Fondamenti di Internet

WAN Technologies

Prof. Gianluca Reali

Foreword

- As economic globalization and digital transformation accelerate, enterprises keep expanding their scales. More and more branches locate in different regions, with each branch network being considered as a local area network (LAN). The headquarters and branches need to cross geographical locations to communicate with each other. To better carry out services, an enterprise needs to connect these geographically dispersed branches through a wide area network (WAN).
- The development of the WAN technologies is accompanied by the continuously increased bandwidth. In the early stage, X.25 provided only the bandwidth of 64 kbit/s. Later, the digital data network (DDN) and Frame Relay (FR) increased the bandwidth to 2 Mbit/s. Synchronous digital hierarchy (SDH) and asynchronous transfer mode (ATM) further increased the bandwidth to 10 Gbit/s. Now, the current IP-based WANs provide 10 Gbit/s or even higher bandwidth.
- This course describes the development history of WAN technologies, especially the implementations and configurations of Point-to-Point Protocol (PPP) and Point-to-Point Protocol over Ethernet (PPPoE).

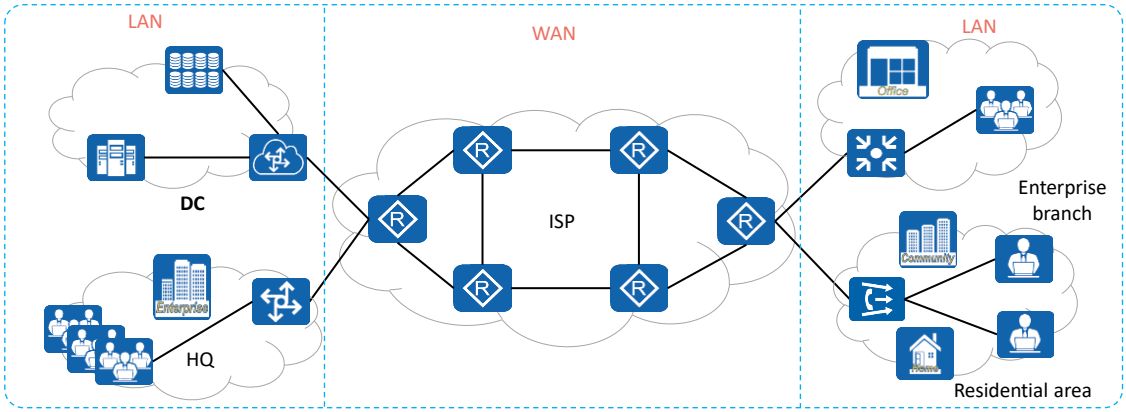
Objectives

- On completion of this course, you will be able to:
  - Understand the basic concepts and development history of WANs.
  - Understand PPP and PPPoE implementations.
  - Master basic PPP and PPPoE configurations.
  - Understand basic MPLS/SR concepts.

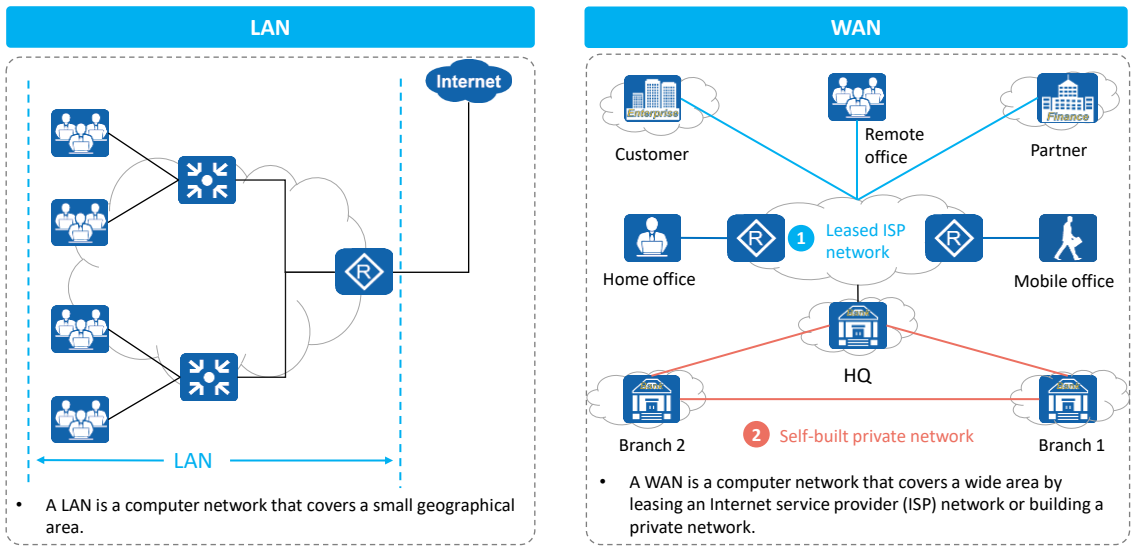
Contents

What Is a WAN?

- A **WAN** is a network that connects LANs in different areas. A WAN generally covers tens of kilometers to thousands of kilometers. It can connect multiple regions, cities, and countries, or provide long-distance communication across several continents, forming an international remote network.



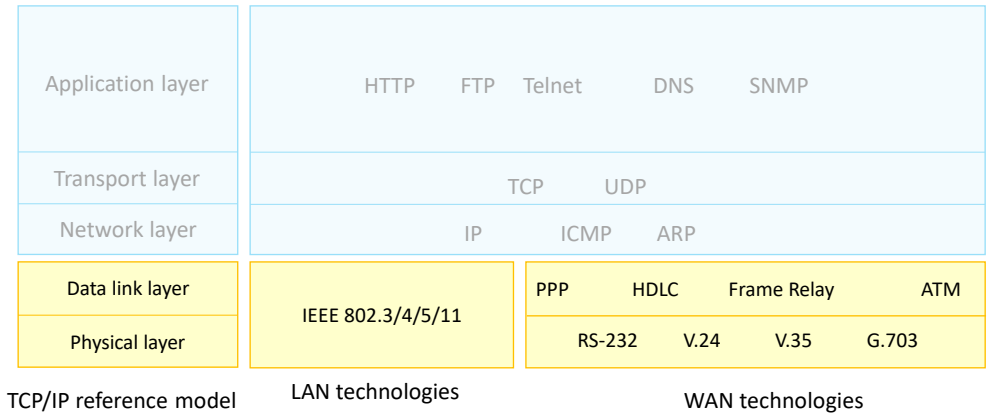
Differences Between a WAN and a LAN



- The main differences between a WAN and a LAN are as follows:
  - A LAN provides high bandwidth but supports only a short transmission distance, which cannot meet the long-distance transmission requirements of a WAN.
  - LAN devices are usually switches, whereas WAN devices are mostly routers.
  - A LAN belongs to an institute or organization, whereas most WAN services are provided by ISPs.
  - WANs and LANs usually use different protocols or technologies only at the physical layer and data link layer. They do not have notable differences in the other layers.
  - The private networks of banks, governments, military, and large companies are also WANs and physically isolated from the Internet.
  - The Internet is only a type of WAN. Small enterprises use the Internet as the WAN connection.

Overview of Early WAN Technologies

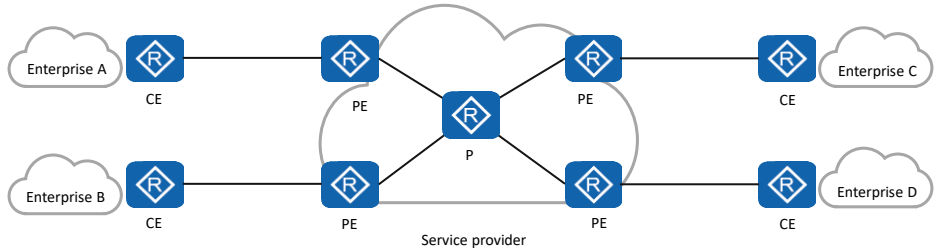
- The early WANs and LANs differ in the data link layer and physical layer and are the same in the other layers in the TCP/IP reference model.



- At the early stage, the common physical layer standards of WANs include common interface standards EIA/TIA-232 (RS-232) formulated by the Electronic Industries Alliance (EIA), and Telecommunications Industry Association (TIA), serial line interface standards V.24 and V.35 formulated by the International Telecommunication Union (ITU), and the G.703 standards related to the physical and electrical features of various digital interfaces.
- The common data link layer standards of WANs include High-Level Data Link Control (HDLC), PPP, FR, and ATM.
    - HDLC is a universal protocol running at the data link layer. Data packets are encapsulated into HDLC frames with the header and tail overheads added. The HDLC frames can be transmitted only on P2P synchronous links and do not support IP address negotiation and authentication. HDLC seeks high reliability by introducing a high overhead, leading to low transmission efficiency.
    - PPP runs at the data link layer for P2P 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.
    - FR is an industry-standard and switched data link protocol. It uses the error-free check mechanism to speed up data forwarding.
    - ATM is a connection-oriented switching technology based on circuit switching and packet switching. It uses 53-byte ATM cells to transmit information.

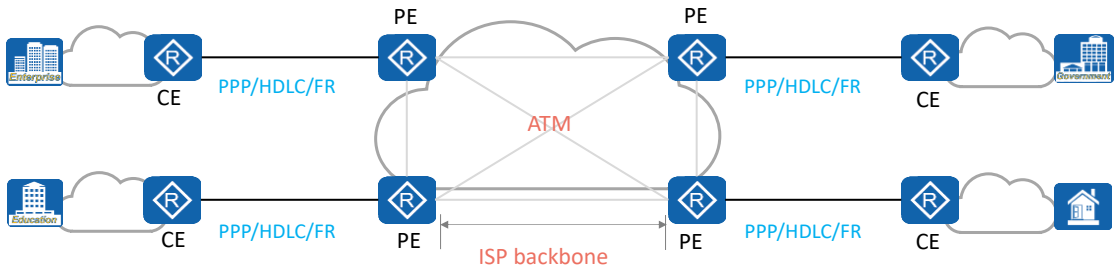
WAN Device Roles

- There are three basic roles of WAN devices: customer edge (CE), provider edge (PE), and provider (P). They are defined as follows:
  - CE: a device located at the customer premises and connected to one or more PEs for user access.
  - PE: a service provider's important edge device that is connected to both a CE and a P.
  - P: a service provider's device that is not connected to any CE.



Application of Early WAN Technologies

- The early WAN technologies perform different Layer 2 encapsulation at the data link layer for different types of physical links. PPP, HDLC, and FR are commonly used between CEs and PEs to implement long-distance transmission of user access packets over a WAN. ATM is commonly used on ISP backbone networks for high-speed forwarding.



