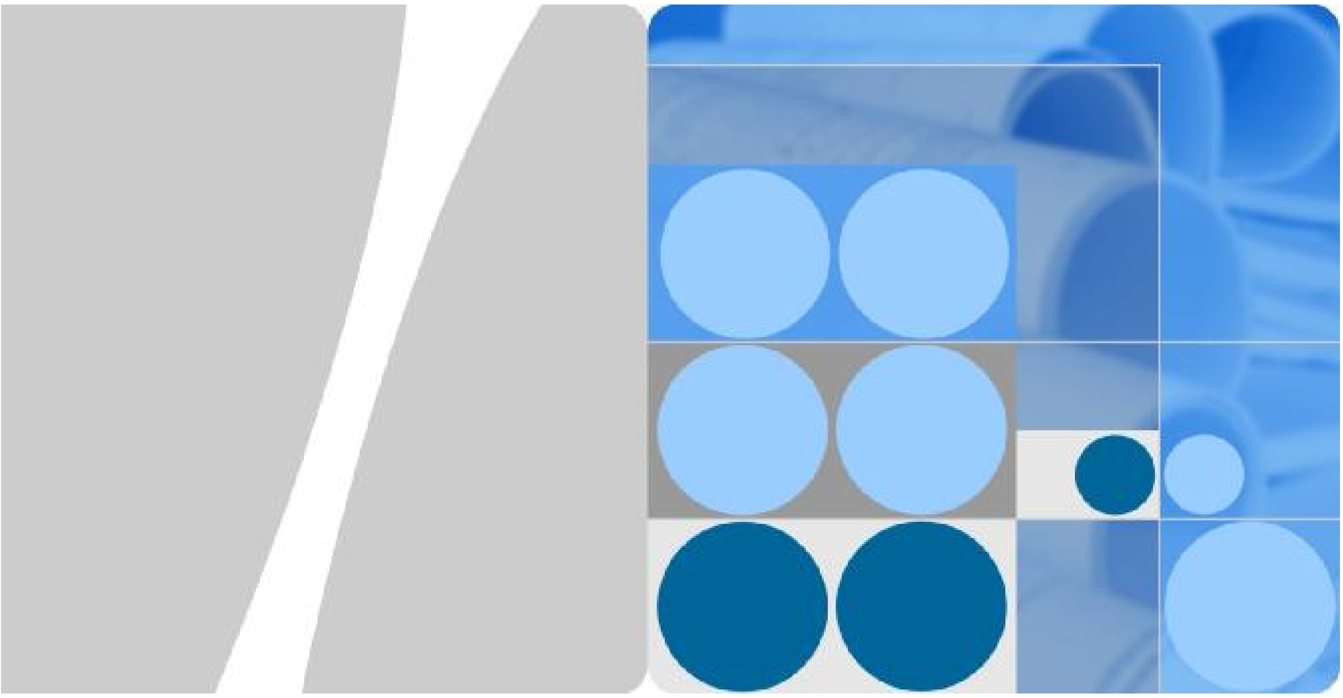


Huawei Sx7 Series Switches

PPPoE Technology White Paper

Issue 01

Date 2016-02-24

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: http://e.huawei.com

Contents

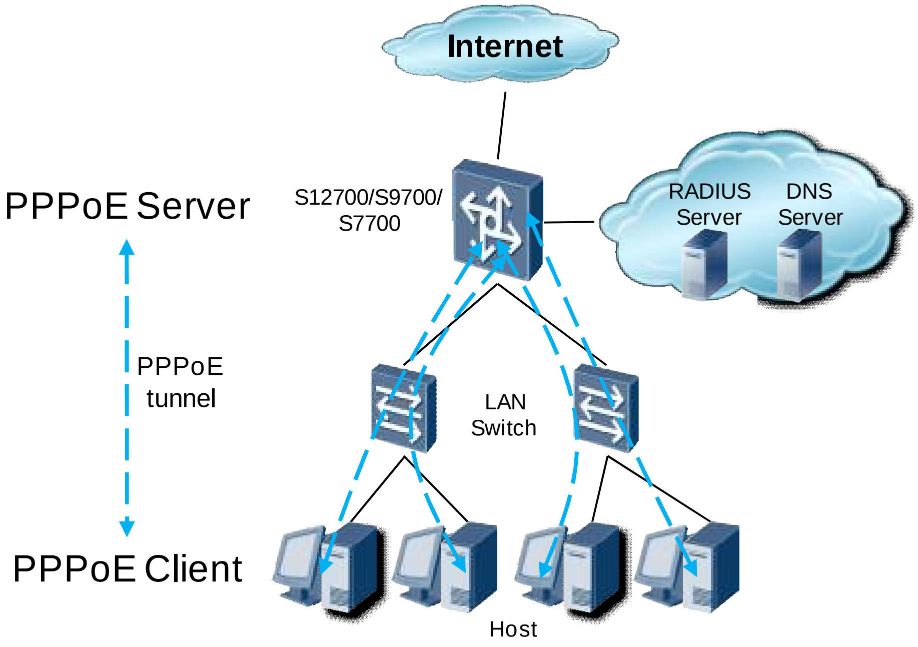
1 Overview

Point-to-Point Protocol (PPP) is a link layer protocol that encapsulates and transmits network layer packets over point-to-point links. PPP is widely used because it provides user authentication methods, supports synchronous and asynchronous communication, and is easy to extend.

