SLIP and PPP

Gursharan Singh Tatla
mailme@gursharansingh.in
www.eazynotes.com

27-Mar-2011
Data Link Layer in Internet

- We know that Internet consists of individual systems that are connected to each other.
- Basically, it is wide area network that is built up from point-to-point leased lines.
- In these point-to-point lines, two major data link protocols are used:
  - Serial Line Internet Protocol (SLIP)
  - Point-to-Point Protocol (PPP)
Serial Line Internet Protocol (SLIP)

- It is a means of sending Internet Protocol datagrams over a serial link.
- It can be used by two systems to communicate via a direct cable connection or modem link.
- The initial purpose of this protocol was to connect Sun workstation to the Internet over a dial-up line using modem.
Problems with SLIP

- It does not perform any error detection and correction.
- It supports only IP (Internet Protocol). So, it cannot be used for other networks that do not use IP (for e.g.: Novell LANs).
- It does not support the allocation of dynamic IP address.
- Both the communicating systems should be assigned a specific IP address before hand.
- It does not provide any authentication.
- It is not an approved Internet standard.
Data Format of SLIP

- The data format of SLIP is:

| Data | End Flag |

- A special END character (equivalent to decimal 192) marks the end of data.
Point-to-Point Protocol (PPP)

- PPP was devised by IETF (Internet Engineering Task Force) to create a data link protocol for point-to-point lines that can solve all the problems of SLIP.
- It is the most commonly used data link protocol.
- It is used to connect the home PC to the ISP server.
Benefits of PPP

- PPP defines the format of the frame to be exchanged between the devices.

- It defines Link Control Protocol (LCP) for:
  - Establishing the link between two devices.
  - Maintaining this established link.
  - Configuring this link.
  - Terminating this link after the transfer.
Benefits of PPP  (Contd…)

• It provides error detection.

• Unlike SLIP, that supports only IP, it supports multiple protocols.

• It supports dynamic allocation of IP address.

• It provides authentication.

• It provides NCP (Network Control Protocol), that supports variety of network layer protocol.
PPP Frame Format

- Frame format of PPP is similar to HDLC frame:

```
    01111110  11111111  00000011
    Flag    Address   Control
    1 Byte   1 Byte    1 Byte
```

<table>
<thead>
<tr>
<th>Flag</th>
<th>Address</th>
<th>Control</th>
<th>Protocol</th>
<th>Information</th>
<th>FCS</th>
<th>Flag</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Byte</td>
<td>1 Byte</td>
<td>1 Byte</td>
<td>1 or 2 Byte</td>
<td>Variable</td>
<td>2 or 4 Byte</td>
<td>1 Byte</td>
</tr>
</tbody>
</table>

- **Flag Field:** It marks the beginning and end of the PPP frame. Flag byte is 01111110.

- **Address Field:** This field is of 1 byte and is always 11111111. This address is the broadcast address i.e. all stations accept this frame.
PPP Frame Format