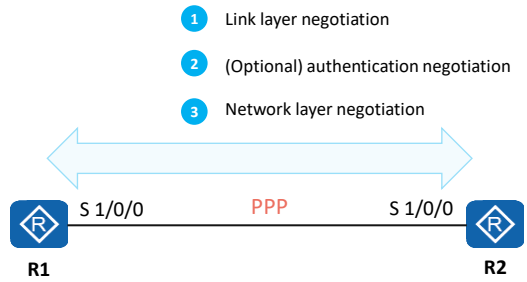
Contents

PPP Introduction

- PPP is a common WAN data link layer protocol. It is used for P2P data encapsulation and transmission on **full-duplex** links.
- PPP provides the **Password Authentication Protocol (PAP)** and **Challenge Handshake Authentication Protocol (CHAP)**.
- PPP features high **extensibility**. For example, PPP can be extended as Point-to-Point Protocol over Ethernet (PPPoE) when PPP packets need to be transmitted over an Ethernet.
- PPP provides the **Link Control Protocol (LCP)**, which is used to negotiate link layer parameters, such as the maximum receive unit (MRU) and authentication mode.
- PPP provides various **Network Control Protocols** (NCPs), such as IP Control Protocol (IPCP), for negotiation of network layer parameters and better support for network layer protocols.

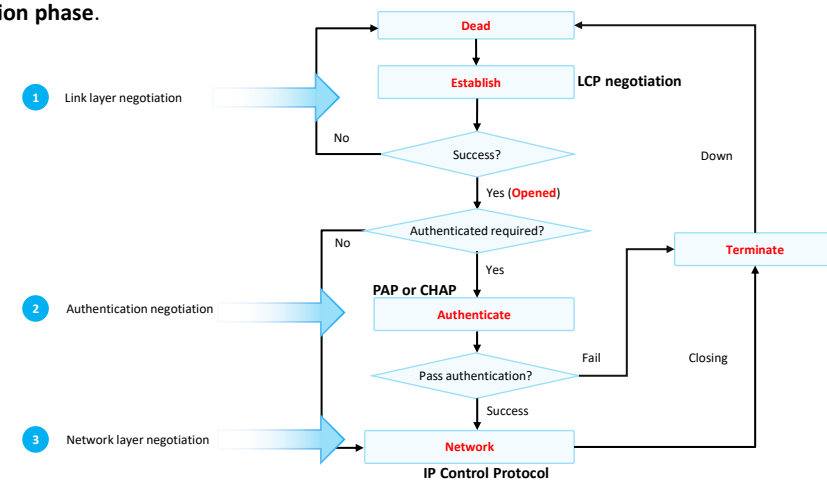
PPP Link Setup Process

- PPP link setup involves **link layer negotiation**, optional **authentication negotiation**, and **network layer negotiation**.
  - Link layer negotiation: LCP packets are used to negotiate link parameters and establish link layer connections.
  - (Optional) authentication negotiation: The authentication mode negotiated during link layer negotiation is used for link authentication.
  - Network layer negotiation: NCP negotiation is used to select and configure a network layer protocol and negotiate network layer parameters.



State Machine of the PPP Link Interface

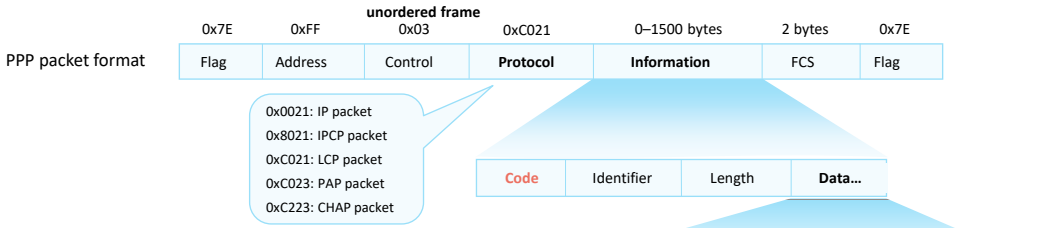
- PPP negotiation is performed by the interfaces at both ends of a link. The interface status indicates the **protocol negotiation phase**.



- A PPP link can be set up after going through the link establishment, authentication, and network layer negotiation phases. The details are as follows:
    1. Two communicating devices enter the Establish phase when starting to set up a PPP connection.
    2. In the Establish phase, they perform LCP negotiation to negotiate an MRU, authentication mode, magic number, and other options. If the negotiation is successful, the devices enter the Opened state, indicating that the lower-layer link has been established.
    3. If authentication is configured, the devices enter the Authenticate phase. Otherwise, the devices directly enter the Network phase.
    4. In the Authenticate phase, link authentication is performed based on the authentication mode negotiated in the link establishment phase. Two authentication modes are available: PAP and CHAP. If the authentication succeeds, the devices enter the Network phase. Otherwise, the devices enter the Terminate phase, tear down the link, and set the LCP status to Down.
    5. In the Network phase, NCP negotiation is performed on the PPP link to select and configure a network layer protocol and to negotiate network layer parameters. The most common NCP protocol is IPCP, which is used to negotiate IP parameters.
    6. In the Terminate phase, if all resources are released, the two communicating devices return to the Dead phase.
- During the PPP operation, the PPP connection can be terminated at any time. A physical link disconnection, authentication failure, timeout timer expiry, and connection close by administrators through configuration can all cause a PPP connection to enter the Terminate phase.

LCP Packet Format

- The Protocol field in a PPP packet identifies the type of the PPP packet. For example, if the Protocol field is 0xC021, the packet is an LCP packet. The Code field is further used to identify different types of LCP packets, as shown in the following table.



Code	Name	Content
0x01	Configure-Request	Configuration request packet.
0x02	Configure-Ack	Configuration success packet.
0x03	Configure-Nak	Configuration parameters need to be negotiated.
0x04	Configure-Reject	Configuration parameters cannot be identified.

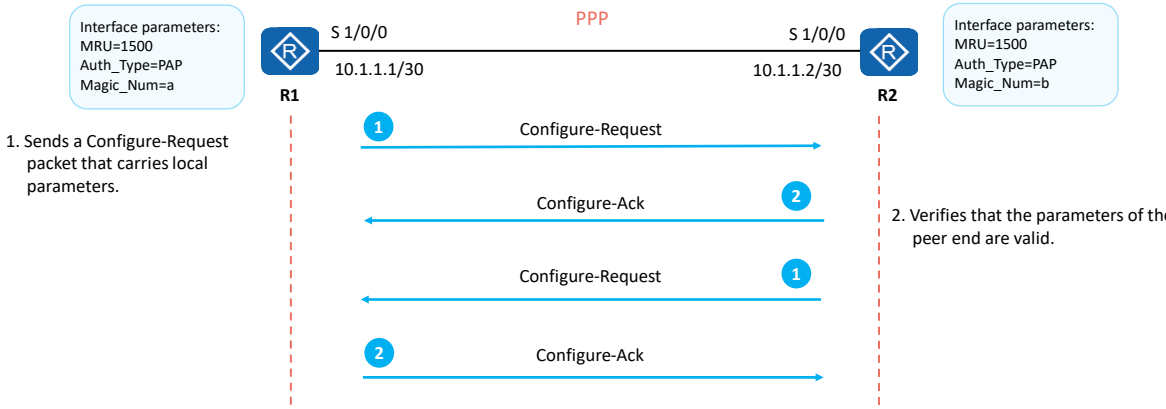
- PPP frame format:
  - The Flag field identifies the start and end of a physical frame and is a binary sequence 01111110 (0X7E).
  - The Address field in a PPP frame represents a broadcast address and has a fixed value of 11111111(0XFF).
  - The Control field of a PPP data frame is 00000011 (0X03) by default, indicating that the frame is an unordered frame.
  - The FCS field is a 16-bit checksum used to check the integrity of PPP frames.
  - The Protocol field indicates the type of protocol packets encapsulated using PPP. 0XC021, 0XC023, and 0XC223 indicate LCP, PAP, and CHAP packets, respectively.
  - The Information field specifies the content of a protocol specified by the Protocol field. The maximum length of this field is called the MRU. The default value is 1500 bytes.
  - When the Protocol field is 0XC021, the Information field structure is as follows:
    - The Identifier field is one byte and is used to match requests and responses.
    - The Length field specifies the total number of bytes in the LCP packet.
    - The Data field carries various TLV parameters for negotiating configuration options, including an MRU, authentication protocol, and the like.
- Common configuration parameters carried by LCP packets include the MRU, authentication protocol, and magic number.
  - On the versatile routing platform (VRP), the MRU is represented by the maximum transmission

unit (MTU) configured on an interface.

- The common PPP authentication protocols are PAP and CHAP. The two ends of a PPP link can use different authentication protocols to authenticate each other. However, the authenticated end must support the authentication protocol required by the authenticating end and be configured with correct authentication information such as the username and password.
- LCP uses magic numbers to detect link loops and other exceptions. A magic number is a random number. The random mechanism must ensure that the probability of generating the same magic number at both ends is almost 0.

LCP Negotiation Process - Normal Negotiation

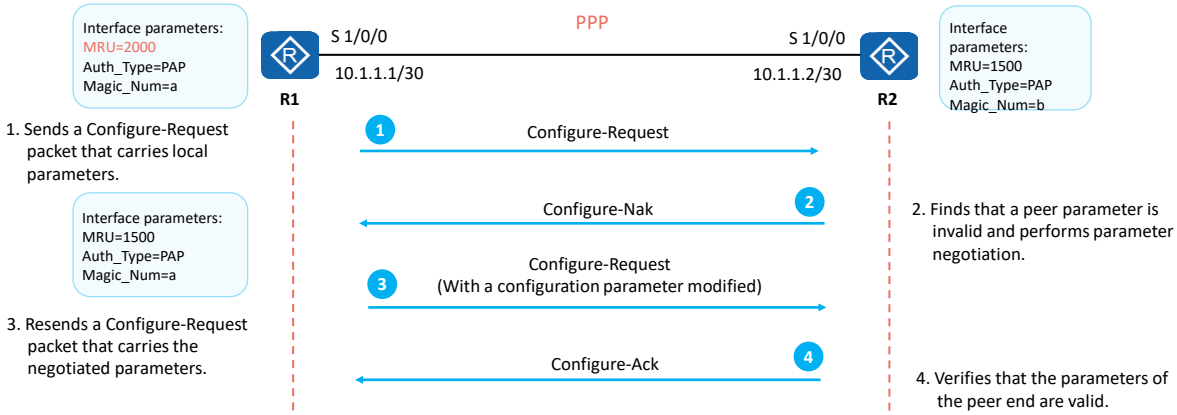
- LCP negotiation is implemented by exchanging different LCP packets. The negotiation is initiated by sending a Configure-Request packet from either party. If the peer end identifies and accepts all parameters in the packet, the peer end returns a Configure-Ack packet to the local end, indicating that the negotiation is successful.



