Point- To- Point Protocol

Immadisetty.L.V.Chandrika, Venkata.Videhi. Balusupati, A.Rama Krishna

Abstract – The telephone line provides a physical link, but to control and manage the transfer of data, there is a need for point-to-point connection. The first protocol devised for this purpose was serial line internet protocol (SLIP). However, SLIP has some deficiencies: it does not support protocols other than internet protocol (IP). It does not allow the IP addresses to be assigned dynamically, and it does not support authentication of the user. The POINT-TO-POINT (PPP) is a protocol designed to respond to respond to the deficiencies. Today the PPP protocol standard finds wide use in asynchronous and synchronous connections between computers, bridges, routers and other intermediate devices.PPP is gaining acceptance as a standard for Integrated Services Digital Network(ISDN), and many implementations of X.25 also support PPP connection.

Keywords- LCP(Link Control Protocol), NCP(Network Control Protocol), CRC(cyclic redundancy check), FCS(Frame check sequence), ISO(International Standards Organization), PDU (Protocol Data Unit), HDLC(High(Level) Data Link Control)

I. INTRODUCTION

The Point-To-Point (PPP) is a data link layer protocol which encapsulates other network layer protocols for transmission on synchronous and asynchronous communication lines. The definition explains the point-to-point aspect of PPP. The protocol aspect lies in the fact that PPP is the intermediate packet structure which facilitates transmission of higher level protocols, such as TCP/IP, across diverse communications links.

PPP was first proposed as an Internet standard in the early 1990's by a working group of the internet activities board's internet engineering task force (IETF). The original purpose was to allow one uniform, standardized way to encapsulate the IP protocol for point-to-point communications in a mixed environment of varying vendors and devices.

Many of the original proponents of the PPP protocol were router vendors who found that the many existing data link protocols used to envelop transport protocols were proprietary in nature. Hence, internetwork connectivity was difficult and limited. In particular, routers vendors could not interoperate over serial dial-up or leased lines because no standard for high-speed synchronous communication.

Today millions of Internet users need to connect their home computer to the computer of an Internet Providers to access the internet. There are also a lot of individuals who need to connect to a computer from home, but they do not want to go through the internet. The majority of these user have either a dialup or leased telephone line. The telephone line provides a physical link, but to control and manage the transfer of data, there is a need for a point-to-point link protocol.

II. TRANSITION STATES

The different phase through which a PPP connection goes can be described using a **transition state** diagram as shown in figure.

- **Idle State:** The idle state means that the link is not being used .There is no active carrier and the line is quiet.
- **Establishing State:** When one of the end point starts the communication, the connection goes into the **establishing state.** In this state, options are negotiated between the two parties. If the negotiation is successful, the system goes to the authenticating state (if authentication is required) or directly to the networking state. The LCP packets are used for this purpose. Several packets may be exchanged during this state.
- **Authenticating State:** The authenticating state is optional; the two end points may decide, during the establishing state, not to go through this state. However, if they decide to proceed with authentication, they send several authentication packets. If the result is successful, the connection goes to the networking state; otherwise, it goes to the terminating state.
- **Networking State:** The networking state is the heart of the transition states. When a connection reaches this state, the exchange of user control and data packets can be started. The connection remains in this state until one of the end points want to terminate the connection.
- **Terminating state:** When the connection is in the terminating state, several packets are exchanged between the two ends for house cleaning and closing the link

2.1 PPP Layers

PPP has only physical ad data link layers. This means that a protocol that wants to use the services of PPP should have other layers (network, transport and so on). PPP operates only at the physical and data link layers.

Physical Layer

No specific protocol is defined for the layer in PPP. it is left to the implementation to use whatever is available . PPP supports any of the protocols recognized by ANSI.

Data Link Layer

At the Data link layer, PPP employs a version of HDLC. HDLC is a bit-oriented data link control protocol which satisfies a wide variety of data link control requirements in including. Point-to-point and point-to-multiple communication, two way simultaneous communication over full duplex circuits, two-way alternate communication over half duplex or full duplex circuits, synchronous and asynchronous communication, between equal stations and

Manuscript Received on November, 2012

Immadisetty L V Chandrika, Electronics and Computer Engineering, K L University, Guntur, Krishna Dt, Andhra Pradesh, India.

Venkata Videhi Balusupati, Electronics and Computer Engineering, KL University, Guntur, Krishna Dt, Andhra Pradesh, India.

A.Rama Krishna, Electronics and computer Engineering, K L University, Guntur, Krishna Dt, Andhra Pradesh, India.

between host and remote stations and full data transparency.

2.2 PPP Frame

PPP adds one significant field to its frame, the protocol field that appears after the control field and before the information field. Hence, the PPP frame structure looks like this:

Flag field: The flag field, like the one in HDLC, identifies the boundaries of a frame. Its value is 01111110.