PPP over Ethernet (PPPoE) is also a link layer protocol that provides point-to-point connections over the Ethernet. It sets up PPP sessions and provides a method to encapsulate PPP data packets. PPPoE is an enhancement of PPP.

PPPoE adopts the client/server architecture. As shown in Figure 1-1, hosts function as PPPoE clients and the switch S12700, S9700, or S7700 functions as the PPPoE server. Each PPPoE client establishes a point-to-point link with the PPPoE server. The PPPoE server performs access control, authentication, and accounting for PPPoE clients.

Figure 1-1 PPPoE architecture



PPPoE allows a large number of hosts on an Ethernet to connect to the Internet using a remote access device and controls each host using PPP. PPPoE features a large application scale, high security, and convenient accounting. The following table compares PPPoE authentication, 802.1x authentication, MAC address authentication, and Portal authentication.

Item	802.1x Authentication	MAC Address Authentication	Portal Authentication	PPPoE Authentication
Client	A client is required or the operating system must have a built-in client.	Not required	Not required	A client is required or the operating system must have a built-in client.
Security	The admission security level is high. Multiple authentication modes are supported, including Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), Protected Extensible Authentication Protocol (PEAP). IP addresses are allocated after successful authentication.	Lowest	Low	The admission security level is high. The PAP and CHAP authentication modes are supported. No ARP broadcast packets are generated. IP addresses are allocated after successful authentication.
Accounting	Supported	N/A	Supported. User offline cannot be detected in time.	The accounting is exact. All traffic flows through the PPPoE server. User offline can be detected in time.
Application scenario	Enterprise networks where users are densely distributed and there are high security requirements	Dumb terminals, such as printers and fax machines, need to connect to the network.	Users are sparsely distributed and have high mobility.	Carrier networks and campus networks where users are densely distributed, there are high security requirements, and accounting is required

2 Implementation

2.1 PPPoE Frame Format

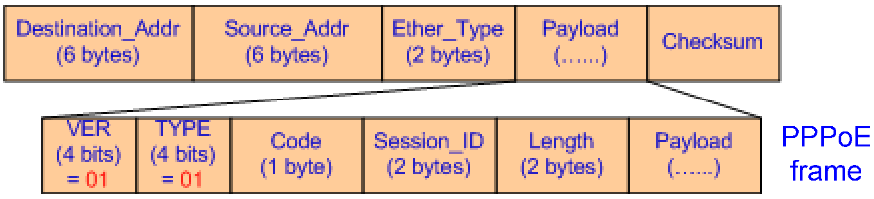
Figure 2-1 shows the PPPoE frame format. PPPoE information is encapsulated within an Ethernet frame.

PPPoE has distinct stages, namely, the Discovery stage and Session stage. The two stages are distinguished by the values of the Ether_Type field of the Ethernet frame.

In the PPPoE Discovery stage, the Ether_Type field is set to 0x8863.

In the PPPoE Session stage, Ether_Type field is set to 0x8864.

Figure 2-1 PPPoE frame format



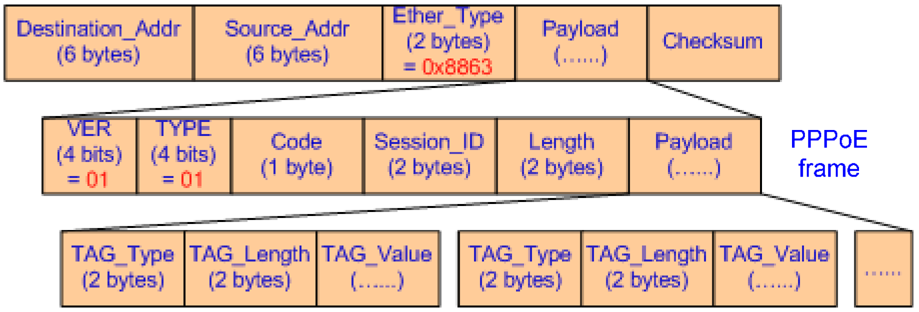
A PPPoE frame consists of fixed-length headers and variable-length payload.

- VER (4 bits): The value of this field is 0x01.
- TYPE (4 bits): The value of this field is 0x01.
- Code (1 byte): The value of this field varies with the PPPoE stages.
- Session_ID (2 bytes): This field must be set to 0x0000 before the PPPoE server assigns a unique session ID to a PPPoE client. After the PPPoE client obtains a session ID, this session ID must be filled in this field in subsequent frames.
- Length (2 bytes): This field indicates the PPPoE payload length.
- Payload: This field carries either the user data or control information.

2.1.1 PPPoE Discovery Frame Format

Figure 2-2 shows the format of frames in PPPoE Discovery stage. In this stage, the Ether_Type field of the Ethernet frame is fixed to 0x8863.