- R1 and R2 are connected through a serial link and run the PPP protocol. After the physical link becomes available, R1 and R2 use LCP to negotiate link parameters.
- In this example, R1 sends a Configure-Request packet that carries link layer parameters configured on R1. After receiving the Configure-Request packet, R2 returns a Configure-Ack packet to R1 if R2 can identify and accept all parameters in the packet. Similarly, R2 also sends a Configure-Request packet to R1, so that R1 checks whether the parameters on R2 are acceptable.
- If R1 does not receive any Configure-Ack packet, it retransmits a Configure-Request packet every 3s. If R1 does not receive any Configure-Ack packet after sending 10 Configure-Request packets consecutively, it considers the peer end unavailable and stops sending Configure-Request packets.

LCP Negotiation Process - Parameter Mismatch

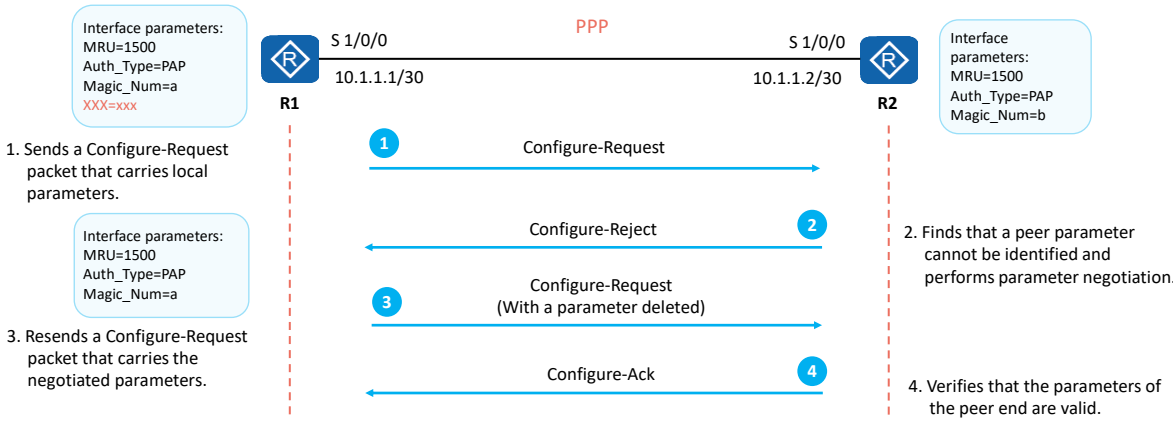
- If LCP parameters do not match during LCP packet exchange, the receiver responds with a Configure-Nak packet to instruct the peer end to modify parameters and perform renegotiation.



- After R2 receives the Configure-Request packet from R1, if R2 can identify all link layer parameters carried in the packet but considers that some or all parameter values are unacceptable (parameter value negotiation fails), R2 returns a Configure-Nak packet to R1.
- The Configure-Nak packet contains only unacceptable link layer parameters, with values (or value ranges) changed to those that can be accepted by R2.
- After receiving the Configure-Nak packet, R1 re-selects other locally configured parameters according to the link layer parameters in the packet and resends a Configure-Request packet.

LCP Negotiation - Unrecognized Parameters

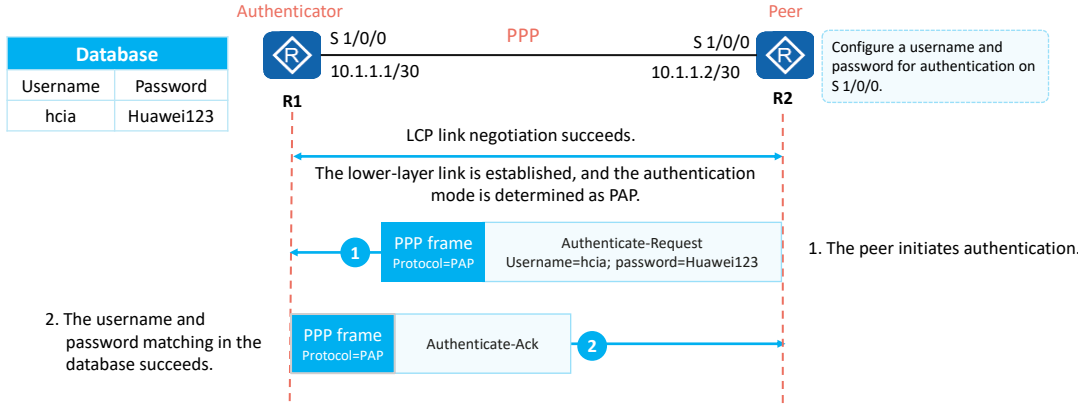
- If LCP parameters cannot be identified during LCP packet exchange, the receiver responds with a Configure-Reject packet to instruct the peer end to delete the unidentifiable parameters and renegotiates with the peer end.



- After receiving a Configure-Request packet from R1, R2 returns a Configure-Reject packet to R1 if R2 cannot identify some or all link layer parameters carried in the packet. The Configure-Reject packet contains only the link layer parameters that cannot be identified.
- After receiving the Configure-Reject packet, R1 resends a Configure-Request packet to R2. This packet contains only parameters that can be identified by R2.

PPP Authentication Mode - PAP

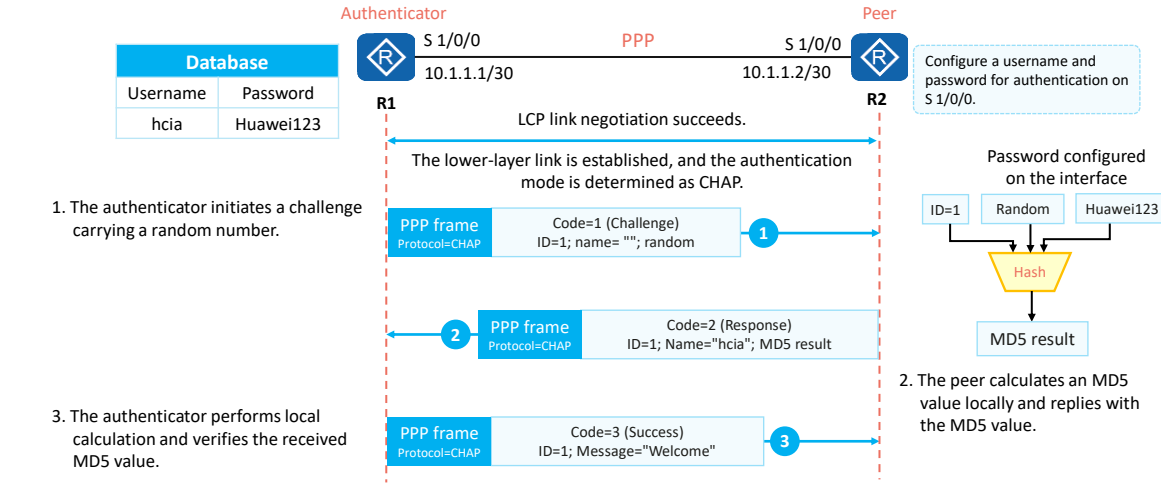
- After the link negotiation is successful, authentication negotiation can be performed. There are two authentication negotiation modes: PAP and CHAP.
- PAP authentication requires a two-way handshake. Negotiation packets are transmitted on the link in clear text.



- After LCP negotiation is complete, the authenticator requires the peer to use PAP for authentication.
- PAP is a two-way handshake authentication protocol. The password is transmitted in clear text on the link. The process is as follows:
  - The peer sends the configured username and password to the authenticator in clear text through an Authenticate-Request packet.
  - After receiving the username and password from the peer, the authenticator checks whether the username and password match those in the locally configured database. If they match, the authenticator returns an Authenticate-Ack packet, indicating that the authentication is successful. If they do not match, the authenticator returns an Authenticate-Nak packet, indicating that the authentication is unsuccessful.

PPP Authentication Mode - CHAP

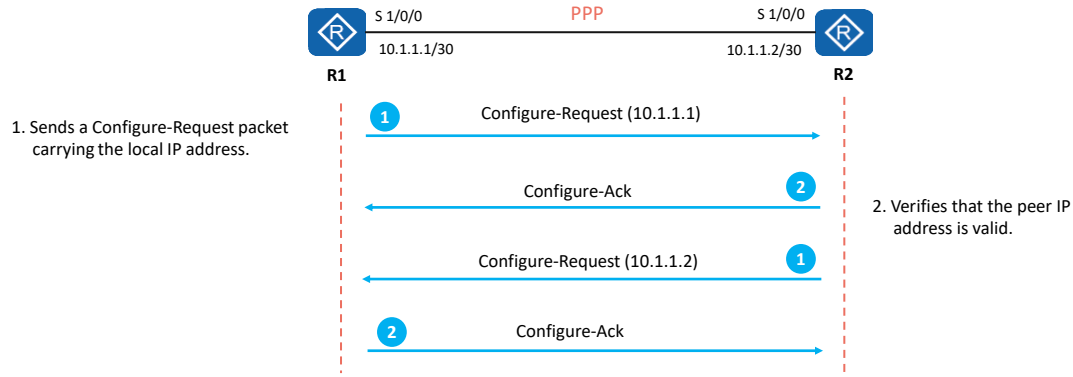
- CHAP authentication requires a three-way handshake. Negotiation packets are encrypted before being transmitted on a link.



- After LCP negotiation is complete, the authenticator requires the peer to use CHAP for authentication.
- CHAP authentication requires three packet exchanges. The process is as follows:
  - The authenticator initiates an authentication request and sends a Challenge packet to the peer. The Challenge packet contains a random number and an ID.
  - After receiving the Challenge packet, the peer performs encryption calculation using the formula MD5{ID+random number+password}. The formula means that the authenticator combines the identifier, random number, and password into a character string and performs an MD5 operation on the character string to obtain a 16-byte digest. The peer then encapsulates the digest and the CHAP username configured on the interface into a Response packet and sends the Response packet to the authenticator.
  - After receiving the Response packet, the authenticator locally searches for the password corresponding to the username in the Response packet. After obtaining the password, the authenticator encrypts the password using the same formula as that used by the peer. Then, the authenticator compares the digest obtained through encryption with that in the Response packet. If they are the same, the authentication succeeds. If they are different, the authentication fails.
- In CHAP authentication, the password of the peer is encrypted before being transmitted, which greatly improves security.
- Notices About Encryption Algorithms
  - The MD5 (digital signature scenario and password encryption) encryption algorithm has security risks. You are advised to use more secure encryption algorithms, such as AES, RSA (2048 bits or above), SHA2, and HMAC-SHA2.

