```
<RouterB> ping 100.10.10.9
PING 100.10.10.9: 56  data bytes, press CTRL_C to break
    Reply from 100.10.10.9: bytes=56 Sequence=1 ttl=255 time=40 ms
    Reply from 100.10.10.9: bytes=56 Sequence=2 ttl=255 time=50 ms
    Reply from 100.10.10.9: bytes=56 Sequence=3 ttl=255 time=60 ms
    Reply from 100.10.10.9: bytes=56 Sequence=4 ttl=255 time=50 ms
    Reply from 100.10.10.9: bytes=56 Sequence=5 ttl=255 time=50 ms

  --- 100.10.10.9 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 40/50/60 ms
```

RouterB can ping RouterA successfully.

----End

Configuration Files

Configuration file of RouterA

```
#
 sysname RouterA
#
```

```
aaa
  authentication-scheme system_a
 domain system
  authentication-scheme system_a
 local-user userb password simple userb
 local-user userb service-type ppp
#
interface Mp-group0/0/1
 ip address 100.10.10.9 255.255.255.252
#
interface Serial1/0/0
 link-protocol ppp
 ppp authentication-mode chap domain system
 ppp chap user usera
 ppp chap password simple usera
 ppp mp mp-group 0/0/1
#
interface Serial2/0/0
 link-protocol ppp
 ppp authentication-mode chap domain system
 ppp chap user usera
 ppp chap password simple usera
 ppp mp mp-group 0/0/1
return
```

Configuration file of RouterB

```
#
 sysname RouterB
#
aaa
  authentication-scheme system_b
 domain system
  authentication-scheme system_b
 local-user usera password simple usera
 local-user usera service-type ppp
#
interface Mp-group0/0/1
 ip address 100.10.10.10 255.255.255.252
#
interface Serial1/0/0
 link-protocol ppp
 ppp authentication-mode chap domain system
 ppp chap user userb
 ppp chap password simple userb
 ppp mp mp-group 0/0/1
#
interface Serial2/0/0
 link-protocol ppp
 ppp authentication-mode chap domain system
 ppp chap user userb
 ppp chap password simple userb
 ppp mp mp-group 0/0/1
return
```

3.7.6 Example for Configuring LFI

This section describes how to configure LFI on the AR2200.

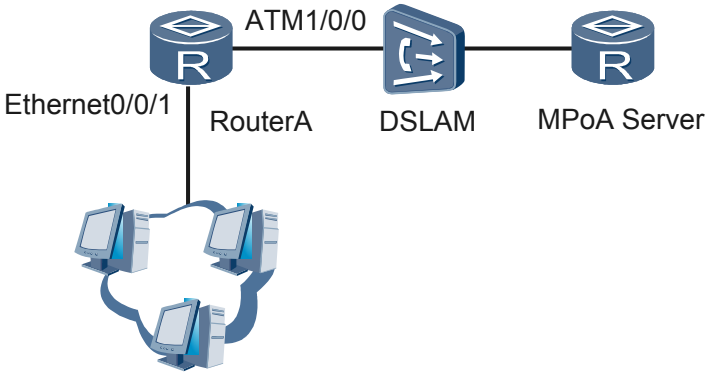
Networking Requirements

As shown in **Figure 3-7**, users on the enterprise network connect to a Layer 2 Ethernet interface of RouterA (an AR2200). RouterA functions as the gateway. A DSLAM connects the ADSL interface of RouterA to the ISP network.

Users on the enterprise network need to use the voice service, which requires real-time transmission. Large data packets require a longer transmission time and occupy a link for a long

time. If there are also voice packets to be transmitted on the link, there may be a delay in transmitting subsequent voice packets. To solve this problem, configure LFI so that voice packets and fragmented data packets can be transmitted on the same link. During transmission, the voice packets are distributed among the fragmented data packets. This reduces the delay in transmitting voice packets on a low-speed link.

Figure 3-7 Networking diagram of the LFI configuration



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the LAN side so that users on the enterprise network can connect to RouterA through the Layer 2 Ethernet interface.
2. Configure the WAN side so that packets sent from the enterprise network can be encapsulated in MP packets and RouterA can use the ADSL interface to communicate with the DSLAM.

   On RouterA, configure an LFI-enabled MP link, configure an MP member link, and bind the member link to a PVC.

Data Preparation

To complete the configuration, you need the following data:

- On the LAN side: allowed VLAN ID 200 and VLANIF interface address, for this example, 22.0.0.1/24
- On the WAN side:
  - On the MP link: virtual template interface number, virtual template interface address (IP address assigned by the remote end), for this example, CIR 100 kbit/s, CBS 100000 bytes, and maximum delay (20 ms) of fragmented packets
  - On the MP member link: virtual template interface number
  - On the PVC to which the member link is bound: interface number, name, and number of the PVC

Procedure

Step 1 Configure RouterA.

Configure the LAN side.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface ethernet 0/0/1
[RouterA-Ethernet0/0/1] port link-type trunk
[RouterA-Ethernet0/0/1] port trunk allow-pass vlan 200
[RouterA-Ethernet0/0/1] undo port trunk allow-pass vlan 1
[RouterA-Ethernet0/0/1] quit
[RouterA] vlan 200
[RouterA-vlan200] quit
[RouterA] interface vlanif 200
[RouterA-Vlanif200] ip address 22.0.0.1 255.255.255.0
[RouterA-Vlanif200] quit
```

Configure the WAN side.

- Configure an MP link.

```
[RouterA] interface virtual-template 1023
[RouterA-Virtual-Template1023] ppp mp lfi
[RouterA-Virtual-Template1023] ip address ppp-negotiate
[RouterA-Virtual-Template1023] qos gts cir 100 cbs 100000
[RouterA-Virtual-Template1023] ppp mp lfi delay-per-frag 20
[RouterA-Virtual-Template1023] quit
```

- Configure an MP member link.

```
[RouterA] interface virtual-template 10
[RouterA-Virtual-Template10] ppp mp virtual-template 1023
[RouterA-Virtual-Template10] quit
```

- Bind the MP member link to a PVC.

```
[RouterA] interface atm 1/0/0
[RouterA-Atm1/0/0] pvc mpoa 1/38
[RouterA-atm-pvc-Atm1/0/0-1/38-mpoa] map ppp virtual-template 10
[RouterA-atm-pvc-Atm1/0/0-1/38-mpoa] quit
[RouterA-Atm1/0/0] quit
```

Step 2 Configure the DSLAM.

See the DSLAM documentation.

Step 3 Configure an MPoA server.

Set the MPoA server address to 23.0.0.2 and configure the MPoA server to assign IP address 23.0.0.1 to the AR2200.

Step 4 Verify the configuration.

- Run the **display interface virtual-template** command to check whether the virtual template interface on RouterA has been assigned a correct IP address.

```
[RouterA] display interface virtual-template 1023
```

The following information indicates that the virtual template interface has been assigned a correct IP address.

```
Internet Address is negotiated, 23.0.0.1/24
```

- Run the **display virtual-access** command to view the MP negotiation status of the virtual access interface created using the virtual template interface.

```
[RouterA] display virtual-access
```

The following information indicates that MP negotiation is successful on the virtual access interface.

```
LCP opened, MP opened, IPCP opened
```

- RouterA can ping the MPoA server successfully.

```
[RouterA] ping 23.0.0.2
PING 23.0.0.2: 56  data bytes, press CTRL_C to break
    Reply from 23.0.0.2: bytes=56 Sequence=1 ttl=255 time=2 ms
    Reply from 23.0.0.2: bytes=56 Sequence=2 ttl=255 time=1 ms
```

```
  Reply from 23.0.0.2: bytes=56 Sequence=3 ttl=255 time=1 ms
  Reply from 23.0.0.2: bytes=56 Sequence=4 ttl=255 time=1 ms
  Reply from 23.0.0.2: bytes=56 Sequence=5 ttl=255 time=1 ms
 --- 23.0.0.2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 1/1/2 ms
```

----End

Configuration File

- Configuration file of RouterA

```
#
 sysname RouterA
#
 vlan batch 200
#
 interface Virtual-Template1023
  ppp mp lfi
  ip address ppp-negotiate
  qos gts cir 100 cbs 100000
  ppp mp lfi delay-per-frag 20
#
 interface Virtual-Template10
  ppp mp Virtual-Template 1023
#
 interface Atm1/0/0
  pvc mpoa 1/38
   map ppp Virtual-Template 10
#
interface
Ethernet0/0/1
 port link-type
trunk
 undo port trunk allow-pass vlan
1
 port trunk allow-pass vlan
200
#

interface
Vlanif200
 ip address 22.0.0.1 255.255.255.0
#
return
```

4 PPPoE Configuration

About This Chapter

This chapter describes the concept of Point-to-Point Protocol over Ethernet (PPPoE) and the procedures for configuring the AR2200 as the PPPoE server and PPPoE client.

4.1 PPPoE Overview

This section describes PPPoE concepts.

The PPPoE technology transmits Point-to-Point Protocol (PPP) packets on an Ethernet.

Carriers want to connect multiple hosts at a remote site to one access device. The access device is expected to provide access control and accounting for different hosts in a manner similar to dial-up services using PPP. However, the configuration is complicated and costs are high when traditional access technologies are used. Using PPPoE, carriers can achieve this goal at lower cost because Ethernet a cost-effective access technology, and PPP implements access control and accounting.

PPPoE uses the client/server model. The PPPoE client sends a connection request to the PPPoE server. After the client and server complete negotiation, the server provides access control and authentication functions.

4.2 PPPoE Features Supported by the AR2200

This section describes the PPPoE features supported by the AR2200. The AR2200 can function as a PPPoE server or a PPPoE client.

- PPPoE server

  When the AR2200 functions as a PPPoE server, it allocates IP addresses to users and provides various authentication modes. The AR2200 can work with firewalls to guarantee security of the internal network. The PPPoE server is applicable to Ethernet networks connecting to the Internet, such as campus networks and intelligent residential networks.

  When the AR2200 functions as a PPPoE server, user hosts must be installed with the PPPoE client software.

- PPPoE client

  When the AR2200 functions as the PPPoE client, user hosts do not need to be installed with the PPPoE client software. All the user hosts on a local area network (LAN) transmit data using the same PPPoE session and use the same user name and password.

4.3 Configuring the AR2200 as a PPPoE Server

This section describes how to configure the AR2200 as a PPPoE server.

4.3.1 Establishing the Configuration Task

Before configuring the PPPoE server, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task quickly and accurately.

Applicable Environment

When the AR2200 functions as a PPPoE server, it allocates IP addresses to users and provides various authentication modes. The AR2200 can work with firewalls to guarantee security of the internal network. The PPPoE server is applicable to Ethernet networks connecting to the Internet,

such as campus networks and intelligent residential networks. When the AR2200 functions as the PPPoE server, user hosts must be installed with the PPPoE client software.

Pre-configuration Tasks

None.

Data Preparation

To configure the PPPoE server, you need the following data.

No.	Data
1	Number, IP address, and authentication mode of the virtual template interface, and IP address or address pool allocated to the remote device
2	Number of the Ethernet interface to which the virtual template interface is bound
3	(Optional) Maximum number of PPPoE sessions
4	User name, password, and service type of PPPoE users

4.3.2 Configuring a Virtual Template Interface

This section describes how to create a virtual template interface and set the parameters of the virtual template interface.

Context

An Ethernet interface provides the PPPoE function after a virtual template interface is bound to the Ethernet interface or PON interface.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface virtual-template vt-number
```

A virtual template interface is created and the virtual template interface view is displayed.

Step 3 (Optional) Run:

```
ppp authentication-mode { chap | pap } [ [ call-in ] domain isp-name ]
```

The PPP authentication mode is configured on the virtual template interface.

By default, the PPPoE server does not authenticate users.

When a network requires high security, perform this step. CHAP authentication provides higher security than PAP authentication.

Step 4 Run:

```
ip address ip-address { mask | mask-length }
```

An IP address is allocated to the virtual template interface.

Step 5 (Optional) Run:

```
remote address { ip-address | pool pool-name }
```

An IP address or address pool is allocated to the remote device.

Perform this step when the remote device does not have an IP address and needs to obtain an IP address from the PPPoE server.

To allocate an IP address pool to the remote device, run the **ip pool** *pool-name* command to configure a global IP address pool, and then run the **network** *ip-address* [**mask** { *mask* | *mask-length* }] command in the global IP address pool view to specify the address range in the address pool and run the **gateway-list** *ip-address* &<1-8> command to configure the egress gateway address for the global address pool.

----End

Follow-up Procedure

If the PPP authentication mode is configured, configure a PPPoE user according to **4.3.5 (Optional) Configuring a PPPoE Local User**.

4.3.3 Enabling PPPoE

The PPPoE function is automatically enabled after a virtual template interface is bound to a WAN Ethernet interface or PON interface.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The WAN Ethernet interface or PON interface view is displayed.

Step 3 Run:

```
pppoe-server bind virtual-template vt-number
```

The specified virtual template interface is bound to the Ethernet interface or PON interface and PPPoE is enabled on the Ethernet interface or PON interface.

By default, PPPoE is disabled.

----End

4.3.4 (Optional) Setting PPPoE Session Parameters

You can set the maximum number of PPPoE sessions on the AR2200.

Context

You can set the following limits on the number of PPPoE sessions:

- Maximum number of PPPoE sessions that can be created on the AR2200
- Maximum number of PPPoE sessions that can be created on a MAC address on the AR2200
- Maximum number of PPPoE sessions that can be created on a MAC address on the remote PPPoE client

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
pppoe-server max-sessions total number
```

The maximum number of PPPoE sessions that can be created on the AR2200 is set.

By default, a maximum of 512 PPPoE sessions can be created on the AR2200.

Step 3 Run:

```
pppoe-server max-sessions local-mac number
```

The maximum number of PPPoE sessions that can be created on a MAC address of the AR2200 is set.

By default, a maximum of 512 PPPoE sessions can be created on a MAC address on the AR2200.

Step 4 Run:

```
pppoe-server max-sessions remote-mac number
```

The maximum number of PPPoE sessions that can be created on a MAC address on the remote PPPoE client is set.

By default, a maximum of 512 PPPoE sessions can be created on a MAC address on the remote PPPoE client.

----End

4.3.5 (Optional) Configuring a PPPoE Local User

When the AR2200 functions as the PPPoE server and uses local authentication, configure a local user on the AR2200.

Context

By default, the PPPoE server does not authenticate users. You do not need to configure a local user if the PPP authentication mode is not configured.

If remote authentication is used, configure the local user according to AAA Configuration in the *Huawei AR2200 Series Enterprise Routers Configuration Guide - Security*.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
aaa
```

The AAA view is displayed.

Step 3 (Optional) Run:

```
domain domain-name
```

A domain is created and the domain view is displayed.

By default, a domain uses local authentication and none accounting.

Step 4 (Optional) Run:

```
quit
```

The AAA view is displayed.

NOTE

If no domain is created, the default domain and default authentication mode are used. By default, if the user name of a user does not contain the domain name, the user is added to the default domain and local authentication is performed for the user.

Step 5 Run:

```
local-user user-name password { simple | cipher } password
```

A local user is created.

Step 6 Run:

```
local-user user-name service-type ppp
```

The service type of the local user is set to PPP.

----End

4.3.6 Checking the Configuration

After the PPPoE server is configured, PPPoE clients dial in to the server. After PPPoE sessions are set up, you can view the PPPoE session status.

Procedure

Step 1 Install the PPPoE client software on a client, and then use the configured user name and password to dial in to the Internet.

Step 2 Run the **display pppoe-server session** command to check the PPPoE session status and statistics about PPPoE packets.

----End

Example

Run the **display pppoe-server session all** command to view information about PPPoE sessions on the PPPoE server, including the session ID, local device MAC address, remote device MAC address, session status, physical interface, and virtual template interface.

```
<Huawei> display pppoe-server session all
SID Intf                    State OIntf          RemMAC         LocMAC
1   Virtual-Template1:0     UP    GE1/0/0        00e0.fc03.0201 0819.a6cd.0680
```

Run the **display pppoe-server session packet** command to view the statistics about PPPoE packets, including the session ID, local device MAC address, remote device MAC address, number of incoming packets and bytes accepted and discarded, and number of outgoing packets and bytes sent and discarded.

```
<Huawei> display pppoe-server session packet
SID     RemMAC       LocMAC         InP      InO   InD     OutP     OutO  OutD
1    00e0fc030201 0819a6cd0680       34      738     0       34      738     0
```

4.4 Configuring the AR2200 as a PPPoE Client

This section describes how to configure the AR2200 as a PPPoE client.

4.4.1 Establishing the Configuration Task

Before configuring the PPPoE client, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task quickly and accurately.

Applicable Environment

When all the hosts on a LAN need to transmit data using the same PPPoE session, the AR2200 must be connected to all hosts on the LAN and function as a PPPoE client to set up a session with the PPPoE server. The hosts use the same user name and password to connect to the Internet and do not need to be installed with the PPPoE client software.

Pre-configuration Tasks

None.

Data Preparation

To configure the PPPoE client, you need the following data.

No.	Data
1	Number, IP address, and other parameters of the dialer interface
2	Number of the Ethernet interface to which the dialer interface is bound

4.4.2 Configuring a Dialer Interface

When the AR2200 functions as the PPPoE client, configure a dialer interface on the AR2200.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
dialer-rule
```

The dialer rule view is displayed.

Step 3 Run:

```
dialer-rule dialer-rule-number { acl { acl-number | name acl-name } | ip { deny |
permit } | ipv6 { deny | permit } }
```

A dialer access control list (ACL) is configured.

Step 4 Run:

```
quit
```

Return to the system view.

Step 5 Run:

```
interface dialer number
```

A dialer interface is created and the dialer interface view is displayed.

Step 6 Run:

```
dialer user user-name
```

The user name is configured for user hosts connected to the AR2200.

Step 7 Run:

```
dialer-group group-number
```

The dialer group of the dialer interface is specified.

The value of *group-number* must be the same as the value of *dialer-number* configured in step 3.

Step 8 Run:

```
dialer bundle number
```

RS-DCC is enabled and a dialer bundle is configured for the dialer interface.

Step 9 Assign an IP address to the dialer interface.

- Assign an IPv4 address to the dialer interface.
  - Run:

    ```
    ip address ip-address { mask | mask-length }
    ```

    An IP address is allocated to the dialer interface.
  - Run:

    ```
    ip address ppp-negotiate
    ```

    The dialer interface is configured to obtain an IP address from the PPPoE server.
- Assign an IPv6 address to the dialer interface.

  Run:

  ```
  ipv6 address { ipv6-address prefix-length | ipv6-address/prefix-length }
  ```

An IPv6 address is assigned to the dialer interface.

NOTE

Before assigning an IPv6 address to an interface, run the **ipv6** command in the system view to enable IPv6 packet forwarding and run the **ipv6 enable** command on the interface to enable IPv6.

----End

4.4.3 Configuring a PPPoE Session

This section describes how to configure a PPPoE session on a physical Ethernet interface or a Pon interface.

Context

A PPPoE session can be created on a physical Ethernet interface or a Pon interface or a virtual Ethernet interface.

- When the AR2200 uses an ADSL interface to directly connect to the Internet, configure a PPPoE session on the virtual Ethernet interface bound to the ADSL interface.

  For details on how to configure a PPPoE session on the virtual Ethernet interface, see **1.4.6 Configuring PPPoEoA Mapping on a PVC**.
- When AR2200 uses an Ethernet interface or a Pon interface to connect to an ADSL modem, configure a PPPoE session on the Ethernet interface or Pon interface.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The WAN Ethernet interface or Pon interface view is displayed.

Step 3 Run:

```
pppoe-client dial-bundle-number number [ on-demand ] [ no-hostuniq ]
```

A dialer bundle is specified for a PPPoE session on the interface.

The specified dialer bundle must be the one configured in **4.4.2 Configuring a Dialer Interface**.

If the **on-demand** parameter is specified, run the **dialer timer idle** *seconds* command to set the link idle time on the dialer interface.

----End

4.4.4 (Optional) Configuring NAT

This section describes the usage scenario of network address translation (NAT).

Context

If the computers on a LAN use private IP addresses, configure NAT on the AR2200. For details, see NAT Configuration in the *Huawei AR2200 Series Enterprise Routers Configuration Guide - Security*.

4.4.5 Checking the Configuration

After the AR2200 is configured as the PPPoE client, hosts on the LAN connected to the AR2200 can dial in to the Internet.

Procedure

Step 1 Run the **display pppoe-client session** { **packet** | **summary** } [**dial-bundle-number** *number*] command to check the PPPoE session status and statistics.

----End

Example

Run the **display pppoe-client session summary** command to view information about the PPPoE session, including the session ID, session status, dialer interface, dialer bundle, physical interface bound to the dialer interface, server MAC address, and client MAC address.

```
<Huawei> display pppoe-client session summary
PPPoE Client Session:
ID   Bundle  Dialer  Intf            Client-MAC    Server-MAC    State
1    1       1       GE1/0/0         00e0fc030201  0819a6cd0680  PPPUP
```

Run the **display pppoe-client session packet** command to view the statistics about PPPoE packets, including the session ID, number of incoming packets accepted and discarded, and number of outgoing packets sent and discarded.

```
<Huawei> display pppoe-client session packet
PPPoE Client Session:
ID     InP        InO        InD         OutP       OutO       OutD
1      36         758        0           50         1222       0
```

4.5 Maintaining PPPoE

4.5.1 Resetting PPPoE Sessions

You may need to reset PPPoE sessions during device maintenance.

Context

To disconnect users from the AR2200 or trigger re-negotiation, reset PPPoE sessions.

CAUTION

User services are interrupted when PPPoE sessions are reset; therefore, reset PPPoE sessions with caution.

Procedure

- Run the **reset pppoe-server** { **all** | **interface** *interface-type interface-number* | **virtual-template** *number* } command to terminate all PPPoE sessions or a specified session on the PPPoE sever.
- Run the **reset pppoe-client** { **all** | **dial-bundle-number** *number* } command to reset all PPPoE sessions or a specified session on the PPPoE client.

  If a PPPoE session in permanent online mode is reset using the **reset pppoe-client** command, the AR2200 will set up the session again after 16 seconds. If a PPPoE session in packet triggered mode is reset using the **reset pppoe-client** command, the AR2200 will set up the session again when data needs to be transmitted.

----End

4.5.2 Terminating PPPoE Sessions

During routine maintenance, administrators can terminate PPPoE sessions based on user IDs.

Context

During routine maintenance, administrators can terminate PPPoE sessions based on user IDs.

CAUTION

User services are interrupted when PPPoE sessions are terminated; therefore, exercise caution when you run the **cut access-user** command.

Procedure

Step 1 Run:

```
display access-user
```

The online user information is displayed.

In the **display access-user** command output, check the ID the of user whose PPPoE session needs to be terminated and record the user ID.

Step 2 Run:

```
system-view
```

The system view is displayed.

Step 3 Run:

```
aaa
```

The AAA view is displayed.

Step 4 Run:

```
cut access-user user-id begin-number [ end-number ]
```

The PPPoE session of a specified user is terminated.

The user ID is the same as that recorded in step 1.

----End

4.6 Configuration Examples

This section describes the networking requirements, configuration roadmap, and data preparation for typical PPPoE applications and provides the configuration files.

4.6.1 Example for Configuring the PPPoE Server

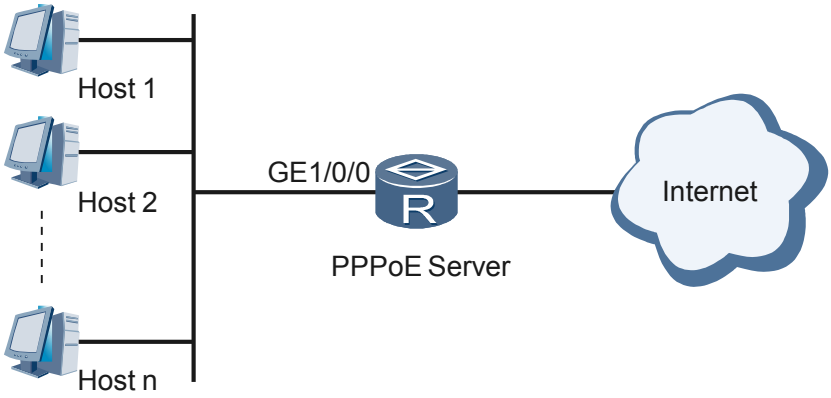
This section provides a PPPoE server configuration example.

Networking Requirements

As shown in **Figure 4-1**, hosts on an enterprise network need to dial in to the Internet using PPPoE. An AR2200 needs to be configured as the PPPoE server to provide the PPPoE service for users on the enterprise network. Each user host sets up a PPPoE session with the PPPoE server and is allocated a user account.

The PPPoE server performs local authentication and allocates IP addresses to user hosts from an IP address pool.

Figure 4-1 AR2200 functions as the PPPoE server



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure a local address pool.
2. Configure a virtual template interface and set PPP parameters on the virtual template interface.
3. Bind the virtual template interface to a physical interface.
4. Configure a PPPoE local user for authentication and accounting.

Data Preparation

To complete the configuration, you need the following data:

- IP address range in the IP address pool and IP address of the gateway
- Number, IP address, and authentication mode of the virtual template interface, and address pool for remote devices
- Number of the physical interface to which the virtual template interface is bound
- Parameters of each PPPoE user, including the user name, password, service type, domain, and authentication scheme in the domain

Procedure

Step 1 Configure the global IP address pool **pool1**.

```
<Huawei> system-view
[Huawei] ip pool pool1
[Huawei-ip-pool-pool1] network 192.168.10.10 mask 255.255.255.0
[Huawei-ip-pool-pool1] gateway-list 192.168.10.1
[Huawei-ip-pool-pool1] quit
```

Step 2 Configure a virtual template interface.

```
<Huawei> system-view
[Huawei] interface virtual-template 1
[Huawei-Virtual-Template1] ppp authentication-mode chap domain system
[Huawei-Virtual-Template1] ip address 192.168.10.1 255.255.255.0
[Huawei-Virtual-Template1] remote address pool pool1
[Huawei-Virtual-Template1] quit
```

Step 3 Enable PPPoE on GE1/0/0 of the PPPoE server.

```
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pppoe-server bind virtual-template 1
[Huawei-GigabitEthernet1/0/0] quit
```

Step 4 Configure a PPPoE local user.

```
[Huawei] aaa
[Huawei-aaa] authentication-scheme system_a
[Huawei-aaa-authen-system_a] authentication-mode local
[Huawei-aaa-authen-system_a] quit
[Huawei-aaa] domain system
[Huawei-aaa-domain-system] authentication-scheme system_a
[Huawei-aaa-domain-system] quit
[Huawei-aaa] local-user user1@system password simple huawei
[Huawei-aaa] local-user user1@system service-type ppp
[Huawei-aaa] quit
```

Step 5 Verify the configuration.

1. On the PPPoE client

   Install the PPPoE client software on a computer and configure the user name **user1@system** and password **huawei** on the computer. Dial in to the PPPoE server.

2. On the PPPoE server

   Run the **display pppoe-server session all** command to check the PPPoE session status and configuration. The following information shows that the PPPoE session status is Up and the session configuration is correct.

```
<Huawei> display pppoe-server session all
SID Intf                      State OIntf          RemMAC         LocMAC
10  Virtual-Template1:0       UP    GE1/0/0        0011.0914.1bd3
00e0.fc99.9999
```

   Run the **display virtual-access** command to view the virtual access interface status, you can check the negotiation status of LCP and IPCP. The status must be **opened**.