Figure 2-2 PPPoE Discovery frame format



The Code field of PPPoE frames indicates the type of PPPoE Discovery frames. The following table describes such codes.

Code	Description
0x09	PPPoE Active Discovery Initiation (PADI)
0x07	PPPoE Active Discovery Offer (PADO)
0x19	PPPoE Active Discovery Request (PADR)
0x65	PPPoE Active Discovery Session-confirmation (PADS)
0xa7	PPPoE Active Discovery Terminate (PADT)

The Payload field of PPPoE Discovery frames can carry multiple tags that are described in the following table.

Tag	Name	Description
0x0000	End-of-list	Indicates the end of multiple continuous tags in a PPPoE frame. This tag is reserved for version compatibility.
0x0101	Service-Name	Indicates a service name. This tag is used to specify the service that the network can provide for users.
0x0102	AC-Name	Indicates the name of the access concentrator (AC). When the host receives the PADO packet sent by the AC, the host can obtain the AC name from this tag in the PADO packet and then select the AC accordingly to access.
0x0103	Host-Uniq	Indicates the unique identity of the host. It is used to associate the sender and receiver.

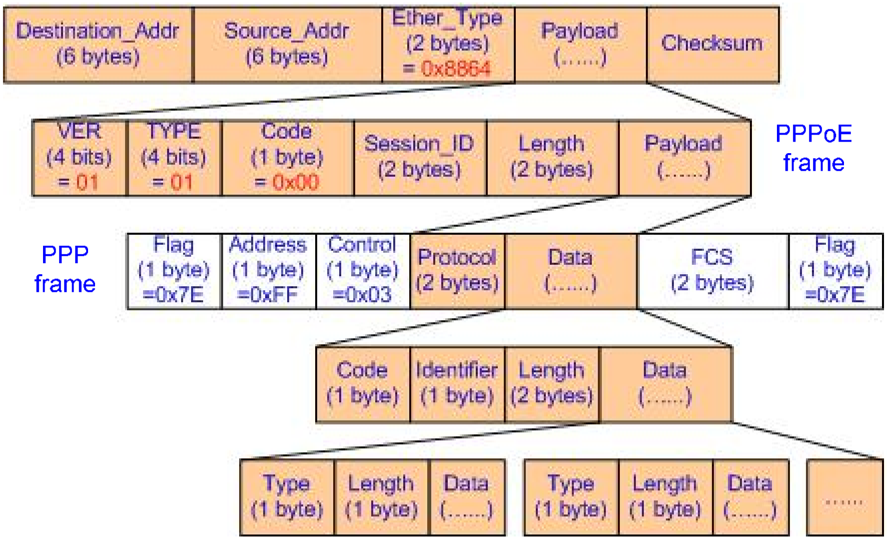
Tag	Name	Description
0x0104	AC-Cookie	This tag is used to protect against denial-of-service (DoS) attacks.
0x0105	Vendor-Specific	Indicates the vendor identity.
0x0110	Relay-Session-ID	Indicates the relay session ID.
0x0201	Service-Name-Error	Indicates that the requested service is not supported by the peer end. This tag is carried in the response from the peer end.
0x0202	AC-System-Error	Indicates that the AC experienced some errors when performing the request from the host.
0x0203	Generic-Error	Indicates a generic error.

2.1.2 PPPoE Session Frame Format

Figure 2-3 shows the format of frames in PPPoE Session stage. In this stage, the Ether_Type field of the Ethernet frame is fixed to 0x8864. The source MAC address of the Ethernet frame is the MAC address of the PPPoE client and the destination MAC address is the MAC address of the PPPoE server.

The Code field of a PPPoE Session frame is set to 0x00. The Session ID field is set to the session ID allocated by the PPPoE server in the Discovery stage. The PPPoE Payload field carries the protocol field and data field of a PPP frame.

Figure 2-3 PPPoE Session frame format



The following tables list the protocols used with PPP.

Protocol	PPP Protocol ID	Description
LCP	0xc021	Link Control Protocol
ECHO	0xc021	Heartbeat packet It is specified by the PPP code.
PAP	0xc023	Password Authentication Protocol (PAP)
CHAP	0xc223	Challenge-Handshake Authentication Protocol (CHAP)
IPCP	0x8021	Internet Protocol Control Protocol (IPCP)
IP	0x0021	Internet Protocol