NCP Negotiation - Static IP Address Negotiation

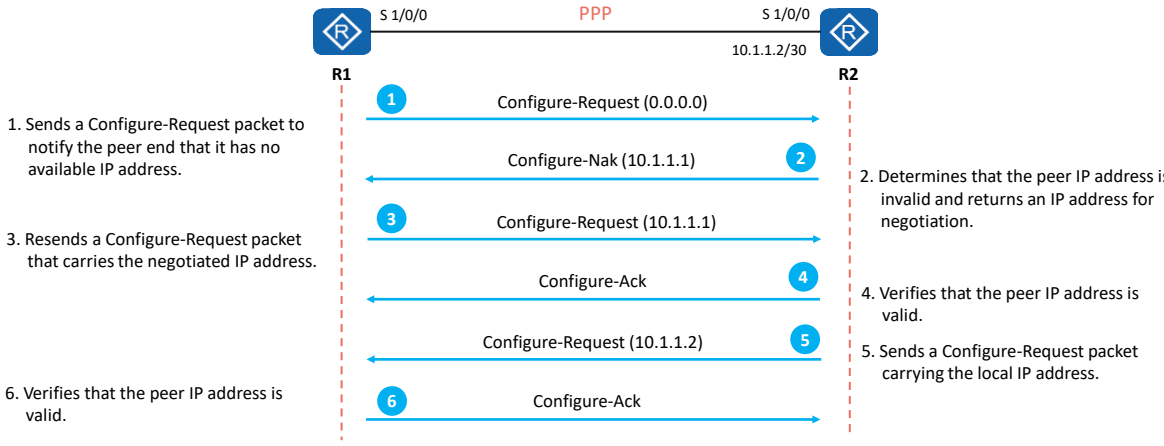
- After PPP authentication negotiation, the two ends enter the NCP negotiation phase to negotiate the format and type of data packets transmitted on the data link. IPCP, for example, is classified into static and dynamic IP address negotiation.
- **Static IP address negotiation requires manual configuration** of IP addresses at both ends of a link.



- NCP is used to establish and configure different network layer protocols and negotiate the format and type of data packets transmitted on a data link. IPCP is a commonly used NCP.
- The static IP address negotiation process is as follows:
  - Each end sends a Configure-Request packet carrying the locally configured IP address.
  - After receiving the packet from the peer end, the local end checks the IP address in the packet. If the IP address is a valid unicast IP address and is different from the locally configured IP address (no IP address conflict), the local end considers that the peer end can use this address and responds with a Configure-Ack packet.

NCP Negotiation - Dynamic IP Address Negotiation

- In dynamic IP address negotiation, one end of a PPP link can assign an IP address to the other end.



- The dynamic IP address negotiation process is as follows:
  - R1 sends a Configure-Request packet to R2. The packet contains an IP address 0.0.0.0, indicating that R1 requests an IP address from R2.
  - After receiving the Configure-Request packet, R2 considers the IP address 0.0.0.0 invalid and replies with a Configure-Nak packet carrying a new IP address 10.1.1.1.
  - After receiving the Configure-Nak packet, R1 updates its local IP address and resends a Configure-Request packet carrying the new IP address 10.1.1.1.
  - After receiving the Configure-Request packet, R2 considers the IP address contained in the packet valid and returns a Configure-Ack packet.
  - R2 also sends a Configure-Request packet to R1 to request use of IP address 10.1.1.2. R1 considers the IP address valid and replies with a Configure-Ack packet.

Contents

Configuring Basic PPP Functions

1. Encapsulate an interface with PPP.

   [Huawei-Serial0/0/0] **link-protocol ppp**

   In the interface view, change the interface encapsulation protocol to PPP. The default encapsulation protocol of Huawei devices' serial interfaces is PPP.

2. Configure a negotiation timeout period.

   [Huawei-Serial0/0/0] **ppp timer negotiate** *seconds*

   During LCP negotiation, the local end sends an LCP negotiation packet to the peer end. If the local end does not receive a reply packet from the peer end within the specified negotiation timeout period, the local end resends an LCP negotiation packet.

Configuring PAP Authentication

1. Configure an authenticator to authenticate a peer using the PAP mode.

   ```
   [Huawei-aaa] local-user user-name  password { cipher | irreversible-cipher } password
   [Huawei-aaa] local-user user-name service-type ppp
   ```

   ```
   [Huawei-Serial0/0/0] ppp authentication-mode pap
   ```

   Before configuring the authenticator to authenticate a peer using the PAP mode, add the username and password of the peer to the local user list in the AAA view. Then select the PAP authentication mode.

2. Configure the peer to be authenticated by the authenticator in PAP mode.

   ```
   [Huawei-Serial0/0/0] ppp pap local-user user-name password { cipher | simple } password
   ```

   This command configures the peer to send its username and password to the authenticator.

Configuring CHAP Authentication

1. Configure an authenticator to authenticate a peer using CHAP mode.

```
[Huawei-aaa] local-user user-name  password { cipher | irreversible-cipher } password
[Huawei-aaa] local-user user-name service-type ppp
```

```
[Huawei-Serial0/0/0] ppp authentication-mode chap
```

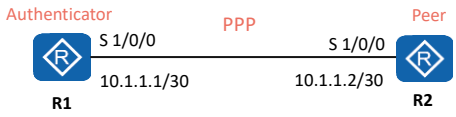
2. Configure the peer to be authenticated by the authenticator in CHAP mode.

```
[Huawei-Serial0/0/0] ppp chap user user-name
```

```
[Huawei-Serial0/0/0] ppp chap password { cipher | simple } password
```

This command configures a local username and a password for CHAP authentication.

Example for Configuring PAP Authentication



- Experiment requirements:
  1. Enable PAP authentication on the PPP link between R1 and R2.
  2. Configure R1 as the authenticator.
  3. Configure R2 as the peer.

Configurations on R1

```
[R1]aaa # Add information about the user to be authenticated.
[R1-aaa]local-user huawei password cipher huawei123
[R1-aaa]local-user huawei service-type ppp
# Specify the service type of the user to be authenticated.
[R1]interface Serial 1/0/0
[R1-Serial1/0/0]link-protocol ppp
[R1-Serial1/0/0]ppp authentication-mode pap
# Set the authentication mode to PAP.
[R1-Serial1/0/0]ip address 10.1.1.1 30
```

Configurations on R2

```
[R2]interface Serial 1/0/0
[R2-Serial1/0/0]link-protocol ppp
[R2-Serial1/0/0]ppp pap local-user huawei password cipher huawei123
# Add user information for PPP authentication.
[R2-Serial1/0/0]ip address 10.1.1.2 30
```

Example for Configuring CHAP Authentication

- Experiment requirements:
  1. Enable CHAP authentication on the PPP link between R1 and R2.
  2. Configure R1 as the authenticator.
  3. Configure R2 as the peer.

Configurations on R1

```
[R1]aaa # Add information about the user to be authenticated.
[R1-aaa]local-user huawei password cipher huawei123
[R1-aaa]local-user huawei service-type ppp
# Specify the service type of the user to be authenticated.
[R1]interface Serial 1/0/0
[R1-Serial1/0/0]link-protocol ppp
[R1-Serial1/0/0]ppp authentication-mode chap
# Set the authentication mode to CHAP.
```

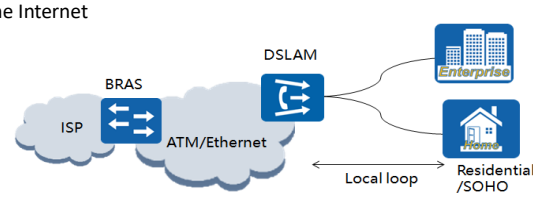
Configurations on R2

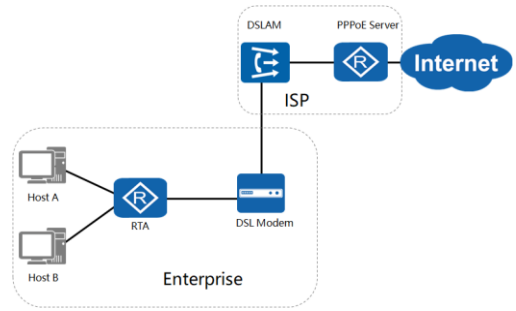
```
[R2]interface Serial 1/0/0
[R2-Serial1/0/0]link-protocol ppp
[R2-Serial1/0/0]ppp chap user huawei
[R2-Serial1/0/0]ppp chap password cipher huawei123
# Add user information for PPP authentication.
```

Contents

What Is PPPoE?

- PPP over Ethernet (PPPoE) is a link layer protocol that encapsulates PPP frames into Ethernet frames. PPPoE enables multiple hosts on an Ethernet to connect to a broadband remote access server (BRAS).
- It was introduced as a solution for tunneling packets over the DSL connection to the ISP's IP network, and from there to the rest of the Internet





DSL Internet access architecture

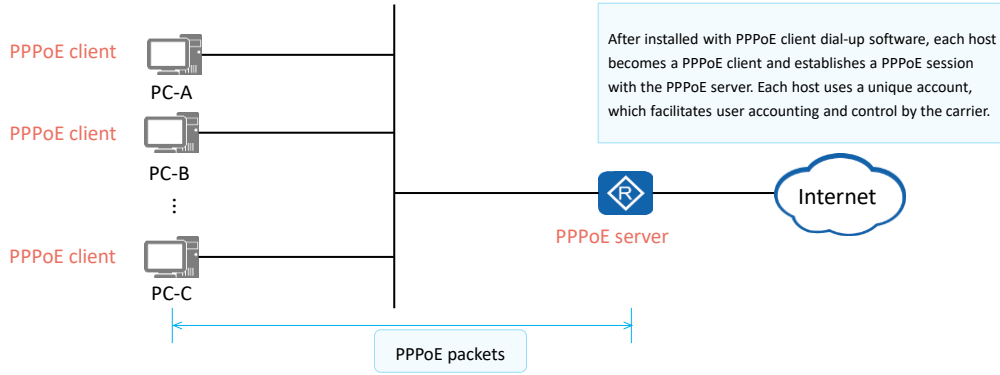
PC or Gateway	DSL modem	DSLAM	Remote access server	(ISP)
(IP)				(IP)
Ethernet PPP			PPP PPP	PPP
PPPoE	PPPoE PPPoA		PPPoA backbone	backbone
Ethernet	Ethernet AAL5	AAL5 backbone	backbone IP	IP
	ATM	ATM		
	DSL	DSL		

- PPPoE is used to connect a PC or a router to a modem via an Ethernet link and it can also be used in Internet access over DSL on a telephone line in the PPPoE over ATM (PPPoEoA) over ADSL protocol stack. PPPoE over ATM has the highest overhead of the popular DSL delivery methods, when compared with for example PPPoA (RFC 2364)
- DSL represents a form of broadband technology that utilizes existing telephony networks to allow for data communications. Communication is facilitated through a remote transceiver unit, or modem at the customer premises, which communicates over the existing telephone lines to a central office transceiver unit that takes the form of the Digital Subscriber Line Access Multiplexer (DSLAM) where traffic is multiplexed onto a high speed ATM or Ethernet network before reaching the broadband remote access server (BRAS) or PPPoA/PPPoE server within the service provider network.
- The distance between the two transceivers can vary depending on the specific DSL technology applied. In the case of an Asynchronous Digital Subscriber Line (ADSL) the distance expands up to around 18000 feet or 5,460 meters traditionally over an ATM network, whereas with a Very High Speed Digital Subscriber Line (VDSL2), local loop distances of only around 1500 meters are supported with fiber (FTTx) technology applied to provide Ethernet based backend transmission to the BRAS (PPPoE server).
- PPPoE refers to the encapsulation of PPP within Ethernet frames to support a connection over broadband technologies to a PPPoE broadband remote access server (BRAS), located within the

service provider network. This is used to support the authentication and accounting process before access to the remote network such as the Internet is provided. The router RTA operates as the client for establishment of the PPPoE session with the PPPoE server via which an authorized connection is established for access to remote networks and resources. The DSL modem provides the modulation and demodulation of signals across the copper telephone wire infrastructure that traditionally exist in homes and offices.