- Frame format of PPP is similar to HDLC frame:

```
<table>
<thead>
<tr>
<th>Flag</th>
<th>Address</th>
<th>Control</th>
<th>Protocol</th>
<th>Information</th>
<th>FCS</th>
<th>Flag</th>
</tr>
</thead>
<tbody>
<tr>
<td>01111110</td>
<td>11111111</td>
<td>00000011</td>
<td>01111110</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

1 Byte  1 Byte  1 Byte  1 or 2 Byte  Variable  2 or 4 Byte  1 Byte

- **Control Field:** It is also of 1 byte. It uses the format of U-Frame in HDLC. The value is always 00000011 to show that the frame does not contain any sequence number and there is no flow control or error control.

- **Protocol Field:** This field specifies the kind of protocol of the data in the information field.
PPP Frame Format

- Frame format of PPP is similar to HDLC frame:

<table>
<thead>
<tr>
<th>Flag</th>
<th>Address</th>
<th>Control</th>
<th>Protocol</th>
<th>Information</th>
<th>FCS</th>
<th>Flag</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Byte</td>
<td>1 Byte</td>
<td>1 Byte</td>
<td>1 or 2 Byte</td>
<td>Variable</td>
<td>2 or 4 Byte</td>
<td>1 Byte</td>
</tr>
</tbody>
</table>

- **Information Field**: Its length is variable. It carries user data or other information.

- **FCS Field**: It stands for Frame Check Sequence. It contains checksum. It is either 2 bytes or 4 bytes.
Transition Phases in PPP

- The PPP connection goes through different states:
Transition Phases in PPP

- **Down:**
  - In down phase, the link is not used.

- **Establish:**
  - Connection goes into this phase when one of the nodes start communication.

- **Authenticate:**
  - This phase is optional. The two nodes may decide during establishment phase, to use this phase.
Transition Phases in PPP

- **Up:**
  - In this phase, data transfer takes place. The connection remains in this phase until one of the node wants to end the connection.

- **Terminate:**
  - In this phase, connection is terminated.
PPP Stack

- PPP uses several other protocols to establish link, authenticate users and to carry the network layer data:

- The various protocols used are:
  - Link Control Protocol
  - Authenticate Protocol
  - Network Control Protocol
Link Control Protocol

- It is responsible for establishing, maintaining, configuring and terminating the link.
- It provides negotiation mechanism to set options between two nodes.
- All LCP packets are carried in the information field of the PPP frame.
Authentication Protocol

- Authentication protocol helps to validate the identity of a user who needs to access the resources.

- There are two authentication protocols:
  - Password Authentication Protocols (PAP)
  - Challenge Handshake Authentication Protocol (CHAP)
Password Authentication Protocol (PAP)

- This protocol provides two step authentication procedure:
  - **Step 1:** Username and password is provided by the user who wants to access the system.
  - **Step 2:** The system checks the validity of username and password, and either accepts or rejects the connection.
Challenge Handshake Authentication Protocol (CHAP)

- It provides more security than PAP.
- In this method, password is kept secret.
- It is a three way authentication protocol:
  
  **Step 1:** System sends a challenge packet to the user. It contains a value, usually a few bytes.
  
  **Step 2:** Using a predefined function, a user combines this challenge value with the user password and sends the resultant packet back to the system.
  
  **Step 3:** System then applies the same function to the password of the user & challenge value, and creates a result. If the result is same as the result sent in the response packet, access is granted, otherwise, it is denied.
Network Control Protocol (NCP)

- After establishing the link & authenticating the user, PPP connects to the network layer.
- This connection is established by NCP.
- Therefore, NCP is a set of control protocols that allow the encapsulation of the data coming from the network layer.
- After the network layer configuration is done by one of the NCP, the user can exchange data from the network layer.
## Differences Between SLIP & PPP

<table>
<thead>
<tr>
<th>S. No.</th>
<th>SLIP</th>
<th>PPP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>SLIP stands for Serial Line Internet Protocol.</td>
<td>PPP stands for Point-to-Point Protocol</td>
</tr>
<tr>
<td>2.</td>
<td>SLIP does not perform error detection &amp; correction.</td>
<td>PPP performs error detection &amp; correction.</td>
</tr>
<tr>
<td>3.</td>
<td>SLIP supports only IP.</td>
<td>PPP supports multiple protocols.</td>
</tr>
<tr>
<td>4.</td>
<td>IP address is assigned statically.</td>
<td>IP address is assigned dynamically</td>
</tr>
<tr>
<td>5.</td>
<td>SLIP does not provide any authentication.</td>
<td>PPP provides authentication.</td>
</tr>
<tr>
<td>6.</td>
<td>SLIP is not approved Internet standard.</td>
<td>PPP is approved Internet standard.</td>
</tr>
</tbody>
</table>
Thank You 😊
Have a Nice Day