```
<Huawei> display virtual-access
Virtual-Template1:0 current state :
UP
```

```
    Line protocol current state :
    UP
    Last line protocol up time : 2010-03-20
    09:59:52
    Description:HUAWEI, AR Series, Virtual-Template1:0 Interface
    Route Port,The Maximum Transmit Unit is
    1492
    Link layer protocol is
    PPP
    LCP opened, IPCP
    opened
    Current system time: 2010-03-20
    12:01:47
        Input bandwidth utilization  :
    0.00%
        Output bandwidth utilization : 0.00%
```

----End

Configuration Files

Configuration file of the AR2200 as the PPPoE server

```
#
 sysname Huawei
#
ip pool pool1
 network 192.168.10.10 mask 255.255.255.0
 gateway-list 192.168.10.1
#
aaa
 authentication-scheme system_a
 domain system
  authentication-scheme system_a
 local-user user1@system password simple huawei
 local-user user1@system service-type ppp
#
interface Virtual-Template1
 ppp authentication-mode chap domain system
 remote address pool pool1
 ip address 192.168.10.1 255.255.255.0
#
interface GigabitEthernet1/0/0
 pppoe-server bind Virtual-Template 1
#
return
```

4.6.2 Example for Configuring the PPPoE Client

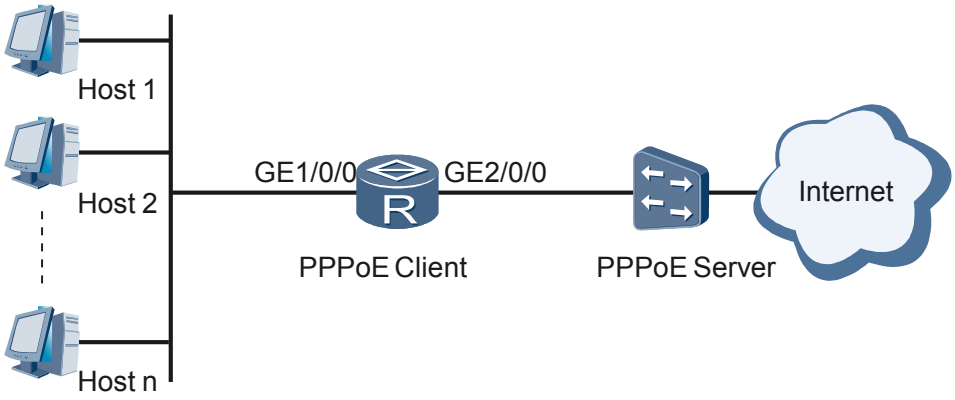
This section provides a PPPoE client configuration example.

Networking Requirements

As shown in **Figure 4-2**, hosts on an enterprise network are required to transmit data using the same PPPoE session to implement uniform accounting. To set up a PPPoE session with the PPPoE server, configure an AR2200 as the PPPoE client. The hosts use the same user name and password. The AR2200 sends the user name and password to the PPPoE server for authentication. After the AR2200 is authenticated, it establishes a PPPoE session with the PPPoE server. If no data is transmitted for a long period of time, the PPPoE client disconnects from the PPPoE server. When data needs to be transmitted, the PPPoE client re-establishes a PPPoE session with the PPPoE server.

The AR2200 obtains an IP address from the PPPoE server.

Figure 4-2 AR2200 functions as the PPPoE client



Configuration Roadmap

The configuration roadmap is as follows:

1. Create a dialer interface and set parameters of the dialer interface.
2. Create a PPPoE session.
3. Configure a static route from the local end to the PPPoE server.

Data Preparation

To complete the configuration, you need the following data:

- Parameters of the dialer interface, including the dialer interface number, dialer interface IP address, dialer bundle, and link idle time
- On-demand dialing used by the AR2200 to establish a PPPoE session
- Destination address, mask, and outbound interface of the static route

Procedure

Step 1 Configure the PPPoE server.

Configure the authentication mode, IP address allocation mode, and IP address or address pool for remote devices. For the configuration procedure, see the documentation of the PPPoE server. If the AR2200 functions as the PPPoE server, see **4.6.1 Example for Configuring the PPPoE Server**.

Step 2 Configure the dialer interface.

```
<Huawei> system-view
[Huawei] dialer-rule
[Huawei-dialer-rule] dialer-rule 1 ip permit
[Huawei-dialer-rule] quit
[Huawei] interface dialer 1
[Huawei-Dialer1] dialer user user2
[Huawei-Dialer1] dialer-group 1
[Huawei-Dialer1] dialer bundle 1
[Huawei-Dialer1] ppp chap user user1
[Huawei-Dialer1] ppp chap password cipher user1
[Huawei-Dialer1] dialer timer idle 300
INFO:  The configuration will become effective after link reset.
[Huawei-Dialer1] dialer queue-length 8
```

```
[Huawei-Dialer1] ip address ppp-negotiate
[Huawei-Dialer1] quit
```

Step 3 Create a PPPoE session.

```
[Huawei] interface gigabitethernet 2/0/0
[Huawei-GigabitEthernet2/0/0] pppoe-client dial-bundle-number 1 on-demand
[Huawei-GigabitEthernet2/0/0] quit
```

Step 4 Configure a static route from the local end to the PPPoE server.

Assume that the IP address of the PPPoE server is 10.10.10.3.

```
[Huawei] ip route-static 0.0.0.0 0 dialer 1
```

Step 5 Verify the configuration.

Run the **display pppoe-client session summary** command to check the PPPoE session status and configuration. The following information shows that the PPPoE session status is Up and the session configuration is the same as the planned data.

```
<Huawei> display pppoe-client session summary
PPPoE Client Session:
ID   Bundle  Dialer  Intf            Client-MAC    Server-MAC    State
1    1       1       GE2/0/0         00e0fc030201  0819a6cd0680  UP
```

----End

Configuration Files

Configuration file of the AR2200 as the PPPoE client

```
#
 sysname Huawei
#
dialer-rule
 dialer-rule 1 ip permit
#
interface Dialer1
 link-protocol ppp
 ip address ppp-negotiate
 dialer user user2
 ppp chap user user1
 ppp chap password cipher user1
 dialer bundle 1
 dialer queue-length 8
 dialer timer idle 300
 dialer-group 1
#
interface GigabitEthernet2/0/0
 pppoe-client dial-bundle-number 1 on-demand
#
 ip route-static 0.0.0.0 0.0.0.0 255.255.255.0 Dialer1
return
```

5 ISDN Configuration

About This Chapter

This chapter describes the concepts and configuration procedures of ISDN on the AR2200, and provides configuration examples.

5.1 ISDN Overview

Integrated Services Digital Network (ISDN) evolves from the Integrated Digital Network (IDN). It provides end-to-end digital connections and supports a wide range of services, including voice, high-speed fax, video conference, intelligent telegraph, and teletext services.

ISDN Background and Reference Model

In 1980s, the telecommunications networks had the following characteristics:

- There were multiple types of networks, which provided different services.
- The same services were transmitted by devices on different networks and converted by gateways so that the devices can communicate.

Complicated service conversion between networks degrades the service efficiency and limits the service usage. Networks were difficult to manage and maintain.

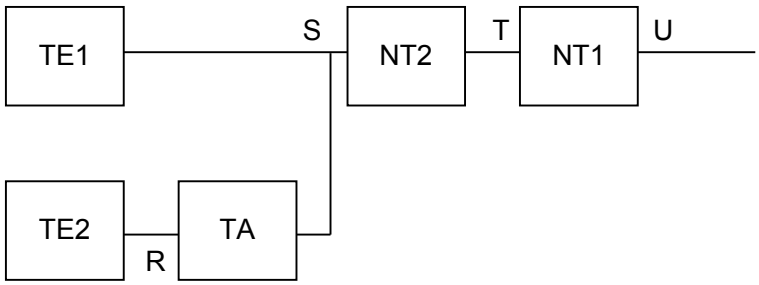
In 1980, the Consultative Committee of International Telegraph and Telephone (CCITT) issued the ISDN recommendation. The ISDN recommendation (blue book) issued in 1988 was well-accepted.

ISDN provides a well-designed network and has the following characteristics:

- Full-digital signals allow networks to provide various services in addition to voice communication.
- ISDN provides voice, high-speed fax, video conference, intelligent telegraph, and teletext services.
- Users access an ISDN network using the same physical interface, and multiple devices use the same ISDN number.

ISDN provides users with a set of user-network interfaces (UNIs) to connect different terminals such as phones, fax machines, computers to ISDN networks. **Figure 5-1** shows the ISDN reference model, which defines multiple function groups and reference points.

Figure 5-1 ISDN reference model



Function groups in the ISDN reference model have the following functions:

- Network Termination 1 (NT1): implements physical layer functions, including subscriber line transmission, loop detection, and D channel preemption.

- Network Termination 2 (NT2): is an intelligent network terminal such as a private branch exchange (PBX) or a local area network (LAN) router. It implements physical layer functions, link layer functions, and call control functions.
- Terminal Equipment Type 1 (TE1): is an ISDN standard terminal complying with the ISDN interface standard, such as a digital phone.
- Terminal Equipment Type 2 (TE2): is a non-ISDN standard terminal, which does not comply with the ISDN interface standard.
- Terminal Adapter (TA): implements the adaptation function to enable a TE2 to access a standard ISDN interface.

Reference points define communication nodes between different devices. UNI interfaces support the following reference points:

- R: a reference point between a TE2 and a TA
- S: a reference point between a TE1 or TA and an NT
- T: a reference point between an NT1 and an NT2
- U: a reference point between an NT and an ISDN network

ISDN Physical Interfaces

ISDN physical interfaces are classified into two types:

- Basic Rate Interface (BRI)
- Primary Rate Interface (PRI)

Both BRI and PRI interfaces contain data channels (B channels) and signaling channels (D channels). B channels transmit data information (IP/IPX packets) of upper layer applications, and D channels transmit all ISDN signaling packets.

A BRI interface contains two 64 kbit/s B channels and one 16 kbit/s D channel, and the interface bandwidth is 2B + D. The two B channels can be used independently or be bundled using the MP binding technique to provide a maximum of 128 kbit/s transmission rate.

PRI interfaces are classified into CE1 PRI interfaces and CT1 PRI interfaces:

- CE1 PRI interface: has the bandwidth of 30B + D. An E1 line has 32 timeslots. Timeslot 0 transmits synchronization signals; timeslot 16 functions as a D channel; the remaining 32 timeslots function as B channels. B and D channels each work at a rate of 64 kbit/s.
- CT1 PRI interface: has the bandwidth of 23B + D. A T1 line contains 24 timeslots. Timeslot 24 functions as a D channel, and the remaining 23 timeslots function as B channels. Each B channel works at a rate of 56 kbit/s or 64 kbit/s, and the D channel works at a rate of 64 kbit/s.

ISDN Protocol Architecture

The ISDN protocol references the Open Systems Interconnection (OSI) model and implements functions of the physical layer, data link layer, and network layer on UNI interfaces. **Figure 5-2** shows the ISDN protocol architecture.

Figure 5-2 ISDN protocol architecture

	D Channel	B Channel
Layer3	DSS1(Q.931)	IP/IPX
Layer2	LAPD(Q.921)	PPP/HDLC/FR
Layer1	I.430/I.431	

Physical layer protocol: B channels and D channels are multiplexed on the same physical interface. Therefore, ISDN B channels and D channels at the physical layer use the same protocols: ITU-T I.430 (BRI) and ITU-T I.431 (PRI).

Data link layer protocol: ISDN does not define Layer 2 protocols dedicated to B channels. Any Layer 2 protocols such as PPP, HDLC, and FR can be used between two communicating devices as long as they can transparently transmit data on B channels. The AR2200 supports Link Access Procedure on the D-channel (LAPD) defined in Q.921 for D channels. These Layer 2 protocols transmit messages and data generated by a Layer 3 or management entity.

Network layer protocol: ISDN does not define Layer 3 protocols dedicated to B channels. It defines only Layer 3 protocols in the Q.931 standard for D channels. The Q.931 standard defines Digital Subscriber Signaling System No.1 (DSS1), which controls and manages call establishment and release on B channels and is developed into different protocols based on service applications. These protocols include National ISDN (NI) and National ISDN-2 (NI2) in the United States, the ISDN protocol proposed by the European Telecommunications Standards Institute (ETSI), and the ISDN protocol proposed by the Nippon Telegraph and Telephone (NTT) Corporation. The AR2200 supports DSS1.

For more information about data link layer protocols and network layer protocols, see ISDN Layer 2 Protocols and ISDN Layer 3 Protocols in the *Huawei AR2200 Series Enterprise Routers Feature Description - WAN Interconnection*. To learn details about these ISDN protocols, see the related standards.

5.2 ISDN Features Supported by the AR2200

This section describes the location of the AR2200 in the ISDN reference model, ISDN physical interfaces supported by the AR2200, and usage scenarios of ISDN features supported by the AR2200.

On the AR2200, ISDN physical interfaces are provided by interface cards:

- The 1E1T1-M/2E1T1-M interface card provides ISDN PRI interfaces.
- BRI interface cards provide ISDN BRI interfaces.

The location of the AR2200 in the ISDN reference model varies according to the interface of the AR2200 accessing an ISDN network. When the AR2200 uses an ISDN PRI interface to access an ISDN network, the AR2200 is directly connected to an ISDN network-side device. When AR2200 uses an ISDN BRI interface to access an ISDN network, the AR2200 connects to an NT1 device, which connects to an ISDN network-side device. **Figure 5-3** and **Figure 5-4** show the typical networking.

Figure 5-3 AR2200 accessing an ISDN network using an ISDN PRI interface

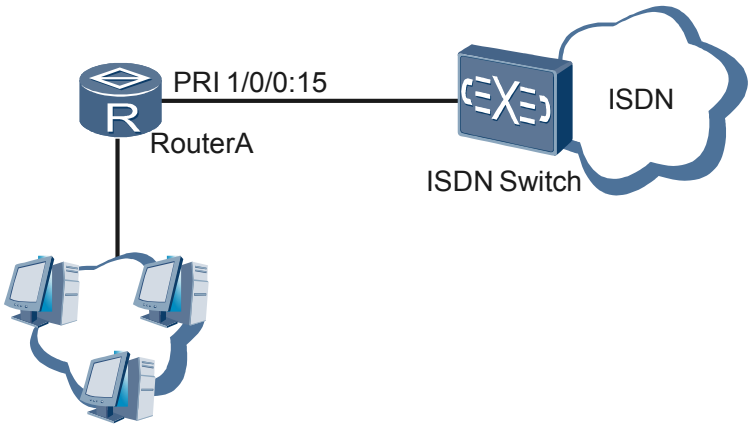
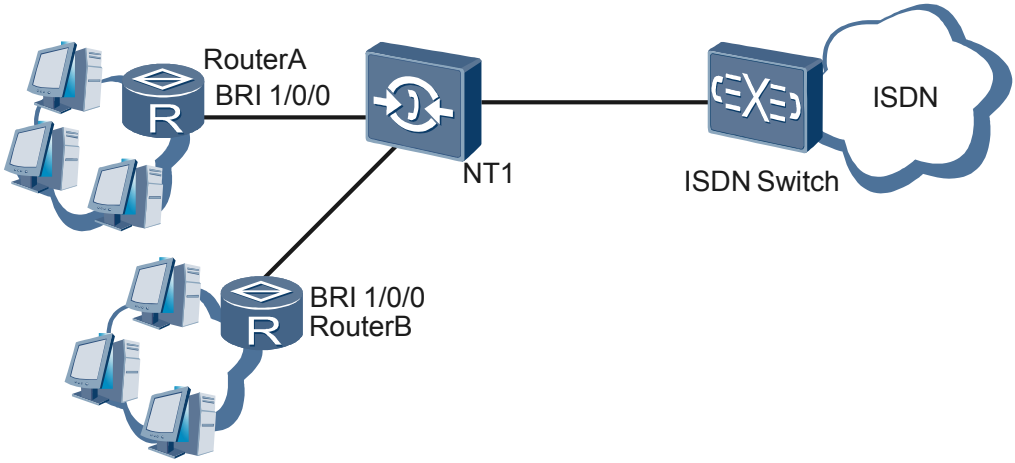


Figure 5-4 AR2200 accessing an ISDN network using an ISDN BRI interface



An NT1 device can connect a maximum of eight AR2200s to an ISDN network. The number of AR2200s varies according to the NT1 device type. When multiple AR2200s connect to one NT1 device, configure AR2200s to work in point-to-multipoint (P2MP) mode.

ISDN features supported by the AR2200 are usually used in the following scenarios:

- ISDN dial-up access
- ISDN leased line access

ISDN features can work with other features to provide different services, such as PPPoISDN, FRoISDN, and MPoISDN. PPP and MP services can also be transmitted over an ISDN leased line.

5.3 Configuring the AR2200 to Dial In to an ISDN Network by Using a PRI/BRI Interface

If the AR2200 dials in to an ISDN network using a PRI interface, the maximum bandwidth is 2.048 Mbit/s; if the AR2200 dials in to an ISDN network using a BRI interface, the maximum bandwidth is 128 kbit/s.

5.3.1 Establishing the Configuration Task

Before configuring the AR2200 to dial in to an ISDN network using a PRI/BRI interface, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task quickly and accurately.

Applicable Environment

When a branch company needs to transmit delay-insensitive and small-volume burst traffic with the headquarters or other branch companies, the branch company can dial in to an ISDN network.

Generally, an ISDN PRI/BRI interface provides only one 64 kbit/s data channel. When multiple B channels are bundled together using the MP binding technique, an ISDN PRI interface provides a maximum of thirty 64 kbit/s data channels on a CE1/PRI interface card or a maximum of twenty-three 64 kbit/s data channels on a CT1/PRI interface card; an ISDN BRI interface provides a maximum of two 64 kbit/s data channels.

The AR2200 can dial in to an ISDN network using a PRI/BRI interface in circular dialer control center (DCC) or resource-shared DCC mode.

For characteristics and usage scenarios of circular DCC and resource-shared DCC, see **7 DCC Configuration**.

Optional configurations of PRI and BRI interfaces vary. **Table 5-1** shows the comparison between procedures for configuring the AR2200 to dial in an ISDN network using PRI and BRI interfaces.

Table 5-1 Comparison between procedures for configuring the AR2200 to dial in an ISDN network using PRI and BRI interfaces

Dialing In to an ISDN Network Using a PRI Interface	Dialing In to an ISDN Network Using a BRI Interface
5.3.2 Configuring a Dialer Control List	**5.3.2 Configuring a Dialer Control List**
5.3.3 Configuring DCC	**5.3.3 Configuring DCC**
5.3.4 (Optional) Configuring PRI Interfaces to Actively Send RESTART Messages	**5.3.5 (Optional) Configuring the Working Mode for a BRI Interface**
5.3.7 (Optional) Setting Negotiation Parameters for the ISDN Layer 3 Protocol	**5.3.6 (Optional) Configuring Automatic Link Establishment on a BRI Interface**

Dialing In to an ISDN Network Using a PRI Interface	Dialing In to an ISDN Network Using a BRI Interface
5.3.8 (Optional) Configuring the Calling Number in an Outgoing Call	5.3.7 (Optional) Setting Negotiation Parameters for the ISDN Layer 3 Protocol
5.3.9 (Optional) Configuring an Allowed Calling Number	5.3.8 (Optional) Configuring the Calling Number in an Outgoing Call
5.3.10 (Optional) Configuring the Called Number and Sub-address to Be Checked in an Incoming Call	5.3.9 (Optional) Configuring an Allowed Calling Number
5.3.11 (Optional) Configuring Local B Channel Management	5.3.10 (Optional) Configuring the Called Number and Sub-address to Be Checked in an Incoming Call
5.3.12 (Optional) Setting the Sliding Window Size of a PRI Interface	5.3.11 (Optional) Configuring Local B Channel Management

NOTE

The following section describes the procedures for configuring the AR2200 to dial in to an ISDN network on a dialer interface in circular or resource-shared DCC mode after a PRI/BRI interface is added to the dialer interface.

When different link layer protocols are configured, different services can be transmitted on ISDN networks, such as PPPoISDN, FRoISDN, and MPoISDN services.

Pre-configuration Tasks

Before configuring the AR2200 to dial in to an ISDN network using a PRI interface, complete the following tasks:

- Installing an interface card that provides CE1/PRI interfaces
- Connecting a CE1/PRI interface to the network-side ISDN device

Before configuring the AR2200 to dial in to an ISDN network using a BRI interface, complete the following tasks:

- Installing an interface card that provides BRI interfaces
- Connecting a BRI interface to an NT1 device and connecting the NT1 device to the network-side ISDN device

Data Preparation

To configure the AR2200 to dial in to an ISDN network using a PRI interface, you need the following data.

No.	Data
1	Dialer control list number and (optional) ACL number referenced by the dialer control list

No.	Data
2	● DCC dial-up parameters in circular DCC mode: Dialer interface number, dialer access group number, IP addresses, dialer routing information, (optional) link layer protocol, and physical interface number to be added to a dialer interface ● DCC dial-up parameters in resource-shared DCC mode: Dialer interface number, dialer bundle number, IP addresses, dialer routing information, (optional) link layer protocol, physical interface number to be added to a dialer interface, and (optional) physical interface priority
3	(Optional) Call reference length
4	(Optional) Calling number in an outgoing call
5	(Optional) Allowed calling number
6	(Optional) Called number and sub-address to be checked in an incoming call
7	(Optional) Sliding window size of a PRI interface

To configure the AR2200 to dial in to an ISDN network using a BRI interface, you need the following data.

No.	Data
1	Dialer control list number and (optional) ACL number referenced by the dialer control list

No.	Data
2	● DCC dial-up parameters in circular DCC mode: Dialer interface number, dialer access group number, IP addresses, dialer routing information, (optional) link layer protocol, and physical interface number to be added to a dialer interface ● DCC dial-up parameters in resource-shared DCC mode: Dialer interface number, dialer bundle number, IP addresses, dialer routing information, (optional) link layer protocol, physical interface number to be added to a dialer interface, and (optional) physical interface priority
3	(Optional) Working mode of the BRI interface
4	(Optional) Call reference length
5	(Optional) Calling number in an outgoing call
6	(Optional) Allowed calling number
7	(Optional) Called number and sub-address to be checked in an incoming call

5.3.2 Configuring a Dialer Control List

A dialer control list filters all the packets that pass through a dialer interface.

Context

To enable the DCC to correctly transmit packets, configure a dialer control list and associate it with physical interfaces and dialer interfaces. Configure filtering rules for the dialer control list or associate an ACL with the dialer control list.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
dialer-rule
```

The dialer rule view is displayed.

Step 3 Run:

```
dialer-rule dialer-rule-number { acl { acl-number | name acl-name } | ip { deny |
permit } | ipv6 { deny | permit } }
```

A dialer control list is specified for a dialer access group to define conditions for initiating calls.

----End

5.3.3 Configuring DCC

The AR2200 can dial in to an ISDN network using a PRI/BRI interface in circular DCC or resource-shared DCC mode.

Context

To configure FRoISDN, you can only use circular DCC. To configure PPPoISDN or MPoISDN, you can use circular DCC and resource-shared DCC.

Procedure

- Configuring circular DCC
  1. Run:
     ```
     system-view
     ```
     The system view is displayed.
  2. Run:
     ```
     interface dialer interface-number
     ```
     A dialer interface is created and the dialer interface view is displayed.
  3. (Optional) Run:
     ```
     link-protocol fr
     ```
     FR is configured as the link layer protocol of the dialer interface.

     By default, the link layer protocol of a dialer interface is PPP.

     This step is required when FRoISDN needs to be configured. If the device functions as a DCE, configure a DLCI on the device. For details, see **2 FR Configuration**.
  4. (Optional) Run:
     ```
     ppp mp
     ```
     The dialer interface is configured to work in MP mode.

     This step is required when the link layer protocol of a dialer interface is PPP and MPoISDN needs to be configured.
  5. Run:
     ```
     dialer enable-circular
     ```
     Circular DCC is enabled.
  6. Run:
     ```
     dialer-group group-number
     ```
     The dialer interface is added to a dialer access group.

     The value of *group-number* must be the same as that of *dialer-rule-number* in step 3 of **5.3.2 Configuring a Dialer Control List**.
  7. Run:

```
ip address ip-address { mask | mask-length }
```

An IP address is configured for the dialer interface.

8. Run:

```
dialer route ip next-hop-address [ user hostname | broadcast ] * [ dial-string ] [ autodial | interface interface-type interface-number ] *
```

A dialer number is configured.

Alternatively, you can run the **dialer number** *dial-number* [**autodial**] command to configure a dialer number.

NOTE

To initiate calls to or receive calls from multiple called parties, run the **dialer route ip** command multiple times.

To configure FRoISDN, you can only use the **dialer number** command to configure a dialer number.

9. Run:

```
quit
```

Return to the system view.

10. Run:

```
interface serial interface-number
```

The specified PRI interface view is displayed.

Or, run:

```
interface bri interface-number
```

The specified BRI interface view is displayed.

Before entering the PRI interface view, configure a CE1/PRI interface or a CT1/PRI interface to work in PRI mode. For details, see Configuring a CE1/PRI Interface to Work in PRI Mode or Configuring a CT1/PRI Interface to Work in PRI Mode in the *Huawei AR2200 Series Enterprise Routers Configuration Guide - Interface Management*.

11. Run:

```
dialer circular-group number
```

The interface is added to the specified dialer circular group.

The value of *number* must be the same as the dialer interface number.

- Configuring resource-shared DCC

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
interface dialer interface-number
```

A dialer interface is created and the dialer interface view is displayed.

3. Run:

```
ip address ip-address { mask | mask-length }
```

An IP address is configured for the dialer interface.

4. (Optional) Run:

   ppp mp

   The dialer interface is configured to work in MP mode.

   This step is required when the link layer protocol of a dialer interface is PPP and MPoISDN needs to be configured.

5. Run:

   dialer user *user-name*

   Resource-shared DCC is enabled and the remote user name of the dialer interface is specified.

6. Run:

   dialer bundle *number*

   A dialer bundle is specified for the dialer interface in resource-shared DCC mode.

7. Run:

   dialer number *dial-number* [**autodial**]

   A dialer number is configured.

8. Run:

   quit

   Return to the system view.

9. Run:

   interface serial *interface-number*

   The specified PRI interface view is displayed.

   Or, run:

   interface bri *interface-number*

   The specified BRI interface view is displayed.

   Before entering the PRI interface view, configure a CE1/PRI interface or a CT1/PRI interface to work in PRI mode. For details, see Configuring a CE1/PRI Interface to Work in PRI Mode or Configuring a CT1/PRI Interface to Work in PRI Mode in the *Huawei AR2200 Series Enterprise Routers Configuration Guide - Interface Management*.

10. Run:

    dialer bundle-member *number* [**priority** *priority*]

    A dialer bundle is specified for a physical interface.

    By default, a physical interface does not belong to any dialer bundle. When a dialer bundle is specified for a physical interface, the default priority of the interface in the dialer bundle is 1.

11. (Optional) Configure PPP authentication. For details, see **3.4 Configuring PPP Authentication**.

    By default, the link layer protocol of a PRI/BRI interface is PPP. When the link layer protocol of an interface is PPP, configure PPP authentication as required.

----End

5.3.4 (Optional) Configuring PRI Interfaces to Actively Send RESTART Messages

Faults may occur during the release of a call, causing a call release failure. If a PRI interface is configured to actively send RESTART messages to a network-side device, the network-side device sets all calls to the NULL state and all B channels to the IDLE state after receiving a RESTART message from the PRI interface.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
isdn send-restart
```

PRI interfaces are configured to actively send RESTART messages.

By default, PRI interfaces actively send RESTART messages. In most cases, this step is not required.

----End

5.3.5 (Optional) Configuring the Working Mode for a BRI Interface

A BRI interface works in point-to-point (P2P) or point-to-multipoint (P2MP) mode.

Context

A BRI interface on an ISDN user-side device is connected to an ISDN switch using a Network Termination 1 (NT1) device. An NT1 device can provide multiple S/T interfaces so that an ISDN switch can connect to multiple ISDN user-side devices.

The AR2200 functions as an ISDN user-side device. To enable only one AR2200 to communicate with an ISDN switch, configure a BRI interface on the AR2200 to work in P2P mode. To enable multiple AR2200s to communicate with an ISDN switch, configure each BRI interface to work in P2MP mode.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface bri interface-number
```

The specified BRI interface view is displayed.

Step 3 Run:

```
isdn link-mode p2p
```

The BRI interface is configured to work in P2P mode.

By default, a BRI interface on the AR2200 works in P2MP mode. In P2MP mode, a network-side ISDN switch can connect to multiple AR2200s.

----End

5.3.6 (Optional) Configuring Automatic Link Establishment on a BRI Interface

After automatic link establishment is enabled, a call can be established rapidly.

Context

The Q.921 layer of a PRI interface has the automatic link establishment function. This function enables two correctly connected interfaces to enter the MULTIPLE_FRAME_ESTABLISHED state and establish a Q.921 link without being triggered by a call. The Q.921 layer of a BRI interface enters the MULTIPLE_FRAME_ESTABLISHED state only when there is a call triggered.

To enable a BRI interface to enter the MULTIPLE_FRAME_ESTABLISHED state immediately after being correctly connected, enable automatic link establishment on the interface.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface bri interface-number
```

The specified BRI interface view is displayed.

