IJCSE International Journal of Computer Sciences and Engineering Open Access

Survey Paper Vol.-7, Issue-1, Jan 2019 E-ISSN: 2347-2693

# A Study on point-to-point protocol in Data Communication and Networking

**J. Saranya**

Department of Computer Applications Chevalier T.Thomas Elizabeth College for Women, Chennai, India

*Corresponding Author: saran.vel1987@gmail.com

**Available online at: www.ijcseonline.org**

Accepted: 19/Jan/2019, Published: 31/Jan/2019

***Abstract* -** The Point-to-point protocol is a protocol designed to respond all the Internet protocol and allow IP addresses to be assigned dynamically as well as support authentication of the User. It connects two routers directly without any host or any other networking device in between These point-to-point protocol can control and manage the transfer of data, connection authentication, transmission encryption and compression.

***Keywords*-** Point-to-point protocol(PPP),Link control protocol(LCP),Network control protocol(NCP),Password authentication protocol(PAP),Challenge handshake authentication protocol(CHAP),Internetwork protocol control protocol(IPCP).

## I. INTRODUCTION

The point-to-point protocol is a physical & data link layer communication protocol used to establish a direct connection between two nodes .It connects two routers directly without any host or any other networking device in between .It can provide connection authentication, transmission encryption and compression .The point-to-point protocol is derived into two categories point-to-point protocol over Ethernet (PPPoE) and point-to-point protocol over ATM (PPPoA).

## II. PPP TRANSITION STATES

The transition states between two end points or nodes from sender to receiver.

A. *Idle state*
The link will be idle in this state there is no active carrier and the line is quiet.

B. *Establishing state*
Several packets are exchanging in this state .If one of the endpoints starts the communication the connection goes into the establishment state.

*C. Authentication state*
The authentication state is an optional. Once the establishing state is decided to proceed it goes to reach network state with authentication.

*D. Network state*
It is the heart of transition states. if the connection reaches this state the exchange of user control and Data packets can be started.

*E. Terminating state*
The connection in the terminating state several packets
Are exchanging between the ends .This is the final transition state. The transition state will be closed the end-
To-end node transitions are stopped in this state.

## III.PPP LAYERS

The point-to-point protocol layers are physical & Data link.
*A .Physical Layer*
The Point-to-point protocol physical layer supports any of the protocols recognized by ANSI.

*B .Data Link Layer*
The data link layer used to establish a direct communication between two nodes

## IV.LINK CONTROL PROTOCOL (LCP)

The Link control protocol (LCP) eshtablish, configures, and tests data-link internet connections. Before establishing communications over a point-to-point link, each end of the PPP link must send out LCP packets.

*A .LCP Packets*
There are three classes of LCP packets
1. Link configuration packets used to establish and configure a link (configure request, configure-ack, configure nak and configure reject)

2. Link termination packets used to terminate a link (terminate-request and terminate-ack).

3. Link maintenance packets used to manage the debug a link (code-reject, protocol-reject, echo request, echo reply, and discard request.

In the interest of simplicity, there is no version field in the LCP packet. A correctly functioning LCP implementation will always respond to unknown protocols and codes with easily recognizable LCP packets, thus providing a deterministic fallback mechanism for implementation of other versions. All LCP Link Configuration, Link transmission, and code-reject packets (codes 1 through 7) are always sent as if no configuration options were negotiated. In particular each configuration option specifies a default value. This ensures that such LCP packets are always recognizable, even when one end of the link mistakenly believes the link to be open. Exactly one LCP packets is encapsulated in the PPP information field, where the PPP protocol field indicates type hex c021(Link Control Protocol).

Table 1: LCP packets and their codes

| Code | Packet type | Description |
|---|---|---|
| $01_{16}$ | Configure-request | Contains the list of proposed option and their values. |
| $02_{16}$ | Configure-ack | Accepts all options proposed. |
| $03_{16}$ | Configure-knack | Announces that some options are not acceptable. |
| $04_{16}$ | Configure-reject | Announces that some options are not recognized. |
| $05_{16}$ | Terminate-request | Request to shut the line down. |
| $06_{16}$ | Terminate-ack | Accepts the shut-down request. |
| $07_{16}$ | Code-reject | Announces an unknown code. |
| $08_{16}$ | Protocol-reject | Announces an unknown protocol. |
| $09_{16}$ | Echo-request | A type of hello message to check if the other end is alive. |
| $0A_{16}$ | Echo-reply | The response to the echo-request message. |
| $0B_{16}$ | Discard-request | A request to discard the packet. |

### *B .Configuration Packets*

*1. Configure-Request*

An implementation wishing to open a connection MUST transmit a configure-request. The options field is filled with any desired changes to the link defaults. Configuration options SHOULD NOT be included with default values. Upon reception of a configure-Request, an appropriate reply MUST be transmitted.

*2. Configure-Ack*

If every configuration option received in a configure-request is recognizable and all values are acceptable, then the implementation MUST transmit a Configure-Ack. The acknowledged Configuration options MUST NOT be recorded or modified in anyway. On reception of a configure-ack, the identifier field MUST match that of the last transmitted configure-Request. Additionally, the configuration options in a configure-ack MUST exactly match those of the last transmitted configure-Request. Invalid packets are silently discarded.