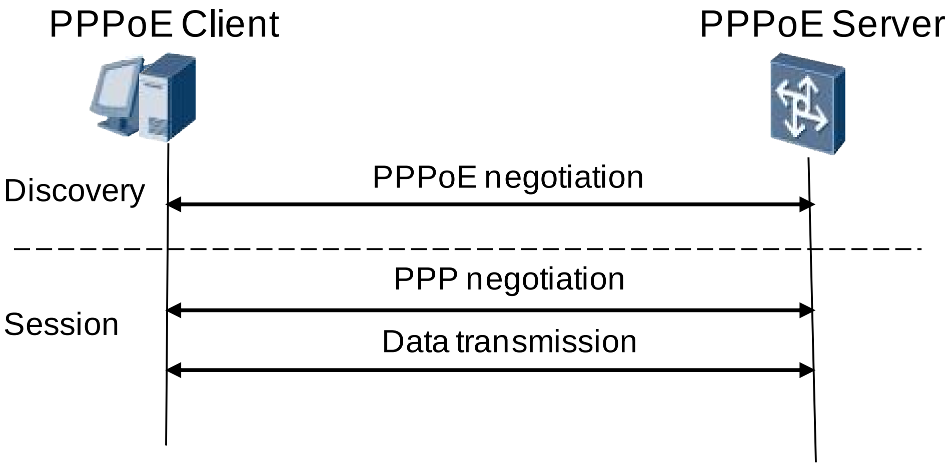
2.2 PPPoE Implementation Process

PPPoE adopts the client/server model. It encapsulates PPP frames within Ethernet frames to provide point-to-point connections on the Ethernet. The establishment of PPPoE requires two stages: PPPoE Discovery stage and PPPoE Session stage, as shown in Figure 2-4.

In the PPPoE Discovery stage, the PPPoE client and PPPoE server obtain each other's MAC address and the PPPoE server allocates a unique session ID.

In the PPPoE Session stage, the PPPoE client and PPPoE server complete authentication, negotiate transmission parameters, and transmit data packets.

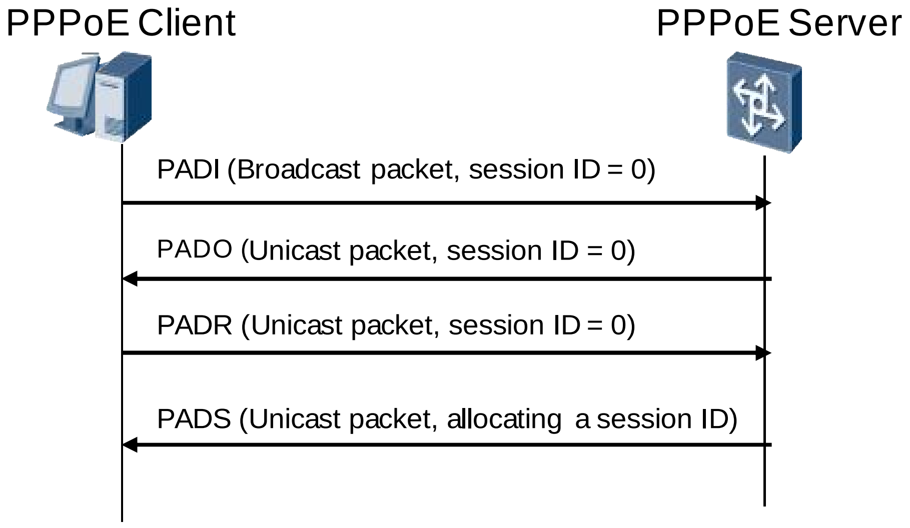
Figure 2-4 PPPoE implementation process



2.2.1 PPPoE Discovery Stage

The PPPoE Discovery stage consists of four steps, as shown in Figure 2-5.

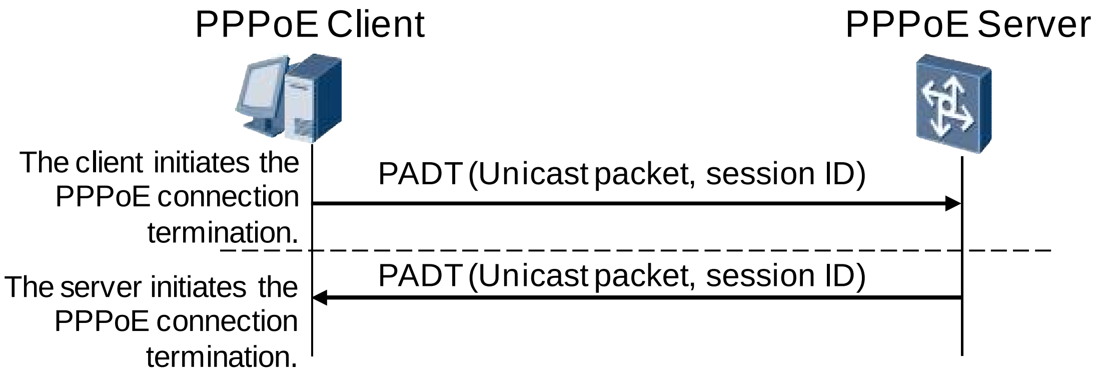
Figure 2-5 PPPoE connection establishment process


PPPoE Client
PPPoE Server
PADI (Broadcast packet, session ID = 0)
PADO (Unicast packet, session ID = 0)
PADR (Unicast packet, session ID = 0)
PADS (Unicast packet, allocating a session ID)