Step 3 Run:

```
isdn q921-permanent
```

Q.921 automatic link establishment is enabled on the BRI interface.

By default, a BRI interface enters the MULTIPLE_FRAME_ESTABLISHED state only when being triggered by a call.

----End

5.3.7 (Optional) Setting Negotiation Parameters for the ISDN Layer 3 Protocol

The ISDN Layer 3 protocol is Q.931. The AR2200 supports configuration of Layer 3 protocol negotiation parameters, including the call reference length, whether to ignore CONNECT ACK messages, values of ISDN Layer 3 timers, number types, encoding schemes, and whether to send called numbers in overlap mode.

Context

Layer 3 protocol negotiation parameters have default values. To modify negotiation parameter values, perform the following steps in any sequence.

The call reference is the sequence number assigned to a call for identification. It is 1 byte or 2 bytes in length. For example, the 1-byte call reference ranges from 0 to 127 to differentiate 128 calls.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface serial interface-number
```

The specified PRI interface view is displayed.

Or, run:

```
interface bri interface-number
```

The specified BRI interface view is displayed.

Step 3 Run:

```
isdn crlength call-reference-length
```

The call reference length is set for the interface.

By default, the call reference length is 2 bytes for a PRI interface and 1 byte for a BRI interface.

Devices on both ends must have the same call reference length.

Step 4 Run:

```
isdn ignore connect-ack [ incoming | outgoing ]
```

The AR2200 is configured to transition to the ACTIVE state without sending or receiving a CONNECT ACK message.

By default, the AR2200 transitions to the ACTIVE state only after sending or receiving a CONNECT ACK message.

In practice, some ISDN switches do not reply with CONNECT ACK messages. To enable the AR2200 to communicate with this type of ISDN switch, run this command to configure the AR2200 to transition to the ACTIVE state without sending or receiving any CONNECT ACK message.

Step 5 Run:

```
isdn l3-timer timer-name timer-value
```

Values of ISDN Layer 3 timers are set.

The following table lists default values of ISDN Layer 3 timers.

ISDN Layer 3 Timer	Default Value (Seconds)
T301	240
T302	15
T303	4

ISDN Layer 3 Timer	Default Value (Seconds)
T304	30
T305	30
T308	4
T309	90
T310	40
T313	4
T316	120
T322	4

Step 6 Run:

```
isdn number-property number-property [ calling | called ] [ out ]
```

The type and encoding scheme are set for a calling or called number in an outgoing call.

By default, the AR2200 selects the ISDN number type and encoding scheme depending on upper layer services.

Step 7 Run:

```
isdn overlap-sending [ digits ]
```

The ISDN interface is configured to send a called number in overlap mode.

By default, an ISDN interface sends a complete called number at a time.

When a remote ISDN switch cannot receive a complete called number or the maximum number of digits the ISDN switch allows is smaller than the number of digits of a called number, run this command to configure the AR2200 to send the called number in overlap mode. Otherwise, the AR2200 cannot establish a call with the ISDN switch.

When an ISDN interface is configured to send a called number in overlap mode, it sends the configured maximum number of digits at a time until all digits of the called number are sent.

If the *digits* parameter is not specified, by default, an ISDN interface sends a maximum of 10 digits of the called number at a time.

Step 8 Run:

```
isdn overlap-receiving
```

The ISDN interface is configured to receive a called number in overlap mode.

By default, an ISDN interface does not receive a called number in overlap mode. It starts establishing a connection immediately after receiving some digits of a called number.

----End

5.3.8 (Optional) Configuring the Calling Number in an Outgoing Call

On networks where charging is performed based on calling numbers, a user can send a specific calling number that enjoys a preferential tariff to reduce the expense.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface serial interface-number
```

The specified PRI interface view is displayed.

Or, run:

```
interface bri interface-number
```

The specified BRI interface view is displayed.

Step 3 Run:

```
isdn calling calling-number
```

The calling number to be contained in a message sent from the calling party to the called party is configured.

By default, a message sent from the calling party to the called party does not contain any calling number.

----End

5.3.9 (Optional) Configuring an Allowed Calling Number

Configuring allowed calling numbers improves security.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface serial interface-number
```

The specified PRI interface view is displayed.

Or, run:

```
interface bri interface-number
```

The specified BRI interface view is displayed.

Step 3 Run:

```
isdn caller-number caller-number
```

An allowed calling number is configured.

By default, all calling numbers are allowed.

----End

5.3.10 (Optional) Configuring the Called Number and Sub-address to Be Checked in an Incoming Call

To ensure security, configure the AR2200 to check called numbers and sub-addresses. The AR2200 will reject a call if the call contains an incorrect called number or sub-address.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface serial interface-number
```

The specified PRI interface view is displayed.

Or, run:

```
interface bri interface-number
```

The specified BRI interface view is displayed.

Step 3 Run:

```
isdn check-called-number called-party-number [ : subaddress ]
```

The called number or sub-address to be checked in an incoming call is configured.

By default, the called number or sub-address in an incoming call is not checked.

----End

5.3.11 (Optional) Configuring Local B Channel Management

During the initiation of a call, the B channel for the call must be properly managed; especially in PRI mode, properly managing B channels can improve call efficiency and reduce call loss.

Context

Generally, B channels are managed by ISDN switches.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface serial interface-number
```

The specified PRI interface view is displayed.

Or, run:

```
interface bri interface-number
```

The specified BRI interface view is displayed.

Step 3 Run:

```
isdn bch-local-manage [ exclusive ]
```

The AR2200 is configured to manage B channels.

By default, B channels are managed by ISDN switches.

When the **exclusive** parameter is specified, exclusive local B channel management is configured. If the B channel specified by an ISDN switch is different from that selected by the AR2200, a call failure occurs.

Step 4 Run:

```
isdn bch-select-way [ ascending | descending ]
```

The order in which B channels will be selected is configured.

By default, B channels are selected in ascending order of channel numbers.

----End

5.3.12 (Optional) Setting the Sliding Window Size of a PRI Interface

The sliding window mechanism is used for flow control. In earlier network communication mechanisms, two communicating devices sent data without checking for network congestion. If too many packets were sent at a time, intermediate nodes were congested and packets were lost, causing a communication failure between the two devices. The sliding window mechanism addresses this problem.

Context

The sliding window size specifies the maximum number of unacknowledged frames allowed on an interface. The ISDN module can retransmit the unacknowledged information frames within the range of the sliding window.

A small sliding window size will increase the packet loss ratio. Generally, the default sliding window size is recommended.

NOTE

The sliding window size of a BRI interface is fixed as 1.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface serial interface-number
```

The specified PRI interface view is displayed.

Step 3 Run:

isdn pri-slipwnd-size { *window-size* | **default** }

The sliding window size is set for an ISDN PRI interface.

By default, the sliding window size of an ISDN PRI interface is 7.

----End

5.3.13 Checking the Configuration

After ISDN protocol parameters are set, run the following commands to verify the configuration.

Context

Before verifying the configuration, ensure that configurations of the network-side ISDN device connecting to the AR2200 are complete. For detailed configuration procedures, see the document of the network-side ISDN device.

Procedure

Step 1 Run the **display isdn dss1-parameters** [**interface** *interface-type interface-number*] command to check ISDN Layer 2 and Layer 3 protocol parameters.

Step 2 Run the **display isdn active-channel** [**interface** *interface-type interface-number*] command to check active call information on the specified ISDN interface.

Step 3 Run the **display isdn call-info** [**interface** *interface-type interface-number*] command to check the call status of the specified ISDN interface.

----End

Example

The following describes how to verify the configuration of a PRI interface.

Run the **display isdn dss1-parameters** command to check ISDN Layer 2 and Layer 3 protocol parameters. According to the command output, check whether the sliding window size of the PRI interface and values of ISDN Layer 3 timers are set correctly.

```
<Huawei> display isdn dss1-parameters interface serial 1/0/0:15
ISDN Q921 system
parameters:

  T200(sec)  T202(sec)  T203(sec)  N200    K1
(PRI)
  1          2          10         3
7


ISDN Q931 system
timers:

  Timer-Number         Value
(sec)

      T301
240

      T302
15
```

```
      T303
4

      T304
30

      T305
30

      T308
4

      T309
90

      T310
40

      T313
4

      T314
4

      T316
120

      T317
10

      T318
4

      T319
4

      T321
30

      T322             4
```

Run the **display isdn active-channel** command. Active call information is displayed on the specified ISDN interface.

```
<Huawei> display isdn active-channel interface serial 1/0/0:15
Serial1/0/0:15

-------------------------------------------------------------------------------

Channel  Call     Call     Calling        Calling     Called
Called
Info     Property Type     Number         Subaddress  Number
Subaddress
-------------------------------------------------------------------------------

B3       Digital  Out      7654321        -           1234567        -
```

Run the **display isdn call-info** command. The call status of the specified ISDN interface is displayed.

```
<Huawei> display isdn call-info interface serial 1/0/0:15
Serial1/0/0:15 :

  Link Layer: TEI = 0, State =
MULTIPLE_FRAME_ESTABLISHED

  Network Layer: 1 connection
(s)
```

```
    Connection
1 :

      CCIndex:0x0002 , State: Active , CES:1 , Channel:
0x00000008
      Calling_Num[:Sub]:
7654321

      Called_Num[:Sub]: 1234567
```

5.4 Configuring an ISDN Leased Line

An ISDN leased line elimintates the delay caused by dial-up during data transmission.

5.4.1 Establishing the Configuration Task

Before configuring an ISDN leased line, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task quickly and accurately.

Applicable Environment

When a branch company needs to exchange a large amount of data with the headquarters or other branch companies for a long period of time, an ISDN leased line established between them ensures timely, high-speed, and reliable data transmission. An ISDN leased line can transmit data at any time without triggering dial-up, eliminating the delay caused by dial-up.

An ISDN leased line can be established on ISDN PRI or BRI interfaces. An ISDN PRI interface supports only a 64 kbit/s ISDN leased line; an ISDN BRI interface supports a 64 kbit/s or 128 kbit/s ISDN leased line. The MP binding technique allows an n x 64 kbit/s high-bandwidth ISDN leased line to be established on PRI interfaces.

NOTE

The ISDN leased line and ISDN dial-up access cannot be configured on the same ISDN interface.

The ISDN leased line function must work with the circular DCC function. For details about circular DCC, see **7.3 Configuring C-DCC**.

The ISDN leased line provided by the AR2200 supports PPP and MP services.

Pre-configuration Tasks

Before configuring an ISDN PRI leased line, complete the following tasks:

- Installing an interface card that provides CE1/PRI interfaces
- Connecting a CE1/PRI interface to the network-side ISDN device correctly
- Deploying a leased line on the network-side ISDN device

Before configuring an ISDN BRI leased line, complete the following tasks:

- Installing an interface card that provides BRI interfaces
- Connecting a BRI interface to an NT1 device and connecting the NT1 device to the network-side ISDN device correctly
- Deploying a leased line on the network-side ISDN device

Data Preparation

To configure an ISDN leased line, you need the following data.

No.	Data
1	Dialer control list number and (optional) ACL number referenced by the dialer control list
2	ISDN interface number, interface IP address, dialer access group number, and (optional) B channel number for the ISDN leased line

5.4.2 Configuring a Dialer Control List

A dialer control list filters all the packets that pass through a leased line.

Context

To enable the DCC to correctly transmit packets, configure a dialer control list and associate it with physical interfaces and dialer interfaces. Configure filtering rules for the dialer control list or associate an ACL with the dialer control list.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
dialer-rule
```

The dialer rule view is displayed.

Step 3 Run:

```
dialer-rule dialer-rule-number { acl { acl-number | name acl-name } | ip { deny |
permit } | ipv6 { deny | permit } }
```

A dialer control list is specified for a dialer access group to define conditions for initiating calls.

----End

5.4.3 Configuring an ISDN Leased Line

ISDN supports two types of physical interfaces (PRI and BRI interfaces), and ISDN leased lines are classified into ISDN PRI and BRI leased lines.

Context

The ISDN leased line function must work with the circular DCC function.

The bandwidth of an ISDN PRI leased line is 64 kbit/s, and the bandwidth of an ISDN BRI leased line is 64 kbit/s or 128 kbit/s.

Multiple ISDN leased lines can be bundled into an MP link to increase the bandwidth. After MP binding is performed, ISDN leased lines support the Link Fragmentation and Interleaving (LFI) function.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface serial interface-number
```

The specified PRI interface view is displayed.

Before entering the PRI interface view, configure a CE1/PRI interface or a CT1/PRI interface to work in PRI mode. For details, see Configuring a CE1/PRI Interface to Work in PRI Mode or Configuring a CT1/PRI Interface to Work in PRI Mode in the *Huawei AR2200 Series Enterprise Routers Configuration Guide - Interface Management*.

Or, run:

```
interface bri interface-number
```

The specified BRI interface view is displayed.

Step 3 Run:

```
ip address ip-address { mask | mask-length }
```

An IP address is configured for the ISDN interface.

Step 4 Run:

```
dialer enable-circular
```

Circular DCC is enabled on the ISDN interface.

Step 5 Run:

```
dialer-group group-number
```

The ISDN interface is added to a dialer access group.

The value of *group-number* must be the same as that of *dialer-rule-number* in step 3 of **5.4.2 Configuring a Dialer Control List**.

Step 6 Run:

```
dialer isdn-leased number
```

A 64 kbit/s ISDN leased line is configured.

Or, run:

```
dialer isdn-leased 128k
```

A 128 kbit/s ISDN BRI leased line is configured.

NOTE

- On an ISDN PRI interface, only a 64 kbit/s ISDN leased line can be established; on an ISDN BRI interface, a 64 kbit/s or 128 kbit/s ISDN leased line can be established.
- If a 64 kbit/s leased line has been configured on an ISDN BRI interface, delete this 64 kbit/s leased line before configuring a 128 kbit/s leased line on this interface.

----End

5.4.4 Checking the Configuration

After an ISDN leased line is configured, you can check whether the ISDN leased line works properly.

Context

All configurations of the peer device that connects to the ISDN leased line are complete.

Procedure

Step 1 Run the **display interface** *interface-type interface-number* command to check the status of and packet statistics about the specified ISDN interface.

According to the interface status and packet statistics, you can check whether the ISDN leased line works properly. In addition, you can ping the peer device to check whether the ISDN leased line works properly.

----End

Example

The following uses an ISDN PRI leased line as an example.

Run the **display interface** command. The status of and packet statistics about the specified PRI interface are displayed.

```
<Huawei> display interface serial 1/0/0:15
Serial1/0/0:15 current state :
UP

Line protocol current state : UP
(spoofing)

Description:HUAWEI, AR Series, Serial1/0/0:15
Interface
Route Port,The Maximum Transmit Unit is
1500
Derived from E1 1/0/0,  Timeslot(s) Used: 1-31,  baudrate is 1984000
bps
Internet Address is 3.3.3.1/24
Encapsulation is
ISDN
Last physical up time   :
-

Last physical down time : 2010-10-10 20:25:42
UTC-05:13
Current system time: 2010-10-12
20:39:36-05:13

Last 300 seconds input rate 0 bytes/sec 0 bits/sec 0 packets/sec
Last 300 seconds output rate 0 bytes/sec 0 bits/sec 0 packets/sec
Input: 20 packets, 60
```

```
bytes

  length errors:           0,  giants:
0
  CRC:                     1,  align errors:
1
  aborts:                  0,  no buffers:
0
Output: 11 packets, 33
bytes

  Total Error:             0,  Too Long Error:          0

    Input bandwidth utilization  :
0.00%
    Output bandwidth utilization : 0.00%
```

5.5 Maintaining ISDN

If users dial in to an ISDN network using an ISDN interface, check Layer 3 messages, call parameters, call status, and historical call statistics on the ISDN interface to ensure that there are no ISDN call faults.

Context

After an ISDN leased line is established, it transmits data at any time without triggering dial-up. You can monitor the leased line status according to packet statistics about interfaces on both ends of the leased line.

5.5.1 Maintaining Message Statistics on an ISDN Interface

Layer 3 protocols of ISDN interfaces interact by exchanging messages. Monitor message statistics to check that a call is correctly established.

Procedure

Step 1 Run:

system-view

The system view is displayed.

Step 2 Run:

interface serial *interface-number*

The specified PRI interface view is displayed.

Or, run:

interface bri *interface-number*

The specified BRI interface view is displayed.

Step 3 Run:

isdn statistics

Message statistics are collected on the ISDN interface.

Use this command as follows:

- Before collecting message statistics on the interface, run the **isdn statistics start** command in the ISDN interface view.
- To stop collecting message statistics, run the **isdn statistics stop** command.
- To view message statistics, run the **isdn statistics display** command.
- To view message statistics in flow format, run the **isdn statistics display flow** command.
- To continue collecting message statistics after stopping collecting message statistics, run the **isdn statistics continue** command.
- To clear message statistics, run the **isdn statistics clear** command.

----End

5.5.2 Viewing ISDN Call Information

ISDN call information includes ISDN parameters, active call information, call status, and historical call statistics.

Procedure

Step 1 Run the **display isdn dss1-parameters** [**interface** *interface-type interface-number*] command to check ISDN Layer 2 and Layer 3 protocol parameters.

Step 2 Run the **display isdn active-channel** [**interface** *interface-type interface-number*] command to check active call information on the specified ISDN interface.

Step 3 Run the **display isdn call-info** [**interface** *interface-type interface-number*] command to check the call status of the specified ISDN interface.

Step 4 Run the **display isdn call-record** [**interface** *interface-type interface-number*] command to check historical call statistics on the specified ISDN interface.

----End

5.6 Configuration Examples

This section describes the networking requirements, configuration roadmap, and data preparation for typical ISDN applications and provides configuration examples.

5.6.1 Example for Implementing MP Interworking by Using PRI Interfaces

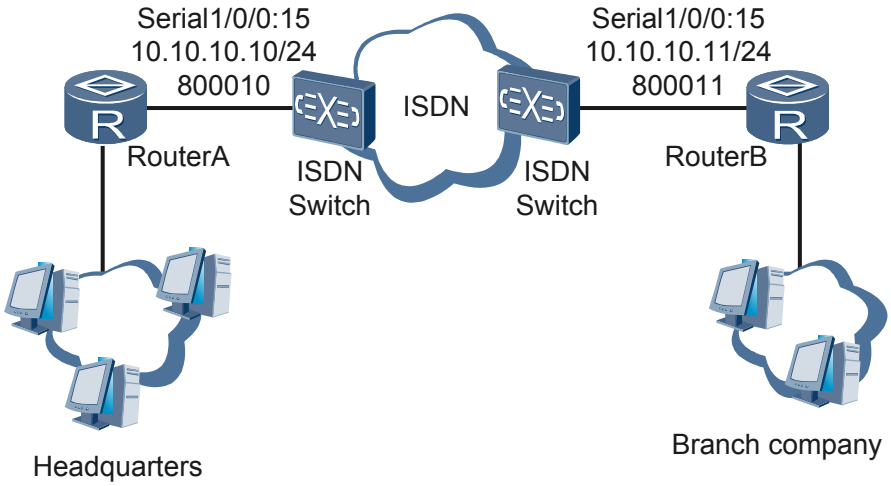
The MP function bundles ISDN B channels to increase bandwidth.

Networking Requirements

When an enterprise egress router has PRI interfaces, it can provide a maximum of twenty-three or thirty 64 kbit/s data channels. When the link layer protocol is PPP, only one link of a PRI interface can be used for each dial-up. Due to the demand of bandwidth by new services, 64 kbit/s bandwidth cannot meet customers' requirements. To address this problem, configure MP to bundle multiple data channels to increase bandwidth. For example, bundle 16 data channels together to provide 16 x 64 kbit/s bandwidth, namely, 1 Mbit/s bandwidth.

As shown in **Figure 5-5**, the enterprise headquarters use RouterA to communicate with its branch company across an ISDN network. RouterA dials in to the ISDN network using PRI interface Serial 1/0/0:15. During dial-up, a maximum of 16 data channels can be used to provide a maximum of 1 Mbit/s bandwidth. The branch company uses RouterB to communicate with the headquarters across the ISDN network. RouterB dials in to the ISDN network using PRI interface Serial 1/0/0:15. During dial-up, a maximum of 16 data channels can be used to provide a maximum of 1 Mbit/s bandwidth.

Figure 5-5 Communication across an ISDN network using PRI interfaces



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure a dialer control list to filter packets passing through a dialer interface.
2. Set circular DCC parameters, including a dialer access group, dialer interface address, and dialer routing information.

NOTE

This example describes how to configure circular DCC dial-up for interworking. Resource-shared DCC can also be configured to implement interworking.

Data Preparation

To complete the configuration, you need the following data:

- Rules of the dialer control list
- DCC dial-up parameters: link layer protocol, dialer interface address, dialer routing information, and physical interface number to be added to a dialer interface

Procedure

Step 1 Configure a dialer control list.

The following are configurations of RouterA. Configurations of RouterB are similar to those of RouterA.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] dialer-rule
[RouterA-dialer-rule] dialer-rule 1 ip permit
[RouterA-dialer-rule] quit
```

Step 2 Set circular DCC parameters.

The following are configurations of RouterA. Configurations of RouterB are similar to those of RouterA.

Create and configure a dialer interface.

```
[RouterA] interface dialer 0
[RouterA-Dialer0] link-protocol ppp
[RouterA-Dialer0] ppp mp max-bind 16
[RouterA-Dialer0] ppp mp
[RouterA-Dialer0] dialer enable-circular
[RouterA-Dialer0] dialer-group 1
[RouterA-Dialer0] ip address 10.10.10.10 24
[RouterA-Dialer0] dialer route ip 10.10.10.11 800011
[RouterA-Dialer0] quit
```

Configure a physical interface and add it to the dialer interface.

```
[RouterA] controller e1 1/0/0
[RouterA-E1 1/0/0] pri-set
[RouterA-E1 1/0/0] quit
[RouterA] interface serial 1/0/0:15
[RouterA-Serial1/0/0:15] dialer circular-group 0
```

Step 3 Verify the configuration.

After RouterA, RouterB, and the ISDN switches connected to the two routers are configured on the ISDN network, ping RouterB from RouterA to check whether dial-up links work properly, and run the **display isdn call-info** [**interface** *interface-type interface-number*] command to check the call status of the specified interface, or run the **isdn statistics** command to collect and check message statistics on the ISDN interface.

----End

Configuration Files

Configuration file of RouterA

```
#
sysname RouterA
#
controller E1 1/0/0
 pri-set
#
interface Dialer0
 link-protocol ppp
 ppp mp
 ip address 10.10.10.10 255.255.255.0
 dialer enable-circular
 dialer-group 1
 dialer route ip 10.10.10.11 800011
#
interface Serial1/0/0:15
 link-protocol ppp
 dialer enable-circular
 dialer-group 1
 dialer circular-group 0
#
 dialer-rule
```

```
 dialer-rule 1 ip permit
#
return
```

Configuration file of RouterB

```
#
sysname RouterB
#
controller E1 1/0/0
 pri-set
#
interface Dialer0
 link-protocol ppp
 ppp mp
 ip address 10.10.10.11 255.255.255.0
 dialer enable-circular
 dialer-group 1
 dialer route ip 10.10.10.10 800010
#
interface Serial1/0/0:15
 link-protocol ppp
 dialer enable-circular
 dialer-group 1
 dialer circular-group 0
#
 dialer-rule
 dialer-rule 1 ip permit
#
return
```

5.6.2 Example for Implementing FR Interworking Using BRI Interfaces

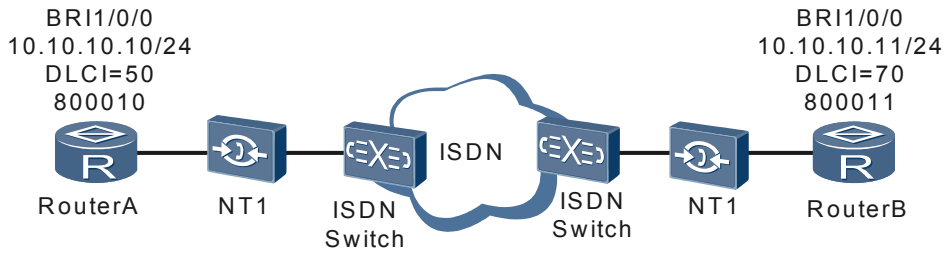
BRI interfaces implement FR interworking so that FR services can be transmitted over an ISDN network.

Networking Requirements

As shown in **Figure 5-6**, RouterA and RouterB function as DTEs to transmit IP packets and transmit FR services over an ISDN network.

In this example, RouterA and RouterB are AR2200s. ISDN switches (such as PBXs) that provide FR switching function as DCEs.

Figure 5-6 Implementing FR interworking using BRI interfaces



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure a dialer control list to filter packets passing through a dialer interface.
2. Set circular DCC parameters, including a dialer access group, and dialer interface address.

Data Preparation

1. Rules of the dialer control list
2. DCC dial-up parameters: link layer protocol, dialer interface address, dialer routing information, and number of the physical interface to be added to a dialer interface

Procedure

Step 1 Configure a dialer control list.

The following lists the configurations of RouterA. The configurations of RouterB are similar to those of RouterA, and are not mentioned here.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] dialer-rule
[RouterA-dialer-rule] dialer-rule 1 ip permit
[RouterA-dialer-rule] quit
```

Step 2 Set circular DCC parameters.

The following lists the configurations of RouterA. The configurations of RouterB are similar to those of RouterA, and are not mentioned here.

Create and configure a dialer interface.

```
[RouterA] interface dialer 0
[RouterA-Dialer0] link-protocol fr
Warning: The encapsulation protocol of the link will be changed. Continue? [Y/N]
:y
[RouterA-Dialer0] fr dlci 50
[RouterA-fr-dlci-Dialer0-50] quit
[RouterA-Dialer0] dialer enable-circular
[RouterA-Dialer0] dialer-group 1
[RouterA-Dialer0] ip address 10.10.10.10 24
[RouterA-Dialer0] dialer number 800011
[RouterA-Dialer0] fr map ip 10.10.10.11 50
[RouterA-Dialer0] quit
```

Configure a physical interface and add it to the dialer interface.

```
[RouterA] interface bri 1/0/0
[RouterA-Bri1/0/0] link-protocol fr
Warning: The encapsulation protocol of the link will be changed. Continue? [Y/N]
:y
[RouterA-Bri1/0/0] dialer circular-group 0
```

Step 3 # Verify the configuration.

After the configurations of RouterA, RouterB, and ISDN switches connected to the two routers on the ISDN network are complete, ping RouterB from RouterA to check whether the dial-up links work properly. Run the **display isdn call-info** [**interface** *interface-type interface-number*] command to check the call status of the specified interface, or run the **isdn statistics** command to collect and check message statistics on the ISDN interface.

----End

Configuration Files

Configuration file of RouterA

```
#
sysname RouterA
#
interface Bri1/0/0
 link-protocol fr
 dialer enable-circular
 dialer-group 1
 dialer circular-group 0
#
interface Dialer0
 link-protocol fr
 fr dlci 50
 fr map ip 10.10.10.11 50
 ip address 10.10.10.10 255.255.255.0
 dialer enable-circular
 dialer-group 1
 dialer number 800011
#
 dialer-rule
 dialer-rule 1 ip permit
#
return
```

Configuration file of RouterB

```
#
sysname RouterB
#
interface Bri1/0/0
 link-protocol fr
 dialer enable-circular
 dialer-group 1
 dialer circular-group 0
#
interface Dialer0
 link-protocol fr
 fr dlci 70
 fr map ip 10.10.10.10 70
 ip address 10.10.10.11 255.255.255.0
 dialer enable-circular
 dialer-group 1
 dialer number 800010
#
 dialer-rule
 dialer-rule 1 ip permit
#
return
```

5.6.3 Example for Configuring a 128 kbit/s ISDN Leased Line

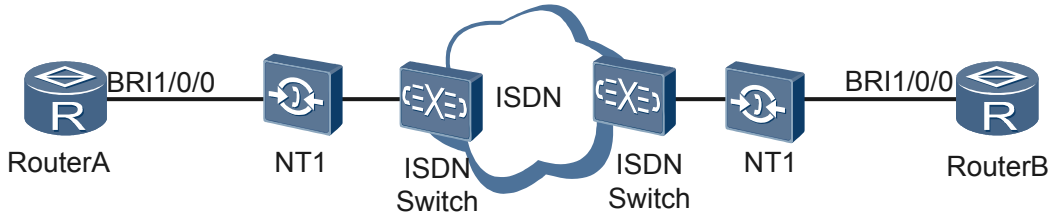
This section describes how to use a BRI interface to configure a 128 kbit/s ISDN leased line.