Address Field: Because PPP is used for a point-to-point connection, it uses the broadcast address of HDLC, 11111111, to avoid a data link address in the protocol.

Control Field: The control field uses the format of the U-frame in HDLC. The value is 11000000 to show that the frame does not contain any sequence number and that there is no flow and error control.

Protocol Field: The protocol field defines what is being carried in the data or other information

Data Field: The field carries either the user data or other information.

FCS: The frame check sequence field, as in HDLC is simple a two-byte or four-byte CRC.

2.3 LCP (Link Control Protocol)

The Link Control Protocol is responsible for establishing maintaining; configuring and terminating links .It also provides negotiation mechanisms to set options between the two end points. Both end Points of the link must reach an agreement about the options before the link can be established.

All LCP packets are carried in the payload field of the PPP frame .What defines the frame as one carrying an LCP packets is the value of the protocol field, which should be set to CO2116 . The figure shows the format of the LCP Packets

The descriptions of the fields are

Code: The field defines the type of LCP packet. We will discuss these packets and their purpose.

ID: This field holds a value used to match a request with the reply. one end point inserts a value in this field, which will be copied in the reply packet.

Length: This field defines the length of the whole LCP packet.

Information: This field contains extra information needed foe some LCP packets.

Link Termination Packets

The termination packets are used to disconnect the link between two end points.

Terminate-request: Either party can Terminate link by sending a terminate request packet

Terminate-ack: The party that receives the terminate-request packet should answer with a terminate-ack packet.

Link Monitoring and Debugging Packets:

These packets are used for monitoring and debugging the link:

Code-reject: if the end point receives a packet with an unrecognized protocol in the packet, it send a code-reject packet.

Protocol reject: If the end point receives a packet with an unrecognized protocol in the frame, it sends a protocol-reject packet.

Echo-request: The packet is sent to monitor the link .its purpose is to see if the link is functioning. The sender expects to receive an echo-reply packet from the other side as proof.

Echo –reply: This packet is sent in response to an echo-request. The information field in the echo-request packet is exactly duplicated and sent v=back to the sender of the echo-request packet.

Discard –request: This kind of loopback test packet. It is used by the sender to check its own loopback condition. The receiver of the packet just discard it.

2.4 IPCP (Internet Protocol Control Protocol)

The set of packets that establish and terminate a network layer connection for IP packets is called internetwork protocol control protocol. The format of an IPCP packet is shown in figure, Note that the value of the protocol field, 802116, defines the packet encapsulated in the protocol as an IPCP packet.

Seven packets are defined for the IPCP protocol, distinguished by their code values shown in table

A party uses the configuration –request packet to negotiate options with the other party and to set the IP address, and so on. After configuration, the link is ready to carry IP protocol data in the payload field of a PPP Frame. This time, the value of the protocol field is 002116 to show that the Ip data packet, not the IPCP packet, is being carried across the link.

After IP has sent all of its packets the IPCP can take control and use the terminate-request and terminate –ack packets to end the network connection.

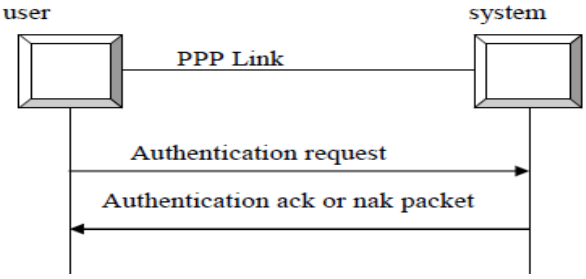
Code	IPCP Packet
01	Conf- request
02	Conf-ack
03	Conf-nak
04	Conf-reject
05	Terminate-request
06	Terminate- ack
07	Code-reject

2.5 Authentication

Authentication plays a very important role in PPP because PPP is designed for use over dial-up links where verification of user identity is necessary. Authentication means validating the identity of a user who needs to access a set of resources. PPP has created two protocols for authentication PAP(Password authentication Protocol) CHAP(Challenge Handshake Authentication Protocol).

2.5.1 PAP (Password Authentication Protocol)

The password authentication Protocol is a simple authentication procedure with a two-step process:



- The user who wants to access a system sends authentication identification (usually the user name) and a password.
- The system checks the validity of the identification and

password and either accepts or denies connection.

For those systems that require more security, PAP is not enough a third party with access to the link can be easily pick up the password and access the system resources.

PAP Packets

PAP packets are encapsulated in a PPP Frame. What distinguishes a PAP packet from other packets is the value of the protocol field, C02316. There are three PAP Packets: authentication-request, authentication-ack and authentication-nak. The first packet is used by the user to send the user name and password. The second is used by the system to allow access. The third is used by the system to deny access. Shows the format of the three packets.

