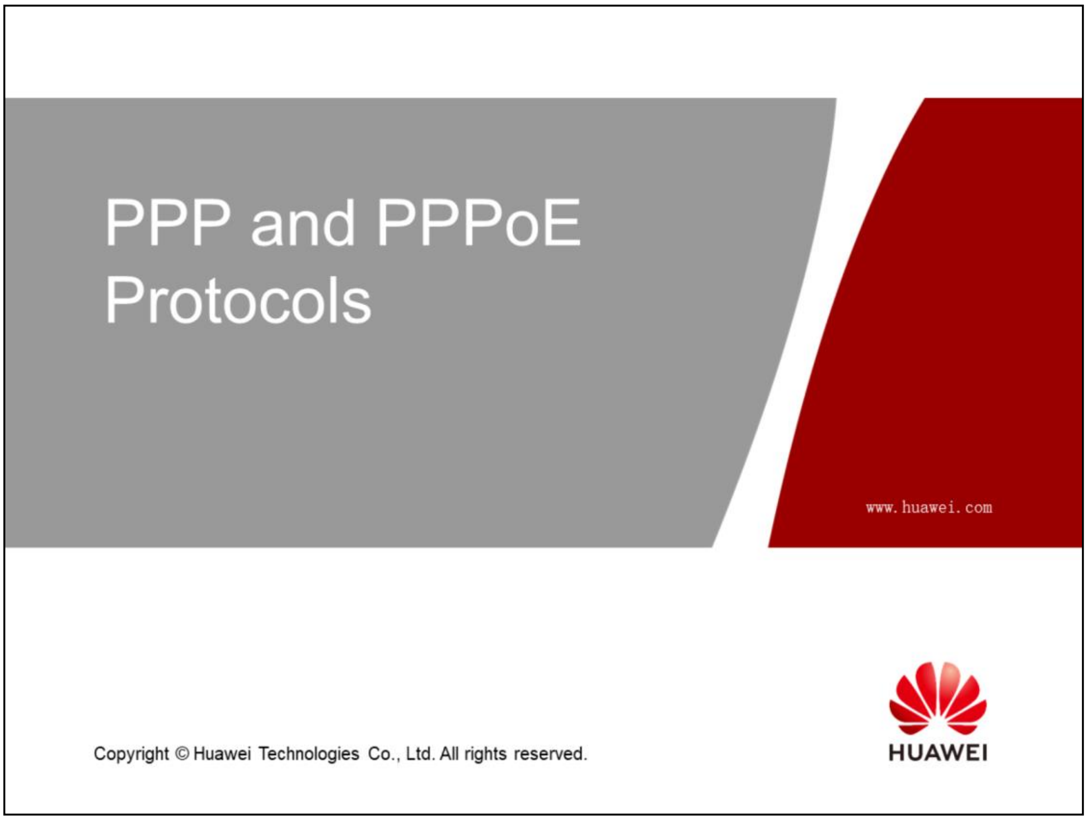
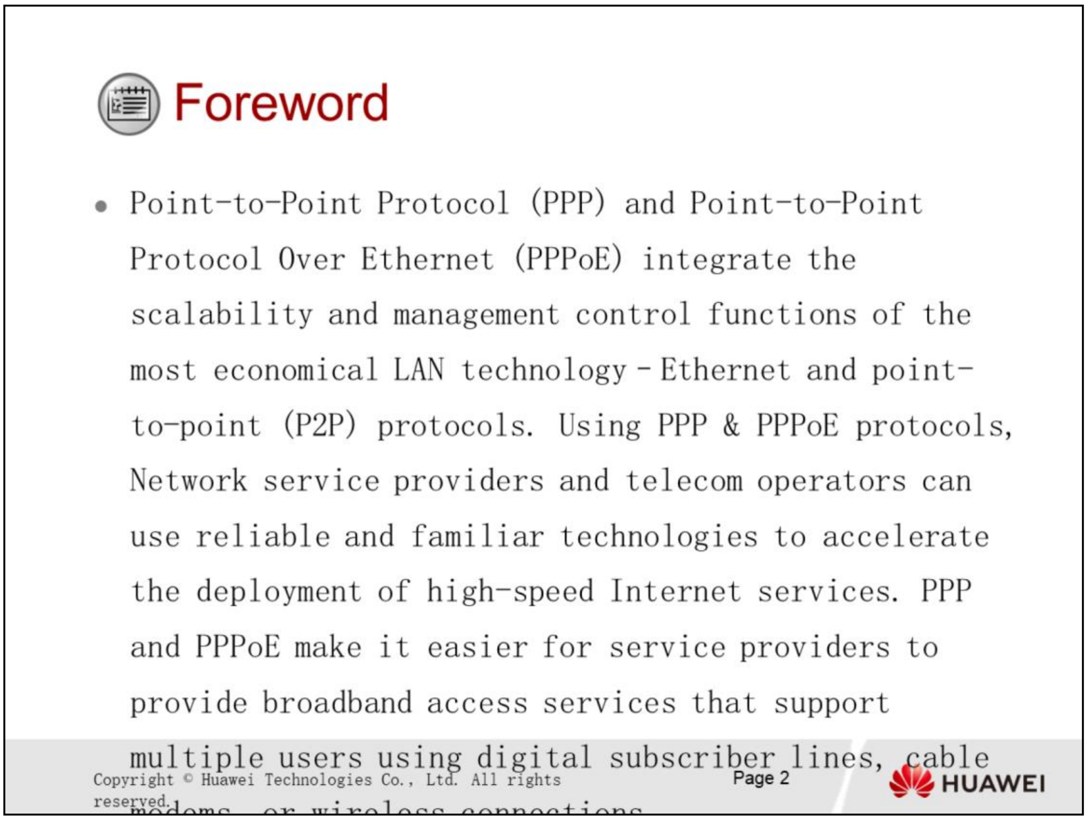


PPP and PPPoE Protocols

www.huawei.com



Foreword

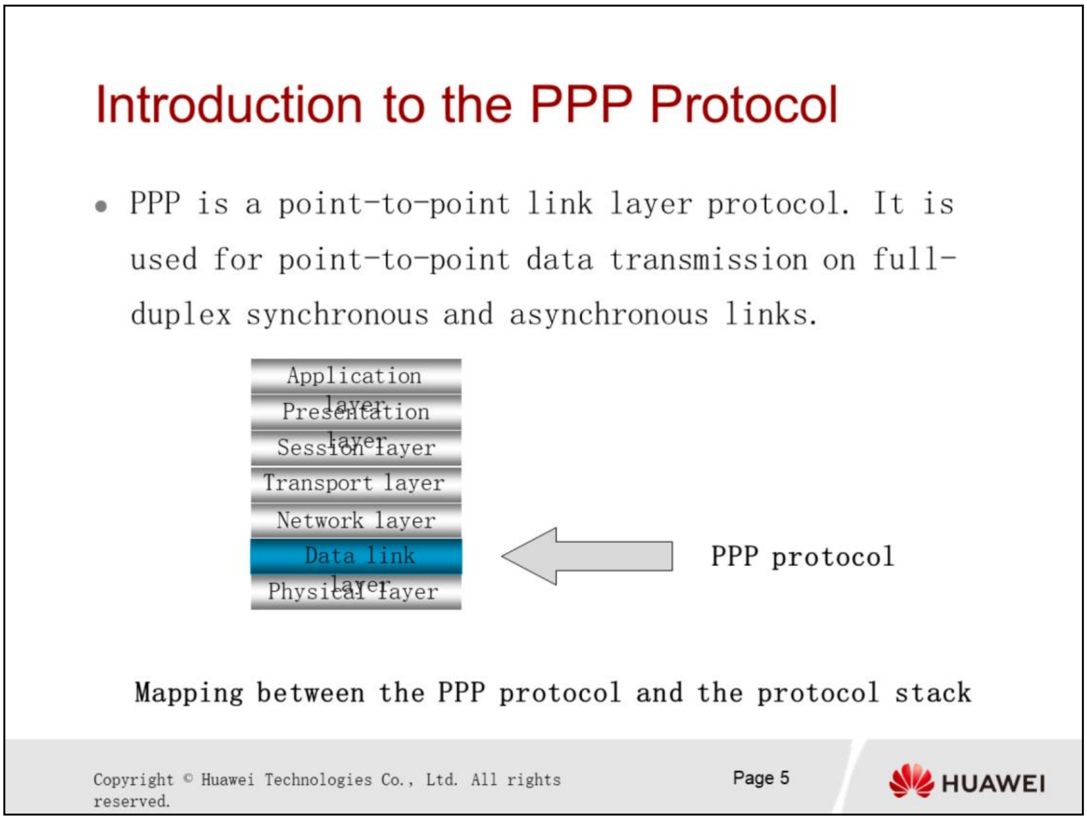
- Point-to-Point Protocol (PPP) and Point-to-Point Protocol Over Ethernet (PPPoE) integrate the scalability and management control functions of the most economical LAN technology - Ethernet and point-to-point (P2P) protocols. Using PPP & PPPoE protocols, Network service providers and telecom operators can use reliable and familiar technologies to accelerate the deployment of high-speed Internet services. PPP and PPPoE make it easier for service providers to provide broadband access services that support multiple users using digital subscriber lines, cable modems, or wireless connections.

Objectives

- Upon completion of this course, you will be able to:
- Understand the basic principles of the PPP protocol.
- Master the process of exchanging LCP and NCP protocol data packets.
- Understand the basic principles of the PPPoE protocol.

Contents

1. PPP Protocol
2. PPPoE Protocol



Introduction to the PPP Protocol

- PPP is a point-to-point link layer protocol. It is used for point-to-point data transmission on full-duplex synchronous and asynchronous links.