Networking Requirements

As shown in **Figure 5-7**, branch A and branch B communicate using an ISDN line and exchange data frequently. If dial-up access is used, a connection needs to be frequently established between branches A and B, wasting time and resources. To address this problem, configure an ISDN leased line between branches A and B (RouterA and RouterB in **Figure 5-7**).

A BRI interface has many applications. This example describes how to establish a 128 kbit/s ISDN leased line on a BRI interface.

Figure 5-7 Configuring a 128 kbit/s ISDN leased line



Configuration Roadmap

You can establish a 128 kbit/s leased line on a BRI interface using either of the following methods:

- Bundle two 64 kbit/s B channels of a BRI interface to form a 128 kbit/s leased line. Then configure the Link Fragmentation and Interleaving (LFI) function to ensure that voice packets are transmitted in a timely manner. For details about LFI configuration, see **3.7.6 Example for Configuring LFI**.
- Configure a 128 kbit/s leased line on a BRI interface.

Data Preparation

To complete the configuration, you need the following data:

- Dialer control list ID, dialer access group ID, and virtual template interface number in MP binding for the first method
- Dialer control list ID and dialer access group ID for the second method

Procedure

- Method 1: Bundle two 64 kbit/s B channels of a BRI interface to form a 128 kbit/s leased line.

  In this example, only the configuration of RouterA is described. The configuration of RouterB is similar to RouterA. Network-side switches on both ends need to provide an ISDN leased line and assign IP addresses to the two routers.

  1. Configure a dialer control list.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] dialer-rule
[RouterA-dialer-rule] dialer-rule 1 ip permit
[RouterA-dialer-rule] quit
```

  2. Bundle B channels of a BRI interface to form a 128 kbit/s leased line.

```
[RouterA] interface bri 1/0/0
[RouterA-Bri1/0/0] link-protocol ppp
[RouterA-Bri1/0/0] ppp mp virtual-template 3
[RouterA-Bri1/0/0] dialer enable-circular
[RouterA-Bri1/0/0] dialer-group 1
[RouterA-Bri1/0/0] dialer isdn-leased 1
[RouterA-Bri1/0/0] dialer isdn-leased 2
[RouterA-Bri1/0/0] quit
[RouterA] interface Virtual-Template 3
[RouterA-Virtual-Template3] ip address ppp-negotiate
[RouterA-Virtual-Template3] quit
```

3. Verify the configuration.

   After all configurations are complete, a 128 kbit/s ISDN leased line is established between RouterA and RouterB.

   Run the **display virtual-access** command to check the virtual access interface status. If the following information is displayed, a 128 kbit/s ISDN leased line has been established.

```
Link layer protocol is
PPP
LCP opened, MP opened, IPCP
opened
Physical is
MP
```

   Alternatively, run the **display ppp mp** command to view the MP binding configuration.

```
[RouterA] display ppp mp
Template is Virtual-Template3
 Bundle 727c4e403cbe, 2 members, slot 0, Master link is Virtual-
Template1:0
  0 lost fragments, 0 reordered, 0 unassigned, 0 interleaved,
 sequence 0/0 rcvd/sent
 The bundled sub channels are:
      Bri1/0/0:1
      Bri1/0/0:2
```

- Method 2: Configure a 128 kbit/s leased line on a BRI interface.

  1. Configure a dialer control list.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] dialer-rule
[RouterA-dialer-rule] dialer-rule 1 ip permit
[RouterA-dialer-rule] quit
```

  2. Configure a 128 kbit/s leased line on a BRI interface.

```
[RouterA] interface bri 1/0/0
[RouterA-Bri1/0/0] link-protocol ppp
[RouterA-Bri1/0/0] ip address ppp-negotiate
[RouterA-Bri1/0/0] dialer enable-circular
[RouterA-Bri1/0/0] dialer-group 1
[RouterA-Bri1/0/0] dialer isdn-leased 128k
[RouterA-Bri1/0/0] quit
```

  3. Verify the configuration.

     After all configurations are complete, run the **display interface bri** command to view the protocol status of the two B channels. If the protocol status is Up, an ISDN leased line has been established. To view the protocol status of the first B channel, run the **display interface bri 1/0/0:1** command.

----End

Configuration Files

Configuration file for method 1

```
sysname RouterA
#
interface Virtual-Template3
 ip address ppp-negotiate
#
interface bri 1/0/0
 link-protocol ppp
 ppp mp virtual-template 3
 dialer enable-circular
```

```
 dialer-group 1
 dialer isdn-leased 1
 dialer isdn-leased 2
#
dialer-rule
 dialer-rule 1 ip permit
#
return
```

Configuration file for method 2

```
sysname RouterA
#
interface bri 1/0/0
 link-protocol ppp
 ip address ppp-negotiate
 dialer enable-circular
 dialer-group 1
 dialer isdn-leased 128k
#
dialer-rule
 dialer-rule 1 ip permit
#
return
```

6 HDLC Configuration

About This Chapter

The High-level Data Link Control (HDLC) is a bit-oriented link layer protocol. HDLC features transparent transmission of any type of bit flow.

6.1 HDLC Overview

The High-level Data Link Control (HDLC) is a typical bit-oriented synchronization data control protocol. It uses the full-duplex mode and CRC check. Its transmission control function is independent of the processing function. It features control capabilities and can be flexibly used.

HDLC allows any type of bit flow to be transparently transmitted. Data does not need to be a character set.

- HDLC supports only P2P links. It does not support P2MP links.
- HDLC does not support IP address negotiation or authentication. In HDLC, Keepalive packets are used to detect the link status.
- HDLC can be configured only on synchronous interfaces. To configure HDLC on a synchronous/asynchronous serial interface, ensure that the interface works in synchronous mode.

6.2 HDLC Features Supported by the AR2200

On the AR2200, interfaces that support HDLC include synchronous serial interfaces, CE1/PRI interfaces, CT1/PRI interfaces, E1-F interfaces, T1-F interfaces, and CPOS sub-channel interfaces.

In HDLC, Keepalive packets are used to detect the link status. On the AR2200, set the interval for sending Keepalive packets by setting the polling interval.

6.3 Configuring HDLC

This section describes how to configure basic HDLC functions, including configuring the data link protocol of an interface as HDLC, an IP address for an interface, and the polling interval.

6.3.1 Establishing the Configuration Task

Before configuring basic HDLC functions, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task quickly and accurately.

Applicable Environment

When you need to enable the bits synchronous transmission using the link layer protocol, you can adopt the HDLC protocol.

Pre-configuration Tasks

Before configuring the basic HDLC functions, configure the physical attributes of the interface to make the physical status of the interface become Up.

Data Preparation

To configure HDLC, you need the following data.

No.	Data
1	Number of the interface to be configured with HDLC
2	Interface address
3	(Optional) Polling interval

6.3.2 Encapsulating an Interface with HDLC

Before configuring HDLC functions on an interface, configure the link layer protocol of the interface as HDLC.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
link-protocol hdlc
```

The interface is configured with HDLC.

----End

6.3.3 Configuring the IP Address of the Interface

You can assign an IP address to an interface or configure IP address unnumbered on the interface.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Choose one of the following steps to configure the IP address or IP unnumbered address of the interface.

- Run the **ip address** *ip-address* { *mask* | *mask-length* } [**sub**] command to configure the IP address of the interface.

- Run the **ip address unnumbered interface** *interface-type interface-number* command to configure the IP unnumbered address.

NOTE

If you configure IP address unnumbered on an interface encapsulated with HDLC, the interface borrowing an IP address from another interface must have the ability to learn about the route to the remote end. Otherwise, the packets sent from the interface cannot reach the remote end.

When you use IP address unnumbered, configure a static route or dynamic routing protocol so that the interface borrowing the interface can learn about the route to the remote end.

When an interface borrows an IP address from another interface, follow the following rules:

- If you use a dynamic routing protocol, ensure the length of the learned route mask is longer than that of the lender's IP address mask, because the AR2200 uses the longest match rule when searching for routes.
- If you use a static route and the IP address of the lender uses a 32-bit mask, the length of the static route mask must be shorter than 32 bits.
- If you use a static route and the IP address of the lender uses a mask less than 32 bits, the length of the static route mask must be longer than that of the lender's IP address mask.

----End

6.3.4 (Optional)Setting the Polling Interval

In HDLC, Keepalive packets are used to detect the link status. On the AR2200, you can set the interval for sending Keepalive packets by setting the polling interval.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
timer hold seconds
```

The polling interval is configured.

By default, the polling interval is 10 seconds. If it is set to 0, then link detection is prohibited.

You can use the default polling interval or adjust the polling interval as required. In the case of long network delay or high congestion, prolong the polling interval to reduce the possibility of network flapping.

----End

6.3.5 Checking the Configuration

After basic HDLC functions are configured, you can view the status, link layer protocol and configuration of the interface.

Procedure

- Run the **display interface** [*interface-type* [*interface-number*]] command to check the status, link layer protocol and configuration of the interface.

----End

6.4 Maintaining HDLC

This section describes how to maintain HDLC. Detailed operations include clearing the statistics about the HDLC interfaces.

6.4.1 Clearing the Statistics About HDLC Interfaces

You can run the reset commands to clear interface statistics before recollecting traffic statistics on the interface.

Context

CAUTION

The previous statistics cannot be restored after you clear them. So, confirm the action before you use the reset command.

To reset the interface statistics about the Network Management System (NMS) or the interface statistics displayed by running the **display interface** command, run the following commands in the user view.

NOTE

For the display of interface statistics in the NMS, see the related NMS manuals.

Procedure

- Run the **reset counters interface** [*interface-type* [*interface-number*]] command to clear the interface statistics displayed by running the **display interface** command.
- Run the **reset counters if-mib interface** [*interface-type* [*interface-number*]] command to clear the interface statistics in the NMS.

----End

6.5 Configuration Examples

This section provides examples for configuring HDLC, including the application scenario, configuration roadmap, and configuration procedure.

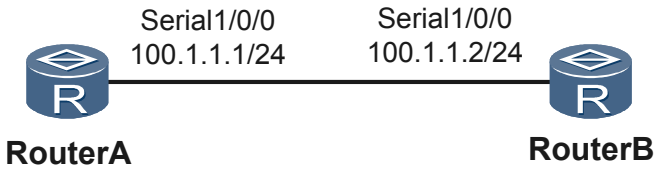
6.5.1 Example for Configuring HDLC

This example shows how to configure HDLC to interconnect devices in typical networking.

Networking Requirements

Router A and Router B are connected through serial interfaces, and the interfaces are required to run HDLC.

Figure 6-1 Networking diagram of the HDLC functions



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the link protocol of each interface as HDLC.
2. Configure the IP address of each interface.

Data Preparation

To configure HDLC, you need the following data:

- IP address of the interface on Router A
- IP address of the interface on Router B

NOTE

The IP addresses of interfaces on Router A and Router B must be on the same network segment; otherwise, the link layer status of the two interfaces cannot be Up.

Procedure

Step 1 Configure Router A.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface serial 1/0/0
[RouterA-Serial1/0/0] link-protocol hdlc
[RouterA-Serial1/0/0] ip address 100.1.1.1 24
[RouterA-Serial1/0/0] quit
```

Step 2 Configure Router B.

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] interface serial 1/0/0
[RouterB-Serial1/0/0] link-protocol hdlc
[RouterB-Serial1/0/0] ip address 100.1.1.2 24
[RouterB-Serial1/0/0] quit
```

Step 3 Verify the configuration.

Run the **display interface serial 1/0/0** command on RouterA to check the interface configuration. The command output shows that both the physical layer status and link layer status of the interface are Up and that RouterA and RouterB can ping each other successfully.

```
[RouterA] display interface serial 1/0/0
Serial1/0/0 current state : UP
Line protocol current state : UP
Last line protocol up time : 2011-11-15 15:01:46
Description:HUAWEI, AR Series, Serial1/0/0 Interface
Route Port,The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet Address is 100.1.1.1/24
Link layer protocol is nonstandard HDLC
Last physical up time   : 2011-11-15 15:01:46
Last physical down time : 2011-11-15 15:01:46
Current system time: 2011-11-15 15:02:56
Physical layer is synchronous, Baudrate is 64000 bps
Interface is DCE, Cable type is V35, Clock mode is DCECLK
Last 300 seconds input rate 4 bytes/sec 32 bits/sec 0 packets/sec
Last 300 seconds output rate 17 bytes/sec 136 bits/sec 0 packets/sec
Input: 89089 packets, 1341532 bytes
  Broadcast:              0,  Multicast:              0
  Errors:                 0,  Runts:                  0
  Giants:                 0,  CRC:                    0

  Alignments:             0,  Overruns:               0
  Dribbles:               0,  Aborts:                 0
  No Buffers:             0,  Frame Error:            0

Output: 173822 packets, 5639896 bytes
  Total Error:            0,  Overruns:               0
  Collisions:             0,  Deferred:               0

DCD=UP DTR=UP DSR=UP RTS=UP CTS=UP

    Input bandwidth utilization  : 1.17%
    Output bandwidth utilization : 0.16%
```

----End

Configuration Files

- Configuration file of Router A

```
#
 sysname RouterA
#
 interface Serial1/0/0
  link-protocol hdlc
  ip address 100.1.1.1 255.255.255.0
#
 return
```

- Configuration file of Router B

```
#
 sysname RouterB
#
 interface Serial1/0/0
  link-protocol hdlc
  ip address 100.1.1.2 255.255.255.0
#
 return
```

6.5.2 Example for Configuring IP Address Unnumbered for HDLC

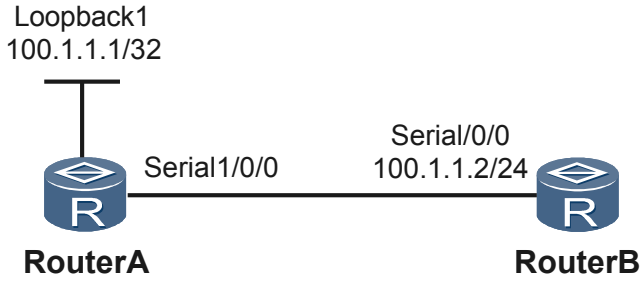
This example describes how to configure IP address unnumbered to interconnect devices running HDLC in typical networking.

Networking Requirements

Router A and Router B are connected through serial interfaces, and the interfaces are required to run HDLC.

Serial 1/0/0 of Router A borrows a loopback interface address. The mask of the loopback interface address is 32 bits.

Figure 6-2 Networking diagram of the HDLC basic function



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the link protocol of each interface as HDLC.
2. On Router A, configure the IP address of the loopback interface whose IP address is unnumbered.
3. Configure the serial interface on Router A to adopt the IP address unnumbered.
4. Configure Router A to learn the opposite routing information through the static route.
5. Configure the IP address of Router B.

Data Preparation

To configure the IP address unnumbered, you need the following data:

- IP address of the loopback interface on Router A
- IP address of the Serial interface on Router B

NOTE

The two IP addresses must be on the same network segment; otherwise, the link layer status of the two interfaces cannot be Up.

Procedure

Step 1 Configure Router A.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface loopback 1
[RouterA-LoopBack1] ip address 100.1.1.1 32
[RouterA-LoopBack1] quit
[RouterA] interface serial 1/0/0
[RouterA-Serial1/0/0] link-protocol hdlc
[RouterA-Serial1/0/0] ip address unnumbered interface loopback 1
[RouterA-Serial1/0/0] quit
```

Step 2 Configure Router B.

```
<Huawei> system-view
[Huawei] sysname RouterB
```

```
[RouterB] interface serial 1/0/0
[RouterB-Serial1/0/0] link-protocol hdlc
[RouterB-Serial1/0/0] ip address 100.1.1.2 24
[RouterB-Serial1/0/0] quit
```

Step 3 Configure the static routing on Router A.

```
[RouterA] ip route-static 100.1.1.0 24 serial 1/0/0
```

Step 4 Verify the configuration.

Run the **display interface serial 1/0/0** command on RouterA to check the interface configuration. The command output shows that both the physical layer status and link layer status of the interface are Up and that RouterA and RouterB can ping each other successfully.

```
[RouterA] display interface serial 1/0/0
Serial1/0/0 current state : UP
Line protocol current state : UP
Last line protocol up time : 2011-12-03 15:00:00
Description:HUAWEI, AR Series, Serial1/0/0 Interface
Route Port,The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet Address is unnumbered, using address of LoopBack0(100.1.1.1/32)
Link layer protocol is nonstandard HDLC
Last physical up time   : 2011-12-03 15:00:00
Last physical down time : 2011-12-03 15:00:00
Current system time: 2011-12-03 15:29:02
Physical layer is synchronous, Virtualbaudrate is 64000 bps
Interface is DTE, Cable type is V35, Clock mode is TC
Last 300 seconds input rate 17 bytes/sec 136 bits/sec 0 packets/sec
Last 300 seconds output rate 3 bytes/sec 24 bits/sec 0 packets/sec
Input: 60724 packets, 1783780 bytes
  broadcasts:            0,  multicasts:            0
  errors:                0,  runts:                 0,  giants:                0
  CRC:                   0,  align errors:          0,  overruns:              0
  dribbles:              0,  aborts:                0,  no buffers:            0
  frame errors:          0
Output: 28481 packets, 393624 bytes
  errors:                0,  underruns:             0,  collisions:            0
  deferred:              0
DCD=UP DTR=UP DSR=UP RTS=UP CTS=UP

    Input bandwidth utilization  : 0.84%
    Output bandwidth utilization : 0.65%
```

----End

Configuration Files

- Configuration file of Router A

```
#
 sysname RouterA
#
 interface Serial1/0/0
  link-protocol hdlc
  ip address unnumbered interface LoopBack1
 interface LoopBack1
  ip address 100.1.1.1 255.255.255.255
 ip route-static 100.1.1.0 255.255.255.0 Serial1/0/0
#
 return
```

- Configuration file of Router B

```
#
 sysname RouterB
 interface Serial1/0/0
  link-protocol hdlc
  ip address 100.1.1.2 255.255.255.0
```

```
#
 return
```

7 DCC Configuration

About This Chapter

This section describes the principles, configuration procedures, and configuration examples of the Dial Control Center (DCC).

7.1 DCC Overview

The dial control center (DCC) provides the dialing service for users. You can configure DCC on the routers connected by an Integrated Services Digital Network (ISDN), a 3G network, or a Public Switched Telephone Network (PSTN) or on the routers functioning as a PPPoE/PPPoEoA/PPPoA client connecting to a PPPoE/PPPoEoA/PPPoA server.

Introduction

When the data to be transmitted is delay-insensitive, bursting, and has a small volume, the routers can use the DCC mode to reduce costs. DCC sets up a call connection only when there is data to be transmitted. DCC is a flexible, cost-effective, and efficient solution.

The routers set up a connection by dialing only when there is data to be transmitted between them. That is, they start the DCC process to transmit signal, and tear down the connection when no data is transmitted on the link.

Usage Scenario

DCC supports extensible dial-on-demand functions to meet various application requirements:

- DCC uses link backup to ensure reliable communication. When communication fails because of a link error or other reasons, the backup link is used to continue the communication.

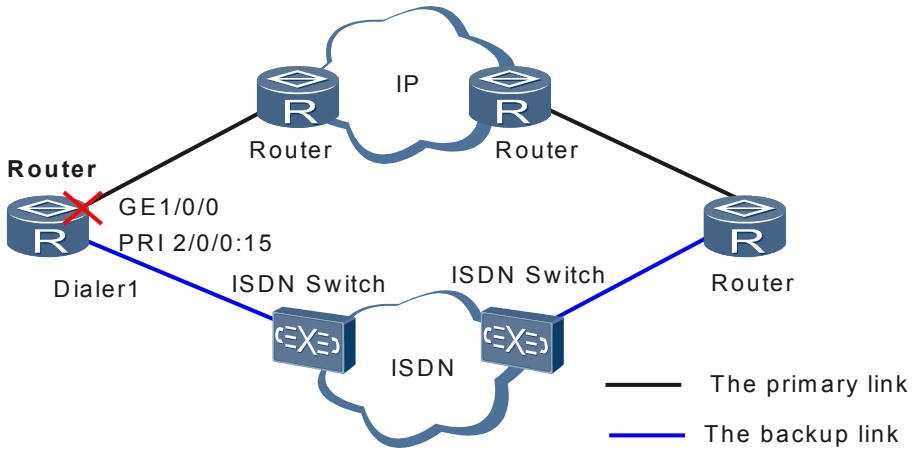
  In most cases, a different type of network is used for link backup. For example, an ISDN network can be used for the link backup of an IP network. The AR2200 implements link backup using either of the following modes:

  - Interface backup
  - Dial-up backup
- DCC on a PPPoE/PPPoEoA/PPPoA client provides cost savings for users.

Link Backup Using the Interface Backup Mode

As shown in **Figure 7-1**, Dialer1 is the dialup interface that backs up GigabitEthernet1/0/0. When GigabitEthernet1/0/0 does not function properly, traffic on GigabitEthernet1/0/0 is switched to PRI2/0/0:15. The DCC dialing process on PRI2/0/0:15 is triggered by the traffic. The ISDN line backup function is implemented by the ISDN.

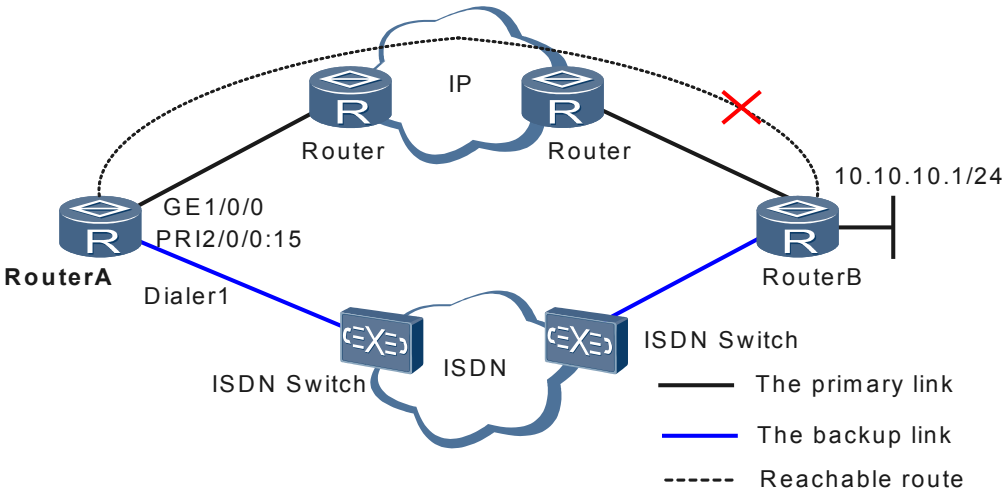
Figure 7-1 Link backup using the interface backup mode



Link Backup Using the Dynamic Routing Standby Mode

As shown in **Figure 7-2**, if RouterA does not have a reachable route to the network segment 10.10.10.1/24 where RouterB resides, the dialup interface of RouterA starts the DCC dialing process to implement ISDN line backup.

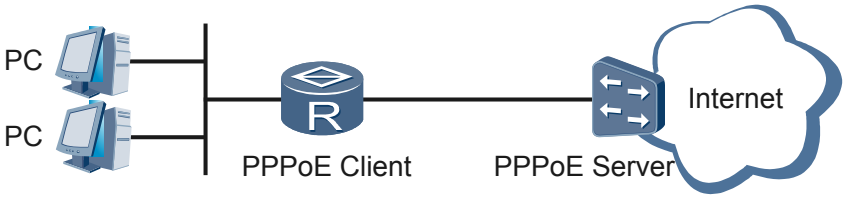
Figure 7-2 Link backup using the dial-up backup mode



DCC on a PPPoE Client

As shown in **Figure 7-3**, a dialing connection has been set up. If no traffic is transmitted between the PPPoE/PPPoEoA client and the PPPoE server, the PPPoE client disconnects the session. When the traffic is restored, the PPPoE client sets up the session again.

Figure 7-3 DCC on a PPPoE client



NOTE

If a router functions as a PPPoEoA/PPPoA client, the router connects to the PPPoEoA/PPPoA server through a DSLAM.

Only the RS-DCC mode can be used in this scenario. For the configurations in this scenario, see **4.4 Configuring the AR2200 as a PPPoE Client** in the *Huawei AR2200 Series Configuration Guide - WAN* "PPPoE Configuration", **1.4.6 Configuring PPPoEoA Mapping on a PVC** and**1.8.4 Example for Configuring PPPoA in On-demand Dialing Mode** in the *Huawei AR2200 Series Configuration Guide - WAN* "ATM Configuration".

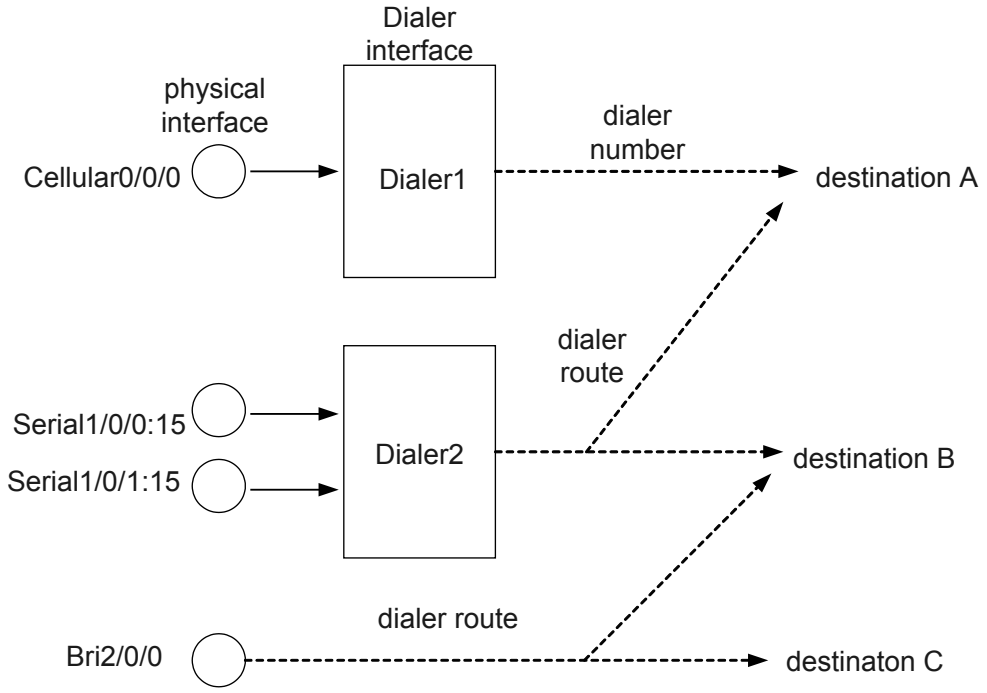
DCC Types

The AR2200 supports two DCC modes: circular DCC (C-DCC) and resource-shared DCC (RS-DCC). The two modes apply to different scenarios. The two ends in communication can use different modes.

DCC Mode	Circular DCC	Resource-Shared DCC
Characteristics	A dialer interface may contain multiple physical interfaces, but a physical interface belongs to only one dialer interface and uses one set of dialer parameters.	A dialer interface may contain multiple physical interfaces, and a physical interface can belong to multiple dialer interfaces.
	After a physical interface is added to a dialer circular group, which is bound to a dialer interface, the physical interface inherits the configurations of the dialer interface. The physical interface can also be configured with DCC parameters.	RS-DCC parameters cannot be directly set on physical interfaces. To implement the RS-DCC function, the physical interfaces must be added to a dialer interface.
	A dialer interface can be bound to multiple destination addresses or one destination address.	A dialer interface is bound to only one destination address.
	All the physical interfaces in a dialer circular group have the same dialer interface attributes.	Physical interface configurations are separated from the logical dialing configurations, and the logical dialing configurations are bound to the physical interfaces. In RS-DCC, a physical interface can use multiple sets of dialing parameters. RS-DCC uses an RS-DCC set to describe dialing attributes. All the calls destined for the same network use the same RS-DCC set. An RS-DCC set contains the parameters of the dialer interface, dialer bundle, and physical interfaces.
Usage scenarios	C-DCC is applicable to the medium- or large-scale sites that have many physical links.	RS-DCC is applicable to the small- or medium-scale sites that have a few physical links but many connected interfaces.

Figure 7-4 shows the relationships between C-DCC physical interfaces and the dialer interface.

Figure 7-4 Relationships between C-DCC physical interfaces and the dialer interface

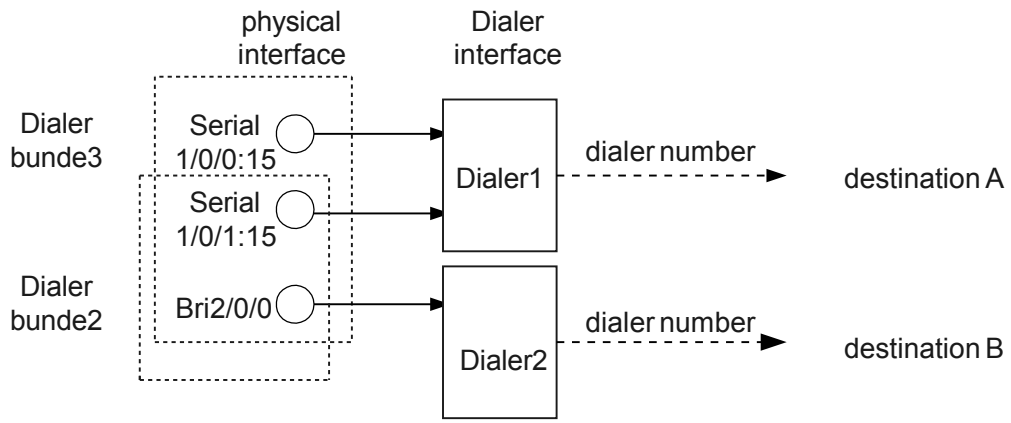


As shown in the figure, a physical interface belongs to only one dialer interface, but each dialer interface can be bound to multiple destination addresses. Each dialer interface can contain multiple physical interfaces.

A physical interface can be directly bound to destination addresses, but does not necessarily belong to any dialer interface.

Figure 7-5 shows the relationships between RS-DCC physical interfaces, dialer bundles, and dialer interfaces.

Figure 7-5 Relationships between RS-DCC physical interfaces, dialer bundles, and dialer interfaces



As shown in the figure, a physical interface can belong to multiple dialer bundles. Each dialer interface can use only one dialer bundle and be bound to only one destination address.

The physical interfaces in a dialer bundle have priorities. The dialer interface corresponding to the dialer bundle chooses physical interfaces according to their priorities. As shown in the figure, Dialer 2 uses Dialer bundle 2, and physical interfaces Serial1/0/1:15 and Serial2/0/0:15 belong to Dialer bundle 2. A large priority value indicates a high priority. If the priority of Serial2/0/0:15 is 100 and the priority of Serial1/0/1:15 is 50, Dialer 2 will select Serial2/0/0:15 from Dialer bundle 2.

A physical interface may have different priorities in different dialer bundles.

7.2 DCC Features Supported by the AR2200

This section describes the DCC features supported by the AR2200.

Interfaces Supporting DCC

On the AR2200, CE1/PRI interfaces, CT1/PRI interfaces, ADSL interfaces, G.SHDSL interfaces, ISDN BRI interfaces, Async interfaces, 3G Cellular interfaces and WAN-side Ethernet interfaces support the DCC function.

- The ADSL, G.SHDSL, and WAN-side Ethernet interfaces of the AR2200 only support RS-DCC.
- The CE1/PRI interfaces, ISDN BRI interfaces and CT1/PRI interfaces support RS-DCC and C-DCC.

  NOTE

  You can only use C-DCC when using a BRI interface to establish an ISDN leased line.
- Async interfaces and 3G Cellular interfaces can only be used for C-DCC.

DCC Configuration Prerequisites

1. Determine the network topology.
   - Determine the routers that need to be configured with the DCC function and plan the connections among these routers.
   - Determine the interfaces on the routers that need to be configured with the DCC function and the purposes of these interfaces.
   - Choose the transmission media, such as ISDN and IP.
2. Plan DCC configuration data.
   - Determine the types of interfaces that you want to use and set physical parameters on the interfaces.
   - Determine the link-layer protocol on the dialup interface, such as PPP and frame relay.
   - Choose routing protocols that will run on the dialup interface, such as RIP and OSPF.
   - Choose network-layer protocol that will be run on the dialup interface, such as IP.
   - Determine the DCC type, such as RS-DCC and C-DCC.
3. Set basic DCC parameters.

   Set the parameters of RS-DCC or C-DCC to implement basic DCC functions. To meet customized requirements, perform additional configurations, such as MP bundle, auto

dialing, and dial string circular backup. You can also adjust the dialup interface attributes according to the actual dialup link status.

7.3 Configuring C-DCC

C-DCC is applicable to the medium- or large-scale sites that have many physical links.

7.3.1 Establishing the Configuration Task

Before configuring C-DCC, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This helps you complete the configuration task quickly and accurately.

Applicable Environment

The usage scenarios of C-DCC and RS-DCC are similar. For details, see **7.1 DCC Overview**. The differences are as follows:

- C-DCC is applicable to the medium- or large-scale sites that have many physical links. RS-DCC is applicable to the small- or medium-scale sites that have a few physical links but many connected interfaces.
- C-DCC cannot be used on the router functioning as the PPPoE/PPPoEoA/PPPoA client.

For more information about C-DCC and RS-DCC supported by interfaces, see **7.2 DCC Features Supported by the AR2200**.

Pre-configuration Tasks

Before configuring C-DCC, complete the following tasks:

- Powering on the AR2200
- Use cables to connect devices properly

Data Preparation

To configure C-DCC, you need the following data.

No.	Data
1	CE1/PRI or CT1/PRI interface number, timeslot ID bound to the PRI set
2	Link-layer protocol and IP address of the dialup interface
3	Dialer interface number, dialer access group, dialer access control list (ACL)
4	Destination address and dialer number on the remote end, (optional) physical interface priority in the dialer circular group
5	(Optional) Maximum link idle time, (optional) link disconnection time, (optional) compete-idle time, (optional) wait-carrier time, (optional) buffer queue length, (optional) auto-dial interval
6	(Optional) Maximum number of links in an MP group

No.	Data
7	(Optional) Number of the standby routing group, (optional) network segment to be monitored, (optional) delay in disconnecting the standby dialer interface, (optional) warmup timer for the dial-up backup function

7.3.2 (Optional) Configuring Working Mode of Physical Interfaces

Before using a PRI interface, configure a CE1/PRI or CT1/PRI interface to work in PRI mode.

Procedure

- To configure a CE1/PRI interface to work in PRI mode, see Configuring a CE1/PRI Interface to Work in PRI Mode.
- To configure a CT1/PRI interface to work in PRI mode, see Configuring a CT1/PRI Interface to Work in PRI Mode.

  NOTE

  For details about other types of physical interfaces, see Configuration Guide - Interface Management.

----End

7.3.3 Configuring Link-Layer Protocol and IP Address

You can configure the link-layer protocol on the dialer interface and assign an IP address to the interface to enable the dialing function.

Context

When the link-layer protocol on the dialup interface is PPP, you can configure PAP or CHAP authentication. For detailed configurations, see **3.4 Configuring PPP Authentication**.

The configuration principles of PPP are as follows:

- When C-DCC is used, configure PPP on the dialer interface.
- When RS-DCC is used, configure PPP on the dialer interface of the calling party. You are also advised to perform the same PPP configurations on the physical interfaces to ensure reliable PPP parameter negotiation. Configure PPP on physical interfaces of the called party.

  In RS-DCC, the initial link-layer protocol of the B channel on an ISDN BRI or PRI interface is PPP. When the B channel is used, it uses the link-layer protocol of the dialer interface. This ensures that the B channel can be used by the dialer interface running multiple link-layer protocols. When the B channel is released, the link-layer protocol is restored to PPP.

The link-layer protocol and IP address need to be configured on the dialup interface (a physical interface or a dialer interface).

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface dialer interface-number
```