1. The PPPoE client does not know the MAC address of the PPPoE server. Therefore, it broadcasts a PPPoE Active Discovery Initial (PADI) packet its MAC address as the source MAC address and session ID 0. The packet carries two tags: Host-Uniq and Service-Name. If the Service-Name tag does not specify any name, the PPPoE client can accept any service provided by the PPPoE server.
2. After receiving the PADI packet, all PPPoE servers compare the requested service with the services they can provide. The PPPoE servers that can provide the requested service unicast PADO packets to the PPPoE client. The Ethernet frame carrying the PADO packets set the source address to the MAC addresses of the PPPoE servers and the destination address to the MAC address of the PPPoE client obtained from the PADI packet. The session ID in the PADO packets is set to 0 and the AC name, namely, the name of the PPPoE server name, is contained in the PADO packet.
3. The PPPoE client receives PADO packets from more than one PPPoE server. The PPPoE client selects one from these PPPoE servers and unicasts a PPPoE Active Discovery Request (PADR) packet to the selected PPPoE server.
4. The PPPoE server generates a unique session ID to identify the PPPoE session with the PPPoE client. The PPPoE server sends a PPPoE Active Discovery Session-confirmation (PADS) packet containing this session ID to the PPPoE client. When the PPPoE session is established, the PPPoE server and PPPoE client enter the PPPoE Session stage.

When the PPPoE Session is established, the PPPoE server and PPPoE client share the unique PPPoE session ID and learn the peer MAC address.

Figure 2-6 PPPoE connection termination process


PPPoE Client
PPPoE Server
The client initiates the PPPoE connection termination.
PADT (Unicast packet, session ID)
The server initiates the PPPoE connection termination.
PADT (Unicast packet, session ID)

The PPPoE server and PPPoE client use PPP protocol packets to terminate the PPPoE session. When the PPP protocol packets are unavailable, PPP communicating parties can use PPPoE Active Discovery Terminate (PADT) packets to terminate the PPPoE session.

In the Session stage, the client and server exchange PADT packets to terminate the PPPoE connection, as shown in Figure 2-6. The PADT packets can be sent anytime after a session is established to indicate that the session has been terminated. When a PADT packet is received, no further PPP traffic can be sent using this session.

2.2.2 PPPoE Session Stage

The PPPoE Session stage involves PPP negotiation and PPP packet transmission.

PPP negotiation process at the PPPoE Session stage is the same as common PPP negotiation process, which includes the LCP, authentication, and NCP phases.

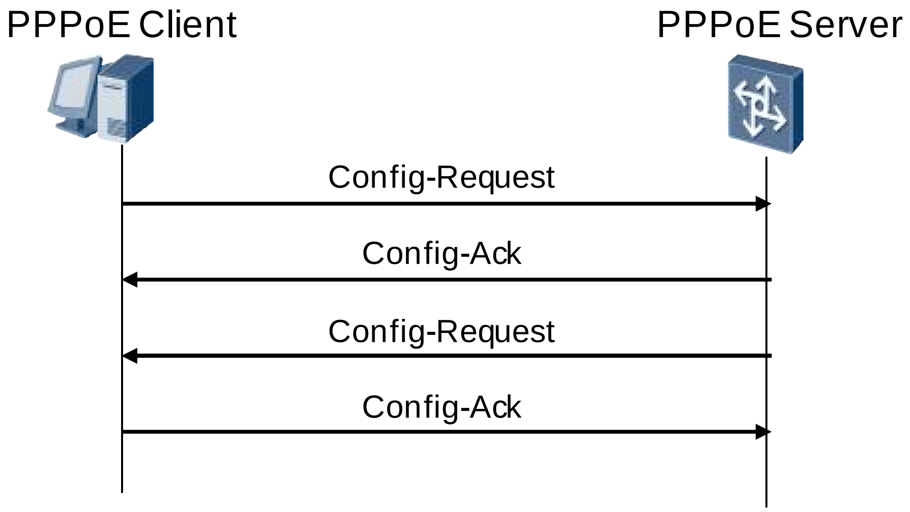
2.2.2.1 LCP Negotiation

In the LCP phase, the PPPoE server and client establish and configure a data link, and verify the data link status. Then, the PPPoE client and PPPoE server negotiate the authentication mode (PAP or CHAP) and maximum receive unit (MRU).

The LCP negotiation process is as follows: The server and client exchange a Config-Request packet and check the negotiation options in the packet. Then they respond a packet depending on whether they accept the options. If both ends respond with a Config-ACK packet, the LCP link is set up successfully. Otherwise, the two ends continue to send Config-Request packets till both of them respond with Config-ACK.

Figure 2-7 shows the LCP negotiation process.

Figure 2-7 LCP negotiation process



2.2.2.2 Authentication

When LCP negotiation is successful, authentication starts. The authentication protocol depends on the LCP negotiation result. The authentication protocol can be Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP). Comparison between CHAP and PAP authentications

- In PAP authentication, passwords are sent over links in plain text. After a PPP link is established, the PPPoE client repeatedly sends the user name and password until the authentication finishes. This mode cannot ensure high security, so it is used on networks that do not require high security.
- CHAP is a three-way handshake authentication protocol. In CHAP authentication, the PPPoE client sends only the user name to the PPPoE server. Compared with PAP, CHAP features higher security because passwords are not transmitted. On networks requiring high security, you can establish a PPP connection by using CHAP authentication.