2.5.2 CHAP (Challenge Hand Shake Authentication Protocol)

The challenge handshake authentication protocol is a three-way hand-shaking authentication protocol that provides more security. In this method the password is kept secret; it is never sent on-line.

- The system sends to the user a challenge packet containing a challenge value, usually a few bytes.
- The user applies predefined function that takes the challenge value and the user's own password and creates a result. The user send the result in the response packet to the system.
- The system does the same .It applies the same function to the password of the user and the challenge value to create a result. If the result created is the same as the result sent in the response packet, access is granted; otherwise, it is denied.

CHAP is more secure than PAP, especially if the system continuously changes the challenge value. Even if the intruder learns the challenge value and the result, the password is still secret

CHAP PACKETS

CHAP packets are encapsulated in the PPP frame. What distinguishes a CHAP packet from other packets is the value of the protocol field, C22316. There are four CHAP packets: challenge, response, success and failure. The first packet is used by the system to send the challenge value. The second is used by the user to return the result of the calculation. The third is used by the system to allow access to the system. The fourth is used by the system to deny access to the system.

2.6 NCP (Network Control Protocol)

After the link has been established and authentication has been successful, the connection goes to the networking state. In this state, PPP uses another protocol called **Network Control Protocol (NCP)**

NCP is a set of control protocols to allow the encapsulation of data coming from network layer protocols in the PPP frame.

III. OTHER PROTOCOLS

Note the other protocols have their own set of the states through which a PPP connection goes to deliver some network layer packets.

Establishing: The user sends the configure-request packet to negotiate the options for establishing the link. The user requests PAP authentication .After user receives the configure-ack packet, link establishing is done.

Authentication: The user sends the configure-request to negotiate the options for the network layer activity. After it receives the configure-ack, the user can send the network layer data, which may consume several frames. After all data are sent the user sends the terminate-request to terminate the network layer activity. When the terminate-ack packet is received the networking phase is complete. The connection goes to the terminating state.

Terminating: The user sends the terminate-request packet to terminate the link. With the receipt of the terminate-ack packet, the link is terminated.

IV. CONCLUSION

The purpose intended for PPP have all been achieved and more. PPP has gained widespread acceptance by the networking industry as a standard for synchronous and asynchronous communication. Now virtually all of the major router vendor enjoy seamless PPP connections with other vendor's intermediate systems. Information system manages no longer have to choose between differing proprietary which would limit access on their LAN or WAN connections.

As noted earlier that PPP is making substantial progress I becoming a standard for ISDN communications, but that's not all. With the rapid expansion of internet users, PPP is sure to increase in importance. The development of new PPP related technologies will enhance this importance. For example, the point-to-point tunneling protocol (PPTP) will use a PPP link to the internet to provide a secure link to a remote LAN. Connections that once required an on-site remote access server will now be made by merely dialing into a local internet service provider.

REFERENCES

1. CCENT: Cisco certified entry networking technician, study guide.
2. CCIE Routing and switching V4.0 quick reference, second edition.
3. Perkins, D., "The point –to– point protocol for transmission of multi –protocol Data grams over point-to-point links".
4. Hobby R., and D. Perkins, "The point-to-point protocol Initial configuration options", CMU, UC Davis, July 1990.
5. IEEE Draft Standard p802.1d/D9 MAC Bridges, Institute of Electrical and electronic engineers, also published as ISO DIS 10038, July 1989.
6. IEEE Draft Standard p802.5d/D13 Draft Addendum to ANSI/IEEE standard 802.5-1988 token ring MAC and PHY Specification Enhancement for Multiple-ring networks, Institute of electrical and electronic engineers, May 1989.
7. Establishing a Point-to-point WAN connection with PPP, Authorized self-study guide interconnecting Cisco network devices, Part 2(ICND2).
8. Authentication protocols: computer TTA network +2009 in depth.
9. Layered Data Link Protocols: Introduction to network security.
10. Control (HDLC) and PPP: CCIE routing and switching v4.0 Quick reference, second edition.
11. Point to point protocol: CCENT, Cisco@ certified entry networking technician, study guide.
12. Network control protocol(NCP): CCNA certification all- in –one dummies
13. PPP Concepts: CCNA 640-802, second edition.

AUTHOR PROFILE

Immadisetty L V Chandrika was born in 1992 at Guntur district, Andhra Pradesh. She is pursuing B.Tech in Koneru Lakshmaiah. Her interested areas are Data communications and Transmission.

B.V.Videhi was born in 1992 at Krishna district, Andhra Pradesh She is pursuing B.TECH in Koneru Lakshmaiah University, Guntur. Her interested areas are data communication and wireless communication.

A. Rama Krishna was born in 1987 at West Godavari District, Andhra Pradesh. He is working as a Assistant Professor, Dept.of ECM, K.L.University, Vaddeswaram, A.P, India.