Application layer

Presentation layer

Session layer

Transport layer

Network layer

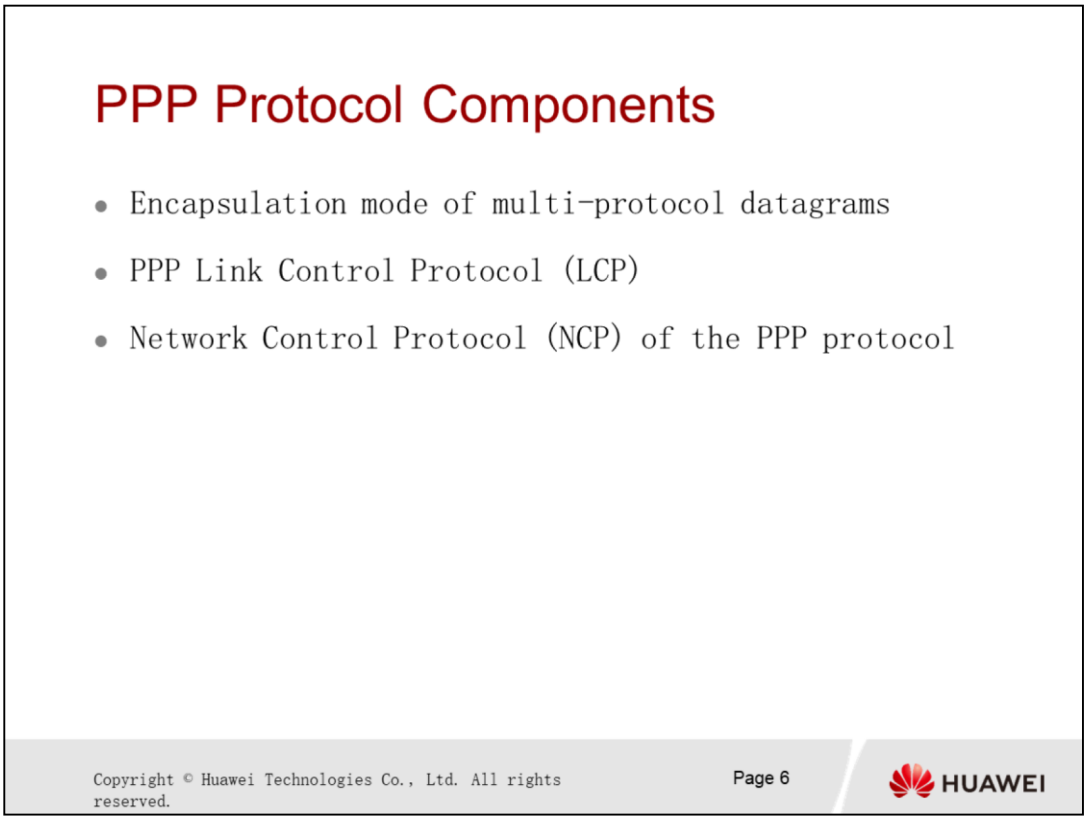
Data link layer

Physical layer

PPP protocol

Mapping between the PPP protocol and the protocol stack

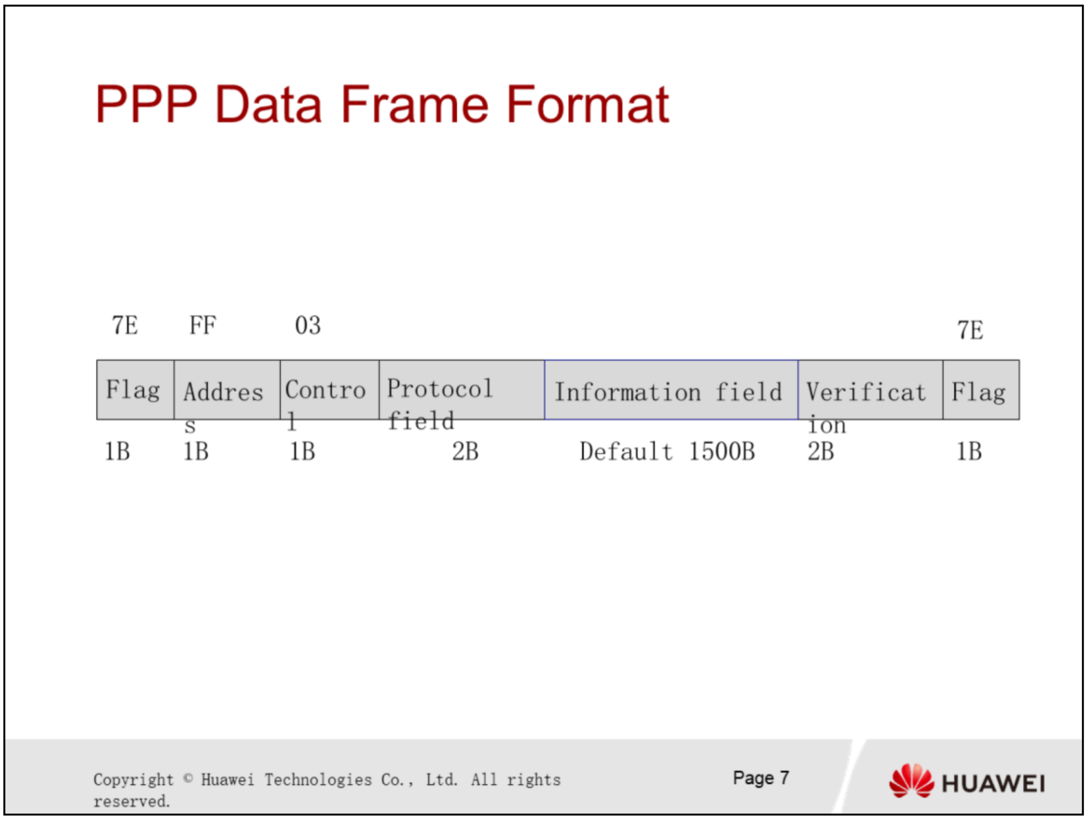
- PPP is a point-to-point link layer protocol. It is used for point-to-point data transmission on full-duplex synchronous and asynchronous links. The PPP protocol has the following advantages:
  - PPP supports both synchronous and asynchronous transmission. Data link layer protocols such as X.25 and Frame Relay (FR) support only synchronous transmission, while SLIP supports only asynchronous transmission.
  - The PPP protocol has good scalability. For example, when the PPP protocol needs to be carried on the Ethernet link, the PPP can be extended to PPPoE.
  - PPP provides the Link Control Protocol (LCP) protocol to negotiate link layer parameters.
  - PPP provides various network control protocols (NCPs), such as IPCP and IPXCP, to negotiate network layer parameters and better support the network layer protocols.
  - PPP provides the Challenge-Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP) authentication protocols to ensure network security.
  - No-retransmission mechanism, low network overhead, and fast speed.



PPP Protocol Components

- Encapsulation mode of multi-protocol datagrams
- PPP Link Control Protocol (LCP)
- Network Control Protocol (NCP) of the PPP protocol

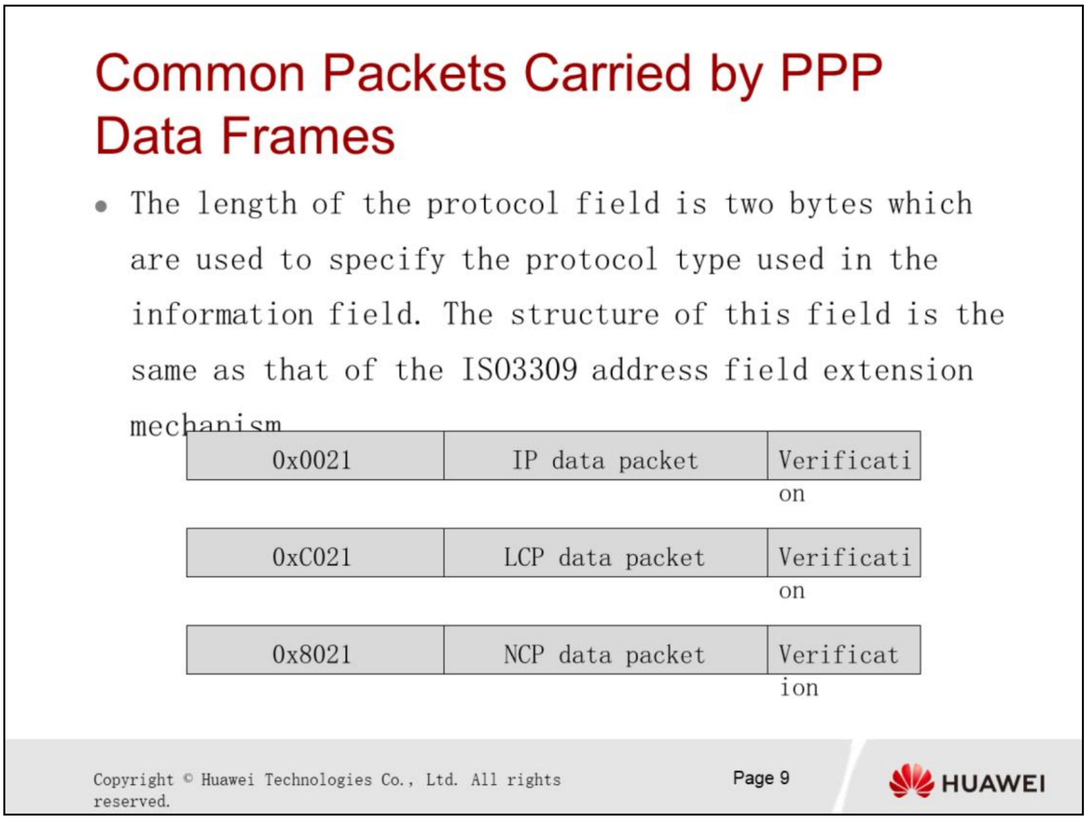
- The PPP protocol consists of 3 parts: Link Control Protocol (LCP), Network Control Protocol (NCP), and extended PPP protocol (such as Multilink Protocol). With the development of network technologies, network bandwidth is no longer a bottleneck. Therefore, the application of PPP extension protocols is less and less, and people tend to ignore PPP extension protocols.



PPP Data Frame Format

7E	FF	03				7E
Flag	Address	Control	Protocol field	Information field	Verification	Flag
1B	1B	1B	2B	Default 1500B	2B	1B

- The same as many other commonly used data link layer protocols, the PPP protocol also uses the delimitation frame format of the HDLC protocol which originates from the SDLC protocol for packet encapsulation.
- The following describes the encapsulation format of the PPP data frame:
- Each PPP data frame starts and ends with a flag byte which is 0x7E.
- The byte following to the start flag byte is the address field, which is 0xFF. We know that a network is layered, peer layers communicate with each other, and a lower layer provides services for the upper layer. When peer layers communicate with each other, the party needs to learn the address of the peer end. In the data link layer, the address refers to the MAC address, X.121 address, and ATM address of the peer. In the network layer, the address refers to the IP address and IPX address of the peer. In the transport layer, the address refers to the protocol port number of the peer. For example, if 2 hosts on an Ethernet network want to communicate with each other, the sender needs to learn the MAC address of the receiver. The PPP protocol, however, is used on point-to-point links. Unlike a broadcast or multipoint network, a point-to-point link can uniquely identify a peer. Therefore, the communication devices at two ends that use the PPP protocol do not need to know the data link layer address of each other. The corresponding address byte is meaningless and filled with a broadcast address with all 1s according to the protocol requirement.

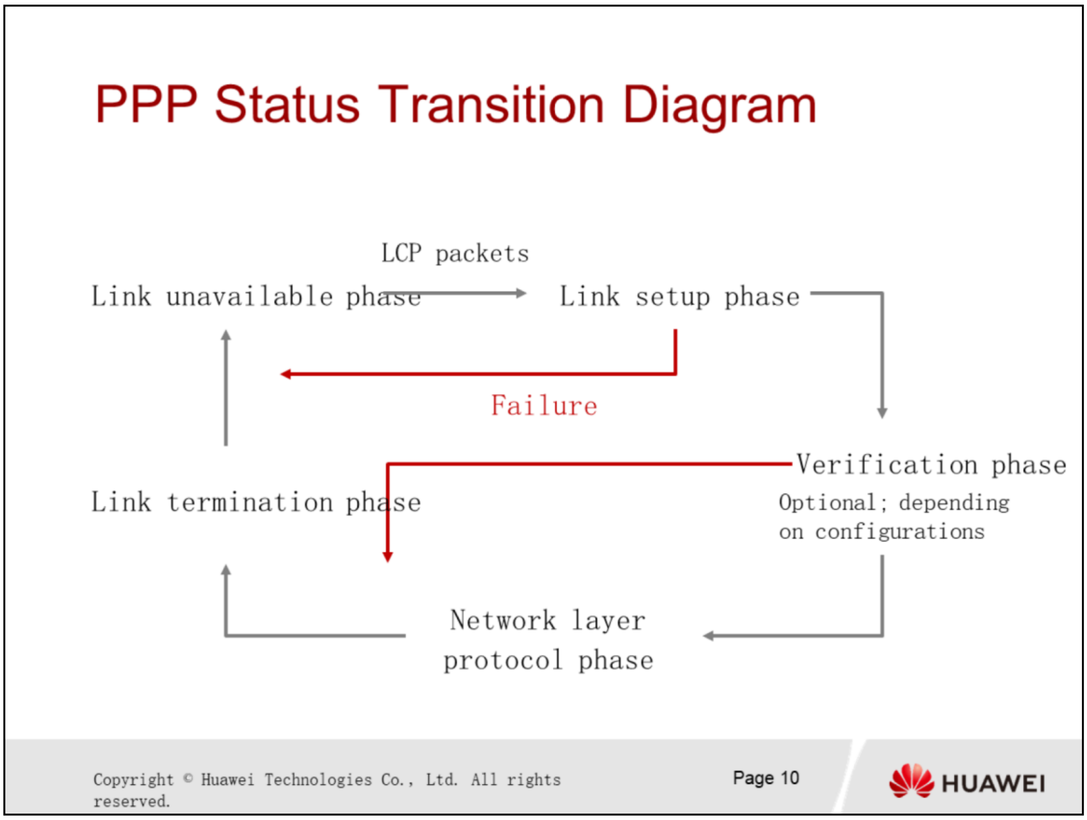


Common Packets Carried by PPP Data Frames

- The length of the protocol field is two bytes which are used to specify the protocol type used in the information field. The structure of this field is the same as that of the IS03309 address field extension mechanism

0x0021	IP data packet	Verification
0xC021	LCP data packet	Verification
0x8021	NCP data packet	Verification

- To adapt to complex and changeable network environments, the PPP protocol provides a Link Control Protocol (LCP) to configure and test data communication links. The LCP protocol can be used to negotiate configuration parameter options of the PPP protocol, process data frames of different sizes, detect link loops and errors, and terminate links.
- The NCP protocol of the PPP provides a family of protocols for different network layer. The common network control protocols include the IPCP for the TCP/IP network and the IPXCP for the SPX/IPX network. The IPCP protocol is most widely used. NCP parameters are negotiated between two ends of a P2P network mainly to communicate the network layer addresses of both ends.



PPP Status Transition Diagram

LCP packets

Link unavailable phase

Link setup phase

Failure

Verification phase

Optional; depending on configurations

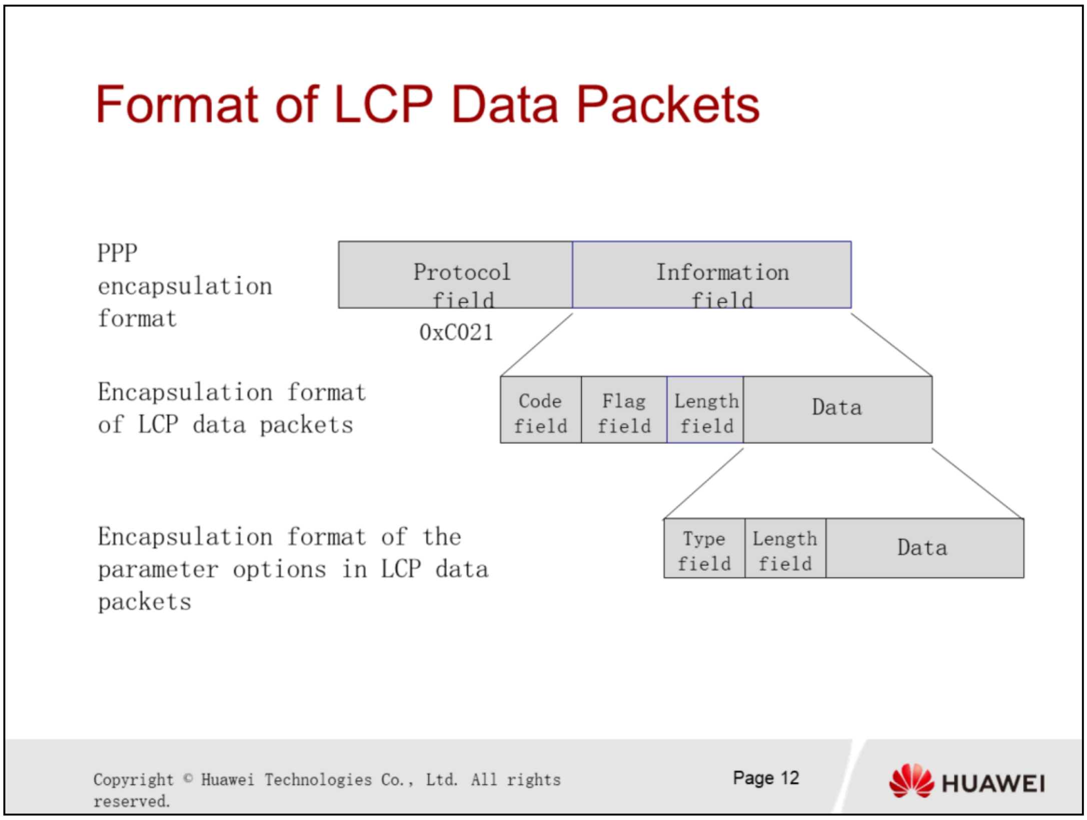
Link termination phase

Network layer protocol phase

- If data communication device (routers in this context) at two ends want to establish P2P communication through the PPP protocol, either end needs to send LCP data packets to configure the link (test link). After the LCP configuration parameters are negotiated, the two communicating parties can determine the authentication modes at both ends of the link based on the authentication configuration parameters negotiated in the LCP configuration request packet. By default, the two parties do not authenticate each other. Instead, they directly negotiate NCP configuration parameter options. After all the configuration procedures are complete, the two parties can transmit data packets at the network layer through the established link. The link is then available. A link is disconnected to shut down the PPP session when either party receives LCP or NCP link shutdown packets, the physical layer cannot detect the carrier, or when a management person shuts down the link. Generally, the NCP does not need to shut down a link, and link shutdown packets are sent in the LCP negotiation or application session phase.