A dialer interface is created and the dialer interface view is displayed.

To configure a physical dialer interface, run the **interface** *interface-type interface number* command to enter the specified physical interface view.

Step 3 Run:

```
link-protocol ppp
```

or

```
link-protocol fr
```

The link-layer protocol is configured for the dialup interface.

By default, all interfaces except Ethernet interfaces run PPP at the link layer. When the FR protocol is used as the encapsulation protocol, the default frame encapsulation format is the IETF format.

NOTE

When DCC dial-up is implemented using an AS interface or a 3G cellular interface, you cannot configure the link-layer protocol of the physical interface (the AS interface or 3G cellular interface) or the dialer interface as FR.

Step 4 Assign an IP address to the dialer interface.

- Assign an IPv4 address to the dialer interface.
  - Run:

    ```
    ip address ip-address { mask | mask-length }
    ```

    An IP address is allocated to the dialer interface.
  - Run:

    ```
    ip address ppp-negotiate
    ```

    The dialer interface is configured to obtain an IP address from the PPPoE server.

----End

7.3.4 Enabling C-DCC and Binding Dialer ACL to Interface

A dialer access control list (ACL) filters all packets passing through a dialup interface.

Context

The dialer ACL is used in one of the two ways:

- If a link has been set up, DCC forwards the packets that match the permit conditions and the packets that do not match the deny conditions. In addition, DCC resets the idle timer. If no link is set up, DCC initiates a new call.
- If a link has been set up, DCC forwards the packets that do not match the permit conditions and the packets that match the deny conditions. In addition, DCC resets the idle timer. If no link is set up, DCC initiates a new call. However, DCC does not reset the idle timer. If no link is set up, DCC does not initiate a new call and discard the packets.

The DCC dialer ACL must be configured and bound to the dialup interface (a physical interface or a dialer interface) using the **dialer-group** command; otherwise, DCC packets cannot be sent.

You can configure filtering rules for a dialer ACL or associate an existing ACL with the dialer ACL.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

Enter the interface view.

Step 3 Run:

```
dialer enable-circular
```

The C-DCC function is enabled.

By default, the C-DCC function is disabled on an interface.

Step 4 Run:

```
dialer-group group-number
```

The dialer group of the dialer interface is specified.

By default, no dialer ACL or dialer group is configured.

Step 5 Run:

```
quit
```

Return to the system view.

Step 6 Run:

```
dialer-rule
```

The dialer rule view is displayed.

Step 7 Run:

```
dialer-rule dialer-rule-number { acl { acl-number | name acl-name } | ip { deny |
permit } | ipv6 { deny | permit } }
```

The dialer ACL corresponding to a dialer group is configured to determine the DCC call initiating conditions.

NOTE

Ensure that the *dialer-rule-number* value in the **dialer-rule** command is the same as the *group-number* value in the **dialer-group** command.

The ACL referenced by **dialer-rule** cannot be configured with **time-range**.

Step 8 Run:

```
quit
```

Return to the system view.

----End

7.3.5 Configuring the Modes Used to Send and Receive Calls

This section describes the modes used to send and receive C-DCC calls.

Context

There are two methods to set C-DCC parameters:

- When an interface initiates a call to one interface or multiple interfaces, set DCC parameters on physical interfaces.
- When multiple interfaces initiate a call to one interface or multiple interfaces, or one interface initiates a call, add physical interfaces to a dialer circular group and bind the dialer circular group to a dialer interface. The physical interfaces will inherit the DCC parameters of the dialer interface.

A dialer circular group binds multiple physical interfaces to a dialer interface. The DCC parameters on the dialer interface will be inherited by all physical interfaces in the dialer circular group.

After you set the parameters of the dialer circular group, any physical interface in the dialer circular group can call any destination address bound to the dialer interface.

Depending on the network topology and dialing requirements, an interface may need to initiate and receive calls. You can choose the following C-DCC configurations according to your needs.

NOTE

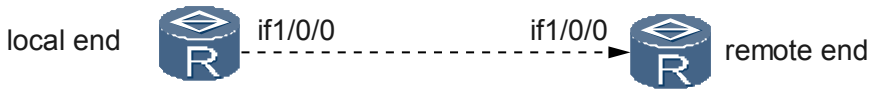
The calling and called parties in C-DCC can use PAP or CHAP authentication. The authentication must be configured on both of them or neither of them. Authentication is recommended to ensure the security of called and calling parties. For details about authentication configurations, see **3.4 Configuring PPP Authentication**. In addition, pay attention to the following restrictions:

- On the calling party, if DCC is enabled on physical interfaces, configure PAP or CHAP authentication on the physical interfaces; if DCC is enabled for the dialer circular group, configure PAP or CHAP authentication on the dialer interface.
- When a physical interface receives a DCC request, it starts PPP negotiation and verifies the identity of calling party, and then forwards the DCC request to the DCC module. Therefore, on the called party, you are advised to configure PAP or CHAP authentication on both physical interfaces and the dialer interface.

DCC calls can be initiated as follows:

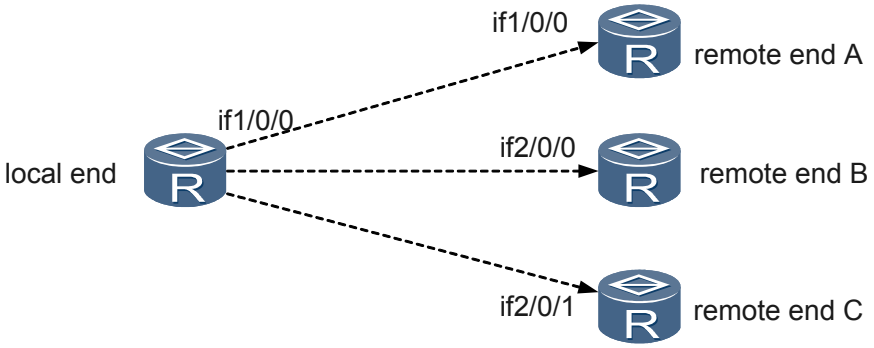
- An interface initiates a call to another interface.

  Figure 7-6 An interface initiates a call to another interface

  As shown in **Figure 7-6**, the local end interface1/0/0 (if1/0/0 for short) initiates a call to if1/0/0 of the remote end. When a call is initiated to one interface, use the **dialer number** or **dialer route** command to configure a dialer number; when a call is initiated by one interface, configure DCC for the dialer circular group. The PAP or CHAP authentication is optional.
- An interface initiates calls to multiple interfaces.

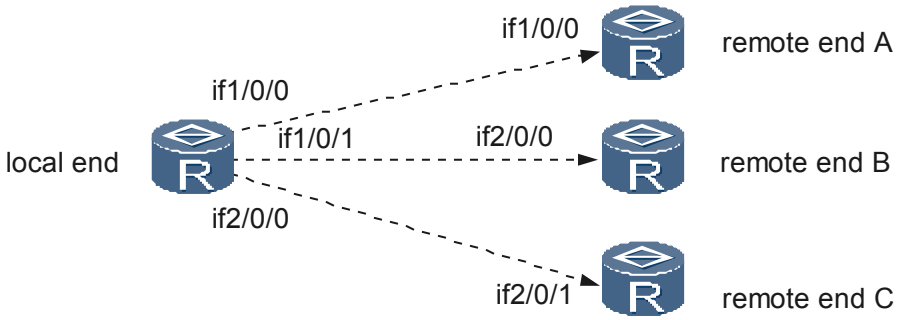
Figure 7-7 An interface initiates calls to multiple interfaces



As shown in **Figure 7-7**, the local end interface1/0/0 (if1/0/0 for short) initiates calls to if1/0/0, if2/0/0, and if2/0/1 of the remote end. Because there are multiple called parties, use the **dialer route** command to configure the dialer numbers and destination addresses. In addition, the calls are initiated by one interface on the local end, so configure DCC for the dialer circular group. The PAP or CHAP authentication is optional.

- Multiple interfaces initiate calls to multiple interfaces.

Figure 7-8 Multiple interfaces initiate calls to multiple interfaces

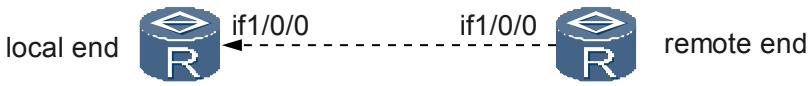


As shown in **Figure 7-8**, if1/0/0, if1/0/1, and if2/0/0 on the local end initiate calls to if1/0/0, if2/0/0, and if2/0/1 of the remote end. Because there are multiple called parties, use the **dialer route** command to configure the dialer numbers and destination addresses. In addition, the calls are initiated by multiple interfaces on the local end, so configure DCC for the dialer circular groups. PAP or CHAP authentication is optional.

DCC calls can be received as follows:

- An interface receives a call from another interface.

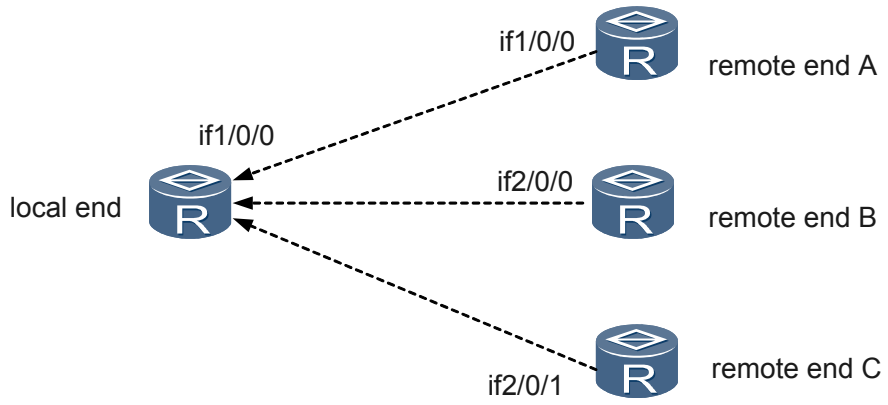
Figure 7-9 An interface receives a call from another interface



As shown in **Figure 7-9**, the local end interface1/0/0 (if1/0/0 for short) receives a call from if1/0/0 of the remote end. Because the called party is one interface, configure DCC for the dialer circular group. PAP or CHAP authentication is optional.

- An interface receives calls from multiple interfaces.

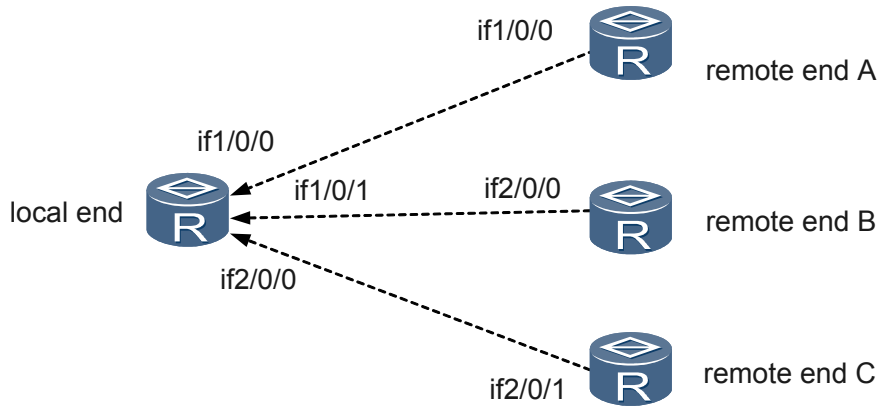
Figure 7-10 An interface receives calls from multiple interfaces



As shown in **Figure 7-10**, the local end interface1/0/0 (if1/0/0 for short) receives calls from if1/0/0, if2/0/0, and if2/0/1 of the remote end. Because the called party is one interface, configure DCC for the dialer circular group. PAP or CHAP authentication is optional.

- Multiple interfaces receive calls from other interfaces.

Figure 7-11 Multiple interfaces receive calls from other interfaces



As shown in **Figure 7-11**, if1/0/0, if1/0/1, and if2/0/0 on the local end receive calls from if1/0/0 and if2/0/0 of the remote end. Because the called parties are multiple interfaces, configure DCC for the dialer circular groups. PAP or CHAP authentication is optional.

NOTE

If a local end receives calls from multiple remote ends, use the **dialer route ip** command even if the local end initiates calls to only one remote end.

A 3G cellular interface or an asynchronous serial interface supports only the **dialer number** command. Calls can only be initiated or received on a single interface.

Procedure

- Configure DCC when an interface initiates a call to another interface.
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     interface *interface-type interface-number*

     Enter the interface view.
  3. Configure a destination address and a dialer number.
     - Run the **dialer number** *dial-number* [**autodial**] command.
     - Run the **dialer route ip** *next-hop-address* [**user** *hostname* | **broadcast**] * [*dial-string*] [**autodial** | **interface** *interface-type interface-number*] * command in the dialer interface view.
     - Run the **dialer route ip** *next-hop-address* [**user** *hostname* | **broadcast**] * [*dial-string*] [**autodial**] command in the PRI or BRI interface view.

     By default, no dialer number is configured. Use either the **dialer route** or **dialer number** command to configure a dialer number.

     By default, the auto-dial function is disabled. The auto-dial function must be used together with C-DCC.
- Configure DCC when an interface initiates calls to multiple interfaces.
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     interface *interface-type interface-number*

     Enter the interface view.
  3. Configure a destination address and a dialer number, or multiple destinations and dialer numbers.
     - Run the **dialer route ip** *next-hop-address* [**user** *hostname* | **broadcast**] * [*dial-string*] [**autodial** | **interface** *interface-type interface-number*] * command in the dialer interface view.
     - Run the **dialer route ip** *next-hop-address* [**user** *hostname* | **broadcast**] * [*dial-string*] [**autodial**] command in the PRI or BRI interface view.

     By default, no dialer number is configured. The **dialer route** command specifies only one destination. To specify multiple destinations for a dialer interface, run this command multiple times.

     By default, the auto-dial function is disabled. The auto-dial function must be used together with C-DCC.
- Configure DCC when multiple interfaces initiate calls to multiple interfaces.
  1. Run:
     system-view

The system view is displayed.

2. Run:

```
interface dialer interface-number
```

A dialer interface is created and the dialer interface view is displayed.

3. Run:

```
dialer route ip next-hop-address [ user hostname | broadcast ] * [ dial-string ] [ autodial | interface interface-type interface-number ] *
```

The destination addresses and dialer numbers are configured.

The **dialer route** command specifies only one destination. To specify multiple destinations for a dialer interface, run this command multiple times.

By default, the auto-dial function is disabled. The auto-dial function must be used together with C-DCC.

4. Run:

```
quit
```

Return to the system view.

5. Run:

```
interface interface-type interface-number
```

Enter the interface view.

6. Run:

```
dialer circular-group number
```

A physical interface is added to the dialer circular group.

The value of *number* must be identical with the value of *interface-number* in the **interface dialer** *interface-number* command. The ISDN PRI or ISDN BRI interface is equivalent to the dialer circular group of B channels, and it can be a physical interface in another dialer circular group.

After this command is executed, C-DCC is enabled on the interface automatically.

7. (Optional) Run:

```
dialer priority priority
```

The priority of a physical interface in a dialer circular group is set.

By default, no dialer interface exists and a physical interface does not belong to any dialer circular group. The default priority of a physical interface in a dialer circular group is 1.

For dialing, a physical interface in a dialer circular group uses the IP address of the dialer interface not its own IP address.

- Configure DCC when an interface receives a call from another interface.

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
interface interface-type interface-number
```

Enter the interface view.

3. (Optional) Configure a destination address and a dialer number.
   - Run the **dialer route ip** *next-hop-address* [**user** *hostname* | **broadcast**] * [*dial-string*] [**autodial** | **interface** *interface-type interface-number*] * command in the dialer interface view.
   - Run the **dialer route ip** *next-hop-address* [**user** *hostname* | **broadcast**] * [*dial-string*] [**autodial**] command in the PRI or BRI interface view.

   NOTE

   If the **dialer route ip** *next-hop-address* **user** *hostname* command has been used on the called party, the called party checks the IP address and user name of the calling party against *next-hop-address* and *hostname*. This step is required only when the IP address and user name of the calling party need to be verified or when the interface initiates and receives calls.

- Configure DCC when an interface receives calls from multiple interfaces.
  1. Run:
     ```
     system-view
     ```
     The system view is displayed.
  2. Run:
     ```
     interface interface-type interface-number
     ```
     Enter the interface view.
  3. (Optional) Configure destination addresses and dialer numbers.
     - Run the **dialer route ip** *next-hop-address* [**user** *hostname* | **broadcast**] * [*dial-string*] [**autodial** | **interface** *interface-type interface-number*] * command in the dialer interface view.
     - Run the **dialer route ip** *next-hop-address* [**user** *hostname* | **broadcast**] * [*dial-string*] [**autodial**] command in the PRI or BRI interface view.

     NOTE

     If the **dialer route ip** *next-hop-address* **user** *hostname* command has been used on the called party, the called party checks the IP address and user name of the calling party against *next-hop-address* and *hostname*. This step is required only when the IP address and user name of the calling party need to be verified or the interface initiates and receives calls.

- Configure DCC when multiple interfaces receive calls from other interfaces.
  1. Run:
     ```
     system-view
     ```
     The system view is displayed.
  2. Run:
     ```
     interface dialer interface-number
     ```
     A dialer interface is created and the dialer interface view is displayed.
  3. (Optional) Run:
     ```
     dialer route ip next-hop-address [ user hostname | broadcast ] * [ dial-string ] [ autodial ]
     ```
     The destination addresses and dialer numbers are configured.

NOTE

If the **dialer route ip** *next-hop-address* **user** *hostname* command has been used on the called party, the called party checks the IP address and user name of the calling party against *next-hop-address* and *hostname*. This step is required only when the IP address and user name of the calling party need to be verified or the interface initiates and receives calls.

4. Run:
   ```
   quit
   ```
   Return to the system view.
5. Run:
   ```
   interface interface-type interface-number
   ```
   Enter the interface view.
6. Run:
   ```
   dialer circular-group number
   ```
   A physical interface is added to the dialer circular group.

   The value of *number* must be identical with the value of *interface-number* in the **interface dialer** *interface-number* command.

   By default, no dialer interface exists and a physical interface does not belong to any dialer circular group.
7. (Optional) Run:
   ```
   dialer priority priority
   ```
   The priority of a physical interface in a dialer circular group is set.

   By default, the priorities of physical interfaces in a dialer circular group are 1.

----End

7.3.6 (Optional) Configuring Attributes of a DCC Dialup Interface

DCC provides optional parameters. These parameters improve dial-on-demand efficiency and meet various service requirements.

Context

- Maximum link idle time

  After the maximum link idle time is set, DCC disconnects calls on dialup interfaces if the link idle timer expires. Link idle time is the period in which no packet is permitted by the dialer access control list (ACL) on the link.
- Link disconnection time before a new call is initiated

  If a CCC line is disconnected due to a fault or hang-up, the link is re-established only after a certain period of time. This prevents PBX overload.
- Link idle cut during interface competition

  When a DCC is initiated, competition occurs if all channels are occupied. The idle timer takes effect for a newly established link. If a call to another destination needs to be established, a competition occurs. The system replaces the idle timer with the compete-idle timer to control the ongoing call. When the idle time of the ongoing call reaches the compete-idle timer, the call is disconnected.
- Call setup timeout

Call setup time may vary with the remote end type. Configure the wait-carrier timer to control the call setup time. If a call is not established within the wait-carrier time, DCC terminates the call.

- Buffer queue length on a dialup interface

  If a dialup interface receives a packet but the call connection is not established, the dialup interface discards the packet. However, if a buffer queue is configured on the dialup interface, the dialup interface stores the packet in the buffer, and sends the packet after the call connection is established.

- Auto-dial interval

  A DCC router immediately attempts to dial the remote end after starting. The dialing process is not triggered by data packets. If a connection cannot be established with the remote end, the router retries at an interval. The call set up automatically will not be disconnected because of timeout. That is, the **dialer timer idle** command does not apply to the calls that are set up automatically.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

Enter the interface view.

Step 3 Run:

```
dialer timer idle seconds
```

The link idle timer is set.

By default, the maximum link idle time is 120 seconds.

Step 4 Run:

```
dialer timer enable seconds
```

The link disconnection time before a new call is initiated is set.

By default, a new call is initiated 5 seconds after the previous call is disconnected.

Step 5 Run:

```
dialer timer compete seconds
```

The compete-idle timer after a competition occurs among interfaces is set.

By default, the compete-idle timer is 20 seconds.

Step 6 Run:

```
dialer timer wait-carrier seconds
```

The wait-carrier timer is set.

By default, the wait-carrier timer is 60 seconds.

Step 7 Run:

```
dialer queue-length packets
```

The buffer queue length on a dialup interface is set.

By default, no buffer queue is configured on a dialup interface.

Step 8 Run:

```
dialer timer autodial
```

The auto-dial interval is set.

By default, the auto-dial function is disabled. After the auto-dial function is enabled, the auto-dial interval is 300 seconds. When using the **dialer route** command to configure the dialer number, specify the **autodial** parameter to enable the auto-dial function.

NOTE

The auto-dial function must be used together with C-DCC.

----End

7.3.7 (Optional) Configuring MP Group for DCC

Context

To provide the required data transmission rate, use the **ppp mp max-bind** command to configure the number of PPP links for each DCC call. For example, the rate of a PPP link on a CE1/PRI interface is 64 kbit/s; if customers require 1024 kbit/s rate, set the number of PPP links to 16.

The **ppp mp max-bind** command can only be used on a dialer interface, and the PPP configurations follow these principles:

- When C-DCC is used, configure PPP on the dialer interface.
- When RS-DCC is used, configure PPP on the dialer interface of the calling party. You are also advised to perform the same PPP configurations on the physical interfaces to ensure reliable PPP parameter negotiation. On the called party, configure PPP on the dialer interface and physical interfaces.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface dialer interface-number
```

The dialer interface view is displayed.