Figure 2-8 PAP authentication

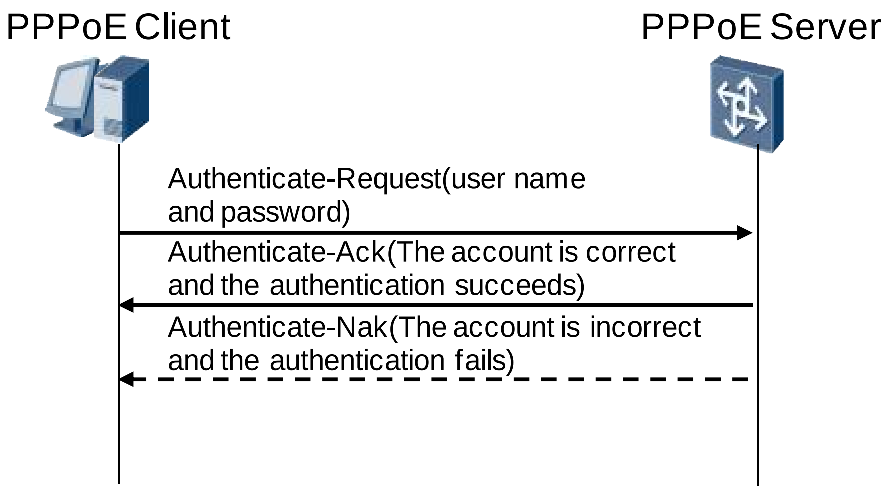

PPPoE Client
PPPoE Server
Authenticate-Request(user name and password)
Authenticate-Ack(The account is correct and the authentication succeeds)
Authenticate-Nak(The account is incorrect and the authentication fails)

Figure 2-8 shows the PAP authentication. The PAP is a two-way handshake authentication protocol that transmits passwords in plain text.

1. The PPPoE client sends the local user name and password to the PPPoE server.
2. The PPPoE server checks whether the user name exists in the local user table.

   If the user name exists, the PPPoE server checks whether the password is correct. If the password is correct, the authentication is successful; otherwise, the authentication fails.

   If the user name does not exist, the authentication fails.

Figure 2-9 CHAP authentication

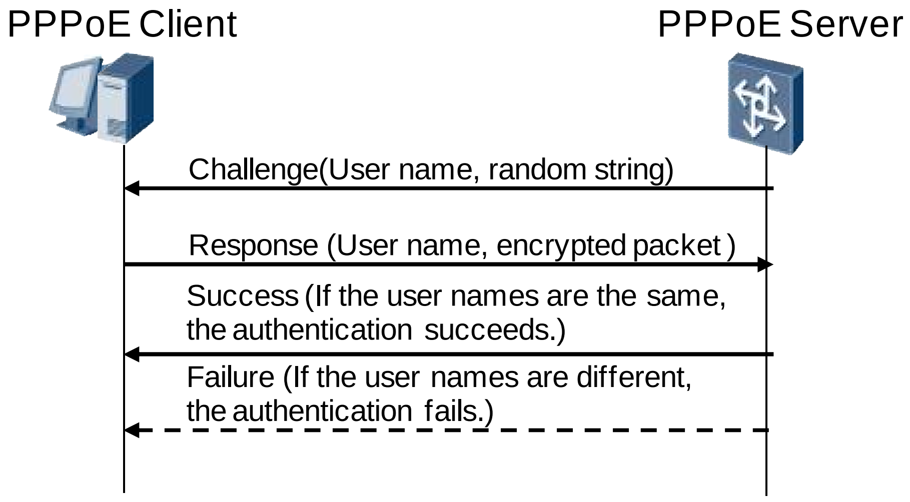

PPPoE Client
PPPoE Server
Challenge(User name, random string)
Response (User name, encrypted packet)
Success (If the user names are the same, the authentication succeeds.)
Failure (If the user names are different, the authentication fails.)

Figure 2-9 shows the CHAP authentication. CHAP is a three-way handshake authentication protocol and transmits passwords in cipher text, so it is more secure than PAP.

1. The PPPoE server sends an authentication request (a Challenge packet randomly generated by the server) to the PPPoE client.
2. The PPPoE client encrypts the authentication request packet by using the packet ID, CHAP password, and MD5 checksum, and then returns the encrypted packet and its own user name (Response) to the server.
3. The PPPoE server encrypts the random packet by using the client's password saved locally and MD5 checksum and compares the encrypted packet with the packet returned by the client. If the packets are the same, the authentication is successful; otherwise, the authentication fails.

2.2.2.3 NCP Negotiation

After the authentication is successful, PPP enters the NCP phase. The NCP phase implements network parameter negotiation, including IP addresses, DNS server addresses, and WINS server addresses.

NCP negotiation supports multiple protocols, for example IPCP and BCP. IPCP is most widely used. IPCP allows PPPoE clients to obtain IP addresses or IP address segment for network access.