- During the configuration, maintenance, and termination of a P2P link, PPP goes through the following phases:

  - Link unavailability phase: This phase is sometimes referred to as the physical layer unavailable phase. All PPP link starts and ends at this phase. When the two ends of a communication detect that the physical line is activated (generally, a carrier signal is detected on the link), the next phase starts (that is, the link setup phase). In short, in link setup phase, the LCP is used to configure link parameters, and the state machine of LCP changes with events. When a link is unavailable, the LCP state machine is in the initial or starting state. Once the physical line is detected to be available, the LCP state machine changes. After a link is disconnected, state machine goes back to the initial or starting state. In the actual process, the time spent in this phase is very short to detect only the presence of peer devices.



Format of LCP Data Packets

PPP encapsulation format

Protocol field

Information field

0xC021

Encapsulation format of LCP data packets

Code field

Flag field

Length field

Data

Encapsulation format of the parameter options in LCP data packets

Type field

Length field

Data

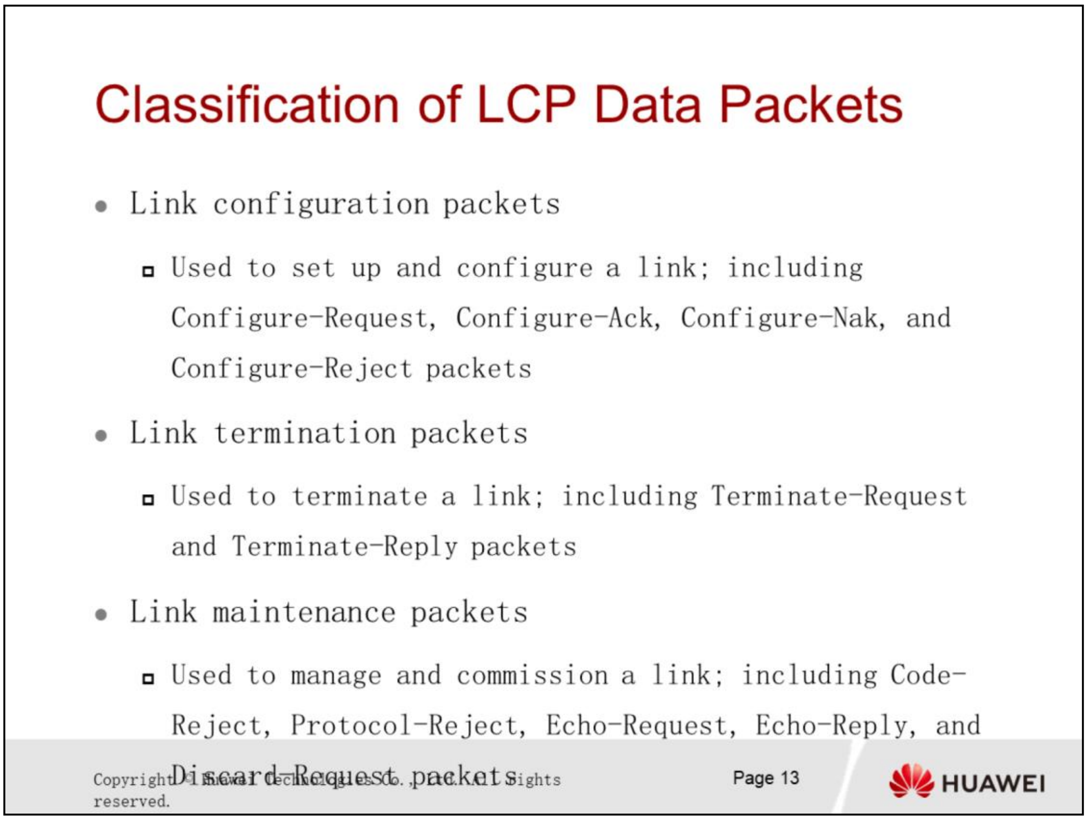
Page 12

HUAWEI

- LCP data packets are exchanged during link setup. As the payload of PPP packets, LCP packets are encapsulated in the information field of PPP data frames. In this case, the protocol field of a PPP data frame is fixed to 0xC021, but the information field changes during the link setup phase, containing many types of packets to be distinguished by the corresponding fields. The figure shows a common encapsulation mode for LCP data packets.
- The length of the code field is one byte, which is used to identify the type of an LCP data packet. In the link setup phase, if the receiver receives an LCP packet with a code field that cannot be identified, it sends an LCP Code-Reject packet to the sender.
- The flag field also contains 1 byte, which is used to match request and response packets. Generally, in the link setup phase, both ends of the communication send several Config-Request packets which may have the same data fields but different flag fields. The ID of a Config-Request packet usually starts from 0x01 and is incremented by 1. After the peer receives the Config-Request packet, it responds with a packet (Config-Ack, Config-Nak, or Config-Reject) with the same ID as that in the Config-Request packet. After receiving the response packet, the sender of the Config-Request packet compares the response packet with the Config-Request packet to determine the next operation.
- Content of the length field = Total byte length (code field + flag field + length field + data field). The bytes not indicated by the length field are considered as padding bytes and ignored. In addition, the content of length

field cannot exceed the MRU value.

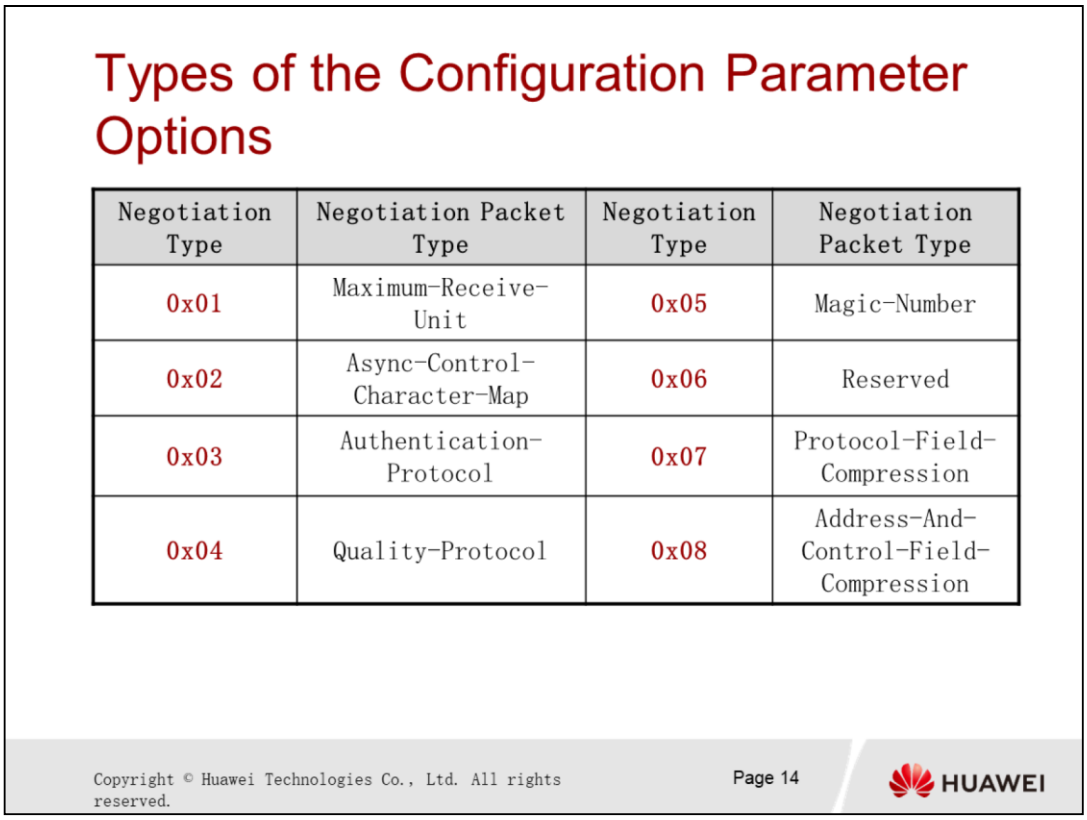
- The content of the data field varies depending on LCP data packets.



Classification of LCP Data Packets

- Link configuration packets
  - Used to set up and configure a link; including Configure-Request, Configure-Ack, Configure-Nak, and Configure-Reject packets
- Link termination packets
  - Used to terminate a link; including Terminate-Request and Terminate-Reply packets
- Link maintenance packets
  - Used to manage and commission a link; including Code-Reject, Protocol-Reject, Echo-Request, Echo-Reply, and Discard-Request packets

- Link termination packets are classified into Terminate-Request and Terminate-Reply packets. LCP packets provide a mechanism to shut down a P2P connection. If one party wants to shut down a link, it continuously sends Terminate-Request packets until receiving a Terminate-Reply packet from the peer. After receiving a Terminate-Request packet, the receiver must respond with a Terminate-Reply packet, wait for the peer end to disconnect the link, and then complete all the link shutdown operations on the local end.
- The data field of an LCP link termination packet is different from that of a link configuration packet. A link termination packet does not need to carry options of configuration parameter. The IDs of link termination packets must also be consistent. A link is terminated only when the Terminate-Reply packet is received.



Types of the Configuration Parameter Options

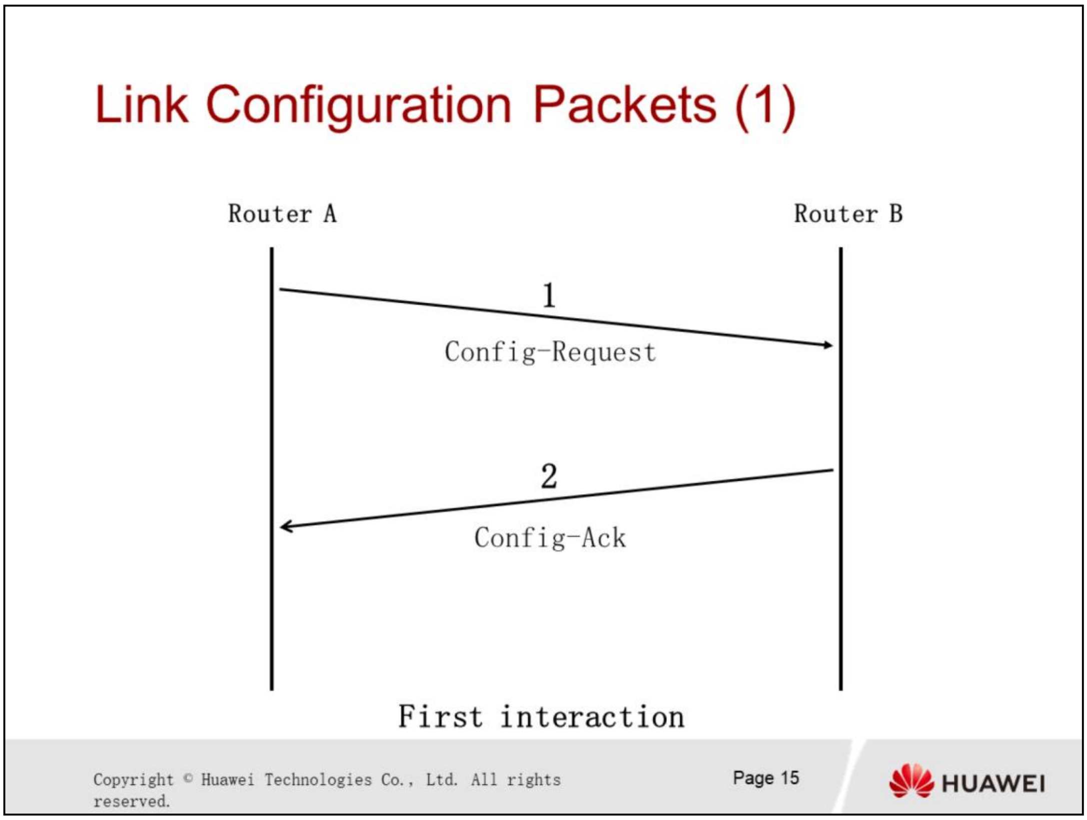
Negotiation Type	Negotiation Packet Type	Negotiation Type	Negotiation Packet Type
0x01	Maximum-Receive-Unit	0x05	Magic-Number
0x02	Async-Control-Character-Map	0x06	Reserved
0x03	Authentication-Protocol	0x07	Protocol-Field-Compression
0x04	Quality-Protocol	0x08	Address-And-Control-Field-Compression

Page 14

- Link configuration packets are different from the other 2 types of packets, and are used to negotiate the configuration parameter options of the link. Therefore, the data fields of this type of packets need to carry various configuration parameter options.
- Link configuration packets include Config-Request, Config-Ack, Config-Nak, and Config-Reject packets.
- When a link needs to be set up between the two communicating parties, either party needs to send Config-Request packets which carry the configuration parameter options to be negotiated.
- Upon receiving a Config-Request packet, the receiver selects one of the remaining 3 packet types to respond to the request packet based on the following conditions:
    - Whether the type fields of all configuration parameter options can be identified. One Config-Request packet may carry multiple configuration parameter options at the same time, but a communication device that supports the PPP protocol does not necessarily support all configuration options. Even if a configuration option is supported, the function may also be disabled in actual applications. For example, a device that supports PPP protocol may disable all configuration options and support only 0x01 and 0x03. In this case, if a Config-Request packet received from the peer end contains the 0x04 configuration option, the local end regards configuration parameter option as unidentifiable, and the negotiation of the configuration parameter option fails.
    - Whether the type fields of all configuration parameter options are acceptable. A peer that can identify configuration parameter options in a received Config-Request packet does not necessarily accept the negotiation. For example, if one party wants the magic number to be set to all 0 but the peer end wants to set it otherwise, the negotiation

fails.