Step 3 Run:

```
link-protocol ppp
```

The PPP protocol is configured as the link-layer protocol on the dialer interface.

By default, all interfaces except Ethernet interfaces run PPP at the link layer.

Step 4 Run:

```
ppp mp
```

The PPP interface is configured to work in Multilink PPP (MP) mode.

Step 5 Run:

```
ppp mp max-bind max-bind-number
```

The maximum number of links in an MP group is set.

By default, a maximum of 16 PPP links can be bound in an MP group.

----End

7.3.8 (Optional) Configuring Dialer Number Backup

When configuring destination addresses for C-DCC, run the **dialer route** command multiple times to configure multiple dialer routes corresponding to different dialer numbers. Each dialer number you configure can serve as a backup for the other dialer number. If a dialer number is invalid, the system chooses a dialer route containing another dialer number.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

Enter the interface view.

Step 3 Configure a destination address and a dialer number for the same remote end.

- Run the **dialer route ip** *next-hop-address* [**user** *hostname* | **broadcast**] * [*dial-string*] [**autodial** | **interface** *interface-type interface-number*] * command in the dialer interface view.
- Run the **dialer route ip** *next-hop-address* [**user** *hostname* | **broadcast**] * [*dial-string*] [**autodial**] command in the PRI/BRI interface view.

----End

7.3.9 (Optional) Configuring Dial-Up Backup

The dial-up backup function dynamically maintains dial-up links based on routes.

Context

The dial-up backup function provides the backup and routing functions, and implements reliable connections and on-demand dialing function.

The dial-up backup function has the following characteristics:

- All routes can be backed up, including the routes generated by routing protocols, static routes, and direct routes.
- Dial-up backup is used between interfaces or routers, but not on a single interface or link.
- If the primary link is broken, the backup link automatically takes over. There is no delay during the switchover except the route convergence period.

- The dial-up backup function is applicable to all routing protocols, including RIP-1, RIP-2, OSPF, IS-IS, and BGP. However, some routing protocols such as BGP choose the optimal routes. If the primary link destined for the monitored network segment is broken, the backup link learns the routes destined for the monitored network segment using BGP. After the primary link recovers, the primary link re-learns the routes, but these routes may not be the optimal routes. The router still uses the routes learned by the backup link. As a result, the backup link cannot be disconnected and the dynamic route monitoring function fails.

  To address this issue:

  - Set the IP address of the backup link to be greater than the IP address of the primary link.
  - Configure load balancing so that one route is learned by multiple links.
- The dial-up backup function causes auto dialing unable to take effect.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
standby routing-rule group-number ip ip-address { mask | mask-length }
```

A dial-up backup group is created and the network segments to be monitored are added to the group.

Step 3 Run:

```
interface interface-type interface-number
```

Enter the interface view.

Step 4 Run:

```
standby routing-group group-number
```

The dial-up backup function is enabled on the interface.

By default, the dial-up backup function is disabled.

Before enabling the dial-up backup function, ensure that basic DCC functions are enabled and the dial-up backup group (configured by **standby routing-rule**) is configured on the interface.

Step 5 (Optional) Run:

```
standby timer routing-disable seconds
```

The delay in disconnecting the standby dialer interface is set.

This delay prevents route flapping after the routes in the network segment are recovered. By default, when the routes in a network segment are recovered, the system disconnects the standby dialer interface after a 20-second delay.

Step 6 Run:

```
quit
```

Return to the system view.

Step 7 (Optional) Run:

```
dialer timer warmup seconds
```

The warmup timer is configured.

By default, the warmup timer is 30 seconds.

After starting, the system restores configurations automatically. During configuration restoration, the main interface is in Down state, so the route on the main interface becomes unreachable. The system starts the backup link. After the configurations are restored, all interfaces become Up, and the call is set up on the backup link. However, after the route on the main interface is recovered, the backup link is disconnected. To prevent status flapping of the backup link after system startup, configure the warmup timer. The system will not use the backup link until the warmup timer expires.

----End

7.3.10 (Optional) Closing a Connection

To reduce network loads or adjust dialing configurations, you may need to tear down a dial-up link using the **dialer disconnect** command.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
dialer disconnect [ interface interface-type interface-number ]
```

A dial-up link is torn down.

After a dial-up link is torn down, all services on the link are interrupted; therefore, ensure that the link is not in use before you tear down the link.

This command only temporarily tears down dial-up links.

- If a disconnected link is enabled with the auto-dial function, it will be re-established when the dialer timer expires.
- If the link is not enabled with the auto-dial function, it will be re-established when data needs to be transmitted over it.

----End

7.3.11 Checking the Configuration

After C-DCC is configured, view the dialup interface information.

Prerequisites

All configurations of C-DCC are complete.

Procedure

Step 1 Run the **display dialer** [**interface** *interface-type interface-number*] command to check DCC information on the dialup interface.

Step 2 Run the **display interface dialer** [*number*] command to check information about the dialer interface.

----End

7.4 Configuring RS-DCC

A physical interface in RS-DCC can belong to multiple dialer bundles and serves multiple dialer interfaces. A dialer interface is bound to only one destination and uses only one dialer bundle. A dialer bundle can contain multiple physical interfaces that have different priorities.

7.4.1 Establishing the Configuration Task

Before configuring resource-shared DCC (RS-DCC), familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This helps you complete the configuration task quickly and accurately.

Applicable Environment

The usage scenarios of C-DCC and RS-DCC are similar. For details, see **7.1 DCC Overview**. The differences are as follows:

- C-DCC is applicable to the medium- or large-scale sites that have many physical links. RS-DCC is applicable to the small- or medium-scale sites that have a few physical links but many connected interfaces.
- C-DCC cannot be used on the router functioning as the PPPoE/PPPoEoA/PPPoA client.

For more information about C-DCC and RS-DCC supported by interfaces, see **7.2 DCC Features Supported by the AR2200**.

Pre-configuration Tasks

Before configuring RS-DCC, complete the following tasks:

- Powering on the router
- Using cables to connect devices properly

Data Preparation

To configure RS-DCC, you need the following data.

No.	Data
1	CE1/PRI or CT1/PRI interface number, timeslot ID bound to the PRI set
2	Link-layer protocol and IP address of the dialup interface
3	Dialer interface number, dialer access group, dialer access control list (ACL)
4	Dialer number on the remote end, association between physical interfaces and dialer bundle, physical interface priorities in the dialer bundle
5	(Optional) Maximum link idle time, (optional) link disconnection time, (optional) compete-idle time, (optional) wait-carrier time, (optional) buffer queue length

No.	Data
6	(Optional) Maximum number of links in an MP group
7	(Optional) Number of the standby routing group, (optional) network segment to be monitored, (optional) delay in disconnecting the standby dialer interface, (optional) warmup timer for the dial-up backup function

7.4.2 Configuring the Mode of the Physical Interface

Before using a PRI interface, configure a CE1/PRI or CT1/PRI interface to work in PRI mode.

Procedure

- To configure a CE1/PRI interface to work in PRI mode, see Configuring a CE1/PRI Interface to Work in PRI Mode.
- To configure a CT1/PRI interface to work in PRI mode, see Configuring a CT1/PRI Interface to Work in PRI Mode.

  NOTE

  For details about other types of physical interfaces, see Configuration Guide - Interface Management.

----End

7.4.3 Configuring Link-Layer Protocol and IP Address

You can configure the link-layer protocol on the dialer interface and assign an IP address to the interface to enable the dialing function.

Context

When the link-layer protocol on the dialup interface is PPP, you can configure PAP or CHAP authentication. For detailed configurations, see **3.4 Configuring PPP Authentication**.

The configuration principles of PPP are as follows:

- When C-DCC is used, configure PPP on the dialer interface.
- When RS-DCC is used, configure PPP on the dialer interface of the calling party. You are also advised to perform the same PPP configurations on the physical interfaces to ensure reliable PPP parameter negotiation. Configure PPP on physical interfaces of the called party.

  In RS-DCC, the initial link-layer protocol of the B channel on an ISDN BRI or PRI interface is PPP. When the B channel is used, it uses the link-layer protocol of the dialer interface. This ensures that the B channel can be used by the dialer interface running multiple link-layer protocols. When the B channel is released, the link-layer protocol is restored to PPP.

The link-layer protocol and IP address need to be configured on the dialup interface (a physical interface or a dialer interface).

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

Enter the interface view.

Step 3 Run:

```
link-protocol ppp
```

or

```
link-protocol fr
```

The link-layer protocol is configured for the dialup interface.

By default, all interfaces except Ethernet interfaces run PPP at the link layer. When the FR protocol is used as the encapsulation protocol, the default frame encapsulation format is the IETF format.

Step 4 Assign an IP address to the dialer interface.

- Assign an IPv4 address to the dialer interface.
  - Run:

    ```
    ip address ip-address { mask | mask-length }
    ```

    An IP address is allocated to the dialer interface.
  - Run:

    ```
    ip address ppp-negotiate
    ```

    The dialer interface is configured to obtain an IP address from the PPPoE server.
- Assign an IPv6 address to the dialer interface.

  Run:

  ```
  ipv6 address { ipv6-address prefix-length | ipv6-address/prefix-length }
  ```

  An IPv6 address is assigned to the dialer interface.

  NOTE

  Before assigning an IPv6 address to an interface, run the **ipv6** command in the system view to enable IPv6 packet forwarding and run the **ipv6 enable** command on the interface to enable IPv6.

----End

7.4.4 Enabling RS-DCC and Binding Dialer ACL to Interface

You can specify the dialer group and the ACL of DCC dialing.

Context

DCC forwards packets based on the permit or deny condition in the dialer ACL:

- If a link has been set up, DCC forwards the packets that match the permit conditions and the packets that do not match the deny conditions. In addition, DCC resets the idle timer. If no link is set up, DCC initiates a new call.
- If a link has been set up, DCC forwards the packets that do not match the permit conditions and the packets that match the deny conditions. In addition, DCC resets the idle timer. If

no link is set up, DCC initiates a new call. However, DCC does not reset the idle timer. If no link is set up, DCC does not initiate a new call and discard the packets.

The DCC dialer ACL must be configured and bound to the dialup interface (a physical interface or a dialer interface) using the **dialer-group** command; otherwise, DCC packets cannot be sent. Configure filtering rules for a dialer ACL or associate an existing ACL with the dialer ACL.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface dialer interface-number
```

The dialer interface view is displayed.

Step 3 Run:

```
dialer user username
```

The RS-DCC function is enabled.

By default, the RS-DCC function is disabled and the remote user name is not set.

Step 4 Run:

```
dialer bundle number
```

A dialer bundle is configured for a dialer interface in RS-DCC.

Step 5 Run:

```
dialer-group group-number
```

The dialer group is specified for the dialer interface.

By default, no dialer ACL or dialer group is configured.

Step 6 Run:

```
quit
```

Return to the system view.

Step 7 Run:

```
dialer-rule
```

The dialer rule view is displayed.

Step 8 Run:

```
dialer-rule dialer-rule-number { acl { acl-number | name acl-name } | ip { deny |
permit } | ipv6 { deny | permit } }
```

The dialer ACL corresponding to a dialer group is configured to determine the DCC call initiating conditions.

NOTE

Ensure that the *dialer-rule-number* value in the **dialer-rule** command is the same as the *group-number* value in the **dialer-group** command.

The ACL referenced by **dialer-rule** cannot be configured with **time-range**.

Step 9 Run:

```
quit
```

Return to the system view.

----End

7.4.5 Configuring RS-DCC

Configure RS-DCC to implement dial-on-demand.

Context

In RS-DCC, the physical interface attributes vary according to the dialer numbers. Set DCC parameters on the dialer interface and use the **dialer number** command to configure the dialer number. Only one dialer number can be configured on a dialer interface.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface dialer interface-number
```

The dialer interface view is displayed.

Step 3 Run:

```
dialer number dial-number [ autodial ]
```

A dialer number is configured.

Step 4 Run:

```
quit
```

Return to the system view.

Step 5 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 6 Run:

```
dialer bundle-member number [ priority priority ]
```

The PRI interface is added to a dialer bundle.

Step 7 Configure PPP as the link-layer protocol and configure PPP authentication (PAP or CHAP). For the detailed configuration procedure, see **3.4 Configuring PPP Authentication**.

----End

7.4.6 (Optional) Configuring Attributes of a DCC Dialup Interface

DCC provides optional parameters. These parameters improve dial-on-demand efficiency and meet various service requirements.

Context

- Maximum link idle time

  After the maximum link idle time is set, DCC disconnects calls on dialup interfaces automatically if the link idle timer expires. Link idle time is the period in which no packet is permitted by the dialer access control list (ACL) on the link.
- Link disconnection time before a new call is initiated

  If a CCC line is disconnected due to a fault or hang-up, the link is re-established only after a certain period of time. This prevents PBX overload.
- Link idle cut during interface competition

  When a DCC is initiated, competition occurs if all channels are occupied. The idle timer takes effect for a newly established link. If a call to another destination needs to be established, a competition occurs. The system replaces the idle timer with the compete-idle timer to control the ongoing call. When the idle time of the ongoing call reaches the compete-idle timer, the call is disconnected.
- Call setup timeout

  Call setup time may vary with the remote end type. Configure the wait-carrier timer to control the call setup time. If a call is not established within the wait-carrier time, DCC terminates the call.
- Buffer queue length on a dialup interface

  If a dialup interface receives a packet but the call connection is not established, the dialup interface discards the packet. However, if a buffer queue is configured on the dialup interface, the dialup interface stores the packet in the buffer, and sends the packet after the call connection is established.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

Enter the interface view.

Step 3 Run:

```
dialer timer idle seconds
```

The link idle timer is set.

By default, the maximum link idle time is 120 seconds.

Step 4 Run:

```
dialer timer enable seconds
```

The link disconnection time before a new call is initiated is set.

By default, a new call is initiated 5 seconds after the previous call is disconnected.

Step 5 Run:

```
dialer timer compete seconds
```

The compete-idle timer after a competition occurs among interfaces is set.

By default, the compete-idle timer is 20 seconds.

Step 6 Run:

```
dialer timer wait-carrier seconds
```

The wait-carrier timer is set.

By default, the wait-carrier timer is 60 seconds.

----End

7.4.7 (Optional) Configuring MP Group for DCC

Context

To provide the required data transmission rate, use the **ppp mp max-bind** command to configure the number of PPP links for each DCC call. For example, the rate of a PPP link on a CE1/PRI interface is 64 kbit/s; if customers require 1024 kbit/s rate, set the number of PPP links to 16.

The **ppp mp max-bind** command can only be used on a dialer interface, and the PPP configurations follow these principles:

- When C-DCC is used, configure PPP on the dialer interface.
- When RS-DCC is used, configure PPP on the dialer interface of the calling party. You are also advised to perform the same PPP configurations on the physical interfaces to ensure reliable PPP parameter negotiation. On the called party, configure PPP on the dialer interface and physical interfaces.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface dialer interface-number
```

The dialer interface view is displayed.

Step 3 Run:

```
link-protocol ppp
```

The PPP protocol is configured as the link-layer protocol on the dialer interface.

By default, all interfaces except Ethernet interfaces run PPP at the link layer.

Step 4 Run:

```
ppp mp
```

The PPP interface is configured to work in Multilink PPP (MP) mode.

Step 5 Run:

```
ppp mp max-bind max-bind-number
```

The maximum number of links in an MP group is set.

By default, a maximum of 16 PPP links can be bound in an MP group.

----End

7.4.8 (Optional) Configuring Dial-Up Backup

The dial-up backup function dynamically maintains dial-up links based on routes.

Context

The dial-up backup function provides the backup and routing functions, and implements reliable connections and on-demand dialing function.

The dial-up backup function has the following characteristics:

- All routes can be backed up, including the routes generated by routing protocols, static routes, and direct routes.
- Dial-up backup is used between interfaces or routers, but not on a single interface or link.
- If the primary link is broken, the backup link automatically takes over. There is no delay during the switchover except the route convergence period.
- The dial-up backup function is applicable to all routing protocols, including RIP-1, RIP-2, OSPF, IS-IS, and BGP. However, some routing protocols such as BGP choose the optimal routes. If the primary link destined for the monitored network segment is broken, the backup link learns the routes destined for the monitored network segment using BGP. After the primary link recovers, the primary link re-learns the routes, but these routes may not be the optimal routes. The router still uses the routes learned by the backup link. As a result, the backup link cannot be disconnected and the dynamic route monitoring function fails.

  To address this issue:
  - Set the IP address of the backup link to be greater than the IP address of the primary link.
  - Configure load balancing so that one route is learned by multiple links.
- The dial-up backup function causes auto dialing unable to take effect.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
standby routing-rule group-number ip ip-address { mask | mask-length }
```

A dial-up backup group is created and the network segments to be monitored are added to the group.

Step 3 Run:

```
interface interface-type interface-number
```

Enter the interface view.

Step 4 Run:

```
standby routing-group group-number
```

The dial-up backup function is enabled on the interface.

By default, the dial-up backup function is disabled.

Before enabling the dial-up backup function, ensure that basic DCC functions are enabled and the dial-up backup group (configured by **standby routing-rule**) is configured on the interface.

Step 5 (Optional) Run:

```
standby timer routing-disable seconds
```

The delay in disconnecting the standby dialer interface is set.

This delay prevents route flapping after the routes in the network segment are recovered. By default, when the routes in a network segment are recovered, the system disconnects the standby dialer interface after a 20-second delay.

Step 6 Run:

```
quit
```

Return to the system view.

Step 7 (Optional) Run:

```
dialer timer warmup seconds
```

The warmup timer is configured.

By default, the warmup timer is 30 seconds.

After starting, the system restores configurations automatically. During configuration restoration, the main interface is in Down state, so the route on the main interface becomes unreachable. The system starts the backup link. After the configurations are restored, all interfaces become Up, and the call is set up on the backup link. However, after the route on the main interface is recovered, the backup link is disconnected. To prevent status flapping of the backup link after system startup, configure the warmup timer. The system will not use the backup link until the warmup timer expires.

----End

7.4.9 (Optional) Closing a Connection

To reduce network loads or adjust dialing configurations, you may need to tear down a dial-up link using the **dialer disconnect** command.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
dialer disconnect [ interface interface-type interface-number ]
```

A dial-up link is torn down.

After a dial-up link is torn down, all services on the link are interrupted; therefore, ensure that the link is not in use before you tear down the link.

This command only temporarily tears down dial-up links.

- If a disconnected link is enabled with the auto-dial function, it will be re-established when the dialer timer expires.
- If the link is not enabled with the auto-dial function, it will be re-established when data needs to be transmitted over it.

----End

7.4.10 Checking the Configuration

After RS-DCC is configured, view the dialup interface information.

Prerequisites

All configurations of RS-DCC are complete.

Procedure

Step 1 Run the **display dialer** [**interface** *interface-type interface-number*] command to check DCC information on the dialup interface.

Step 2 Run the **display interface dialer** [*number*] command to check information about the dialer interface.

----End

7.5 Maintaining DCC

This section describes how to maintain DCC, including clearing dialer interface statistics and monitoring DCC status.

7.5.1 Clearing Dialer Interface Statistics

This section describes how to clear dialer interface statistics.

Context

CAUTION

The statistics cannot be restored after being cleared. So, confirm the action before you use the command.

Procedure

Step 1 To clear statistics on the dialer interface, run the **reset counters interface** [**dialer** [*number*]] command in the user view.

----End

7.5.2 Monitoring the DCC Status

This section describes how to monitor DCC status using the display commands.

Context

In routine maintenance, you can run the following commands in any view to view the running status of DCC.

Procedure

Step 1 Run the **display dialer** [**interface** *interface-type interface-number*] command in any view to check DCC information.

Step 2 Run the **display interface dialer** [*number*] command in any view to check dialer interface information.

----End

7.6 Configuration Examples

This section provides DCC configuration examples, including networking requirements, configuration notes, and configuration roadmaps.

7.6.1 Example for Configuring C-DCC on an ISDN Network

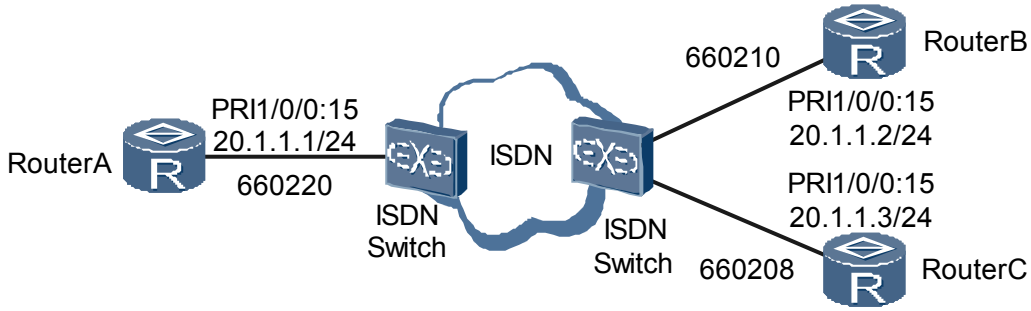
This example shows how to use ISDN PRI interfaces to configure C-DCC on an ISDN network.

Networking Requirements

As shown in **Figure 7-12**, RouterA, RouterB, and RouterC connect to an ISDN network through interfaces PRI1/0/0:15.

RouterA is the egress gateway of the headquarters. To reduce network construction costs, the enterprise applies for only one physical link from the carrier. RouterB and RouterC are the egress gateways of branches. The enterprise requires that the headquarters and branches establish connections to transmit data and disconnect the connections when there is no data to transmit. This dial-on-demand feature reduces costs for the enterprise. In addition, branches do not need to communicate with each other.

Figure 7-12 Configuring C-DCC on an ISDN network



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure C-DCC on RouterA and set the dialer numbers to 660210 and 660208 so that RouterA can initiate calls to and receive calls from RouterB and RouterC.
2. Configure C-DCC on RouterB and RouterC and set the dialer number to 660220 so that RouterB and RouterC can initiate calls to and receive calls from RouterA.

Data Preparation

To complete the configuration, you need the following data:

- On RouterA: IP address of the PRI interface and dialer numbers
- On RouterB: IP address of the PRI interface and dialer number
- On RouterC: IP address of the PRI interface and dialer number

Procedure

Step 1 Configure RouterA.

Configure dialer group 1 and the dialer ACL.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] dialer-rule
[RouterA-dialer-rule] dialer-rule 1 ip permit
[RouterA-dialer-rule] quit
```

Configure the physical interface.

```
[RouterA] controller e1 1/0/0
[RouterA-E1 1/0/0] pri-set
[RouterA-E1 1/0/0] quit
```

Assign an IP address to PRI1/0/0:15, enable C-DCC, and configure the dialer number.

```
[RouterA] interface Serial 1/0/0:15
[RouterA-Serial1/0/0:15] ip address 20.1.1.1 24
[RouterA-Serial1/0/0:15] dialer enable-circular
[RouterA-Serial1/0/0:15] dialer-group 1
[RouterA-Serial1/0/0:15] dialer route ip 20.1.1.2 660210
[RouterA-Serial1/0/0:15] dialer route ip 20.1.1.3 660208
```

Step 2 Configure RouterB.

Configure dialer group 2 and the dialer ACL.

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] dialer-rule
[RouterB-dialer-rule] dialer-rule 2 ip permit
[RouterB-dialer-rule] quit
```

Configure the physical interface.

```
[RouterB] controller e1 1/0/0
[RouterB-E1 1/0/0] pri-set
[RouterB-E1 1/0/0] quit
```

Assign an IP address to PRI1/0/0:15, enable C-DCC, and configure the dialer number.

```
[RouterB] interface Serial 1/0/0:15
[RouterB-Serial1/0/0:15] ip address 20.1.1.2 24
[RouterB-Serial1/0/0:15] dialer enable-circular
[RouterB-Serial1/0/0:15] dialer-group 2
[RouterB-Serial1/0/0:15] dialer route ip 20.1.1.1 660220
[RouterB-Serial1/0/0:15] quit
```

Step 3 Configure RouterC.

Configure dialer group 1 and the dialer ACL.

```
<Huawei> system-view
[Huawei] sysname RouterC
[RouterC] dialer-rule
[RouterC-dialer-rule] dialer-rule 1 ip permit
[RouterC-dialer-rule] quit
```

Configure the physical interface.

```
[RouterC] controller e1 1/0/0
[RouterC-E1 1/0/0] pri-set
[RouterC-E1 1/0/0] quit
```

Assign an IP address to PRI1/0/0:15, enable C-DCC, and configure the dialer number.

