The Notebook
of
CCNA

Huy Bui

THE PUBLISHER

Contents

0.1 List of Codes

Chapter 1

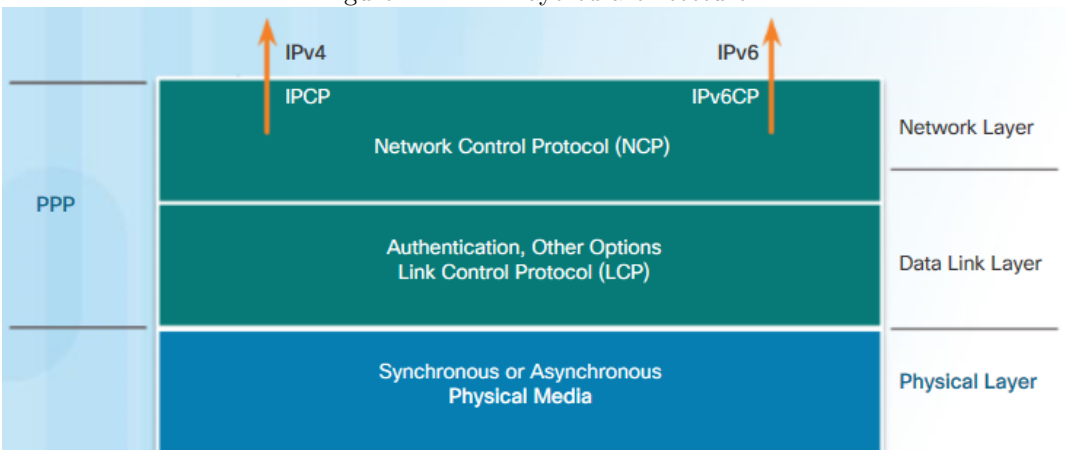
PPP

1.1 Introduction

HDLC is the default serial encapsulation method when connecting two Cisco routers and it can only work with other Cisco devices. HDLC is now the basis for *synchronous* point-to-point used by many servers to connect to a WAN, most commonly the Internet. However, when there is a need to connect to a non-Cisco router, PPP encapsulation should be used.

There are many advantages to using PPP, including the fact that it is not proprietary. PPP provides router-to-router and host-to-network connections over *synchronous* and *asynchronous* circuits. PPP includes many features not available in HDLC: The link quality management feature (LQM) monitors the quality of the link, PAP and CHAP authentication.

Figure 1.1: PPP layered architecture



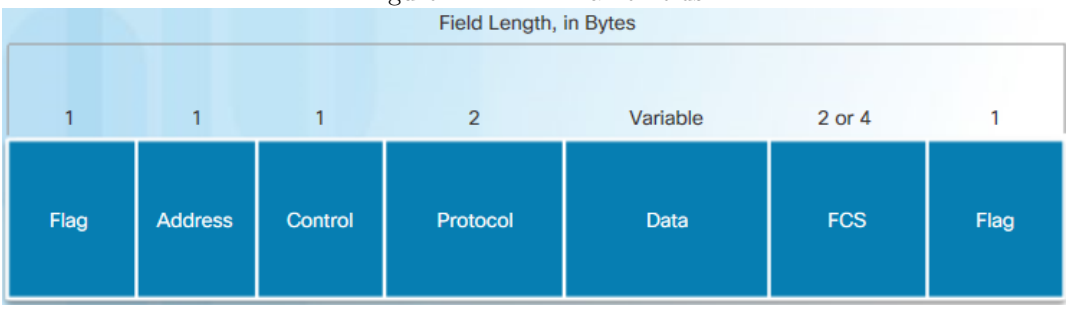
PPP contains three main components: HDLC-like framing, LCP, and NCPs. Figure 1.1 maps the layered architecture of PPP against the OSI model. PPP and OSI share the same physical layer, but PPP distributes the functions of LCP and NCP differently. Most of the work done by PPP happens at the data link and network layers, by LCP and NCPs.