- Response packets are selected based on the 2 two conditions to respond to configuration request packets.



Link Configuration Packets (1)

Router A

Router B

1

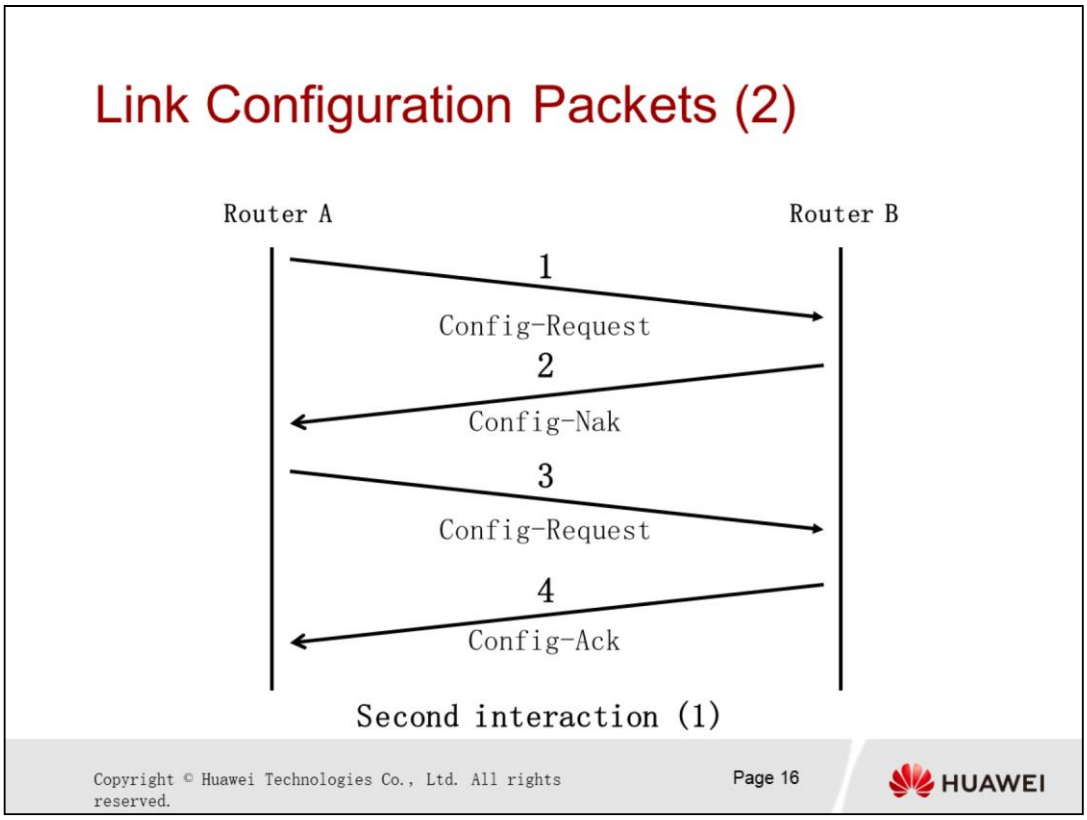
Config-Request

2

Config-Ack

First interaction

- If the receiver of a Config-Request packet can identify all configuration parameter options and accepts the parameter options, the receiver places configuration parameter options without any change in the data field of a Config-Ack packet, and sends the Config-Ack packet as a response to the request sender. According to the protocol, the sequence of configuration parameter options cannot be changed. After the Config-Request sender receives the Config-Ack packet from the peer end, the next phase starts.



Link Configuration Packets (2)

Router A

Router B

1

Config-Request

2

Config-Nak

3

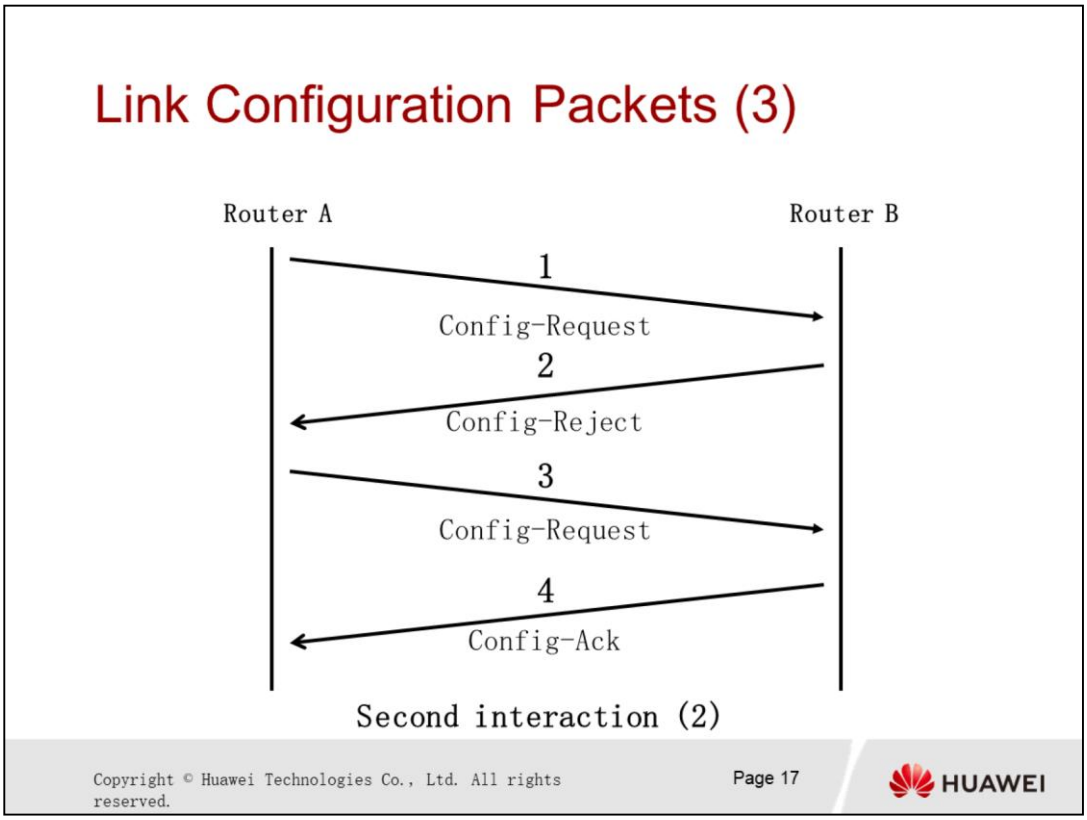
Config-Request

4

Config-Ack

Second interaction (1)

- If the receiver of a Config-Request packet can identify all configuration parameter options but accepts only some of the parameter options, the receiver returns a Config-Nak packet that contains only unacceptable configuration parameter options and the acceptable values to the request sender. Upon receiving the Config-Nak packet, the request sender sends another Config-Request packet with acceptable parameter options the same as those in the previous one and unacceptable parameter options set to the values acceptable to the receiver (as specified in the Config-Nak packet).

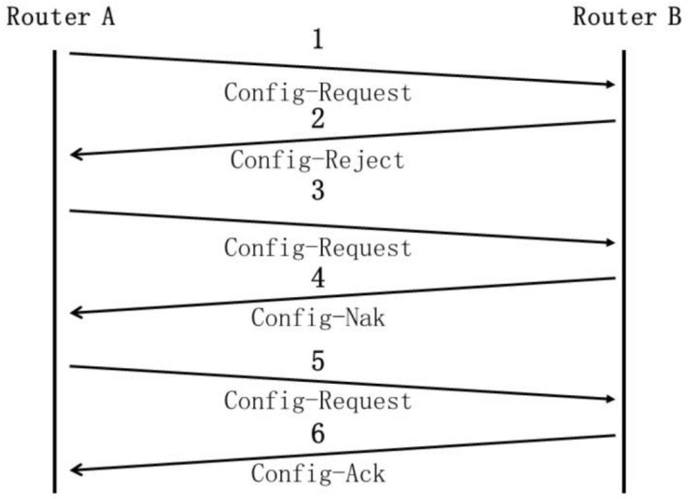


Link Configuration Packets (3)

Second interaction (2)

- If the receiver of a Config-Request packet cannot identify all configuration parameter options, the receiver returns a Config-Reject packet that contains only parameter options whose type field cannot be identified to the request sender. Upon receiving the Config-Reject packet, the request sender sends another Config-Request packet with identifiable parameter options the same as those in the previous one and unidentifiable parameter options deleted.
- It can be seen that the link configuration phase may involve several rounds of negotiations depending on devices at the two ends of a P2P link. The two parties of a PPP link independently complete the negotiation process of their respective configuration parameter options.

Link Configuration Packets (4)



