Point to Point Protocol (PPP)

PPP is built on the High-Level Data link Control (HDLC) platform, which defines the standards for data transmission of DTE and DCE interfaces of WANs such as V. 35, T1, E1, HSSI, EIA-232-D, EIA-449. PPP was created as an alternative to Serial Line Internet Protocol (SLIP), a simple form of TCP / IP.

PPP is built on the High-Level Data link Control (HDLC) platform, which defines the standards for data transmission of DTE and DCE interfaces of WANs such as V. 35, T1, E1, HSSI, EIA-232-D, EIA-449. PPP was created as an alternative to Serial Line Internet Protocol (SLIP), a simple form of TCP / IP.

PPP provides a mechanism for transferring data of multiple protocols on a single link, a mechanism to correct header compression errors, data compression and multilink.PPP has two components:

- **Link Control Protocol (LCP):** (mentioned in **RFC 1570**) set up, adjust configuration, and cancel a link.Moreover, LCP also has a Link Quality Monitoring (LQM) mechanism that can be configured in conjunction with either Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP).

- **Network Control Protocol (NCP):**NCP is responsible for establishing, configuring and canceling data transmission of network layer protocols such as IP, IPX, AppleTalk and DECnet.

Both LCP and NCP operate in layer 2. There is now a PPP extension for data transmission using multiple links at once, **Multilink PPP (MPPP)** which uses **Multilink Protocol (MLP)** to link Link LCP and NCP classes.

RFC 1661 provides an overview of the PPP protocol.

Format data frames

Details of PPP frame format are as follows:

Picture 1 of Point to Point Protocol (PPP)

There are 5 phases in establishing a PPP connection:

- **Dead:** connection is not active
- **Establish:**initializes LCP and after receiving the Configure ACK message the link will go to the following phase: authentication
- **Authenticate:**can choose either PAP or CHAP mechanism.
- **Network:**in this phase, the data transfer mechanism for supported Network layer protocols will be established and the data transfer will start.
- **Terminate:**Disconnect

Piggyback routing mechanism can be used to cache routing information and only transmit when the connection is smooth.

In the LCP package (contained in the Information field of the PPP packet), the Code field will specify the Configure Request (1), Configure Ack (2) packets, Configure Nak (3) means not accepting and Configure Reject (4).

Each layer 3 protocol has a specific NCP code for it, and this code value is placed in the protocol field of the NCP packet, some values ??are as follows:

Code

Protocol

8021

IP

8029

AT

8025

XNS, Vines

8027

DECnet

8031

Bridge

8023

OSI

Refer to **RFC 1662** and **RFC 1549** to describe specific framing mechanism.

Authentication

Password Authentication Protocol (PAP)

In the LCP phase, when a PPP connection is requested by the client and PAP is selected, the access server will tell the client to use PAP.The client will then have to send his username and password, which will be transmitted in clear text without any encryption and packaged in PPP data packets.The server then decides to accept or reject the connection setup. This is a one-way PAP mechanism between a client and a server.If two routers talk to each other, Two-way PAP will be used where each router sends a username and password, so each router authenticates each other.

Challenge Handshake Protocol (CHAP)

CHAP is more commonly used than PAP, since it has the ability to encrypt passwords as well as data.

Picture 2 of Point to Point Protocol (PPP)

The two connectors share the **secret** CHAP **secret** code and each is assigned a **local local name** .

- Suppose a user **A** dials access to access server **B.**

- The access server will send a transmission of a **Type 1** authentication initialization packet called a **Challenge** packet.This Challenge packet contains a randomly generated number, an ID sequence number to identify the challenge and the authentication name of the challenager.

- The caller will retrieve the chain authentication name, and look in the data of the password string CHAP corresponding to the user name received.

- Caller will enter the CHAP password, ID sequence number and a randomly generated numeric value into the **Message Digest 5 (MD5)** hashing **algorithm** .

- The result value after calculating the hash function is sent back to the Challenger (Access server) in a package CHAP Response (Type 2) containing the hash string, caller authentication name and finally the ID (Sequence Number) taken from Challenge package.

- When receiving the Response Type 2 package, Challenger will use the ID to find the original Challenge package.

- The username of the caller (**A**) is used to search for the secret code CHAP from a local database, or a RADIUS server or a TACACS + server.

- The ID, the original Challande value is born spontaneously and the value of the original random CHAP and the secret code is taken into account by the MD5 hash function.

- The resulting hash string is then compared to the value received in the Response packet.

- If the two strings are the same, CHAP authentication is successful and **Type 3** packets are sent to the caller containing the ID. This means that the connection has been validated.

- If CHAP authentication fails, a **Type 4** packet will be sent to the caller which contains the original ID, confirming that the authentication process is unsuccessful.

Hashing is completely different from encrypting information because the information will not be restored after executing the hash function.In Nortel Networks routers Code C223 determines CHAP operation.

RFC 1994 describes CHAP details while **RFC 1334** describes other authentication protocols.

guides. Thank you for reading and for following us regularly.