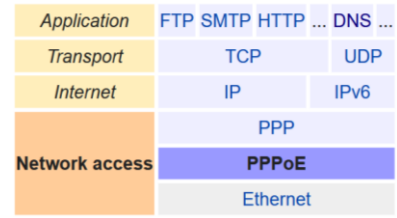
PPPoE Application Scenarios

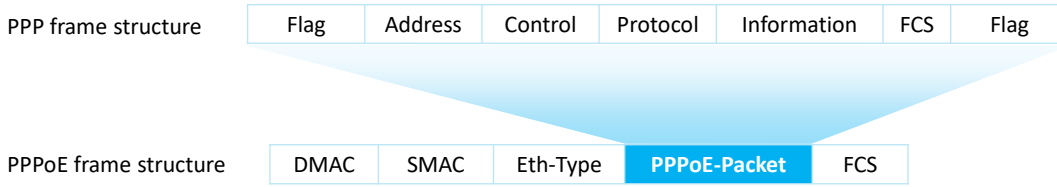
- PPPoE provides P2P connections on an Ethernet. A PPPoE client and a PPPoE server establish a PPP session to encapsulate PPP data packets and provide access services for hosts on the Ethernet, implementing user control and accounting. PPPoE is widely used on enterprise and carrier networks.
- PPPoE is usually used by home users and enterprise users to dial up to access the Internet.



What Is PPPoE?

- PPPoE integrates the advantages of Ethernet and PPP. It has the flexible networking advantage of Ethernet and can use PPP to implement authentication and accounting.

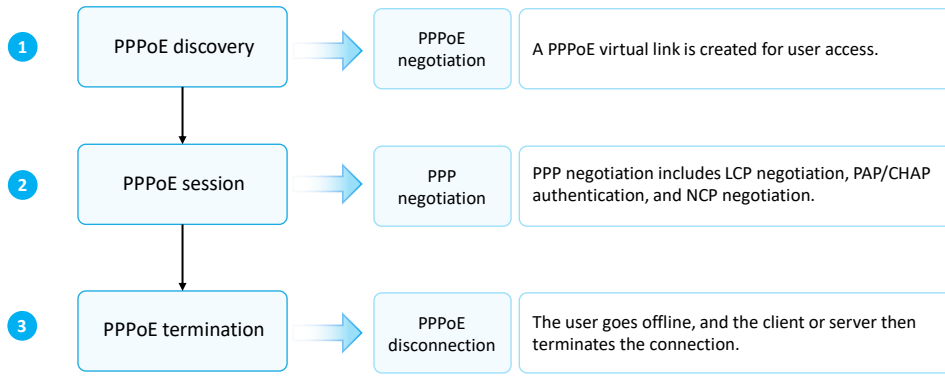




- Carriers want to connect multiple hosts at a site to a remote access device, which can provide access control and accounting for these hosts in a manner similar to dial-up access. Ethernet is the most cost-effective technology among all access technologies that connect multiple hosts to an access device. PPP provides good access control and accounting functions. PPPoE therefore was introduced to transmit PPP packets on the Ethernet.
- PPPoE uses Ethernet to connect a large number of hosts to the Internet through a remote access device and uses PPP to control each host. PPPoE applies to various scenarios, and provides high security as well as convenient accounting.

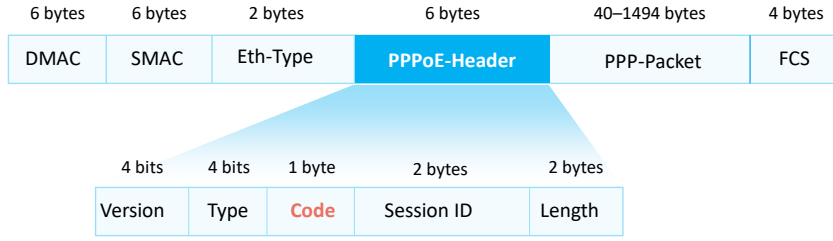
PPPoE Session Establishment

- PPPoE session establishment involves three stages: PPPoE discovery, session, and termination stages.



PPPoE Packets

- A PPPoE session is established by exchanging different PPPoE packets. The PPPoE packet structure and common packet types are as follows.

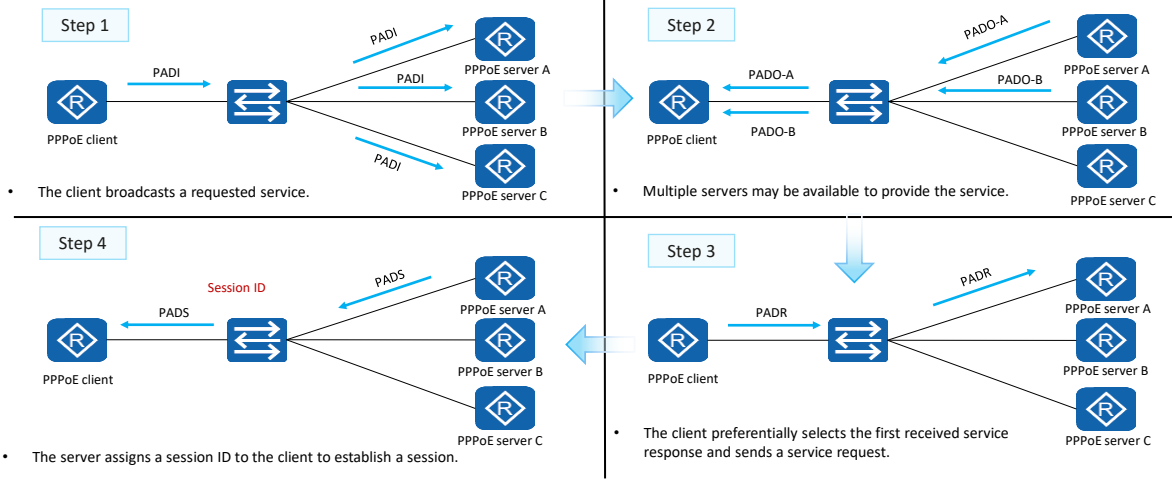


Code	Name	Content
0x09	PADI	PPPoE Active Discovery Initiation packet
0x07	PADO	PPPoE Active Discovery Offer packet
0x19	PADR	PPPoE Active Discovery Request packet
0x65	PADS	PPPoE Active Discovery Session-confirmation packet
0xa7	PADT	PPPoE Active Discovery Terminate packet

- PPPoE packets are encapsulated in Ethernet frames. The fields in an Ethernet frame are described as follows:
- DMAC: indicates the MAC address of a destination device, which is usually an Ethernet unicast or broadcast address (0xFFFFFFFF).
- SMAC: indicates the MAC address of a source device.
- Eth-Type: indicates the protocol type. The value 0x8863 indicates that PPPoE discovery packets are carried. The value 0x8864 indicates that PPPoE session packets are carried.
- The fields in a PPPoE packet are described as follows:
  - VER: indicates a PPPoE version. The value is 0x01.
  - Type: indicates the PPPoE type. The value is 0x01.
  - Code: indicates a PPPoE packet type. Different values indicate different PPPoE packet types.
  - Session ID: indicates a PPPoE session ID. This field defines a PPPoE session, together with the Ethernet SMAC and DMAC fields.
  - Length: indicates the length of a PPPoE packet.

PPPoE Discovery Stage

- PPPoE discovery involves four steps: 1) the client sends a request, 2) the servers respond to the request, 3) the client confirms a response and 4) establishes a session.

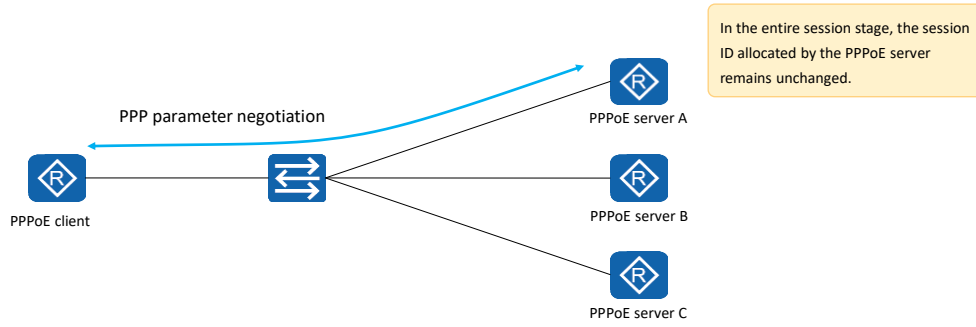


1. The PPPoE client broadcasts a PADI packet that contains the required service information on the local Ethernet.
   - The destination MAC address of the PADI packet is a broadcast address, the Code field is set to 0x09, and the Session ID field is set to 0x0000.
   - After receiving the PADI packet, all PPPoE servers compare the requested services with the services that they can provide.
2. If a server can provide the requested service, it replies with a PADO packet.
   - The destination address of the PADO packet is the MAC address of the client that sends the PADI packet. The Code field is set to 0x07 and the Session ID field is set to 0x0000.
3. The PPPoE client may receive multiple PADO packets. In this case, the PPPoE client selects the PPPoE server whose PADO packet is first received by the client and sends a PADR packet to the PPPoE server.
   - The destination address of the PADR packet is the MAC address of the selected server, the Code field is set to 0x19, and the Session ID field is set to 0x0000.
4. After receiving the PADR packet, the PPPoE server generates a unique session ID to identify the session with the PPPoE client and sends a PADS packet.
   - The destination address of the PADS packet is the MAC address of the PPPoE client, the Code field is set to 0x65, and the Session ID field is set to the uniquely generated session ID.