Router A

Router B

1 Config-Request

2 Config-Reject

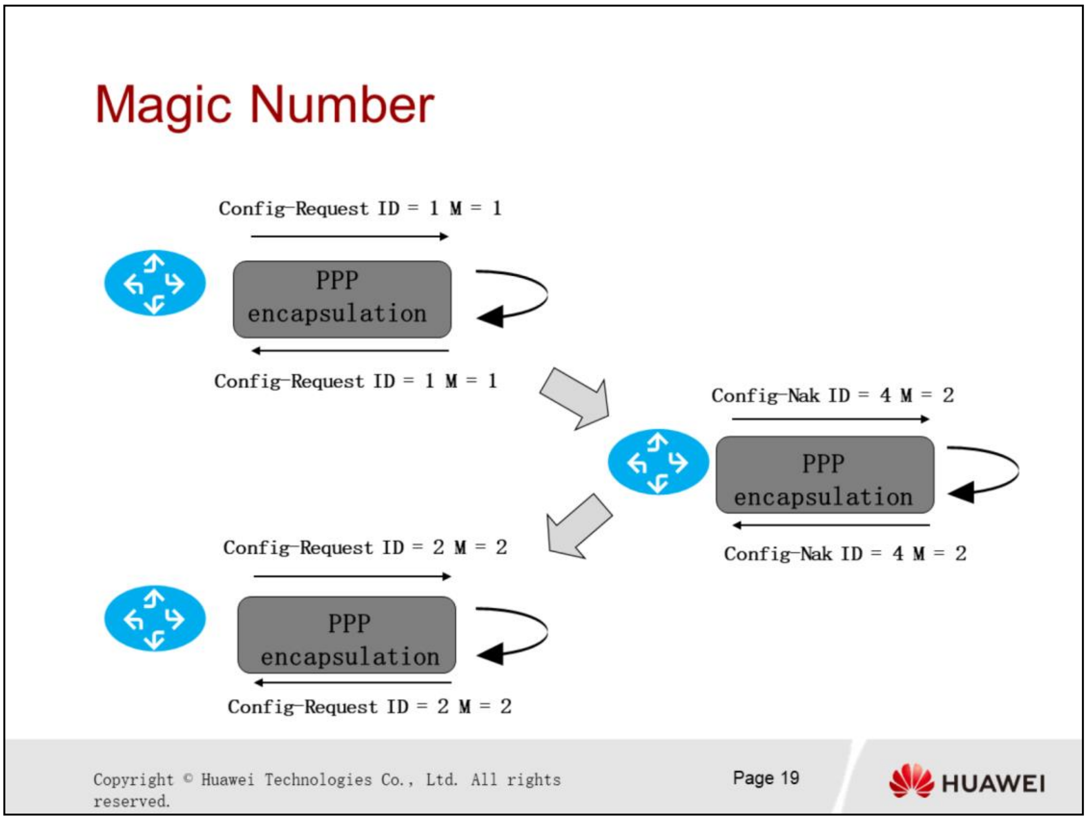
3 Config-Request

4 Config-Nak

5 Config-Request

6 Config-Ack

Multiple interactions



Magic Number

Config-Request ID = 1 M = 1

PPP encapsulation

Config-Request ID = 1 M = 1

Config-Nak ID = 4 M = 2

PPP encapsulation

Config-Nak ID = 4 M = 2

Config-Request ID = 2 M = 2

PPP encapsulation

Config-Request ID = 2 M = 2

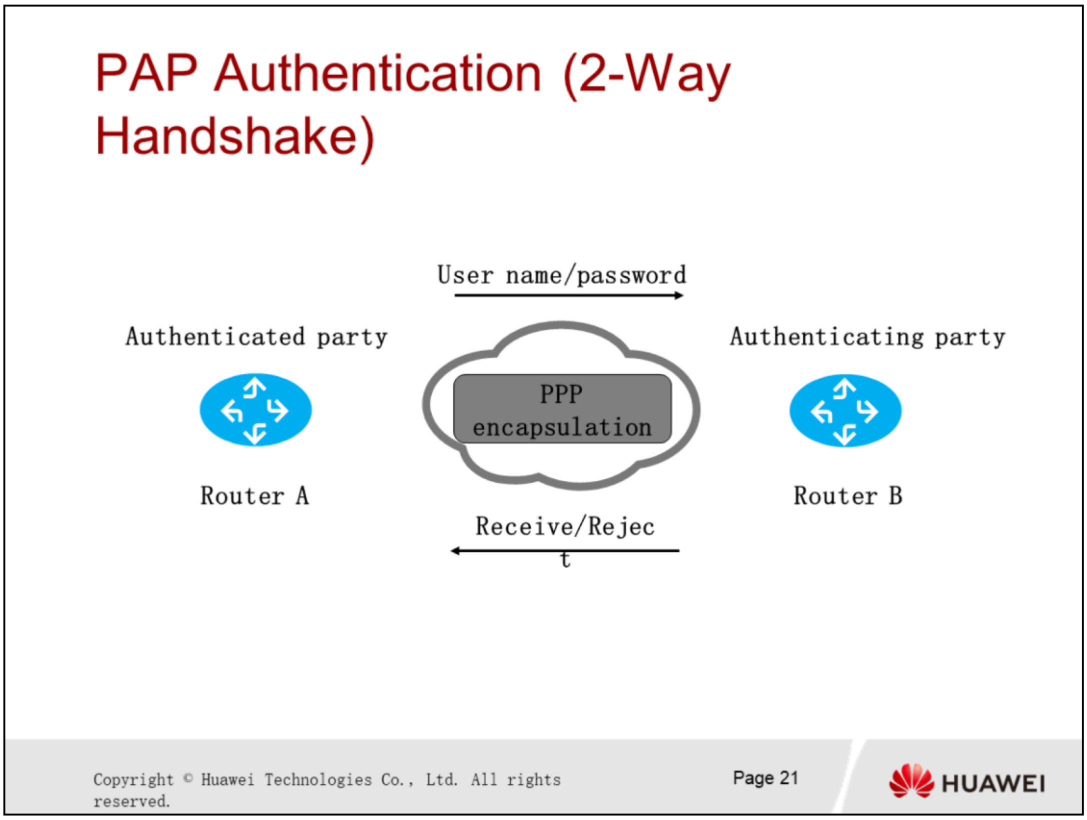
Page 19

HUAWEI

- The magic number is negotiated in LCP Config-Request packets and can be used by other types of LCP packets, such as Echo-Request, Echo-Reply, and Quality-Protocol packets. The PPP protocol does not require the negotiation of the magic number. If the magic number is not negotiated between the two parties but needs to be used in some LCP packets, the magic number is filled as 0. If the magic number is negotiated, it is set to the negotiation result.

- The magic number needs to be negotiated on all current devices, and is sent in the configuration option parameters of a Config-Request packet. A magic number is generated by a communication device randomly and must be unique in a data link to avoid communication conflicts. Generally, a magic number is the series number, network hardware address, or clock of a device. The possibility that the two parties generate the same magic number cannot be eliminated but should be avoided if possible. If two devices of the same manufacturer are interconnected, they may generate the same magic number as the method for generating magic numbers is the same for the devices produced by the same manufacturer.

- Magic numbers are used to check whether a loop exists on a link. Upon receiving a Config-Request packet, the receiver compares the packet with the Config-Request received last time. If the two packets contain different magic numbers, no loop exists on the link. If the magic numbers are the same, the receiver considers that a loop may exist on the link, and further confirmation is required. In this case, the receiver sends a Config-Nak packet carrying a new magic number, and does not send any Config-Request packet before receiving a Config-Request or Config-Nak packet. There are two possibilities in this scenario:



PAP Authentication (2-Way Handshake)

User name/password

Authenticated party

Authenticating party

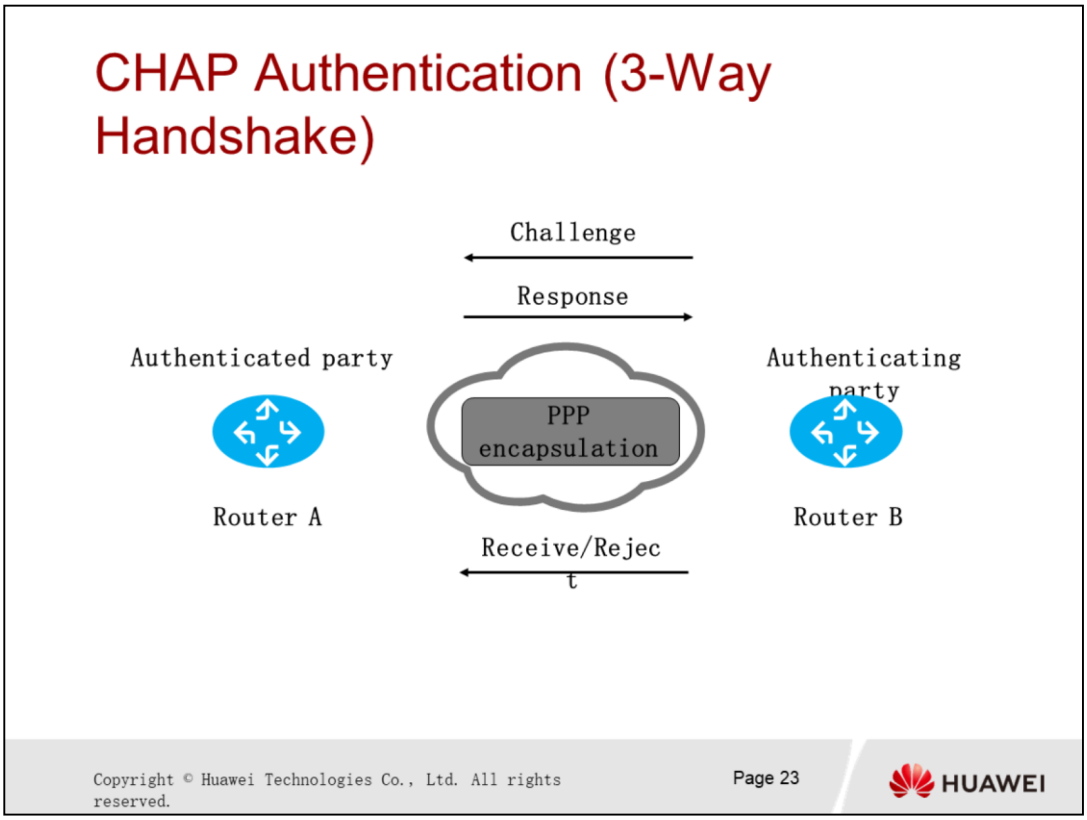
PPP encapsulation

Router A

Router B

Receive/Rejec t

- The PPP protocol also provides optional authentication configuration parameters. By default, the two ends of P2P communication do not authenticate each other. An LCP Config-Request packet can carry only one authentication option at a time (PAP/CHAP as configured on a device interconnected with the PPP device). A device usually supports a default authentication mode (PAP for most devices). After receiving a configuration request packet, the receiver responds with a Config-Ack packet if it supports the authentication mode in the configuration parameter option; otherwise, it responds with a Config-Nak packet containing the supported authentication mode. If the request sender receives a Config-Ack packet, the authentication starts. If the request sender receives a Config-Nak packet, it responds to the peer depending on whether it supports the authentication mode proposed in the Config-Nak packet. If yes, the request sender responds with a new Config-Request (containing the authentication protocol proposed in the Config-Nak packet); otherwise, the request sender responds with a Config-Reject packet, and the two parties cannot pass the authentication. In this case, a PPP link cannot be set up.
- PPP supports two authorization protocols: Password Authentication Protocol (PAP) and Challenge Hand Authentication Protocol (CHAP).



CHAP Authentication (3-Way Handshake)

Challenge

Response

Authenticated party

Authenticating party

PPP encapsulation

Router A

Router B

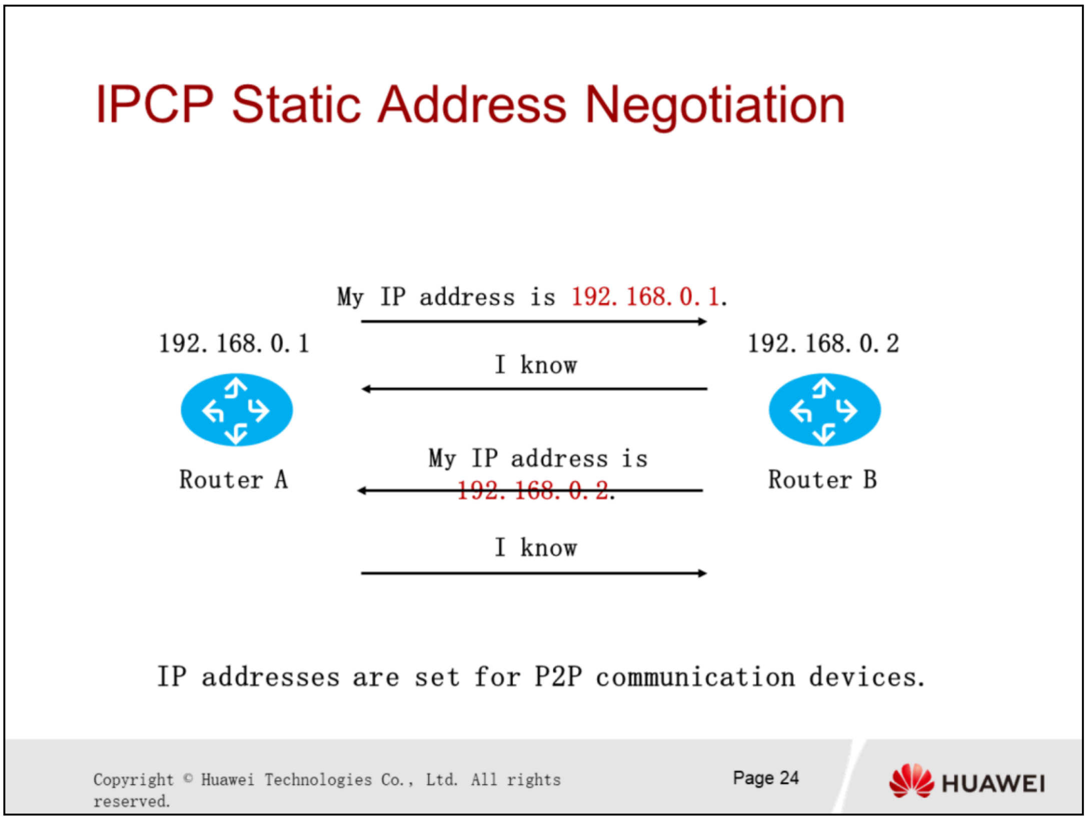
Receive/Reject

Page 23

HUAWEI

- Compared with PAP authentication, CHAP authentication is more secure. In PAP authentication, the user name and password are directly sent to the authenticating party in plain text, which is not the case in CHAP authentication.
- CHAP is a 3-way handshake protocol. It transmits user names on the network without passwords. Therefore, CHAP is more secure than PAP. Unlike PAP which requires the authenticated party to send an authentication request packet when the authentication starts, CHAP requires the authenticating party to send a random packet with its host name. This process is called a challenge. Upon receiving the authentication request, the authenticated party extracts the host name, and searches the corresponding key in its background database. Then the authenticated party generates a response packet using the MD5 encryption algorithm based on the key, packet ID, and random packet received from the authenticating party. The authenticated party sends the response packet with its host name to the authenticating party. Upon receiving the response from the authenticated party, the authenticating party extracts the user name of the authenticated party and searches the corresponding key in the local database. Then the authenticating party generates a result using the MD5 encryption algorithm based on the key, reserved packet ID, and random packet. The authenticating party compares the result with response returned by the authenticated party. If the information is consistent, the authenticating party returns an ACK packet; otherwise, it returns a Nak

packet.



IPCP Static Address Negotiation

My IP address is 192.168.0.1.