IPCP negotiation is based on PPP state machine. The server and client exchange Configure-Request, Configure-ACK, and Configure-Rej packets during the negotiation. When both the server and client have sent and received Configure-ACK packets, the PPP status can change from Initial (or Closed) to Opened.

An IPCA negotiation packet carries multiple options, namely, parameters. Whether the options are accepted or rejected does not affect the IPCP negotiation result. The IPCP negotiation can be Up even if no option is used. The options include IP address, gateway, and mask. The devices of some vendors require that the IP address option must be accepted. However, the devices of most vendors allow this option to be empty.

The NCP negotiation is similar to LCP negotiation. In NCP negotiation, the server and client exchange NCP packets. When the two ends respond with ACK packets, NCP negotiation is successful. Users can go online and access networks.

Figure 2-10 NCP negotiation process

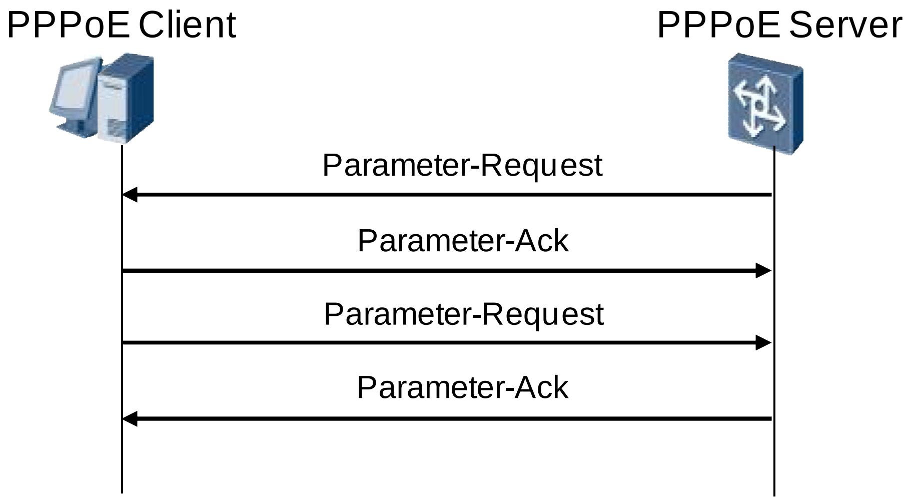


Figure 2-10 shows the basic NCP negotiation process. When PPP negotiation succeeds, PPP data packets can be forwarded. At the PPPoE Session Stage, the PPPoE server and client send all Ethernet data packets in unicast mode.

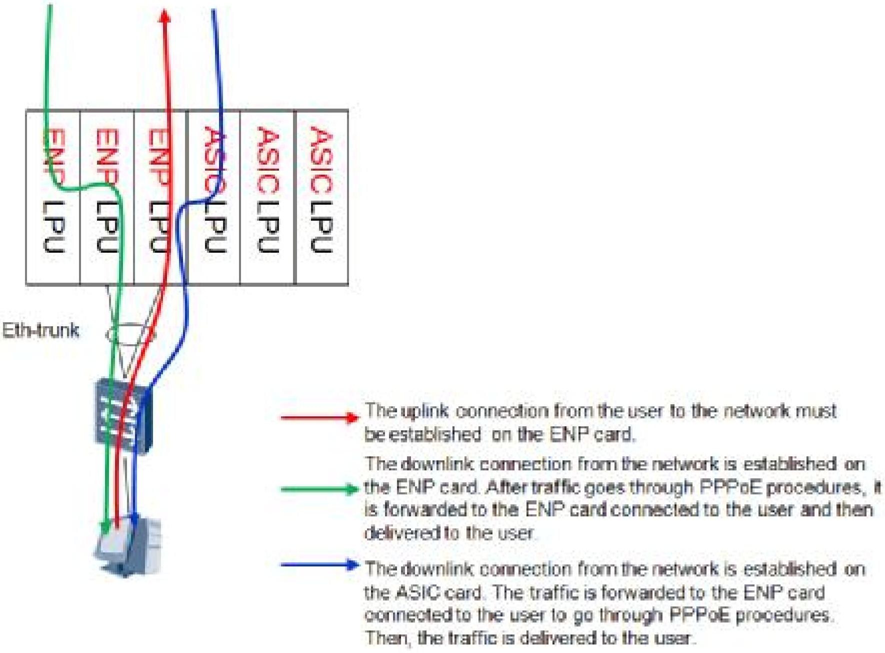
2.3 PPPoE Data Flow Processing on a Switch

S12700, S9700, and S7700 switches can act as PPPoE servers. Only the ENP card (also called X1E) supports PPPoE.

- In the uplink direction, namely, traffic from users to networks, users must be connected to ENP cards. In Eth-Trunk networking scenarios, all Eth-Trunk member ports must be configured on ENP cards.
- In the downlink direction, namely traffic from networks to users, connections can be established on ASIC or ENP cards. In Eth-Trunk networking scenarios, Eth-Trunk member ports can be configured on ASIC or ENP cards. If traffic arrives ASIC cards first, the traffic is forwarded to user-side ENP cards.