- After a PPPoE session is established, the PPPoE client and server enter the PPPoE session stage.

PPPoE Session Stage

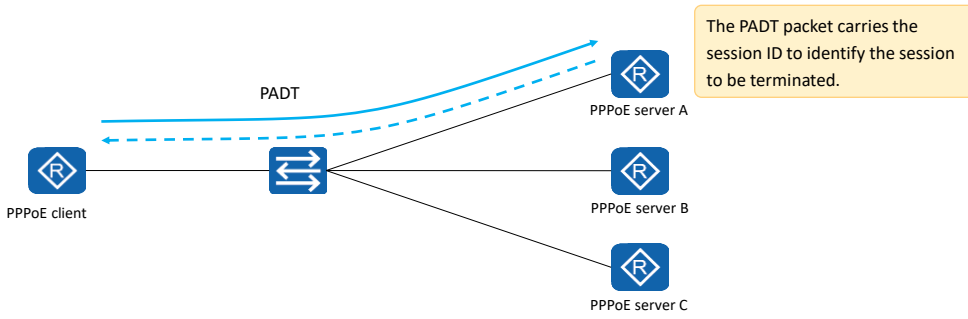
- In the PPPoE session stage, PPP negotiation, including LCP, authentication, and NCP negotiation, is performed.



- In the PPPoE session stage, PPP negotiation and PPP packet transmission are performed.
- PPP negotiation in the PPPoE session stage is the same as common PPP negotiation, which includes the LCP, authentication, and NCP negotiation phases.
  - In the LCP phase, the PPPoE server and PPPoE client establish and configure a data link, and verify the data link status.
  - After LCP negotiation succeeds, authentication starts. The authentication protocol type is determined by the LCP negotiation result.
  - After authentication succeeds, PPP enters the NCP negotiation phase. NCP is a protocol suite used to configure different network layer protocols. A commonly used network-layer protocol is IPCP, which is responsible for configuring IP addresses for users and domain name servers (DNSs).
- After PPP negotiation succeeds, PPP data packets can be forwarded over the established PPP link. The data packets transmitted in this phase must contain the session ID determined in the discovery stage, and the session ID must remain unchanged.

PPPoE Session Termination Stage

- If the PPPoE client wants to terminate the session, it sends a PADT packet to the PPPoE server.
- Similarly, if the PPPoE server wants to terminate the session, it sends a PADT packet to the PPPoE client.



- In a PADT packet, the destination MAC address is a unicast address, and the session ID is the ID of the session to be closed. Once a PADT packet is received, the session is closed.

Contents

Configuring Basic PPPoE Functions

1. Configure a dialer rule and set conditions for initiating a PPPoE session under the rule.

   [Huawei] **dialer-rule**

   Configure a username on the dialer interface. The username must be the same as that of the peer server.

   [Huawei-Dialer1]**dialer user** *username*

3. Add the interface to a dialer group.

   [Huawei-Dialer1]**dialer-group** *group-number*

4. Specify a dialer bundle for the interface.

   [Huawei-Dialer1]**dialer-bundle** *number*

5. Bind a physical interface to the dialer bundle.

   [Huawei-Ethernet0/0/0]**pppoe-client dial-bundle-number** *number*

- A Dialer interface is a virtual interface used to implement the Dialer Control Center (DCC) function. A physical interface can be bound to a dialer interface to inherit the configuration of the dialer interface.

Dialer interfaces had been introduced in the dial-up era and in ISDN access, they provide an abstraction layer from the physical interfaces that actually perform the dial-up. Dialer interfaces have found usage for PPPoE or other forms like PPPoA or PPPoEoA in broadband access.
Dialer interfaces support PAP/CHAP auuthentication, which is frequently used in order to authenticate towards an ISP.
Physical interfaces cannot do authentication

Dialer interfaces are still very much in use. They indeed originated in the 'old' (ISDN) daysbut they have found application in broadband access so they are still in use and not only legacy.

- (Optional) Run **dialer-group** *group-number*

  dialer-group: Dialer grous are used to enforce controls access by configuring an interface to belong to a specific dialing group.

  The dialer-group command enables the logic that determines what is interesting. It refers to a dialer-list, which can refer to either an entire protocol suite or an access list.

Using the **dialer-group** command, you can add an interface to a dialer access group. You can configure a dial ACL and associate it with the concerned dial interface (physical or dialer) by using the **dialer-group command**

- Run **dialer bundle** *number*

Each PPPoE session uniquely corresponds to a dialer bundle, and each dialer bundle uniquely corresponds to a dialer interface. Therefore, a PPPoE session uniquely corresponds to a dialer interface.

The **dialer bundle** *number* command specifies a dialer bundle for the dialer interface, that is a numenber of interfaces are aggregates to operate as I single virtual interface (bundle). **The device associates a physical interface with the dialer interface through the dialer bundle**.

By default, a dialer interface does not have a dialer bundle.

Multiple PPPoE sessions can be established on an Ethernet interface. That is, **an Ethernet interface can belong to multiple dialer bundles**. **A dialer bundle can contain only one Ethernet interface**.

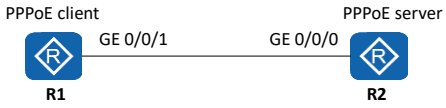
One dialer bundle maps one PPPoE session. If the dialer bundle of a dialer interface already has

an Ethernet interface used for PPPoE, no interface can be added to the dialer bundle. If the dialer

bundle contains other interfaces, no Ethernet interface can be added to the dialer bundle to establish PPPoE sessions on the PPPoE client.

- https://support.huawei.com/enterprise/de/doc/EDOC1100203257/8c68362b/overview-of-logical-interfaces

Example for Configuring a PPPoE Client (1)



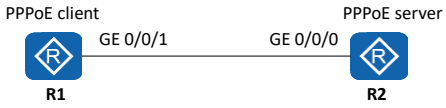
- Experiment requirements:
  1. Configure R1 as a PPPoE client and R2 as a PPPoE server.
  2. Configure a dialer interface for the PPPoE client on R1.
  3. Configure the authentication function on the dialer interface on R1.
  4. The dialer interface on R1 can obtain the IP address allocated by the PPPoE server.
  5. R1 can access the server through the dialer interface.

1. Create a dialer interface and configure a username and password for authentication.

```
[R1]dialer-rule
[R1-dialer-rule]dialer-rule 1 ip permit
[R1-dialer-rule]quit
[R1]interface dialer 1
[R1-Dialer1] dialer user enterprise
[R1-Dialer1] dialer-group 1  # adds an interface to a dialer group
[R1-Dialer1] dialer bundle 1 # specifies a dialer bundle for the dialer interface
[R1-Dialer1] ppp chap user huawei1
[R1-Dialer1] ppp chap password cipher huawei123
[R1-Dialer1] ip address ppp-negotiate
```


- The configuration of the PPPoE client includes three steps:
- Step 1: Configure a dialer interface.
  - The **dialer-rule** command displays the dialer rule view. In this view, you can configure the conditions for initiating a PPPoE session.
  - The **interface dialer** *number* command creates a dialer interface and displays the dialer interface view.
  - The **dialer user** *user-name* command configures a username for the peer end. This username must be the same as the PPP username on the peer server.
  - The **dialer-group** *group-number* command adds an interface to a dialer group.
  - The **dialer bundle** *number* command specifies a dialer bundle for the dialer interface. The device associates a physical interface with the dialer interface through the dialer bundle.
- Note: Ensure that the *group-number* parameter in the **dialer-group** command is the same as the *dialer-rule-number* parameter in the **dialer-rule** command.

Example for Configuring a PPPoE Client (2)



- Experiment requirements:
  1. Configure R1 as a PPPoE client and R2 as a PPPoE server.
  2. Configure a dialer interface for the PPPoE client on R1.
  3. Configure the authentication function on the dialer interface on R1.
  4. The dialer interface on R1 can obtain the IP address allocated by the PPPoE server.
  5. R1 can access the server through the dialer interface.

2. Bind the dialer interface to an outbound interface.

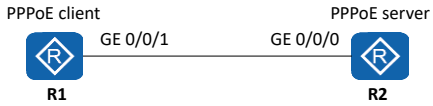
```
[R1]interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1]pppoe-client dial-bundle-number 1
[R1-GigabitEthernet0/0/1]quit
```

3. Configure a default route from the PPPoE client to the server.

```
[R1]ip route-static 0.0.0.0  0.0.0.0  dialer 1
```


- Step 2: Bind the dialer bundle to a physical interface.
  - The **pppoe-client dial-bundle-number** *number* command binds the dialer bundle to a physical interface and specifies the dialer bundle for the PPPoE session. number specifies the dialer bundle number corresponding to the PPPoE session.
- Step 3: Configure a default static route. This route allows the traffic that does not match any entry in the routing table to initiate a PPPoE session through the dialer interface.

Example for Configuring a PPPoE Server



- Experiment requirements:
  1. Create an address pool on the PPPoE server for address allocation to the PPPoE client.
  2. The PPPoE server authenticates the PPPoE client and assigns a valid IP address to the client.

1. Create an address pool and a virtual template.

```
[R2]ip pool pool1 # Create an address pool and specify the range of the IP addresses to be allocated and a gateway.
[R2-ip-pool-pool1]network 192.168.1.0 mask 255.255.255.0
[R2-ip-pool-pool1]gateway-list 192.168.1.254
[R2]interface Virtual-Template 1 # Create a virtual template interface.
[R2-Virtual-Template1]ppp authentication-mode chap
[R2-Virtual-Template1]ip address 192.168.1.254 255.255.255.0
[R2-Virtual-Template1]remote address pool pool1
```

2. Bind a physical interface to the virtual template.

```
[R2]interface GigabitEthernet 0/0/0
[R2-GigabitEthernet0/0/0]pppoe-server bind virtual-template 1
[R2-GigabitEthernet0/0/0]quit
```

3. Create an access user.

```
[R2]aaa # Add information about the user to be authenticated.
[R2-aaa]local-user huawei1 password cipher huawei123
[R2-aaa]local-user huawei1 service-type ppp
```


- A virtual-template interface is a logical entity that can be used to apply predefined interface configurations for virtual-access interfaces.
- Virtual template interfaces is configured independently of any physical interface and applied dynamically, as needed, to create virtual access interfaces.

- PPPoE Server Configurations
  - The **interface virtual-template** command creates a virtual template interface or displays the view of an existing virtual template interface.
  - The **pppoe-server bind** command binds an interface to the virtual template interface for PPPoE access.