192.168.0.1

I know

192.168.0.2

Router A

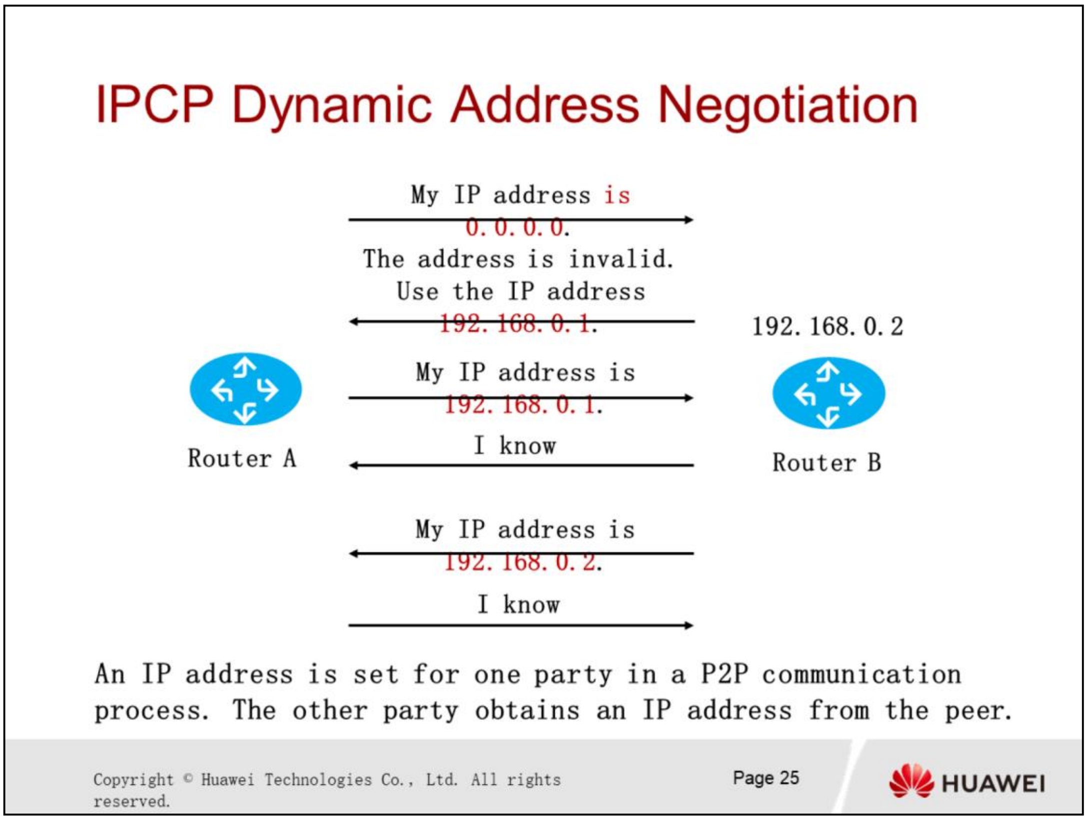
My IP address is 192.168.0.2.

Router B

I know

IP addresses are set for P2P communication devices.

- The IPCP uses the same negotiation mechanism and packet types as the LCP. Although their working process and packets are the same, the IPCP does not invoke the LCP.
- IP address negotiation can be performed in static configuration negotiation and dynamic configuration negotiation modes.
- As shown in the figure, the IP addresses of the two routers are 192.168.0.1/30 and 192.168.0.2/30 respectively.
- The procedure for negotiating a static IP address is as follows:
- 1. Each party sends a Configure-Request packet containing the locally configured IP address.
- 2. Upon receiving a Configure-Request packet, either party checks the IP address. If the IP address is a valid unicast IP address and is different from the locally configured IP address (no IP address conflict), the current party considers that the peer can use this address and responds with a Configure-Ack packet.



IPCP Dynamic Address Negotiation

My IP address is 0.0.0.0.

The address is invalid. Use the IP address 192.168.0.1.

192.168.0.2

Router A

My IP address is 192.168.0.1.

I know

Router B

My IP address is 192.168.0.2.

I know

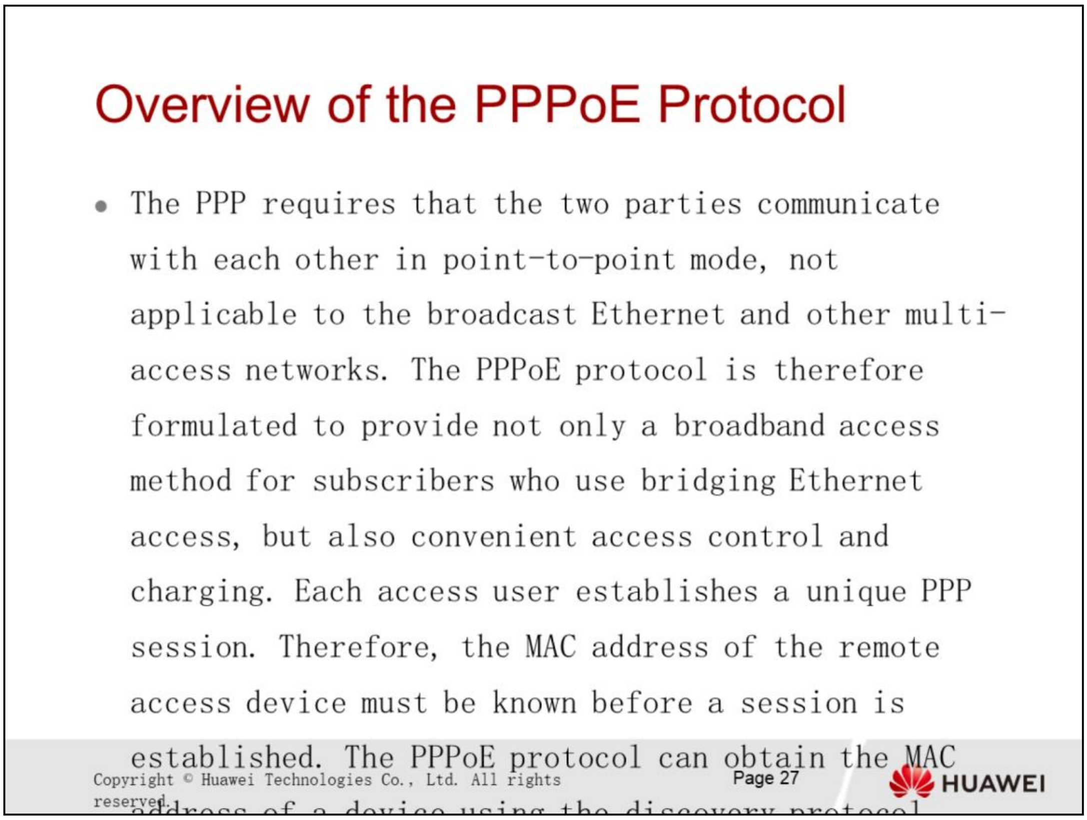
An IP address is set for one party in a P2P communication process. The other party obtains an IP address from the peer.

HUAWEI

- The procedure for negotiating a dynamic IP address is as follows:
- Router A sends a Configure-Request packet to router B. The packet contains IP address 0.0.0.0, indicating that the IP address is requested from the peer end.
- Upon receiving the Configure-Request packet, router B considers that the address (0.0.0.0) contained in the packet is invalid and responds with a Configure-Nak packet containing the new IP address 192.168.0.1.
- Upon receiving the Configure-Nak packet, router A updates the local IP address and sends another Configure-Request packet containing the new IP address 192.168.0.1.
- Upon receiving the Configure-Request packet, router B considers that the IP address contained in the packet is a valid address and returns a Configure-Ack packet.
- In addition, router B sends a Configure-Request packet to router A to request the address 192.168.0.2. Router A considers that the address is valid and returns a Configure-Ack packet.

Contents

1. PPP Protocol
2. PPPoE Protocol

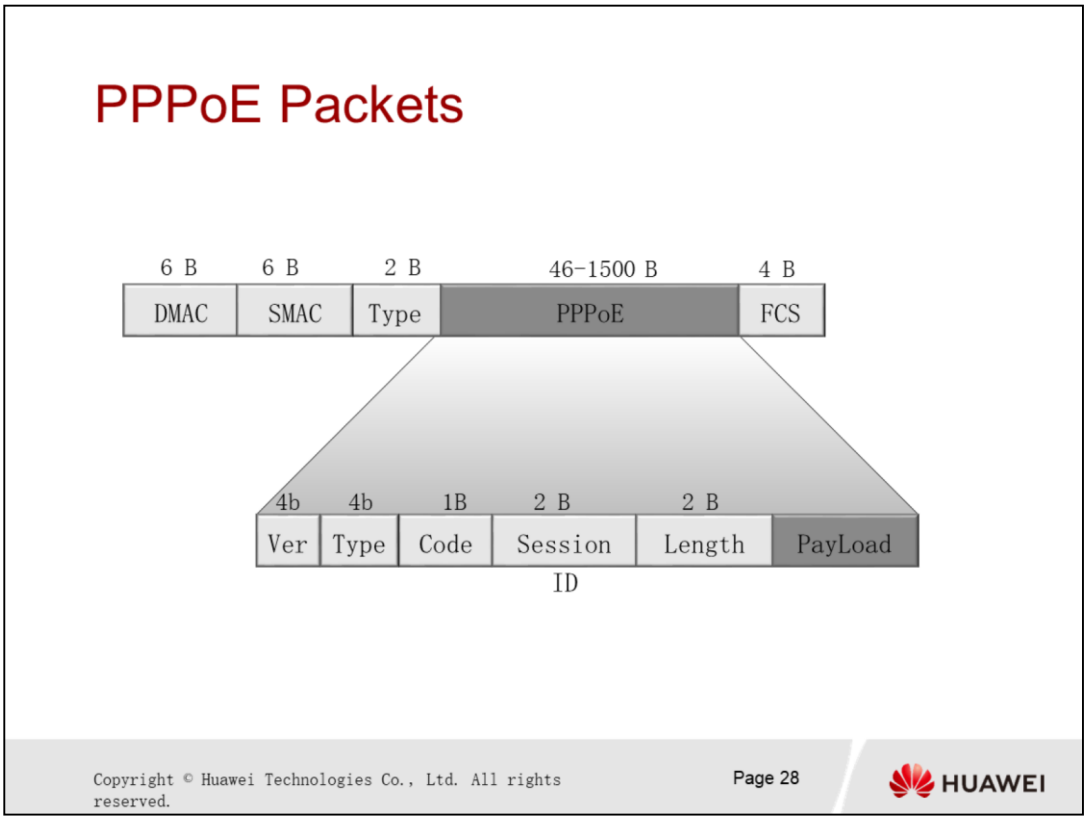


Overview of the PPPoE Protocol

- The PPP requires that the two parties communicate with each other in point-to-point mode, not applicable to the broadcast Ethernet and other multi-access networks. The PPPoE protocol is therefore formulated to provide not only a broadband access method for subscribers who use bridging Ethernet access, but also convenient access control and charging. Each access user establishes a unique PPP session. Therefore, the MAC address of the remote access device must be known before a session is established. The PPPoE protocol can obtain the MAC address of a device using the discovery protocol

- With the development of broadband network technologies, the applications of mainstream broadband access technologies, such as xDSL, cable modem, and Ethernet, are in full swing. At the same time, network operators are confused. Regardless of which access technology is used, how to effectively manage subscribers get profits from network investment are their primary concerns. Therefore, charging becomes critical for various broadband access technologies. In the traditional Ethernet model, there is no concept of subscriber charging. Subscribers can either obtain IP addresses to access the Internet, or cannot access the Internet. IETF engineers developed the PPPoE protocol to transmit PPP data packets on the Ethernet (using NAS devices to terminate subscriber PPP packets). After the protocol is established, network device manufacturers also launch broadband access servers (BASs) with their own brands. These BASs support not only the termination of PPPoE data packets, but also many other protocols.
- The PPPoE protocol provides a standard for connecting multiple hosts in a broadcast network (such as an Ethernet) to a remote access concentrator (also called a broadband access server). In this network model, each subscriber host needs to independently initialize its own PPP protocol stack. In addition, using features of the PPP protocol, subscribers can be charged and managed on a broadcast network. To establish and maintain a P2P relationship between hosts and access concentrators on a broadcast network, a unique P2P session must be established between each host and the access

concentrator.



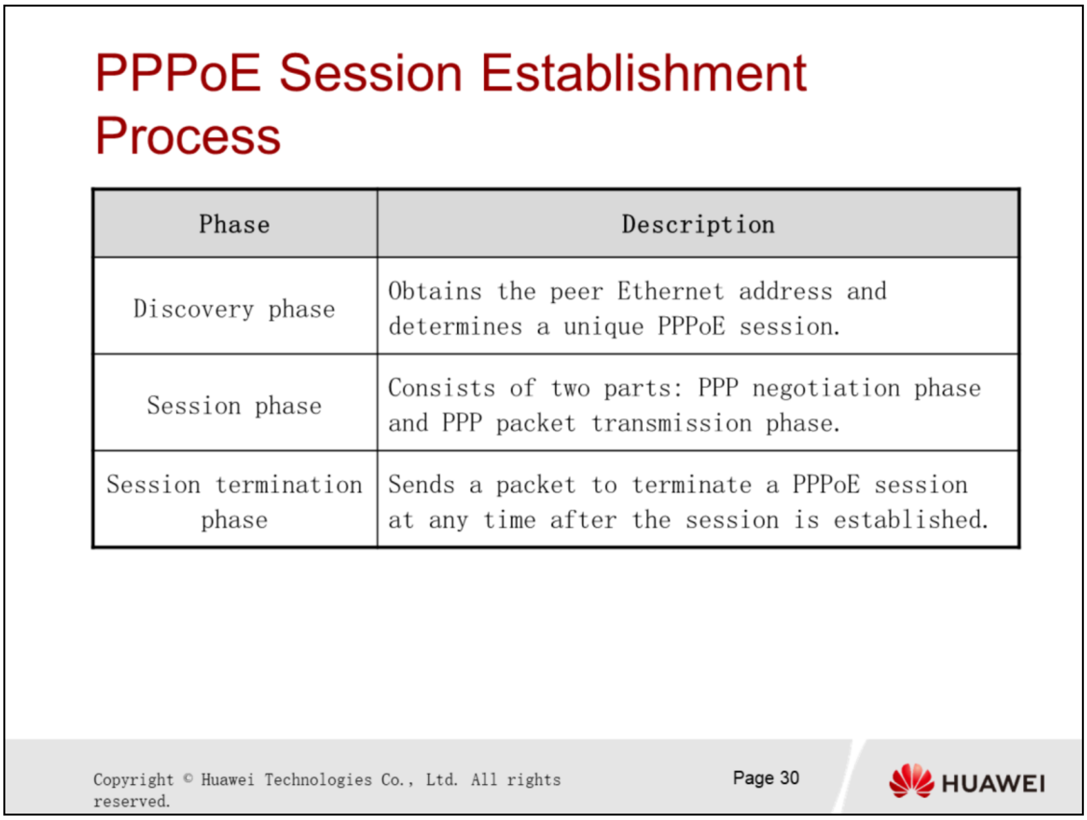
PPPoE Packets

6 B	6 B	2 B	46-1500 B	4 B
DMAC	SMAC	Type	PPPoE	FCS

4b	4b	1B	2 B	2 B	
Ver	Type	Code	Session ID	Length	PayLoad

- The PPPoE initialization process is very important. It not only needs to determine the one-to-one logical relationship on the broadcast network, but also prepares necessary conditions for the PPPoE session, such as the unique session ID allocated by the access concentrator. Before introducing the PPPoE history, we will review the encapsulation format of Ethernet frames. All PPPoE data packets are encapsulated in the data fields (payload area) of the Ethernet frames for transmission.
- The Ethernet frame format is not strange to most network engineers. Currently, most networks use the Ethernet 2.0 version. Therefore, EthernetII is widely used as a factual industrial standard.
  - The Ethernet destination address (destination MAC address) and Ethernet source address (source MAC address) are the most commonly used data link layer addresses. They are classified into unicast addresses, multicast addresses, and broadcast addresses. Unicast and broadcast addresses are used in the PPPoE protocol. For a data link layer protocol such as PPP, the layer 2 address communication is different from common layer 2 communications.
  - The Ethernet type field is also one of the most concerned fields. It was maintained by Xerox before 1997, and was handed over to the IEEE802 team later. Based on the content of this field, the receiver of a data packet can identify the protocol type carried in the data field of the Ethernet packet. The two phases of PPPoE are distinguished by the type field of Ethernet packets. In the PPPoE discovery phase, the Ethernet

type field is set to 0x8863. In the PPPoE session phase, this field is set to 0x8864.