Figure 2-11 shows how a switch processes PPPoE data flows.

Figure 2-11 PPPoE data flows on the switch



The uplink connection from the user to the network must be established on the ENP card.

The downlink connection from the network is established on the ENP card. After traffic goes through PPPoE procedures, it is forwarded to the ENP card connected to the user and then delivered to the user.

The downlink connection from the network is established on the ASIC card. The traffic is forwarded to the ENP card connected to the user to go through PPPoE procedures. Then, the traffic is delivered to the user.

2.4 Product Capability

Huawei S12700, S9700, and S7700 switches and switch cluster systems support PPPoE and they can act as a PPPoE server. Only XIE cards support the access of PPPoE clients. The following table lists the PPPoE capability of switches.

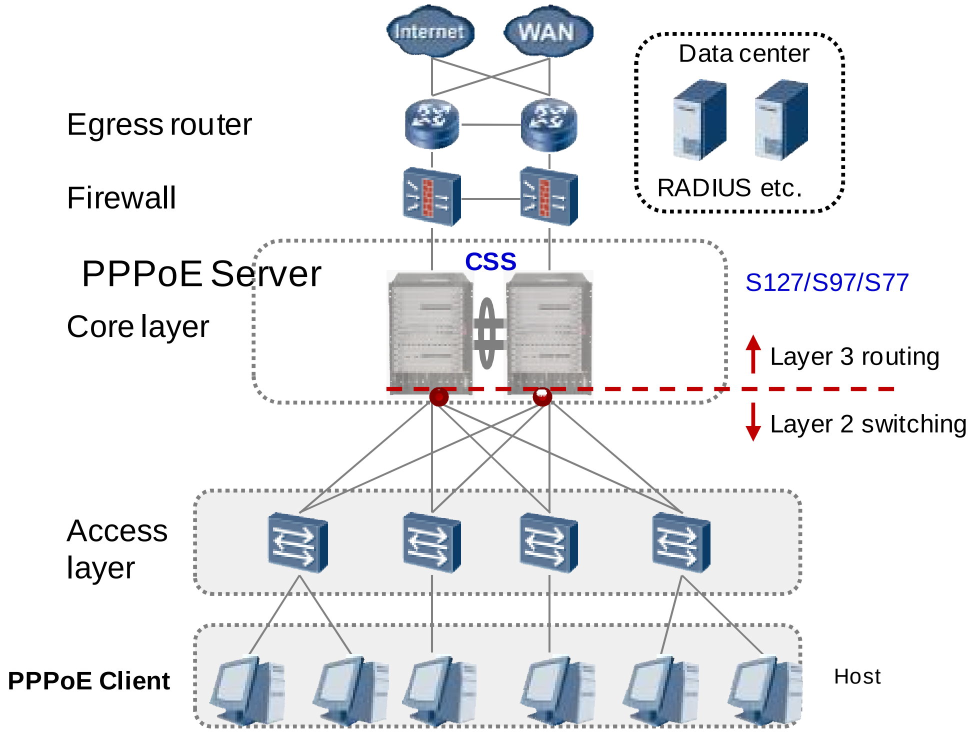
Item	Switch Model	Specification
Number of access users supported by the entire system	S12712/S12708/S12704	64k - 1
	S9712/S9706	32k
	S7712/S7706	16k
	S9703/S7703	8k
User access rate supported by the entire system	S12712/S12708/S12704	Default value: 40 users/s Maximum: 100 users/s
	S9712/S9706/S9703	Default value: 40 users/s Maximum: 100 users/s
	S7712/S7706/S7703	Default value: 25 users/s Maximum: 75 users/s
Number of users supported by a card (X1E)	S12712/S12708/S12704	16k
	S9712/S9706/S9703	8k
	S7712/S7706/S7703	8k

3 Typical Networking

Figure 3-1 shows a typical PPPoE networking.

- Network architecture: The network adopts a two-layer architecture, namely, core layer and access layer. The S12700, S9700, or S7700 switches as the PPPoE servers are deployed at the core layer. The access layer adopts layer 2 switching. Wired hosts are PPPoE clients.
- Security: Port isolation is configured on the access layer to prevent unauthorized communications between users.
- User gateway: The core layer acts as the gateway. Users are connected to X1E cards and access interfaces are VLANIF interfaces.
- Reliability: CSS/CSS2 is adopted and the core layer is connected to the access layer over Eth-Trunk interfaces.
- Access authentication: The RADIUS server is deployed in bypass mode. The S12700, S9700, or S7700 switches authenticate and authorize hosts.
- IP address allocation: The S12700, S9700, or S7700 switches allocate IP addresses.
- Accounting: Accounting can be based on traffic, duration, and destination address.

Figure 3-1 Typical PPPoE networking



A Acronyms and Abbreviations

Acronym/Abbreviation	Full Name
PPP	Point-to-Point Protocol
PPPoE	PPP over Ethernet