```
[RouterC] interface Serial 1/0/0:15
[RouterC-Serial1/0/0:15] ip address 20.1.1.3 24
[RouterC-Serial1/0/0:15] dialer enable-circular
[RouterC-Serial1/0/0:15] dialer-group 1
[RouterC-Serial1/0/0:15] dialer route ip 20.1.1.1 660220
```

----End

Configuration Files

Configuration file of RouterA

```
#
sysname RouterA
#
controller E1 1/0/0
 pri-set
#
interface Serial1/0/0:15
 link-protocol ppp
 ip address 20.1.1.1 255.255.255.0
 dialer enable-circular
 dialer-group 1
 dialer route ip 20.1.1.2 660210
 dialer route ip 20.1.1.3 660208
#
 dialer-rule
 dialer-rule 1 ip permit
```

Configuration file of RouterB

```
#
sysname RouterB
#
controller E1 1/0/0
 pri-set
#
interface Serial1/0/0:15
 link-protocol ppp
 ip address 20.1.1.2 255.255.255.0
 dialer enable-circular
 dialer-group 2
 dialer route ip 20.1.1.1 660220
#
 dialer-rule
 dialer-rule 2 ip permit
```

```
# Configuration file of RouterC
#
sysname RouterC
#
controller E1 1/0/0
 pri-set
#
interface Serial1/0/0:15
 link-protocol ppp
 ip address 20.1.1.3 255.255.255.0
 dialer enable-circular
 dialer-group 1
 dialer route ip 20.1.1.1 660220
#
 dialer-rule
 dialer-rule 1 ip permit
```

7.6.2 Example for Configuring RS-DCC on an ISDN Network

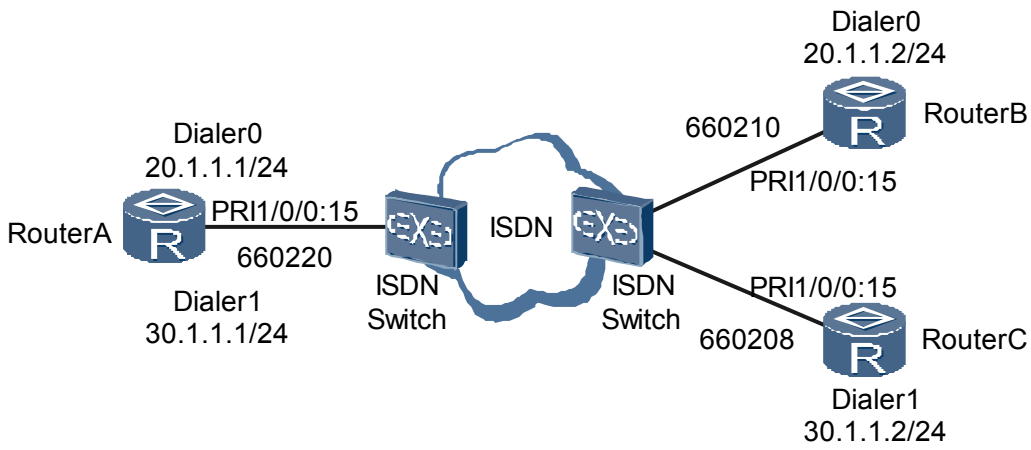
This example shows how to use ISDN PRI interfaces to configure RS-DCC on an ISDN network.

Networking Requirements

As shown in **Figure 7-13**, RouterA, RouterB, and RouterC connect to an ISDN network through interfaces PRI1/0/0:15.

RouterA is the egress gateway of the headquarters. To reduce network construction costs, the enterprise applies for only one physical link from the carrier. RouterB and RouterC are the egress gateways of branches. The enterprise requires that the headquarters and branches establish connections to transmit data and disconnect the connections when there is no data to transmit. This dial-on-demand feature reduces costs for the enterprise. Authentication is required when the headquarters and branches call each other. In addition, branches do not need to communicate with each other.

Figure 7-13 Configuring RS-DCC on an ISDN network



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure RS-DCC on RouterA and set the dialer numbers to 660210 and 660208 so that RouterA can initiate calls to and receive calls from RouterB and RouterC.
2. Configure RS-DCC on RouterB and RouterC and set the dialer number to 660220 so that RouterB and RouterC can initiate calls to and receive calls from RouterA.
3. Configure PAP authentication on the dialer interface and the PRI interface.

Data Preparation

To complete the configuration, you need the following data:

- On RouterA: IP address of the dialer interface and dialer numbers of the remote ends
- On RouterB: IP address of the dialer interface and dialer number of the remote end
- On RouterC: IP address of the dialer interface and dialer number of the remote end

Procedure

Step 1 Configure RouterA.

Configure dialer group 1 and the dialer ACL, and set the local user names for PPP authentication to userb and userc.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] dialer-rule
[RouterA-dialer-rule] dialer-rule 1 ip permit
[RouterA-dialer-rule] quit
[RouterA] aaa
[RouterA-aaa] local-user userb password simple userb
[RouterA-aaa] local-user userb service-type ppp
[RouterA-aaa] quit
[RouterA] aaa
[RouterA-aaa] local-user userc password simple userc
[RouterA-aaa] local-user userc service-type ppp
[RouterA-aaa] quit
```

Configure the physical interface.

```
[RouterA] controller e1 1/0/0
[RouterA-E1 1/0/0] pri-set
[RouterA-E1 1/0/0] quit
```

Assign an IP address to Dialer0 and enable RS-DCC, configure the user name allowed to perform dial-up, configure PAP authentication, and set the dialer number.

```
[RouterA] interface Dialer 0
[RouterA-Dialer0] link-protocol ppp
[RouterA-Dialer0] ppp authentication-mode pap
[RouterA-Dialer0] ppp pap local-user usera password simple usera
[RouterA-Dialer0] ip address 20.1.1.1 24
[RouterA-Dialer0] dialer user userb
[RouterA-Dialer0] dialer bundle 1
[RouterA-Dialer0] dialer-group 1
[RouterA-Dialer0] dialer number 660210
[RouterA-Dialer0] quit
```

Assign an IP address to Dialer1 and enable RS-DCC, configure the user name allowed to perform dial-up, configure PAP authentication, and set the dialer number.

```
[RouterA] interface Dialer 1
[RouterA-Dialer1] link-protocol ppp
[RouterA-Dialer1] ppp authentication-mode pap
[RouterA-Dialer1] ppp pap local-user usera password simple usera
[RouterA-Dialer1] ip address 30.1.1.1 24
```

```
[RouterA-Dialer1] dialer user userc
[RouterA-Dialer1] dialer bundle 2
[RouterA-Dialer1] dialer-group 1
[RouterA-Dialer1] dialer number 660208
[RouterA-Dialer1] quit
```

Set the link-layer protocol on PRI1/0/0:15 to PPP, configure PPP authentication, and add the interface to Dialer bundle 1 and Dialer bundle 2.

```
[RouterA] interface Serial 1/0/0:15
[RouterA-Serial1/0/0:15] dialer bundle-member 1
[RouterA-Serial1/0/0:15] dialer bundle-member 2
[RouterA-Serial1/0/0:15] link-protocol ppp
[RouterA-Serial1/0/0:15] ppp authentication-mode pap
[RouterA-Serial1/0/0:15] ppp pap local-user usera password simple usera
```

Step 2 Configure RouterB.

Configure dialer group 2 and the dialer ACL, and set the local user name for PPP authentication to usera.

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] dialer-rule
[RouterB-dialer-rule] dialer-rule 2 ip permit
[RouterB-dialer-rule] quit
[RouterB] aaa
[RouterB-aaa] local-user usera password simple usera
[RouterB-aaa] local-user usera service-type ppp
[RouterB-aaa] quit
```

Configure the physical interface.

```
[RouterB] controller e1 1/0/0
[RouterB-E1 1/0/0] pri-set
[RouterB-E1 1/0/0] quit
```

Assign an IP address to Dialer0 and enable RS-DCC, configure the user name allowed to perform dial-up, configure PAP authentication, and set the dialer number.

```
[RouterB] interface Dialer 0
[RouterB-Dialer0] link-protocol ppp
[RouterB-Dialer0] ppp authentication-mode pap
[RouterB-Dialer0] ppp pap local-user userb password simple userb
[RouterB-Dialer0] ip address 20.1.1.2 24
[RouterB-Dialer0] dialer user usera
[RouterB-Dialer0] dialer bundle 1
[RouterB-Dialer0] dialer-group 2
[RouterB-Dialer0] dialer number 660220
[RouterB-Dialer0] quit
```

Set the link-layer protocol on PRI1/0/0:15 to PPP, configure PPP authentication, and add the interface to Dialer bundle 1.

```
[RouterB] interface Serial 1/0/0:15
[RouterB-Serial1/0/0:15] dialer bundle-member 1
[RouterB-Serial1/0/0:15] link-protocol ppp
[RouterB-Serial1/0/0:15] ppp authentication-mode pap
[RouterB-Serial1/0/0:15] ppp pap local-user userb password simple userb
```

Step 3 Configure RouterC.

Configure dialer group 1 and the dialer ACL, and set the local user name for PPP authentication to usera.

```
<Huawei> system-view
[Huawei] sysname RouterC
[RouterC] dialer-rule
```

```
[RouterC-dialer-rule] dialer-rule 1 ip permit
[RouterC-dialer-rule] quit
[RouterC] aaa
[RouterC-aaa] local-user usera password simple usera
[RouterC-aaa] local-user usera service-type ppp
[RouterC-aaa] quit
```

Configure the physical interface.

```
[RouterC] controller e1 1/0/0
[RouterC-E1 1/0/0] pri-set
[RouterC-E1 1/0/0] quit
```

Assign an IP address to Dialer1 and enable RS-DCC, configure the user name allowed to perform dial-up, configure PAP authentication, and set the dialer number.

```
[RouterC] interface Dialer 1
[RouterC-Dialer1] link-protocol ppp
[RouterC-Dialer1] ppp authentication-mode pap
[RouterC-Dialer1] ppp pap local-user userc password simple userc
[RouterC-Dialer1] ip address 30.1.1.2 24
[RouterC-Dialer1] dialer user usera
[RouterC-Dialer1] dialer bundle 1
[RouterC-Dialer1] dialer-group 1
[RouterC-Dialer1] dialer number 660220
[RouterC-Dialer1] quit
```

Set the link-layer protocol on PRI1/0/0:15 to PPP, configure PPP authentication, and add the interface to Dialer bundle 1.

```
[RouterC] interface Serial 1/0/0:15
[RouterC-Serial1/0/0:15] dialer bundle-member 1
[RouterC-Serial1/0/0:15] link-protocol ppp
[RouterC-Serial1/0/0:15] ppp authentication-mode pap
[RouterC-Serial1/0/0:15] ppp pap local-user userc password simple userc
```

----End

Configuration Files

Configuration file of RouterA

```
#
sysname RouterA
#
aaa
 local-user userb password simple userb
 local-user userb service-type ppp
 local-user userc password simple userc
 local-user userc service-type ppp
#
controller E1 1/0/0
 pri-set
#
interface Dialer0
 link-protocol ppp
 ppp authentication-mode pap
 ppp pap local-user usera password simple usera
 ip address 20.1.1.1 255.255.255.0
 dialer user userb
 dialer bundle 1
 dialer number 660210
 dialer-group 1
#
interface Dialer1
 link-protocol ppp
 ppp authentication-mode pap
 ppp pap local-user usera password simple usera
 ip address 30.1.1.1 255.255.255.0
```

```
 dialer user userc
 dialer bundle 2
 dialer number 660208
 dialer-group 1
#
interface Serial1/0/0:15
 link-protocol ppp
 ppp authentication-mode pap
 ppp pap local-user usera password simple usera
 dialer bundle-member 1
 dialer bundle-member 2
#
 dialer-rule
 dialer-rule 1 ip permit
#
return
```

Configuration file of RouterB

```
#
sysname RouterB
#
aaa
 local-user usera password simple usera
 local-user usera service-type ppp
#
controller E1 1/0/0
 pri-set
#
interface Dialer0
 link-protocol ppp
 ppp authentication-mode pap
 ppp pap local-user userb password simple userb
 ip address 20.1.1.2 255.255.255.0
 dialer user usera
 dialer bundle 1
 dialer number 660220
 dialer-group 2
#
interface Serial1/0/0:15
 link-protocol ppp
 ppp authentication-mode pap
 ppp pap local-user userb password simple userb
 dialer bundle-member 1
#
 dialer-rule
 dialer-rule 2 ip permit
#
return
```

Configuration file of RouterC

```
#
sysname RouterC
#
aaa
 local-user usera password simple usera
 local-user usera service-type ppp
#
controller E1 1/0/0
 pri-set
#
interface Dialer1
 link-protocol ppp
 ppp authentication-mode pap
 ppp pap local-user userc password simple userc
 ip address 30.1.1.2 255.255.255.0
 dialer user usera
 dialer bundle 1
 dialer number 660220
 dialer-group 1
#
```

```
interface Serial1/0/0:15
 link-protocol ppp
 ppp authentication-mode pap
 ppp pap local-user userc password simple userc
 dialer bundle-member 1
#
 dialer-rule
 dialer-rule 1 ip permit
#
return
```

7.6.3 Example for Configuring Link Backup by Using the Interface Backup Mode on an ISDN Network (C-DCC+Dialer Number Backup)

This example shows how to configure link backup using the interface backup mode on an ISDN network.

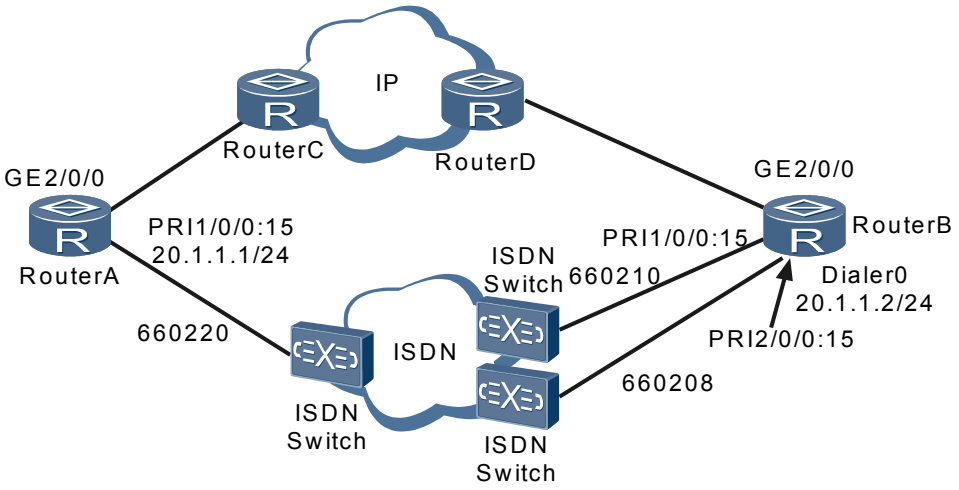
Networking Requirements

As shown in **Figure 7-14**, RouterA connects to an ISDN network through PRI1/0/0:15 and an IP network through GigabitEthernet2/0/0. RouterB connects to an ISDN network through PRI1/0/0:15 and PRI2/0/0:15 and an IP network through GigabitEthernet2/0/0.

RouterA is the egress gateway of the headquarters. RouterB is located in a branch.

RouterA communicates with RouterB over an IP network. However, if GigabitEthernet2/0/0 of RouterA is faulty, the headquarters and the branch cannot exchange data. To prevent this fault, the enterprise leases an ISDN line as a backup of the IP network. The ISDN line is used only when faults occur on the IP network. This improves communication reliability.

Figure 7-14 Configuring link backup using the interface backup mode on an ISDN network



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure C-DCC on RouterA and set the dialer numbers to 660210 and 660208 so that RouterA can initiate calls to and receive calls from RouterB. In addition, each configured dialer number acts as a backup to the other.
2. Configure the PRI interface of RouterA as the backup for GigabitEthernet2/0/0. When GigabitEthernet2/0/0 is faulty, traffic is switched to the PRI interface.

Data Preparation

To complete the configuration, you need the following data:

- On RouterA: IP address of the PRI interface, dialer number and IP address of the remote end, and network segment running RIP
- On RouterB: IP address of the dialer interface, dialer number and IP address of the remote end, and network segment running RIP

Procedure

Step 1 Configure RouterA.

Configure dialer group 1 and the dialer ACL.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] dialer-rule
[RouterA-dialer-rule] dialer-rule 1 ip permit
[RouterA-dialer-rule] quit
```

Configure the physical interface.

```
[RouterA] controller e1 1/0/0
[RouterA-E1 1/0/0] pri-set
[RouterA-E1 1/0/0] quit
```

Assign an IP address to PRI1/0/0:15, enable C-DCC, and configure the dialer number.

```
[RouterA] interface Serial 1/0/0:15
[RouterA-Serial1/0/0:15] ip address 20.1.1.1 24
[RouterA-Serial1/0/0:15] dialer enable-circular
[RouterA-Serial1/0/0:15] dialer-group 1
[RouterA-Serial1/0/0:15] dialer route ip 20.1.1.2 broadcast 660210
[RouterA-Serial1/0/0:15] dialer route ip 20.1.1.2 broadcast 660208
[RouterA-Serial1/0/0:15] quit
```

Configure a backup interface for GigabitEthernet2/0/0.

```
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] standby interface Serial 1/0/0:15
[RouterA-GigabitEthernet2/0/0] quit
```

Configure a routing protocol.

```
[RouterA] rip
[RouterA-rip-1] network 20.0.0.0
[RouterA-rip-1] import-route direct
[RouterA-rip-1] quit
```

Step 2 Configure RouterB.

Configure dialer group 2 and the dialer ACL.

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] dialer-rule
[RouterB-dialer-rule] dialer-rule 2 ip permit
```

Configure the physical interface.

```
[RouterB] controller e1 1/0/0
[RouterB-E1 1/0/0] pri-set
[RouterB-E1 1/0/0] quit
[RouterB] controller e1 2/0/0
[RouterB-E1 2/0/0] pri-set
[RouterB-E1 2/0/0] quit
```

Assign an IP address to Dialer0, enable C-DCC, and configure the dialer number.

```
[RouterB] interface Dialer 0
[RouterB-Dialer0] ip address 20.1.1.2 24
[RouterB-Dialer0] dialer enable-circular
[RouterB-Dialer0] dialer-group 2
[RouterB-Dialer0] dialer route ip 20.1.1.1 broadcast 660220
[RouterB-Dialer0] quit
```

Add PRI1/0/0:15 and PRI2/0/0:15 to the dialer circular group.

```
[RouterB] interface Serial 1/0/0:15
[RouterB-Serial1/0/0:15] dialer circular-group 0
[RouterB-Serial1/0/0:15] quit
[RouterB] interface Serial 2/0/0:15
[RouterB-Serial2/0/0:15] dialer circular-group 0
[RouterB-Serial2/0/0:15] quit
```

Configure a routing protocol.

```
[RouterB] rip
[RouterB-rip-1] network 20.0.0.0
[RouterB-rip-1] import-route direct
[RouterB-rip-1] quit
```

----End

Configuration Files

Configuration file of RouterA

```
#
sysname RouterA
#
controller E1 1/0/0
 pri-set
#
interface Serial1/0/0:15
 link-protocol ppp
 ip address 20.1.1.1 255.255.255.0
 dialer enable-circular
 dialer-group 1
 dialer route ip 20.1.1.2 broadcast
660210
 dialer route ip 20.1.1.2 broadcast 660208
#
interface GigabitEthernet2/0/0
 standby interface Serial1/0/0:15
#
 dialer-rule
 dialer-rule 1 ip permit
#
rip 1
 network 20.0.0.0
 import-route direct
#
return
```

Configuration file of RouterB

```
#
sysname RouterB
```

```
#
controller E1 1/0/0
 pri-set
#
controller E1 2/0/0
 pri-set
#
interface Dialer0
 link-protocol ppp
 ip address 20.1.1.2 255.255.255.0
 dialer enable-circular
 dialer-group 2
 dialer route ip 20.1.1.1 broadcast 660220
#
interface Serial1/0/0:15
 link-protocol ppp
 dialer circular-group 0
#
interface Serial2/0/0:15
 link-protocol ppp
 dialer circular-group 0
#
 dialer-rule
 dialer-rule 2 ip permit
#
rip 1
 network 20.0.0.0
 import-route direct
#
return
```

7.6.4 Example for Configuring Link Backup in Interface Backup Mode on a 3G Network (C-DCC)

This section describes how to configure link backup in interface backup mode on a 3G network.

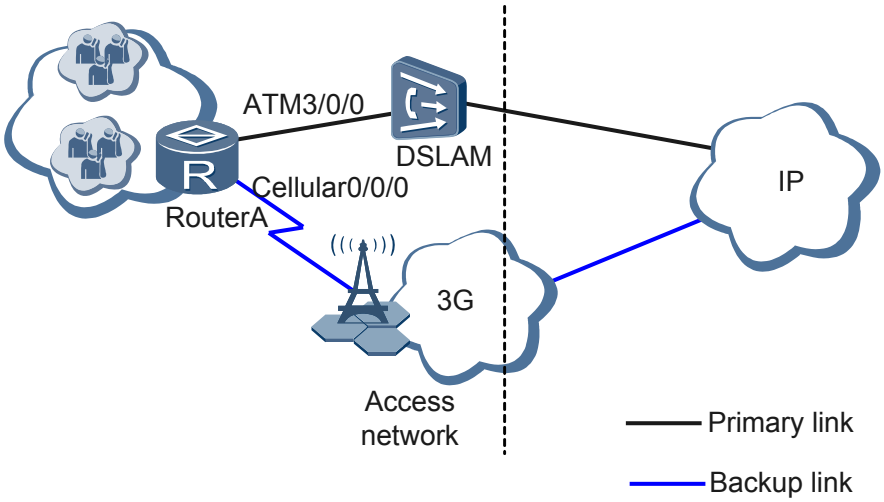
Networking Requirements

As shown in **Figure 7-15**, RouterA is an egress gateway of an enterprise. RouterA connects to an IP network using an ADSL interface in normal situations. However, if the ADSL interface is faulty, enterprise users cannot connect to the IP network. To prevent this fault, the enterprise uses the backup interface (a 3G interface in **Figure 7-15**) to connect to the IP network. Backing up the enterprise's outbound interface improves line reliability.

NOTE

Figure 7-15 shows only the access-side networking. Deploy devices on the aggregation and core networks according to site requirements.

Figure 7-15 Networking diagram of link backup configurations in interface backup mode on a 3G network



Configuration Roadmap

1. Configure an enterprise intranet, specify RouterA as an egress gateway of the enterprise, and configure RouterA to assign IP addresses to users in the enterprise.
2. Configure the uplink primary interface of RouterA.
3. Configure the uplink backup interface of RouterA.
4. Configure a static route so that RouterA can connect to the WAN.

Data Preparation

To complete the configuration, you need the following data:

- Downlink interface: Layer 2 Ethernet interface number, intranet network segment, and IP address pool from which RouterA assigns IP addresses to intranet users
- Uplink primary interface: interface number, IP address segment on which IP addresses need to be translated using NAT, backup interface number, and interface switching delay
- Uplink backup interface: interface number, IP address segment on which IP addresses need to be translated using NAT, dial-up parameters (including the dial rule, allowed idle duration, dial group number, and dial string)
- Static route: destination IP address, mask, and outbound interface type and number

Procedure

Step 1 Configure an enterprise intranet and specify RouterA as the egress gateway of the enterprise.

Assume that the enterprise intranet uses only one network segment 192.168.100.1/24 and intranet users connect to RouterA through Layer 2 Ethernet interface Ethernet2/0/0.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] vlan 123
[RouterA-vlan123] quit
[RouterA] dhcp enable
```

```
[RouterA] interface vlanif 123
[RouterA-Vlanif123] ip address 192.168.100.1 255.255.255.0
[RouterA-Vlanif123] dhcp select global
[RouterA-Vlanif123] quit
[RouterA] ip pool lan
[RouterA-ip-pool-lan] gateway-list 192.168.100.1
[RouterA-ip-pool-lan] network 192.168.100.0 mask 24
[RouterA-ip-pool-lan] quit
[RouterA] interface ethernet 2/0/0
[RouterA-Ethernet2/0/0] port link-type hybrid
[RouterA-Ethernet2/0/0] port hybrid pvid vlan 123
[RouterA-Ethernet2/0/0] port hybrid untagged vlan 123
[RouterA-Ethernet2/0/0] quit
```

Step 2 Configure the uplink primary interface of RouterA.

NOTE

This example only describes the configuration of the uplink primary interface. For details about other uplink devices, see the related manuals.

```
[RouterA] acl number 3002
[RouterA-acl-adv-3002] rule 5 permit ip source 192.168.100.0 0.0.0.255
[RouterA-acl-adv-3002] quit
[RouterA] interface virtual-template 10
[RouterA-Virtual-Template10] ip address ppp-negotiate
[RouterA-Virtual-Template10] nat outbound 3002
[RouterA-Virtual-Template10] quit
[RouterA] interface atm 3/0/0
[RouterA-Atm3/0/0] pvc voip 1/35
[RouterA-atm-pvc-Atm3/0/0-1/35-voip] map ppp virtual-template 10
[RouterA-atm-pvc-Atm3/0/0-1/35-voip] quit
[RouterA-Atm3/0/0] standby interface Cellular 0/0/0
[RouterA-Atm3/0/0] standby timer delay 10 10
[RouterA-Atm3/0/0] quit
```

Step 3 Configure the uplink backup interface of RouterA.

In this example, the connected 3G network is a WCDMA network. To connect to the PS region of the WCDMA network, set the dial string to *99#.

The APN name must be the same as that of the carrier. In this example, the name of the connected APN is wcdma.

NOTE

Before configuring interface backup, ensure that a 3G modem and the SIM/UIM card are properly installed.

This example describes only the configuration of the uplink backup interface. For details about other uplink devices, see the related manuals.

```
[RouterA] dialer-rule
[RouterA-dialer-rule] dialer-rule 1 ip permit
[RouterA-dialer-rule] quit
[RouterA] interface Cellular 0/0/0
[RouterA-Cellular0/0/0] profile create 1 static wcdma
[RouterA-Cellular0/0/0] link-protocol ppp
[RouterA-Cellular0/0/0] ip address ppp-negotiate
[RouterA-Cellular0/0/0] dialer enable-circular
[RouterA-Cellular0/0/0] dialer-group 1
[RouterA-Cellular0/0/0] dialer timer idle 0
Info: The configuration will take effect for the next call.
[RouterA-Cellular0/0/0] dialer number *99#
[RouterA-Cellular0/0/0] nat outbound 3002
[RouterA-Cellular0/0/0] quit
```

Step 4 Configure a static route.

```
[RouterA] ip route-static 0.0.0.0 0.0.0.0 virtual-template 10
[RouterA] ip route-static 0.0.0.0 0.0.0.0 cellular 0/0/0
```

----End

Configuration Files

Configuration file of RouterA

```
#
 sysname RouterA
#
 vlan batch 123
#
 dhcp enable
#
 acl number 3002
 rule 5 permit ip source 192.168.100.0 0.0.0.255
#
 ip pool lan
 gateway-list 192.168.100.1
 network 192.168.100.0 mask 255.255.255.0
#
interface Vlanif123
 ip address 192.168.100.1 255.255.255.0
 dhcp select global
#
interface Ethernet2/0/0
 port hybrid pvid vlan 123
 port hybrid untagged vlan
123
#
interface Cellular0/0/0
 link-protocol ppp
 ip address ppp-negotiate
 dialer enable-circular
 dialer-group 1
 dialer timer idle 0
 dialer number *99#
 nat outbound 3002
#
interface Atm3/0/0
 pvc voip 1/35
  map ppp Virtual-Template10
 standby interface Cellular0/0/0
 standby timer delay 10 10
#
interface Virtual-Template10
 ip address ppp-negotiate
 nat outbound 3002
#
dialer-rule
 dialer-rule 1 ip permit
#
 ip route-static 0.0.0.0 0.0.0.0 Virtual-Template 10
 ip route-static 0.0.0.0 0.0.0.0 cellular 0/0/0
#
return
```

7.6.5 Example for Configuring Link Backup by Using the Dial-Up Backup Mode on an ISDN Network (RS-DCC+MP Group)

This example shows how to configure link backup using the dial-up backup mode on an ISDN network.

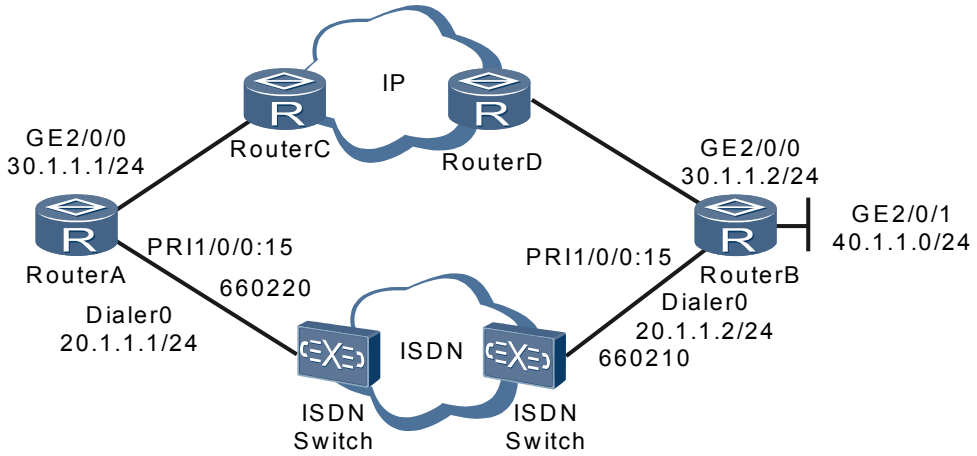
Networking Requirements

As shown in **Figure 7-16**, RouterA and RouterB are connected by an IP network and an ISDN network.

RouterA is the egress gateway of the headquarters. RouterB is the egress gateway of a branch.

RouterA communicates with RouterB over an IP network. However, if the IP network is faulty, the headquarters and the branch cannot exchange data. To prevent this fault, the enterprise uses the ISDN network as the backup of the IP network. The ISDN line is used only when faults occur on the IP network. Communication reliability is improved. The minimum transmission rate of the ISDN line is 1 Mbit/s.