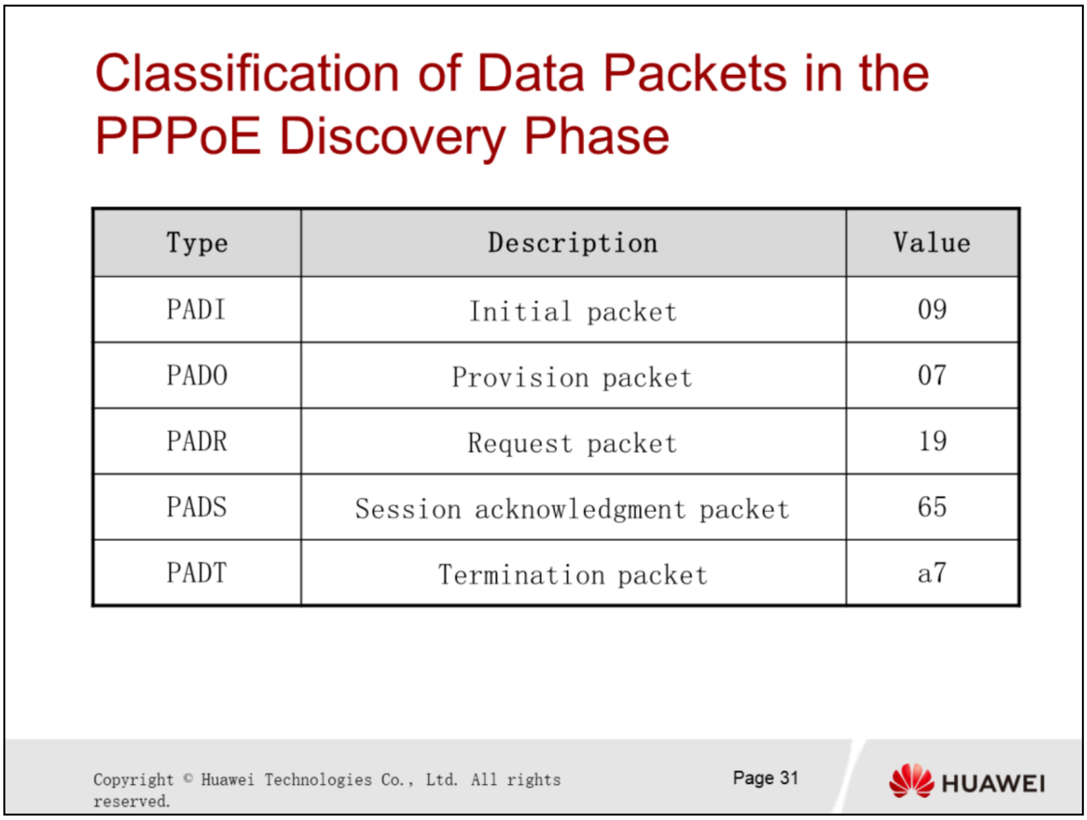
PPPoE Session Establishment Process

Phase	Description
Discovery phase	Obtains the peer Ethernet address and determines a unique PPPoE session.
Session phase	Consists of two parts: PPP negotiation phase and PPP packet transmission phase.
Session termination phase	Sends a packet to terminate a PPPoE session at any time after the session is established.

- The PPPoE can be divided into three phases: discovery, session, and session termination.

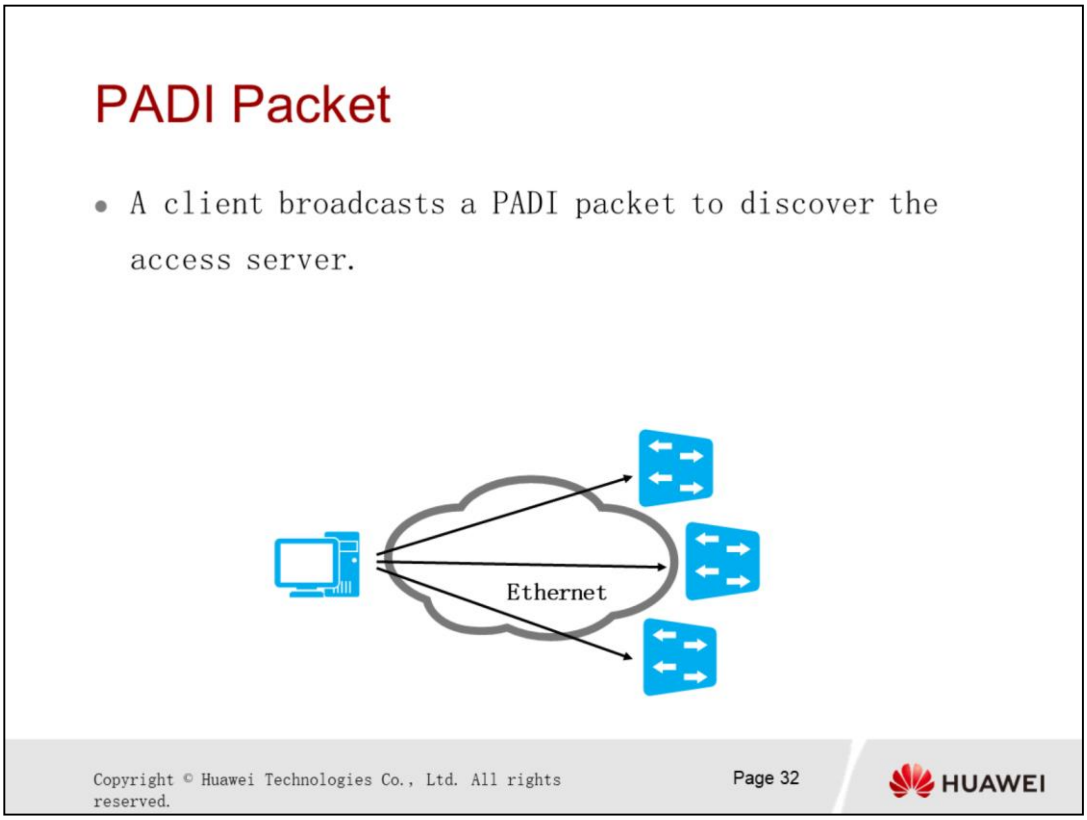
- When a host wants to start a PPPoE session, it needs to perform a discovery process to identify the MAC address of the peer, and then determine a unique PPPoE session ID. The serve this purpose, the PPPoE uses a discovery protocol based on the client/server model. Due to the broadcast feature of the Ethernet, the host (client) discovers all access concentrators (servers) in this process, selects one of them, and establishes a P2P connection with the peer according to the obtained information. After a PPP session is set up, the PPPoE discovery phase is complete.

- After the PPPoE session phase starts, the host and the access concentrator transmit PPP data based on the PPP protocol to perform PPP negotiation and data transmission. The data packets transmitted in this phase must always contain the session identifier determined in the discovery phase. In normal cases, the session phase is terminated by the PPP protocol. However, a PADT packet is also defined in PPPoE to terminate sessions. The host or access concentrator can terminate a session by sending the packet at any time after the PPP session starts.



Classification of Data Packets in the PPPoE Discovery Phase

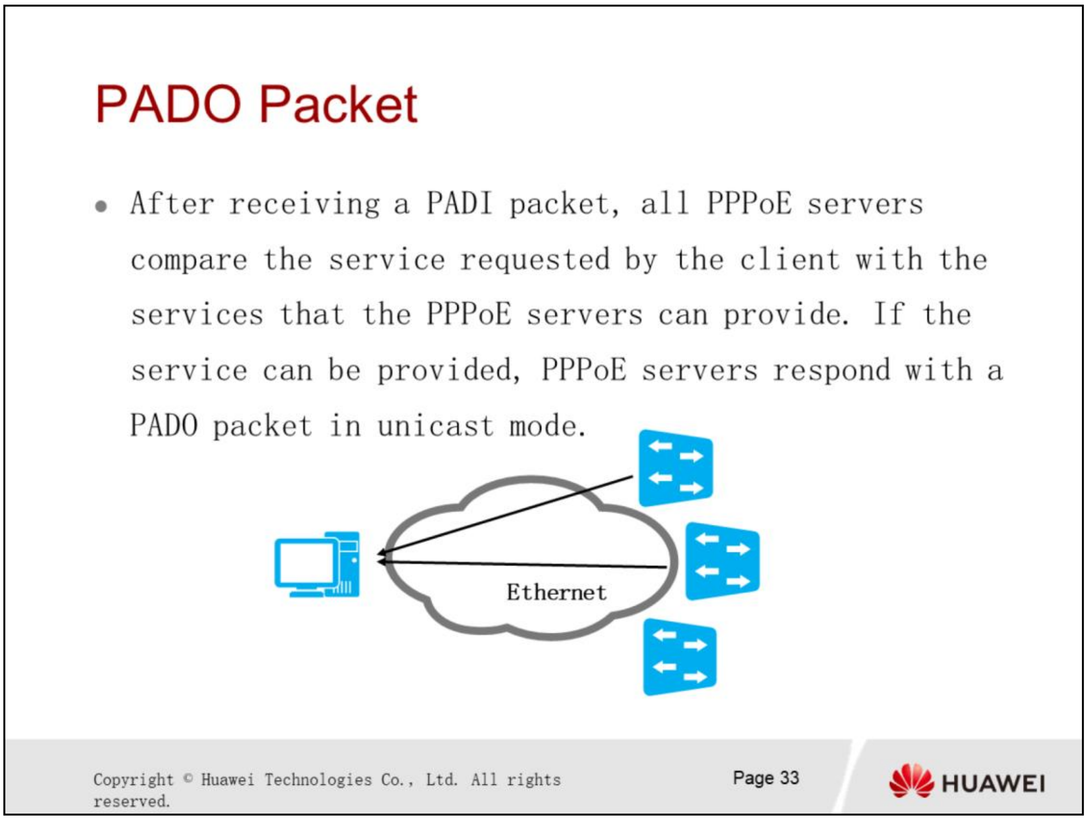
Type	Description	Value
PADI	Initial packet	09
PADO	Provision packet	07
PADR	Request packet	19
PADS	Session acknowledgment packet	65
PADT	Termination packet	a7



PADI Packet

- A client broadcasts a PADI packet to discover the access server.