Verifying the Configuration

1. Check detailed information about the dialer interface.

```
<R1>display interface Dialer 1
Dialer1 current state: UP
Line protocol current state: UP (spoofing)
Description: HUAWEI, AR Series, Dialer1 Interface
Route Port, The Maximum Transmit Unit is 1500, Hold timer is
10(sec)
Internet Address is negotiated, 192.168.10.254/32
Link layer protocol is PPP
LCP initial
Physical is Dialer
Bound to Dialer1:0:
Dialer1:0 current state : UP
Line protocol current state : UP
Link layer protocol is PPP
LCP opened, IPCP opened
```

2. Check the initial status of the PPPoE session on the client.

```
[R1]display pppoe-client session summary
PPPoE Client Session:
ID  Bundle  Dialer  Intf      Client-MAC      Server-MAC    State
0     1       1    GE0/0/1  54899876830c  000000000000  IDLE
```

3. Check the establishment status of the PPPoE session on the client.

```
[R1]display pppoe-client session summary
PPPoE Client Session:
ID  Bundle  Dialer  Intf      Client-MAC     Server-MAC     State
1     1       1    GE0/0/1  00e0fc0308f6  00e0fc036781   UP
```


- The **display interface dialer** *number* command displays the configuration of the dialer interface. The command output helps locate faults on the dialer interface.
- LCP opened, IPCP opened indicates that the link is working properly.
- The **display pppoe-client session summary** command displays the PPPoE session status and statistics on the PPPoE client.
  - **ID** indicates a PPPoE session ID. The values of the bundle ID and dialer ID are determined by the configured dialer parameters.
  - **Intf** indicates the physical interface used for negotiation on the PPPoE client.
  - **State** indicates the status of a PPPoE session, which can be:
    1. IDLE: The current session is idle.
    2. PADI: The current session is in the discovery stage, and a PADI packet has been sent.
    3. PADR: The current session is in the discovery stage, and a PADR packet has been sent.
    4. UP: The current session is set up successfully.

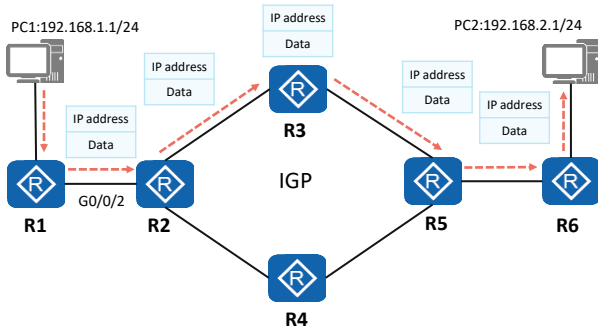
Contents

Evolution of WAN Technologies

- The data link layer protocols commonly used on early WANs include PPP, HDLC, and ATM. With the network evolution towards all-IP, the IP-based Internet becomes popular. However, the IP technology based on the longest match rule must use software to search for routes, resulting in low forwarding performance, which has become the bottleneck that restricts the network development.
- Multiprotocol Label Switching (MPLS) was originally proposed to improve the forwarding speeds of routers. Compared with the traditional IP routing mode, MPLS parses IP packet headers only at the network edges during data forwarding. Transit nodes forward packets based on labels, without the need to parse IP packet headers. This speeds up software processing.
- With the improvement of router performance, the route search speed is no longer a bottleneck for network development. Thus, MPLS loses its advantage in fast forwarding speed. However, leveraging support for multi-layer labels and a connection-oriented forwarding plane, MPLS is widely applied in various scenarios, such as virtual private network (VPN), traffic engineering (TE), and quality of service (QoS) scenarios.

Traditional IP Routing and Forwarding

- Traditional IP forwarding uses hop-by-hop forwarding. Each time a data packet passes through a router, the router decapsulates the packet to check the network layer information and searches its routing table based on the longest match rule to guide packet forwarding. The repeat process of decapsulating packets, searching routing tables, and re-encapsulating the packets on routers lead to low forwarding performance.

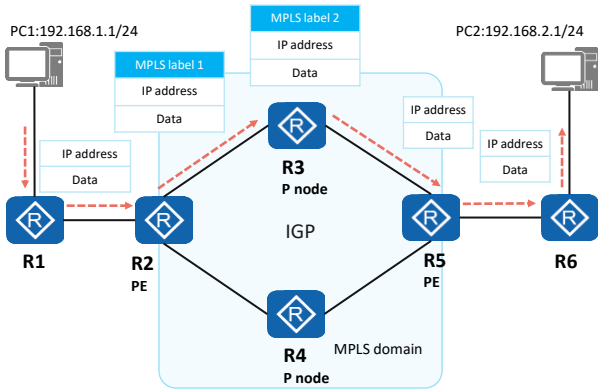


- Characteristics of traditional IP routing and forwarding:
  - All routers need to know the network-wide routes.
  - Traditional IP forwarding is connectionless-oriented and cannot provide good end-to-end QoS guarantee.

R1 routing table

Destination/Mask	Protocol	Preference	Cost	NextHop	Interface
192.168.1.0/24	Direct	0	0	192.168.1.254	GE 0/0/0
192.168.12.0/24	Direct	0	0	192.168.12.1	GE 0/0/2
192.168.2.0/24	OSPF	10	3	192.168.12.2	GE 0/0/2

MPLS Label-based Forwarding



- MPLS is used on IP backbone networks.
- MPLS is a tunneling technology that provides connection-oriented switching for the network layer based on IP routing and control protocols. It provides better QoS guarantee.
- MPLS labels, instead of IP routes, are searched for to forward packets, which greatly improves forwarding efficiency.
- Labels used in MPLS forwarding can be manually configured or dynamically allocated using a label distribution protocol.

MPLS Encapsulation

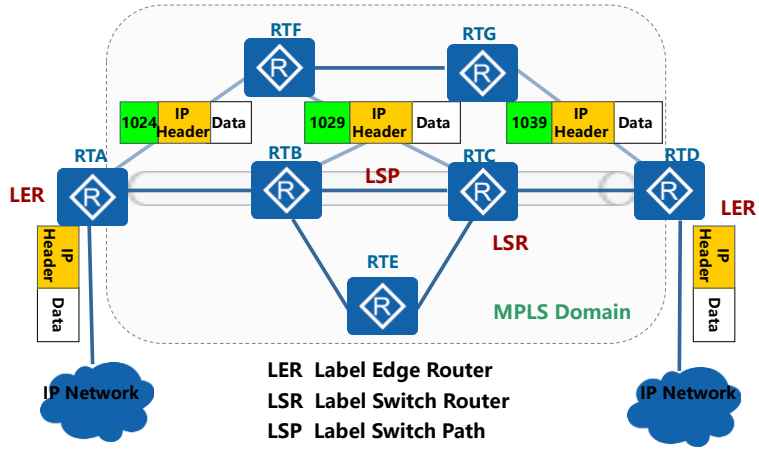
- An MPLS label header is added between the Layer 2 header and Layer 3 header of a packet. Ethernet and PPP use this encapsulation mode.

Layer 2 frame format

MPLS frame mode encapsulation

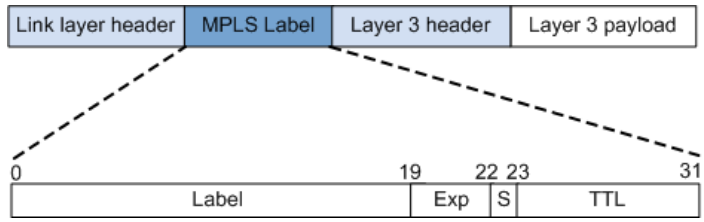
- MPLS labels are used to transmit MPLS information. Routers exchange labels to transmit data on the established label forwarding paths.

MPLS network model



- The typical structure of MPLS network is shown in this slide: the router and ATM switch located inside of MPLS domain are called LSR, router and ATM switch located at the edge of MPLS domain that used to connect IP network or other kinds of network are called LER.
- In IP network, it implements traditional IP forwarding; in MPLS domain, it implements label forwarding.
- Both of LER and LSR have the ability of label forwarding, but they are located in different position, the packet processing is different. LER's charge is to receive IP packet from IP network and insert label into the packet, then transmit it to LSR, whereas, its charge is also to receive labeled packet from LSR and remove label, transmit it to IP network; LSR's charge is to forward according to the label.
- The path that packet passes through in MPLS domain is called Label Switch Path (LSP), this path is already confirmed and established by kinds of protocols before packet forwarding, packet will be transmitted along the specified LSP.

MPLS Header



- The total length of MPLS header is 4bytes (32bits)
- The length of Label field is 20bits
- The length of EXP（Experimental Use）field is 3bits
- The length of S（Bottom of Stack）field is1bit
- The length of TTL field is 8bits

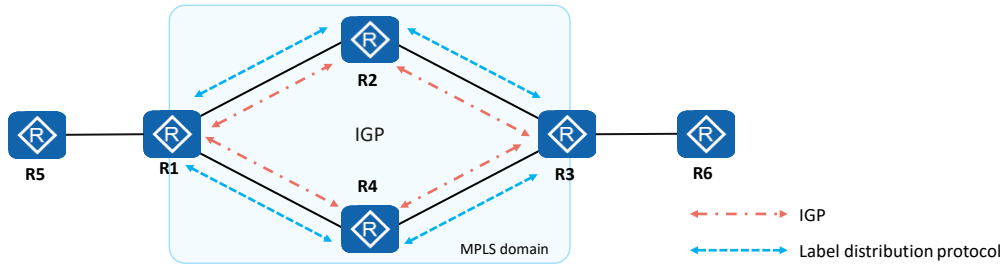
Page 48

The length of MPLS header is 32 bits.

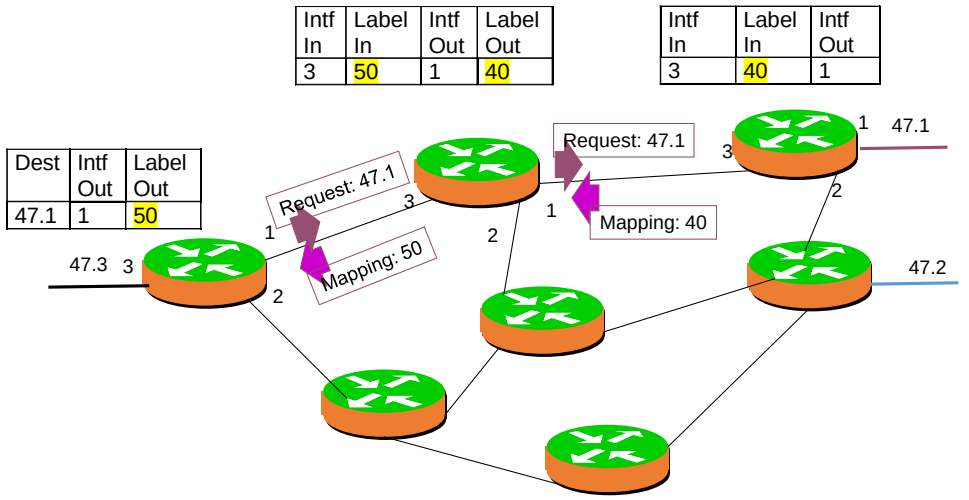
- Label: 20-bit label value.
- Exp: 3-bit, used as an extension, used to carry precedence of IP packet. Generally, this field is used as the class of service (CoS) field. When congestion occurs, devices prioritize packets that have a larger value in this field.
- S: 1-bit value indicating the bottom of a label stack. MPLS supports nesting of multiple labels. When the S field is 1, the label is at the bottom of the label stack.
- TTL: time to live. It is used to prevent data from looping; Its function is similar to TTL of IP header.