Figure 7-16 Configuring link backup using the dial-up backup mode on an ISDN network



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure RS-DCC on RouterA and set the dialer number to 660210 so that RouterA can initiate calls to and receive calls from RouterB.
2. Configure RS-DCC on RouterB and set the dialer number to 660220 so that RouterB can initiate calls to and receive calls from RouterA.
3. Configure dial-up backup on RouterA. If there is no reachable route to network segment 40.1.1.0/24, traffic is switched from the IP network to the ISDN network.
4. Configure an MP group on RouterA to achieve 1 Mbit/s transmission rate on the ISDN network.

Data Preparation

To complete the configuration, you need the following data:

- On RouterA: IP address of the dialer interface and dialer number of the remote end, and the network segment running RIP
- On RouterB: IP address of the dialer interface and dialer number of the remote end, and the network segment running RIP

Procedure

Step 1 Configure RouterA.

Configure dialer group 1 and the dialer ACL, and set the local user name for PPP authentication to userb.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] dialer-rule
[RouterA-dialer-rule] dialer-rule 1 ip permit
[RouterA-dialer-rule] quit
[RouterA] aaa
[RouterA-aaa] local-user userb password simple userb
[RouterA-aaa] local-user userb service-type ppp
[RouterA-aaa] quit
```

Configure the physical interface.

```
[RouterA] controller e1 1/0/0
[RouterA-E1 1/0/0] pri-set
[RouterA-E1 1/0/0] quit
```

Assign an IP address to Dialer0 and enable RS-DCC, configure the user name allowed to perform dial-up, configure PAP authentication, and set the dialer number.

```
[RouterA] interface Dialer 0
[RouterA-Dialer0] link-protocol ppp
[RouterA-Dialer0] ppp authentication-mode pap
[RouterA-Dialer0] ppp pap local-user usera password simple usera
[RouterA-Dialer0] ppp mp
[RouterA-Dialer0] ip address 20.1.1.1 24
[RouterA-Dialer0] dialer user userb
[RouterA-Dialer0] dialer bundle 1
[RouterA-Dialer0] dialer-group 1
[RouterA-Dialer0] dialer number 660210
[RouterA-Dialer0] quit
```

Set the link-layer protocol on PRI1/0/0:15 to PPP, configure PPP authentication, and add the interface to Dialer bundle 1.

```
[RouterA] interface Serial 1/0/0:15
[RouterA-Serial1/0/0:15] dialer bundle-member 1
[RouterA-Serial1/0/0:15] link-protocol ppp
[RouterA-Serial1/0/0:15] ppp mp
[RouterA-Serial1/0/0:15] ppp authentication-mode pap
[RouterA-Serial1/0/0:15] ppp pap local-user usera password simple usera
[RouterA-Serial1/0/0:15] quit
```

Configure a routing protocol.

```
[RouterA] rip
[RouterA-rip-1] network 30.0.0.0
[RouterA-rip-1] network 20.0.0.0
[RouterA-rip-1] import-route direct
[RouterA-rip-1] quit
```

Configure dial-up backup.

```
[RouterA] standby routing-rule 1 ip 40.1.1.0 24
[RouterA] interface Dialer 0
[RouterA-Dialer0] standby routing-group 1
[RouterA-Dialer0] quit
```

Step 2 Configure RouterB.

Configure dialer group 2 and the dialer ACL, and set the local user name for PPP authentication to usera.

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] dialer-rule
[RouterB-dialer-rule] dialer-rule 2 ip permit
[RouterB-dialer-rule] quit
[RouterB] aaa
[RouterB-aaa] local-user usera password simple usera
```

```
[RouterB-aaa] local-user usera service-type ppp
[RouterB-aaa] quit
```

Configure the physical interface.

```
[RouterB] controller e1 1/0/0
[RouterB-E1 1/0/0] pri-set
[RouterB-E1 1/0/0] quit
```

Assign an IP address to Dialer0 and enable RS-DCC, configure the user name allowed to perform dial-up, configure PAP authentication, and set the dialer number.

```
[RouterB] interface Dialer 0
[RouterB-Dialer0] link-protocol ppp
[RouterB-Dialer0] ppp authentication-mode pap
[RouterB-Dialer0] ppp pap local-user userb password simple userb
[RouterB-Dialer0] ppp mp
[RouterB-Dialer0] ip address 20.1.1.2 24
[RouterB-Dialer0] dialer user usera
[RouterB-Dialer0] dialer bundle 1
[RouterB-Dialer0] dialer-group 2
[RouterB-Dialer0] dialer number 660220
[RouterB-Dialer0] quit
```

Set the link-layer protocol on PRI1/0/0:15 to PPP, configure PPP authentication, and add the interface to Dialer bundle 1.

```
[RouterB] interface Serial 1/0/0:15
[RouterB-Serial1/0/0:15] dialer bundle-member 1
[RouterB-Serial1/0/0:15] link-protocol ppp
[RouterA-Serial1/0/0:15] ppp mp
[RouterB-Serial1/0/0:15] ppp authentication-mode pap
[RouterB-Serial1/0/0:15] ppp pap local-user userb password simple userb
```

Configure a routing protocol.

```
[RouterB] rip
[RouterB-rip-1] network 10.0.0.0
[RouterB-rip-1] network 20.0.0.0
[RouterB-rip-1] network 40.0.0.0
[RouterB-rip-1] import-route direct
[RouterB-rip-1] quit
```

----End

Configuration Files

Configuration file of RouterA

```
#
sysname RouterA
#
 standby routing-rule 1 ip 40.1.1.0 255.255.255.0
#
aaa
 local-user userb password simple userb
 local-user userb service-type ppp
#
controller E1 1/0/0
 pri-set
#
interface Dialer0
 link-protocol ppp
 ppp authentication-mode pap
 ppp pap local-user usera password simple usera
 ppp mp
 ip address 20.1.1.1 255.255.255.0
 dialer user userb
 dialer bundle 1
```

```
 dialer number 660210
 standby routing-group 1
 dialer-group
1
#
interface Serial1/0/0:15
 link-protocol ppp
 ppp mp
 ppp authentication-mode pap
 ppp pap local-user usera password simple usera
 dialer bundle-member 1
#
 dialer-rule
 dialer-rule 1 ip permit
#
rip 1
 network 30.0.0.0
 network 20.0.0.0
 import-route direct
#
return
```

Configuration file of RouterB

```
#
sysname RouterB
#
aaa
 local-user usera password simple usera
 local-user usera service-type ppp
#
controller E1 1/0/0
 pri-set
#
interface Dialer0
 link-protocol ppp
 ppp authentication-mode pap
 ppp pap local-user userb password simple userb
 ppp mp
 ip address 20.1.1.2 255.255.255.0
 dialer user userb
 dialer bundle 1
 dialer number 660220
 dialer-group 2
#
interface Serial1/0/0:15
 link-protocol ppp
 ppp mp
 ppp authentication-mode pap
 ppp pap local-user userb password simple userb
 dialer bundle-member 1
#
 dialer-rule
 dialer-rule 2 ip permit
#
rip 1
 network 10.0.0.0
 network 20.0.0.0
 network 40.0.0.0
 import-route direct
#
return
```

7.6.6 Example for Configuring Link Backup by Using the Dial-Up Backup Mode on an ISDN Network (C-DCC)

This example shows how to configure Link Backup by Using the Dial-Up Backup Mode on an ISDN Network.

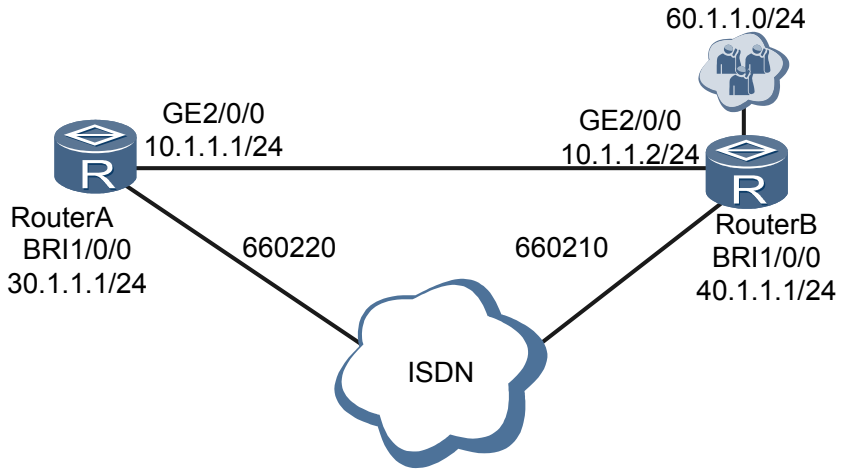
Networking Requirements

As shown in **Figure 7-17**, RouterA and RouterB are connected by an IP network and an ISDN network.

RouterA is the egress gateway of the headquarters. RouterB is the egress gateway of a branch.

RouterA communicates with RouterB over an IP network. However, if the IP network is faulty, the headquarters and the branch cannot exchange data. To prevent this fault, the enterprise uses the ISDN network as the backup of the IP network. The ISDN line is used only when faults occur on the IP network.

Figure 7-17 Link backup in dial-up backup mode



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure C-DCC on RouterA and set destination IP addresses so that RouterA can initiate calls to and receive calls from RouterB.
2. Configure dial-up backup on RouterA. If there is no reachable route to network segments 60.1.1.0/24, traffic is switched from the IP network to the ISDN network.

Data Preparation

To complete the configuration, you need the following data:

- RouterA: GE interface's IP address, dialer interface's IP address, network segment where destination addresses are located, RIP-enabled network segment, dial-up backup group, and rule in the dial-up backup group
- RouterB: GE interface's IP address, dialer interface's IP address, network segment where destination addresses are located, and RIP-enabled network segment

Procedure

Step 1 Configure RouterA.

Assign an IP address to a GE interface.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip address 10.1.1.1 24
[RouterA-GigabitEthernet2/0/0] quit
```

Create dialer group 1 and configure a dialer rule in the group.

```
[RouterA] dialer-rule
[RouterA-dialer-rule] dialer-rule 1 ip permit
[RouterA-dialer-rule] quit
```

Assign an IP address to the dialer interface, enable C-DCC, and configure destination addresses.

```
[RouterA] interface bri 1/0/0
[RouterA-Bri1/0/0] ip address 30.1.1.1 24
[RouterA-Bri1/0/0] dialer enable-circular
[RouterA-Bri1/0/0] dialer-group 1
[RouterA-Bri1/0/0] dialer route ip 40.1.1.1 broadcast 660210
[RouterA-Bri1/0/0] quit
```

Configure dynamic routes.

```
[RouterA] rip
[RouterA-rip-1] network 30.0.0.0
[RouterA-rip-1] network 20.0.0.0
[RouterA-rip-1] network 10.0.0.0
[RouterA-rip-1] import-route direct
[RouterA-rip-1] quit
```

Configure dial-up backup.

```
[RouterA] standby routing-rule 1 ip 60.1.1.0 24
[RouterA] interface bri 1/0/0
[RouterA-Bri1/0/0] standby routing-group 1
[RouterA-Bri1/0/0] quit
```

Step 2 Configure RouterB.

Assign an IP address to a GE interface.

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] ip address 10.1.1.2 24
[RouterB-GigabitEthernet2/0/0] quit
```

Create dialer group 1 and configure a dialer rule in the group.

```
[RouterB] dialer-rule
[RouterB-dialer-rule] dialer-rule 1 ip permit
[RouterB-dialer-rule] quit
```

Assign an IP address to the dialer interface and enable C-DCC.

```
[RouterB] interface bri 1/0/0
[RouterB-Bri1/0/0] ip address 40.1.1.1 24
[RouterB-Bri1/0/0] dialer enable-circular
[RouterB-Bri1/0/0] dialer-group 1
[RouterB-Bri1/0/0] dialer route ip 30.1.1.1 broadcast 660220
[RouterB-Bri1/0/0] quit
```

Configure dynamic routes.

```
[RouterB] rip
[RouterB-rip-1] network 10.0.0.0
[RouterB-rip-1] network 40.0.0.0
```

```
[RouterB-rip-1] import-route direct
[RouterB-rip-1] quit
```

Step 3 Configure RouterC.

The configuration of RouterC is similar to that of RouterB, and is not mentioned here.

----End

Configuration Files

Configuration file of RouterA

```
#
sysname RouterA
#
 standby routing-rule 1 ip 60.1.1.0 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 10.1.1.1 255.255.255.0
#
interface Bri1/0/0
 link-protocol ppp
 ip address 30.1.1.1 255.255.255.0
 dialer enable-circular
 dialer-group 1
 dialer route ip 40.1.1.1 broadcast 660210
 standby routing-group 1
#
dialer-rule
 dialer-rule 1 ip permit
#
rip 1
 network 30.0.0.0
 network 20.0.0.0
 network 10.0.0.0
 import-route direct
```

Configuration file of RouterB

```
#
sysname RouterB
#
interface GigabitEthernet2/0/0
 ip address 10.1.1.2 255.255.255.0
#
interface Bri1/0/0
 ip address 40.1.1.1 255.255.255.0
 dialer enable-circular
 dialer-group 1
 dialer route ip 30.1.1.1 broadcast 660220
#
 dialer-rule
 dialer-rule 1 ip permit
#
rip 1
 network 10.0.0.0
 network 40.0.0.0
 network 60.0.0.0
 import-route direct
#
return
```

8 Modem Configuration

About This Chapter

A modem is a widely used network device. The AR2200 uses a modem to communicate with devices on a Public Switched Telephone Network (PSTN).

8.1 Overview

This section describes a modem and its functions on a PSTN.

Concept

Traditional data communication systems communicate with each other over the PSTN. Analog signals are transmitted on a PSTN. As the Internet develops rapidly, IP-based communication systems have been well developed and widely applied. Digital signals are transmitted on IP networks and terminals. A modem enables devices on an IP network to communicate with devices on a PTSN without changing deployment on the PTSN. A modem converts analog to digital signals, as well as digital to analog signals.

Many manufacturers produce different types of modems. These modems support the standard AT command set but differ in implementation and configuration commands, making it difficult to manage modems. To facilitate modem management, configure the modem function on the AR2200. The AR2200 can communicate with devices on a PSTN through a modem.

Applications

As shown in **Figure 8-1**, RouterA and RouterB connect to the PSTN through ModemA and ModemB. The modem function is configured on RouterA and RouterB to allow the two routers to communicate with each other over the PSTN. When RouterA, functioning as the calling party, needs to exchange data with RouterB, RouterA sends an AT command to instruct ModemA to dial the number of RouterB. RouterB receives the incoming call signal and decides whether to send an AT command to enable ModemB to answer the call according to the modem answer mode configuration.

Figure 8-1 Modem networking diagram

8.2 Modem Features Supported by the AR2200

This section describes the modem features supported by the AR2200.

You can perform the following modem configurations on the AR2200:

- Set modem call-in and call-out permissions.
- Set the modem answer mode.
- Configure a modem using AT commands.

NOTE

Currently, only the asynchronous serial interfaces on the 8AS board support the modem function.

8.3 Configuring a Modem for Interworking on a PSTN

You can set the call-in permission, call-out permission, and answer mode for a modem, and use AT commands to configure the modem function.

8.3.1 Establishing the Configuration Task

Before configuring a modem, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task quickly and accurately.

Applicable Environment

As shown in **Figure 8-2**, RouterA and RouterB connect to the PSTN through ModemA and ModemB. Configure the routers to manage the modems for data service transmission.

Figure 8-2 Networking diagram for modem management

Pre-configuration Tasks

Before configuring a modem, complete the following tasks:

- Starting the modem
- Connecting the modem to the routers
- Configuring C-DCC according to **7.3 Configuring C-DCC**

Data Preparation

To configure a modem, you need the following data.

No.	Data
1	Number of the TTY user interface
2	(Optional) Modem answer timeout period

8.3.2 Setting the Modem Call-in and Call-out Permissions

When the router needs to communicate with devices on the PSTN through a modem, set modem call-in and call-out permissions.

Context

To enable the router to communicate with devices on the PSTN through a modem, set modem call-in and call-out permissions in the TTY user interface view. Configure the calling router to allow modem call-in and call-out and the called router to allow only modem call-in.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
user-interface tty ui-number
```

The TTY user interface view is displayed.

NOTE

- To view the TTY user interface number of an asynchronous serial interface, run the **display user-interface** command.
- If the redirection function is enabled on a TTY user interface, the modem function does not take effect.

Step 3 Set modem call-in and call-out permissions.

Run the following commands according to networking requirements.

- Run:

  ```
  modem call-in
  ```

  Only modem call-in is allowed.
- Run:

  ```
  modem both
  ```

  Both modem call-in and call-out are allowed.

By default, the AR2200 does not allow modem call-in or call-out.

----End

8.3.3 (Optional) Setting the Modem Answer Mode

You can set the modem answer mode and modem answer timeout period according to networking requirements.

Context

There are two modem answer modes: auto-answer mode and non-auto answer mode. If the AA indicator of a modem is on, the modem works in auto-answer mode. The modem answer mode configured on a router must be the same as the answer mode of the modem connected to the router asynchronous serial interface.

- If the modem works in auto-answer mode, run the **modem auto-answer** command before using the dialing function.
- If the modem works in non-auto answer mode, run the **undo modem auto-answer** command.

NOTE

The modem answer mode configured on a router must be the same as the answer mode of the modem connected to the router asynchronous serial interface. If the two answer modes are different, the modem may fail to function properly.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
user-interface tty ui-number
```

The TTY user interface view is displayed.

Step 3 Set the modem answer mode.

Run the following commands according to networking requirements.

- Run:

  ```
  modem auto-answer
  ```

  The modem is configured to work in auto-answer mode.

- Run:

  ```
  undo modem auto-answer
  ```

  The modem is configured to work in non-auto answer mode.

By default, a modem works in non-auto answer mode.

Step 4 (Optional) Run:

```
modem timer answer seconds
```

The modem answer timeout period is set.

By default, the modem answer timeout period is 30s.

NOTE

During modem dial-up, to improve the dial success rate, you are advised to set parameters in the **modem timer answer** and **ppp timer negotiation** commands to the maximum values.

----End

8.3.4 (Optional) Configuring a Modem Using AT Commands

To control the working status of a modem, configure the router to send AT commands to the modem according to the AT command set supported by the modem.

Context

Many manufacturers produce different types of modems. These modems support the standard AT command set but differ in implementations and configuration commands. To enable the router to communicate with devices on a PSTN through a modem, you can configure the router to send AT commands to the modem according to the AT command set supported by the modem.

CAUTION

Incorrect configuration may cause incorrect modem status, affecting the dialing function. Therefore, exercise caution when using AT commands to configure a modem.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface async interface-number
```

The asynchronous serial interface view is displayed.

Step 3 Run:

```
sendat at-string
```

The router is configured to send AT commands to a modem.

----End

8.4 Configuration Examples

This section describes how to configure a modem for interworking on a PSTN.

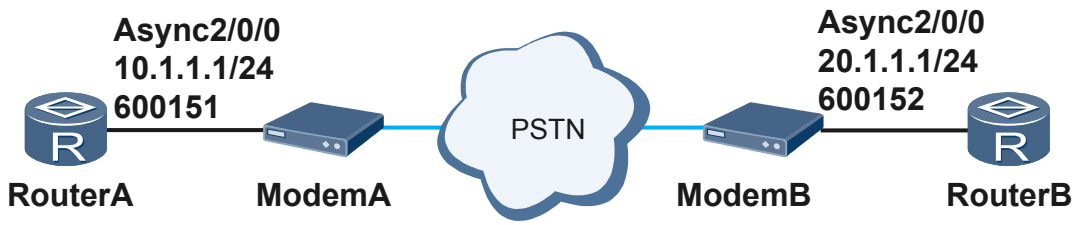
8.4.1 Example for Configuring the Router to Connect to the PSTN Using Modem Dial-up

This section describes how to configure the router to connect to the PSTN using modem dial-up in a typical networking.

Networking Requirements

As shown in **Figure 8-3**, RouterA and RouterB connect to the PSTN through ModemA and ModemB. After the modem function is configured on RouterA and RouterB, Async2/0/0 of RouterA can establish a dial-up connection with RouterB using C-DCC to exchange data.

Figure 8-3 Interworking using modem dial-up



Configuration Roadmap

The configuration roadmap is as follows:

1. Power on the modems and routers and correctly connect them.
2. Configure an IP address for Async2/0/0 of RouterA, configure C-DCC, and set the modem call-in permission, call-out permission, and answer mode to enable RouterA to initiate calls to and receive calls from RouterB.
3. Configure an IP address for Async2/0/0 of RouterB, configure C-DCC, and set the modem call-in permission, call-out permission, and answer mode to enable RouterB to initiate calls to and receive calls from RouterA.

Data Preparation

To complete the configuration, you need the following data:

- IP addresses of Async2/0/0 on RouterA and RouterB
- Call numbers of RouterA and RouterB
- TTY user interface number
- (Optional) Modem answer timeout period

Procedure

Step 1 Configure RouterA.

Configure the asynchronous serial interface.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface async 2/0/0
[RouterA-Async2/0/0] async mode protocol
[RouterA-Async2/0/0] ppp timer negotiate 10
[RouterA-Async2/0/0] ip address 10.1.1.1 255.255.255.0
[RouterA-Async2/0/0] quit
[RouterA] ip route-static 20.1.1.1 32 async 2/0/0
```

Enable C-DCC, configure a DCC dialer ACL, and bind the dialer ACL to the asynchronous serial interface.

```
[RouterA] dialer-rule
[RouterA-dialer-rule] dialer-rule 1 ip permit
[RouterA-dialer-rule] quit
[RouterA] interface async 2/0/0
[RouterA-Async2/0/0] dialer enable-circular
[RouterA-Async2/0/0] dialer-group 1
[RouterA-Async2/0/0] dialer number 600152
[RouterA-Async2/0/0] dialer timer wait-carrier 300
[RouterA-Async2/0/0] quit
```

View the TTY user interface number of the asynchronous serial interface.

```
[RouterA] display user-interface
Idx  Type     Tx/Rx      Modem Privi ActualPrivi Auth  Int
  0    CON 0    9600       -     15    -           N     -
   9   TTY  9   9600       -     0     -           N     2/0/0
  10   TTY 10   9600       -     0     -           N     2/0/1
  11   TTY 11   9600       -     0     -           N     2/0/2
  12   TTY 12   9600       -     0     -           N     2/0/3
  13   TTY 13   9600       -     0     -           N     2/0/4
  14   TTY 14   9600       -     0     -           N     2/0/5
  15   TTY 15   9600       -     0     -           N     2/0/6
```

```
  16   TTY 16   9600       -     0     -           N     2/0/7
+ 129  VTY 0               -     15    4           N     -
  130  VTY 1               -     15    -           N     -
  131  VTY 2               -     15    -           N     -
  132  VTY 3               -     15    -           N     -
  133  VTY 4               -     15    -           N     -
  145  VTY 16              -     0     -           P     -
  146  VTY 17              -     0     -           P     -
  147  VTY 18              -     0     -           P     -
  148  VTY 19              -     0     -           P     -
  149  VTY 20              -     0     -           P     -
  150  Web 0    9600       -     15    -           A     -
  151  Web 1    9600       -     15    -           A     -
  152  Web 2    9600       -     15    -           A     -
  153  Web 3    9600       -     15    -           A     -
  154  Web 4    9600       -     15    -           A     -
  155  XML 0    9600       -     0     -           A     -
  156  XML 1    9600       -     0     -           A     -
  157  XML 2    9600       -     0     -           A     -
UI(s) not in async mode -or- with no hardware support:
1-40  49-128
  +    : Current UI is active.
  F    : Current UI is active and work in async mode.
  Idx  : Absolute index of UIs.
  Type : Type and relative index of UIs.
  Privi: The privilege of UIs.
  ActualPrivi: The actual privilege of user-interface.
  Auth : The authentication mode of UIs.
      A: Authenticate use AAA.
      N: Current UI need not authentication.
      P: Authenticate use current UI's password.
  Int  : The physical location of UIs.
```

Configure the modem function.

```
[RouterA] user-interface tty 9
[RouterA-ui-tty9] modem both
[RouterA-ui-tty9] modem auto-answer
[RouterA-ui-tty9] modem timer answer 60
```

Step 2 Configure RouterB.

Configure the asynchronous serial interface.

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] interface async 2/0/0
[RouterB-Async2/0/0] async mode protocol
[RouterB-Async2/0/0] ppp timer negotiate 10
[RouterB-Async2/0/0] ip address 20.1.1.1 255.255.255.0
[RouterB-Async2/0/0] quit
[RouterB] ip route-static 10.1.1.1 32 async 2/0/0
```

Enable C-DCC, configure a DCC dialer ACL, and bind the dialer ACL to the asynchronous serial interface.

```
[RouterB] dialer-rule
[RouterB-dialer-rule] dialer-rule 2 ip permit
[RouterB-dialer-rule] quit
[RouterB] interface async 2/0/0
[RouterB-Async2/0/0] dialer enable-circular
[RouterB-Async2/0/0] dialer-group 2
[RouterB-Async2/0/0] dialer number 600151
[RouterB-Async2/0/0] dialer timer wait-carrier 300
[RouterB-Async2/0/0] quit
```

View the TTY user interface number of the asynchronous serial interface.

```
[RouterB] display user-interface
Idx  Type     Tx/Rx      Modem Privi ActualPrivi Auth  Int
```

```
  0    CON 0    9600       -     15    -           N     -
   9   TTY  9   9600       -     0     -           N     2/0/0
  10   TTY 10   9600       -     0     -           N     2/0/1
  11   TTY 11   9600       -     0     -           N     2/0/2
  12   TTY 12   9600       -     0     -           N     2/0/3
  13   TTY 13   9600       -     0     -           N     2/0/4
  14   TTY 14   9600       -     0     -           N     2/0/5
  15   TTY 15   9600       -     0     -           N     2/0/6
  16   TTY 16   9600       -     0     -           N     2/0/7
+ 129  VTY 0               -     15    4           N     -
  130  VTY 1               -     15    -           N     -
  131  VTY 2               -     15    -           N     -
  132  VTY 3               -     15    -           N     -
  133  VTY 4               -     15    -           N     -
  145  VTY 16              -     0     -           P     -
  146  VTY 17              -     0     -           P     -
  147  VTY 18              -     0     -           P     -
  148  VTY 19              -     0     -           P     -
  149  VTY 20              -     0     -           P     -
  150  Web 0    9600       -     15    -           A     -
  151  Web 1    9600       -     15    -           A     -
  152  Web 2    9600       -     15    -           A     -
  153  Web 3    9600       -     15    -           A     -
  154  Web 4    9600       -     15    -           A     -
  155  XML 0    9600       -     0     -           A     -
  156  XML 1    9600       -     0     -           A     -
  157  XML 2    9600       -     0     -           A     -
UI(s) not in async mode -or- with no hardware support:
1-40  49-128
  +    : Current UI is active.
  F    : Current UI is active and work in async mode.
  Idx  : Absolute index of UIs.
  Type : Type and relative index of UIs.
  Privi: The privilege of UIs.
  ActualPrivi: The actual privilege of user-interface.
  Auth : The authentication mode of UIs.
      A: Authenticate use AAA.
      N: Current UI need not authentication.
      P: Authenticate use current UI's password.
  Int  : The physical location of UIs.
```

Configure the modem function.

```
[RouterB] user-interface tty 9
[RouterB-ui-tty9] modem both
[RouterB-ui-tty9] modem auto-answer
[RouterB-ui-tty9] modem timer answer 60
```

----End

Configuration Files

- Configuration file of RouterA

```
#
 sysname RouterA
#
user-interface tty 9
 modem both
 modem auto-answer
 modem timer answer 60
#
interface Async2/0/0
 link-protocol ppp
 ppp timer negotiate 10
 ip address 10.1.1.1 255.255.255.0
 dialer enable-circular
 dialer-group 1
 dialer number 600152
```

```
 dialer timer wait-carrier 300
#
dialer-rule
 dialer-rule 1 ip permit
#
 ip route-static 20.1.1.1 255.255.255.255 Async2/0/0
#
return
```

- Configuration file of RouterB

```
#
 sysname RouterB
#
user-interface tty 9
 modem both
 modem auto-answer
 modem timer answer 60
#
interface Async2/0/0
 link-protocol ppp
 ppp timer negotiate 10
 ip address 20.1.1.1 255.255.255.0
 dialer enable-circular
 dialer-group 2
 dialer number 600151
 dialer timer wait-carrier 300
#
dialer-rule
 dialer-rule 2 ip permit
#
 ip route-static 10.1.1.1 255.255.255.255 Async2/0/0
#
return
```