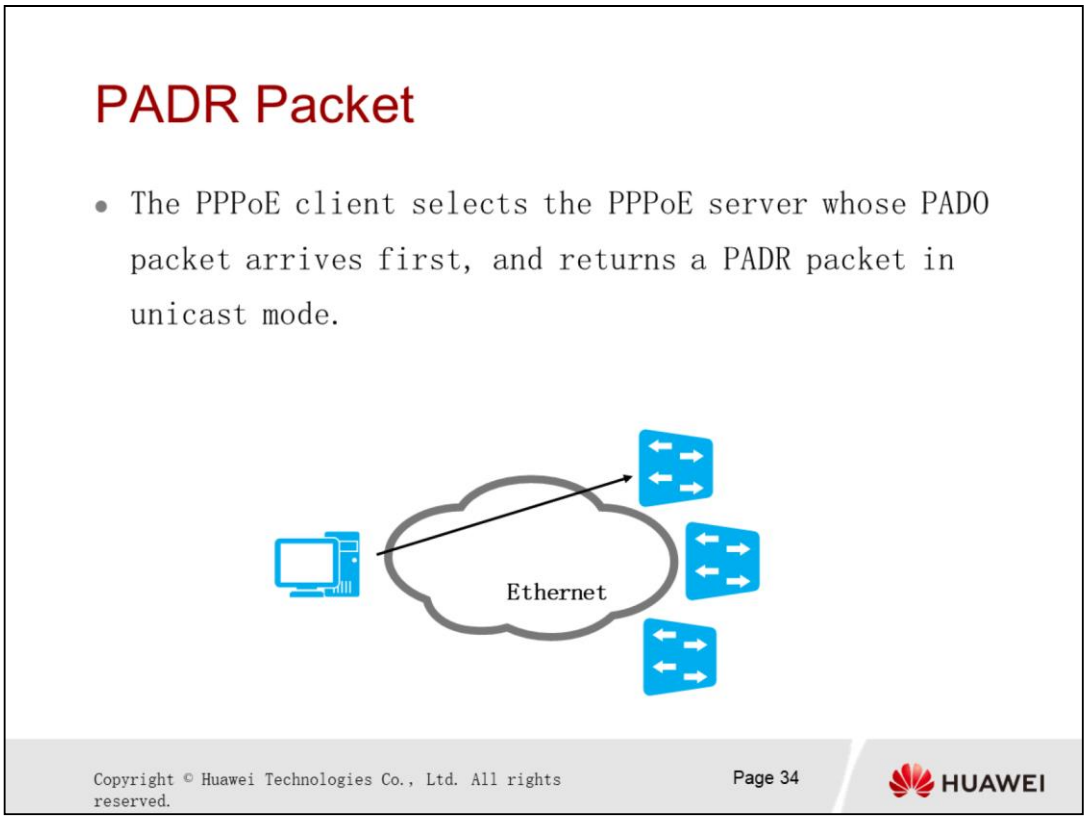
- The destination address is the broadcast address 0xffffffff, and the source address is the Ethernet address of the host. The value of ETHER_TYPE is 0x8863, the code value is 0x09, and the value of SESSION-ID is 0x0000. TAG_TYPE: Only one Service-Name indicates the service requested by the host. There can be any number of other tags. The length of a PADI packet cannot exceed 1484 bytes. Space needs to be reserved for the Relay-Session-Id TAG field.



PADO Packet

- After receiving a PADI packet, all PPPoE servers compare the service requested by the client with the services that the PPPoE servers can provide. If the service can be provided, PPPoE servers respond with a PADO packet in unicast mode.

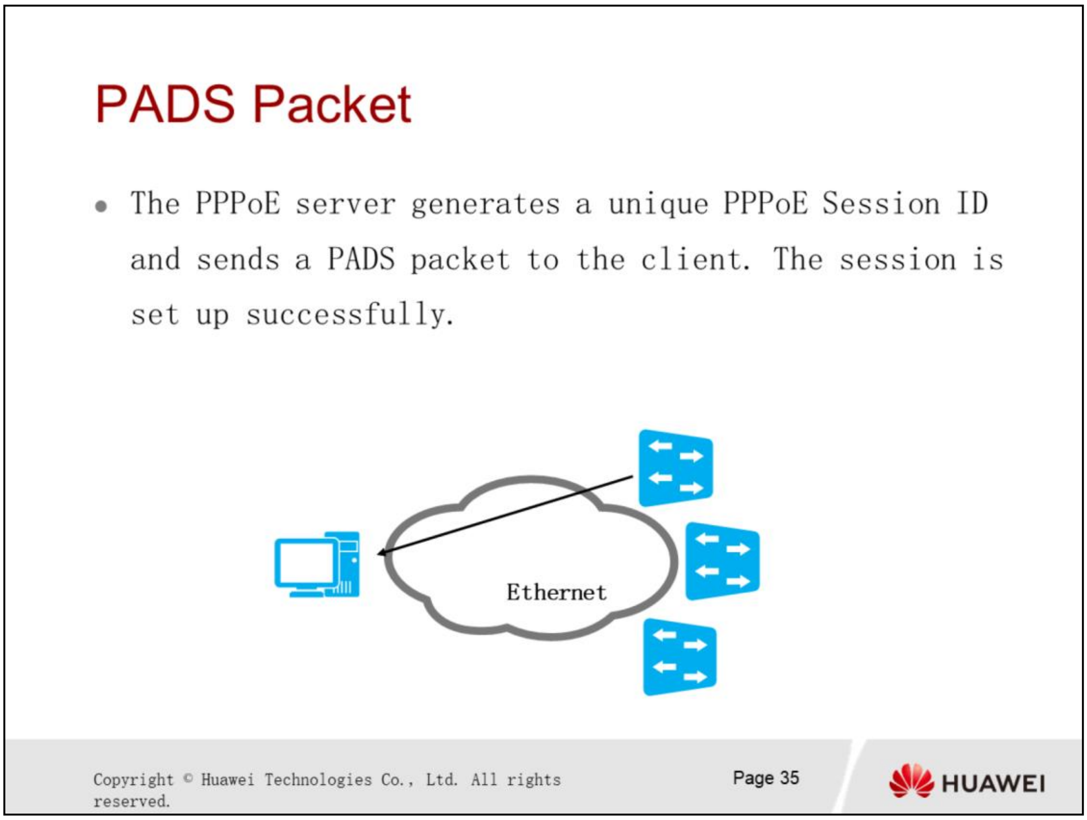
- The destination address is the Ethernet address of the host. The source address is the Ethernet address of the access concentrator. The value of ETHER_TYPE is 0x8863, the code value is 0x07, and the value of SESSION-ID is 0x0000. The value of TAG_TYPE must have an AC-Name TAG that contains the name of the access concentrator. It must contain a Service-Name TAG that is the same as the received PADI and any number of other Service-Name TAGs indicating the services that the concentrator can provide.



PADR Packet

- The PPPoE client selects the PPPoE server whose PADO packet arrives first, and returns a PADR packet in unicast mode.

- The destination address is the Ethernet address of the access concentrator, and the source address is the Ethernet address of the host. The value of ETHER_TYPE is 0x8863, the code value is 0x19, and the value of SESSION-ID is 0x0000. The value of TAG_TYPE must contain a TAG of the Service-Name type to specify the service requested from the concentrator. There can be any number of other tags.



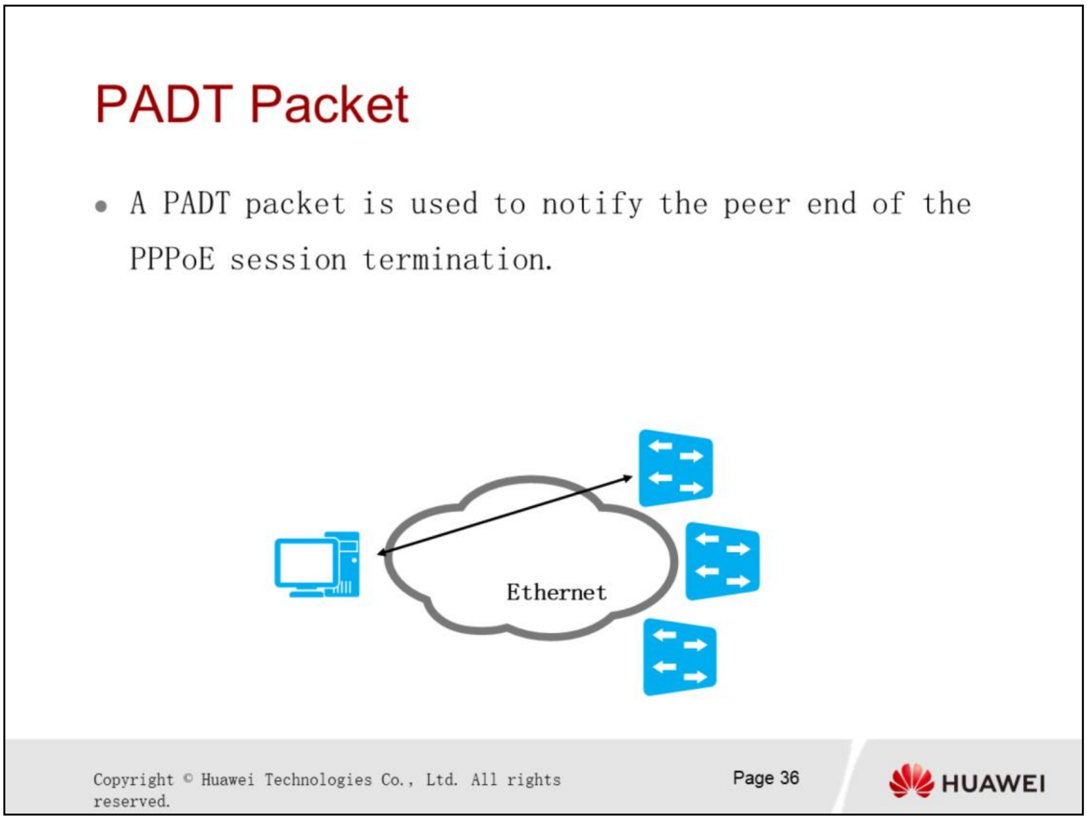
PADS Packet

- The PPPoE server generates a unique PPPoE Session ID and sends a PADS packet to the client. The session is set up successfully.

Page 35

HUAWEI

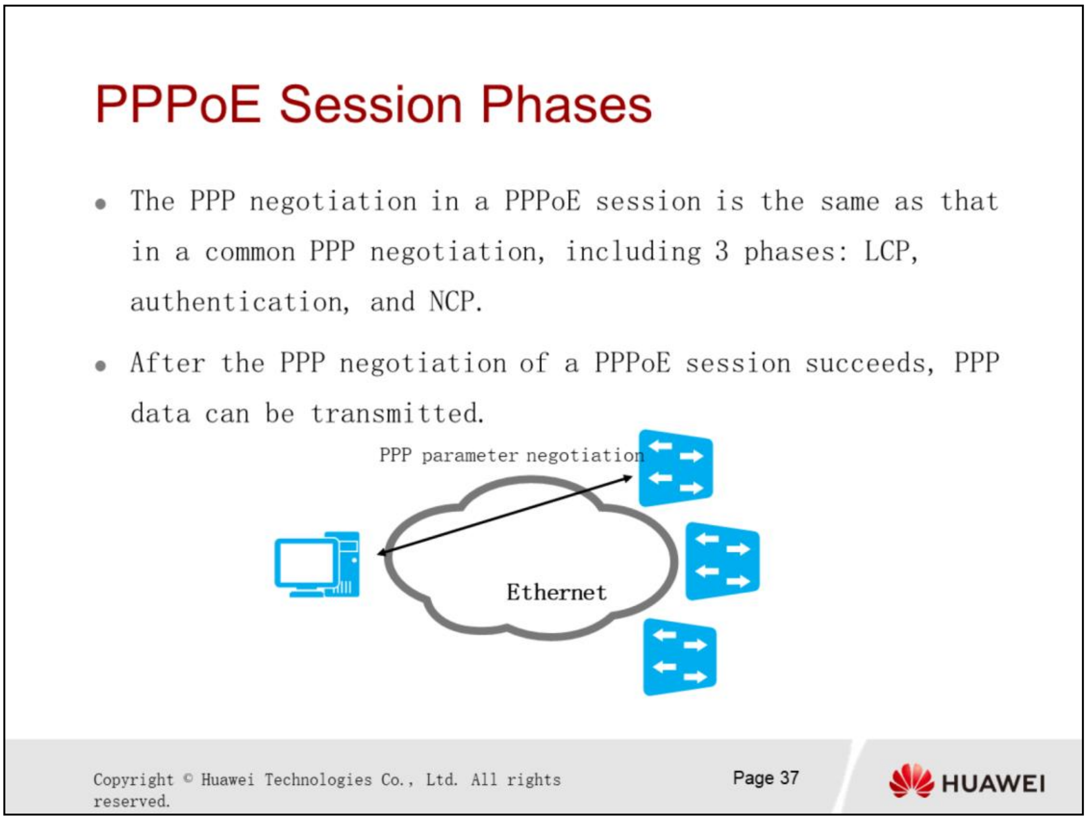
- The destination address is the Ethernet address of the host, and the source address is the Ethernet address of the access concentrator. The value of ETHER_TYPE is 0x8863, the code value is 0x65, and the value of SESSION-ID is a unique value specified by the concentrator to identify a PPPoE session. TAG_ TYPE: Contains a tag of the Service-Name type, indicating the service provided by the concentrator to the session. There can be any number of other tags.
- After a session is set up, the PPPoE client and server enter the PPPoE session phase.



PADT Packet

- A PADT packet is used to notify the peer end of the PPPoE session termination.

- This packet can be sent by the host or concentrator at any time after a session is established. The destination address is a single Ethernet address. The value of ETHER_TYPE is 0x8863, the code value is 0xa7, and the value of SESSION-ID is the SESSION-ID of the session to be terminated. No tag is required.
- In a PADT packet, the destination MAC address is a unicast address, and the session ID is the session ID of the connection to be closed. Once a PADT packet is received, the connection is closed.



PPPoE Session Phases

- The PPP negotiation in a PPPoE session is the same as that in a common PPP negotiation, including 3 phases: LCP, authentication, and NCP.
- After the PPP negotiation of a PPPoE session succeeds, PPP data can be transmitted.

Page 37

HUAWEI

- After a PPPoE session is set up, PPP data is transmitted between the host and the access device based on the PPP protocol. Each Ethernet frame has a single address. The value of ETHER_TYPE is 0x8864, the code value is 0x00, and the value of SESSION-ID remains unchanged during the entire session. The PPPOE payload field contains a PPP packet.

Summary

- The 3 components of the PPP protocol include the encapsulation mode of the PPP protocol, LCP protocol, and NCP protocol.
- The PPP protocol configures and tests data links using the LCP protocol.
- The PPP protocol uses the NCP protocol to configure parameters required for network layer communication between P2P communication devices.
- Magic number functions
- PAP/CHAP authentication principles
- PPPoE discovery and session phases

Thank You

www.huawei.com