1.2 Operation

1.2.1 Frame Structure

A PPP frame consists of six fields. The following descriptions summarize the PPP frame fields illustrated in the figure 1.2:

Figure 1.2: PPP Frame fields



- **Flag:** A single byte that indicates the beginning or end of a frame. The Flag field consists of the binary sequence 01111110 (63 in decimal).
- **Address:** A single byte that contains the broadcast address because PPP does not assign individual station addresses.
- **Control:** A single byte that contains the binary sequence 00000011, which calls for transmission of user data in an unsequenced frame.
- **Protocol:** Two bytes that identify the protocol encapsulated in the information field of the frame. The 2-byte Protocol field identifies the protocol of the PPP payload.
- **Frame Check Sequence (FCS):** This is 2 bytes. If the receiver's calculation of the FCS does not match the FCS in the PPP frame, the PPP frame is silently discarded.

1.2.2 Establishing a PPP Session

There are three phases of establishing a PPP session:

- **Phase 1: Link establishment and configuration negotiation** – The LCP opens the connection and negotiates configuration options. This phase is complete when the receiving router sends a configuration-acknowledgment frame back to the router initiating the connection.
- **Phase 2: Link quality determination (optional)** – The LCP tests the link to determine whether the link quality is sufficient to bring up network layer protocols. The LCP can delay transmission of network layer protocol information until this phase is complete.
- **Phase 3: Network layer protocol configuration negotiation** – After the LCP has finished the link quality determination phase, the appropriate NCP can separately configure the network layer protocols. If the LCP closes the link, it informs NCPs so that they can take appropriate action.

1.2.3 LCP

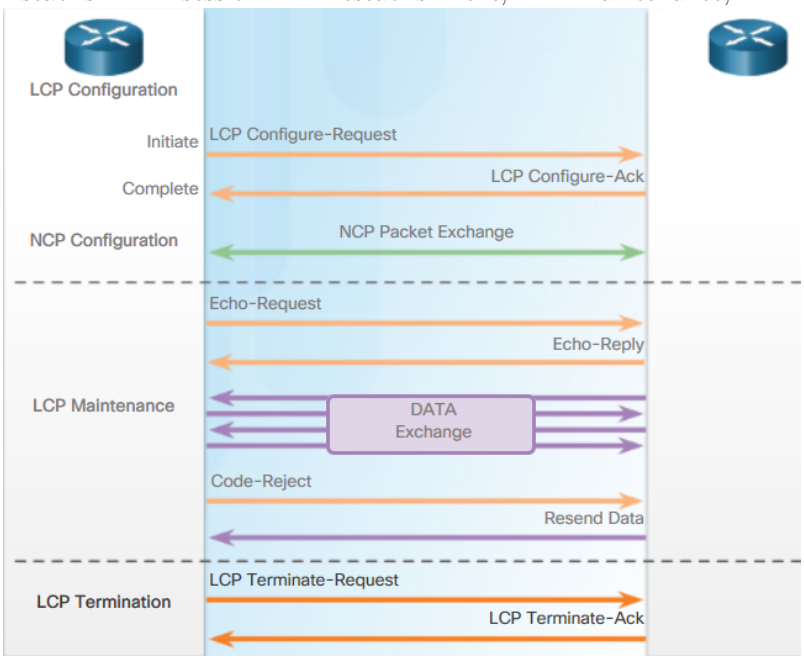
Link Control Protocol (LCP) operation uses three classes of LCP frames to accomplish the work of each of the LCP phases: Link-establishment → Link-maintenance → Link-termination (Figure 1.3).

Link Establishment

The link establishment process starts with the initiating device sending a Configure-Request frame to the responder. The initiator includes the options for how it wants the link created, including protocol or authentication parameters. The responder processes the request:

- If the options are not acceptable or not recognized, the responder sends a Configure-Nak or Configure-Reject message. If this occurs and the negotiation fails, the initiator must restart the process with new options.
- If the options are acceptable, the responder responds with a Configure-Ack message and the process moves on to the authentication stage. The operation of the link is handed over to the NCP.

Figure 1.3: Establish PPP session: Link-establishment, Link-maintenance, Link-termination



Link Maintenance

When NCP has completed all necessary configurations, LCP transitions into link maintenance. During link maintenance, LCP can use messages to provide feedback and test the link using:

- Echo-Request, Echo-Reply, and Discard-Request: These frames can be used for testing the link.
- Code-Reject and Protocol-Reject: These frame types provide feedback when one device receives an invalid frame. The sending device will resend the packet.