*3. Configure-Nak*

The configure-nak if every instance of the received configuration options is recognizable, but some values are not acceptable, then the implementation MUST transmit a configure-nak. The options field is filled with only the unacceptable configuration options from the configure-request. All accept-table configuration options are filtered out of the configure-nak, but otherwise the configuration Options from the configure-Request MUST NOT be recorded.

*4. Configure-Reject*

The configure-reject options received in a configure-request are not recognizable or are not acceptable for negotiation (as configured by a network administrator), then the implementation MUST transmit a configure-reject. The options field is filled with only the unacceptable configuration options from the configure-request. All recognizable and configuration options are filtered out of the configure-reject, but otherwise the configuration options MUST NOT be recorded or modified in anyway. On reception of a configure-reject, the identifier field MUST match that of the last transmitted configure-request. Additionally, the configuration options in a configure-reject MUST be a

Proper subset of those in the last transmitted configure-request. Invalid packets are silently discarded. Reception Of a valid Configure-reject indicates that when a new configures- request is sent, it MUST NOT include any of the configuration options listed in the configure-Reject.

### *C. Link Termination packets*

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

*1. Terminate-Request*

Either party can terminate the link by sending a terminate-Request packet.

*2. Terminate-Ack*

The party that receives the terminate-Request packet should answer with a terminate-ack packet

.

### *D. Link monitoring and debugging packets*

1. Code-Reject

If the endpoint receives a packet with an unrecognized code in the packet, it sends a code-reject packet.

*2. Protocol-Reject*

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

*3. Echo-Request*

This 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.

*4. Echo-Reply*

This packet is sent in response to an echo-request. The information field in the echo-request packet I exactly duplicated and sent back to the sender of the echo-request packet.

*5. Discard-Request*

This is a kind of loopback test packet. It is used by the sender to check its own loopback condition. The receiver of the packet just discards it.

## V.PASSWORD AUTHENTICATION PROTOCOL (PAP)

The Password authentication protocol (PAP) is a simple user authentication protocol that does not encrypt the data and sends the password and username to the authentication server as plain text. The PAP is a very vulnerable to being read from the point-to-point protocol (PPP) data packets exchanged between the authentication server and the user's machine. This was primarily used when connecting to old Unix - based servers with no support for more advanced encryption protocols.

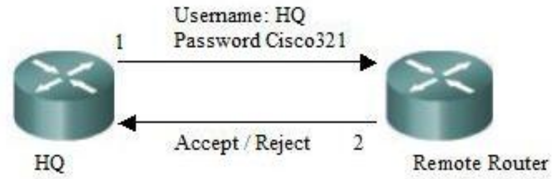

Figure 1 : Password Authentication Protocol(PAP) PAP 2 Way handshake

## VI.CHALLENGE HANDSHAKE AUTHTICATION PROTOCOL (CHAP)

The CHAP (Challenge – Handshake authentication protocol) is more secure procedure for connecting to a system than the password authentication protocol(PAP).

After the link is made, the server sends a challenge message to the connection requestor. The requestor responds with a value obtained by using a one-way hash function. The server checks the response by comparing it its own calculation of the expected hash value. If the value matches, the authentication is acknowledged otherwise the connection is usually terminated. At the time the server can request the connected party t send a new challenge message. Because CHAP identification are changed frequently and authentication can be request by the server at any time. CHAP provides more security than PAP.

## VII.NETWORK CONTROL PROTOCOL (NCP)

The network control protocol (NCP), a protocol in the point to point protocol (PPP) suite, provides services in the PPP link connection process to establish and configure different network-layer such as IP, IPX or AppleTalk. After a NCP has reached the opened state, PPP will carry the corresponding network – layer protocol packets. Any supported network layer protocol packets received when the corresponding NCP is not in the opened state must be silently discarded. During this phase, link traffic consists of any possible combination of LCP, NCP and network layer protocol packets.

## VIII.INTERNETWORK PROTOCOL CONTROL PROTOCOL (IPCP)

The IPCP is responsible for configuring, enabling, and disabling the IP protocol modules on both ends of the point-to-point link. IPCP uses the same packet exchange mechanism as the link control protocol (LCP). IPCP packets may not be exchanged until PPP has reached the Network-layer protocol phase. IPCP packets received before this phase is reached should be silently discarded.

Before any IP packets may be communicated, PPP must reach the Network-Layer protocol phase, and the IP control protocol must reach the opened state.

Table 2: IPCP Packets code value

| Code | IPCP packets |
|---|---|
| **01** | Configure-request |
| **02** | Configure-ack |
| **03** | Configure-nak |
| **04** | Configure-reject |
| **05** | Terminate-request |
| **06** | Terminate-ack |
| **07** | Code-reject |

## IX. CONCLUSION

In this paper we reviewed the point-to-point Communication protocol and analyzed the different transmission control process and security issues.

A comparative study of PPP and the configure packets was also be done. By implementing the NCP and PAP for various Network authentication issues are solved.In communication PPP can be enhanced these networks.

## REFERENCES

[1]. Computer Networking: principles, Protocols and Practices.
[2]. Point-to-point protocol and feature overview and configuration guide – Allied Telesis.
[3]. Networking model and packet guide to core network protocols.
[4]. Data communication and networking –Behrouz A.forouzan.
[5]. A pointed look at the point-to-point protocol IEEE Internet computing – C.Metz.
[6]. D.Perkins,"The point-to-point protocol for the transmission of multi-protocol data grams over point-to-point Links"
[7]. Stallings, William, cryptography and network Security (6th edition.). Upper Saddle River, N.J.: Prentic Hall.