MPLS Forwarding Problems

- MPLS labels can be statically or dynamically distributed. The involved problems are as follows:
  - Static label distribution requires manual configuration. As the network scale expands, network topologies are prone to change. Static label configuration cannot meet the requirements of large-scale networks.
  - Some dynamic label distribution protocols do not have the path computation capability and need to use IGPs to compute paths. In addition, the control planes of these protocols are complex, requiring devices to send a large number of messages to maintain peer and path status, wasting link bandwidth and device resources. What is more, despite supporting TE, some label distribution protocols require complex configurations and do not support load balancing. Devices have to send a large number of protocol packets to maintain proper paths. In addition, as devices are independent and know only their own status, they need to exchange signaling packets, which also waste link bandwidth and device resources.



RSVP-TE Procedure for Establishing Dynamic LSPs

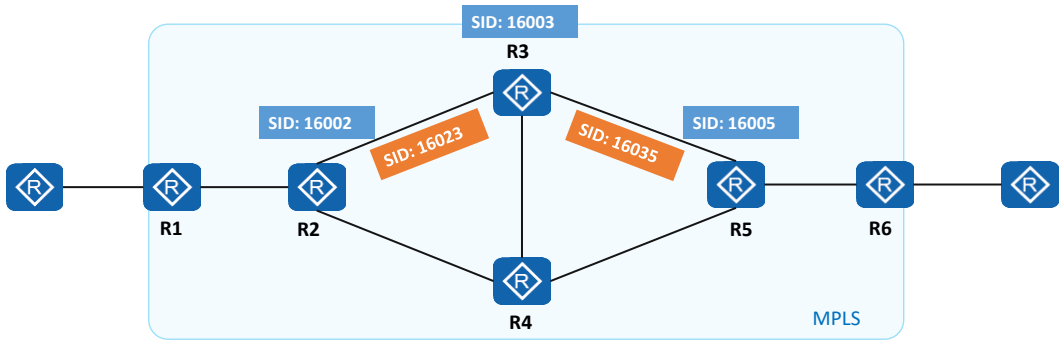


Introduction to Segment Routing

- To solve the problems facing traditional IP forwarding and MPLS forwarding, the industry proposed Segment Routing (SR). SR makes the following improvements:
  1. Extends the existing protocols.
     - The extended IGPs and BGP have the label distribution capability, eliminating the need for other label distribution protocols on networks, and thereby simplifying protocols.
  2. Introduces the source routing mechanism.
     - Using the source routing mechanism, controllers can centrally calculate paths.
  3. Allows networks to be defined by services.
     - Networks are driven by services. After service requirements, such as latency, bandwidth, and packet loss rate requirements, are raised by applications, a controller can collect information such as the network topology, bandwidth usage, and latency, and calculate explicit paths based on these requirements.

SR Forwarding Implementation (1)

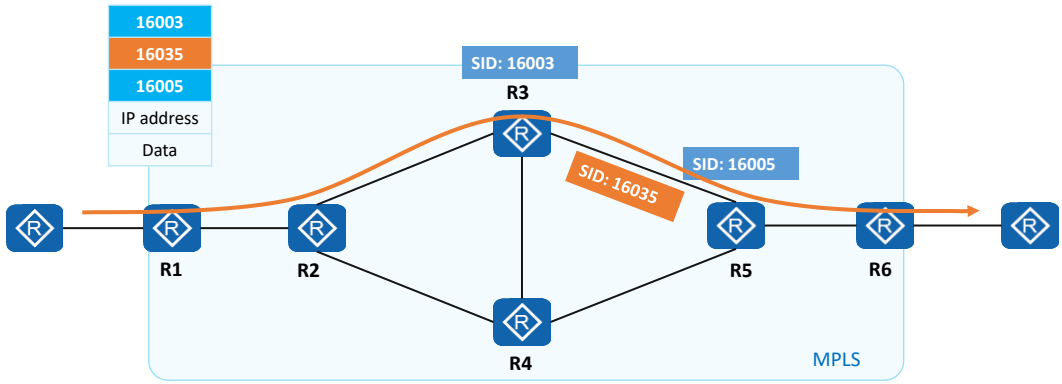
- **SR divides a network path into segments and assigns segment IDs (SIDs) to these segments**.
- **SIDs** are allocated to **forwarding nodes, adjacency links, and destination subnets**. In this example, SIDs of the forwarding nodes are expressed in 1600X, where X is a node ID; SIDs of the adjacency links are expressed in 160XX, where XX indicates the node IDs at both ends of a link.



- SIDs are used to identify segments. The format of SIDs depends on the implementation of technologies. For example, SIDs can be MPLS labels, indexes in an MPLS label space, or IPv6 packet headers. SR using MPLS labels is called SR-MPLS and using IPv6 is called SRv6.

SR Forwarding Implementation (2)

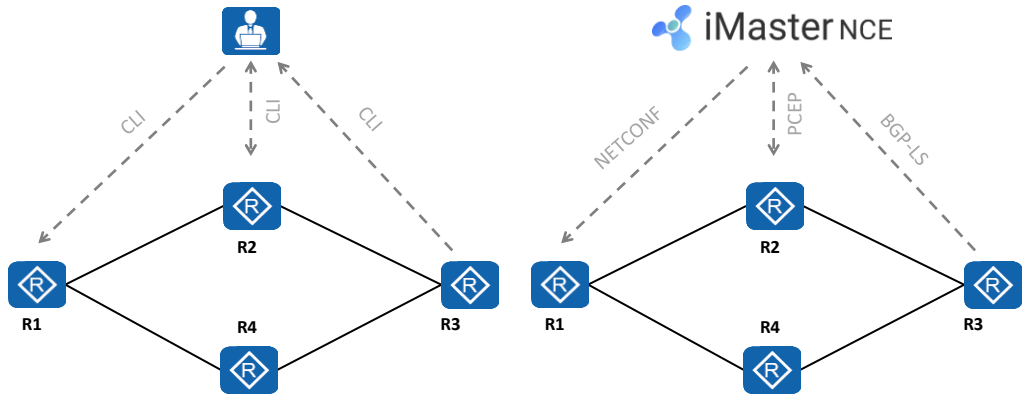
- SIDs of adjacency links and network nodes are arranged in order to form a segment list, which represents a forwarding path. The segment list is encoded by the source node in a header of a data packet, and is transmitted with the data packet. The essence of SR is instructions, which guide where and how packets go.



- After receiving a packet, the receive end parses the segment list. If the top SID in the segment list identifies the local node, the node removes the SID and proceeds with the follow-up procedures. If the top SID does not identify the local node, the node forwards the packet to a next node in equal cost multiple path (ECMP) mode.

SR Deployment Modes

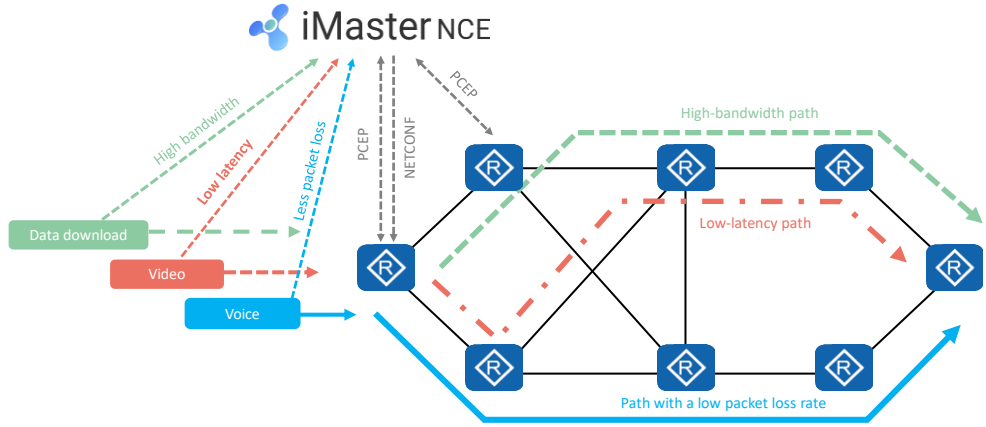
- SR can be deployed with or without a controller. If a controller is used, the controller collects information, reserves path resources, computes paths, and delivers the results to the source node. This mode is preferred.



- PCEP: Path Computation Element Communication Protocol
- NETCONF: Network Configuration Protocol

SR Application

- SR can be used to easily specify packet forwarding paths. On a live network, different paths can be defined for different services. In this example, three explicit paths are defined to implement the service-driven network: one each for data download, video, and voice services. Devices are managed by the controller, which can quickly provision paths in real time.



Quiz

1. (Multiple) Which of the following statements about PPP are true?
   A. PPP supports the bundling of multiple physical links into a logical link to increase the bandwidth.
   B. PPP supports cleartext and ciphertext authentication.
   C. PPP cannot be deployed on Ethernet links because of its poor scalability.
   D. PPP supports asynchronous and synchronous links for the physical layer.
   E. PPP supports multiple network layer protocols, such as IPCP.
2. (Single) After a PPPoE client sends a PADI packet to PPPoE servers, the PPPoE servers reply with a PADO packet. Which kind of frame is the PADO packet?
   A. A. Multicast B. Broadcast C. Unicast D. Anycast
3. (Single) Which of the following values of the Length/Type field in an Ethernet data frame indicates that the Ethernet data frame carries PPPoE discovery packets?
   A. A. 0x0800 B. 0x8864 C. 0x8863 D. 0x0806

1. ABDE
2. B
3. C

More Information

- (Multimedia) Segment Routing MPLS Advanced Series
  - https://support.huawei.com/carrier/docview?nid=DOC1100645168&path=PBI1-7275726/PBI1-21782273/PBI1-7275849/PBI1-7276518/PBI1-15837
- (Multimedia) Segment Routing IPv6 Advanced Series
  - https://support.huawei.com/enterprise/en/doc/EDOC1100133514?idPath=24030814%7C9856750%7C22715517%7C9858933%7C15837