Link termination

After the transfer of data at the network layer completes, the LCP terminates the link, as shown in Figure 1.3. NCP only terminates the network layer and NCP link. The link remains open until the LCP terminates it. If the LCP terminates the link before NCP, the NCP session is also terminated.

The LCP closes the link by exchanging Terminate packets. The device initiating the shutdown sends a Terminate-Request message. The other device replies with a Terminate-Ack.

1.2.4 NCP

After the LCP has configured and authenticated the basic link, the appropriate NCP is invoked to complete the specific configuration of the network layer protocol being used.

IPCP is an example of NCP. IPCP is responsible for configuring, enabling, and disabling the IPv4 modules on both ends of the link. IPCP negotiates two options:

- **Compression:** Allows devices to negotiate an algorithm to compress TCP and IP headers and save bandwidth.
- **IPv4-Address:** Allows the initiating device to specify an IPv4 address to use for routing IP over the PPP link, or to request an IPv4 address for the responder.

1.2.5 Authentication

PAP is a very basic **two-way handshake**. There is no encryption. The username and password are sent in plaintext. If it is accepted, the connection is allowed. CHAP is more secure than PAP. PAP may be used in the following environments: CHAP is not supported, or simulate a login at the remote host.

PAP Process *After link establishment phase*, the remote node sends a username-password pair in plain text across the link. At the receiving node, the username-password is checked. This device either allows or denies the connection. An accept or reject message is returned to the requester.

CHAP Unlike PAP, which only authenticates once, CHAP uses a **three-way handshake**, and conducts periodic challenges to make sure that the remote node still has a valid password value. The password value is variable and changes unpredictably while the link exists. Thus, CHAP provides protection against a playback attack.

CHAP process *After link establishment phase*, the local router sends a challenge message to the remote node. The remote node responds with a value that is calculated using a one-way hash function. The local router checks the response against its own calculation. If the values match, the initiating node acknowledges the authentication. If the values do not match, the initiating node immediately terminates the connection.

1.3 Configuration

To set PPP as the encapsulation method used by a serial interface, use the `encapsulation ppp` interface configuration command. Point-to-point software compression on serial interfaces can be configured after PPP encapsulation is enabled. If the traffic already consists of compressed files, such as .zip, .tar, or .mpeg, do not use this option. The `ppp quality 80` command ensures that the link meets the quality requirement set (80%); otherwise, the link closes down.

Listing 1: Basic PPP configuration

```
interface s0/0/0
  encapsulation ppp
  ppp quality 80
  compress [predictor | stac]
  no shutdown
```

Multilink PPP: provides a method for spreading traffic across multiple physical WAN links. allows packets to be fragmented and sends these fragments simultaneously over multiple point-to-point links to the same remote address.

Listing 2: Multilink PPP

```
interface s0/0/0
  no ip address
  encapsulation ppp
  ppp multilink
  ppp multilink group 1
  no shutdown

interface s0/0/1
  no ip address
  encapsulation ppp
  ppp multilink
  ppp multilink group 1
  no shutdown

interface Multilink 1
  ip address 10.0.1.1 255.255.255.252
  ppp multilink
  ppp multilink group 1
```

CHAP Authentication: The hostname (e.g. R3, R2, ISP) on one router must match the username the other router has configured in the command `username <name> password <password>` . The passwords must also match.

Listing 3: CHAP authentication

```
#ROUTER ISP
hostname ISP
username R3 secret cisco
interface s0/0/0
  encapsulation ppp
  ppp authentication chap
  no shutdown

#ROUTER R3
hostname R3
username ISP secret cisco
interface serial0/1/0
  encapsulation ppp
  ppp authentication chap
  no shutdown
```

PAP Authentication: The PAP username and password are configured in the command `ppp pap sent-username`. Theses username and password must match those specified with the `username <name> password <password>` command on the other router.

Listing 4: PAP authentication

```
#ROUTER R1
username R3 secret class
interface s0/0/0
  encapsulation ppp
  ppp authentication pap
  ppp pap sent-username R1 password cisco
  no shutdown

#ROUTER R3
username R1 secret cisco
interface s0/0/0
  encapsulation ppp
  ppp authentication pap
  ppp pap sent-username R3 password class
  no shutdown
```