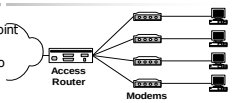
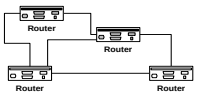
Point-to-Point DLC protocols

Point-to-Point (serial) links

- Many data link connections are point-to-point serial links:
  - Dial-in or DSL access connects hosts to access routers
  - Routers are connected by high-speed point-to-point links
- Here, IP hosts and routers are connected by a serial cable
- Data link layer protocols for point-to-point links are simple:
  - Main role is encapsulation of IP datagrams
  - No media access control needed



Dial-Up Access



Point-to-Point Links

Data Link Protocols for Point-to-Point links

- **SLIP (Serial Line IP) (RFC 1055)**
  - First protocol for sending IP datagrams over dial-up links (from 1988)
  - Encapsulation, not much else
- **PPP (Point-to-Point Protocol) (RFC 1661)**
  - Successor to SLIP (1992), with added functionality
  - Used for dial-in and for high-speed routers
- **HDLC (High-Level Data Link) (ISO)**
  - Widely used and influential standard (1979)
  - Default protocol for serial links on Cisco routers
  - Actually, PPP is based on a variant of HDLC

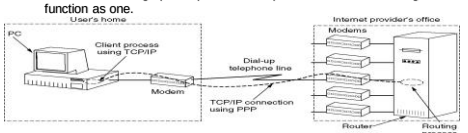
High-level data link control (HDLC) Point to Point Protocol (PPP)

- Suppose IICT is connected to the Internet, right?
- So what WAN protocol do you use to connect to the Internet?
- Chances are, that if you have a E1 or T1 leased line to the Internet or a private network between locations, you use one of these three WAN Protocols: HDLC, PPP, Frame-relay or Ethernet.
- Let's explore the differences and similarities of these protocols.
- HDLC is actually the default protocol on all Cisco serial interfaces.

What is PPP?

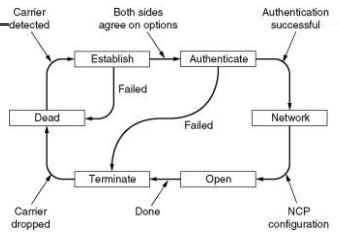
- Point to Point Protocol (PPP) is used for most every dial up connection to the Internet.
- PPP is based on HDLC and is very similar.
- Both work well to connect point to point leased lines.
- The differences between PPP and HDLC are:
- PPP is not proprietary when used on a Cisco router
- PPP has several sub-protocols that make it function.
- PPP is feature-rich with dial up networking features

- It has become the most popular dial up networking protocol in use today.
- Here are some of the dial-up networking features it offers:
- Link quality management monitors the quality of the dial-up link and how many errors have been taken.
- It can bring the link down if the link is receiving too many errors.
- Multilink can bring up multiple PPP dialup links and bond them together to function as one.



A home personal computer acting as an internet host.

- These protocols take your username and password to ensure that you are allowed access to the network you are dialing in to.

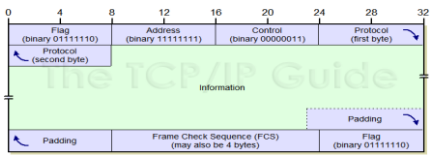


A simplified phase diagram for bring a line up and down.

PPP General Frame Format

Field Name	Size (bytes)	Description
Flag	1	***Flag:*** Indicates the start of a PPP frame. Always has the value "01111110" binary (0x7E hexadecimal, or 126 decimal).
Address	1	***Address:*** In HDLC this is the address of the destination of the frame. But in PPP we are dealing with a direct link between two devices, so this field has no real meaning. It is thus always set to "11111111" (0xFF or 255 decimal), which is equivalent to a broadcast (it means "all stations").
Control	1	***Control:*** This field is used in HDLC for various control purposes, but in PPP it is set to "00000011" (3 decimal).
Protocol	2	***Protocol:*** Identifies the protocol of the datagram encapsulated in the information field of the frame. See below for more information on the *Protocol* field.
Information	Variable	***Information:*** Zero or more bytes of payload that contains either data or control information, depending on the frame type. For regular PPP data frames the network-layer datagram is encapsulated here. For control frames, the control information fields are placed here instead.
Padding	Variable	***Padding:*** In some cases, additional dummy bytes may be added to pad out the size of the PPP frame.
FCS	2 (or 4)	***Frame Check Sequence (FCS):*** A checksum computed over the frame to provide basic protection against errors in transmission. This is a CRC code similar to the one used for other layer two protocol error protection schemes such as the one used in Ethernet. It can be either 16 bits or 32 bits in size (default is 16 bits). The FCS is calculated over the *Address*, *Control*, *Protocol*, *Information* and *Padding* fields.
Flag	1	***Flag:*** Indicates the end of a PPP frame. Always has the value "01111110" binary (0x7E hexadecimal, or 126 decimal).

PPP General Frame Format



Additional PPP functionality

- In addition to encapsulation, PPP supports:
  - multiple network layer protocols (protocol multiplexing)
  - Link configuration
  - Link quality testing
  - Error detection
  - Option negotiation
  - Address notification
  - Authentication
- The above functions are supported by helper protocols:
  - LCP
  - PAP, CHAP
  - NCP

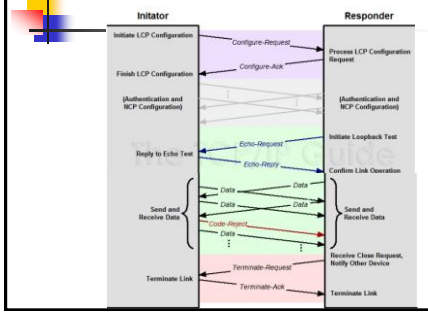
PPP Support protocols

- **Link management:** The link control protocol (LCP) is responsible for establishing, configuring, and negotiating a data-link connection.
- LCP also monitors the link quality and is used to terminate the link.

Authentication: Authentication is optional. PPP supports two authentication protocols: Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP).

- **Network protocol configuration:** PPP has network control protocols (NCPs) for numerous network layer protocols.
- The IP control protocol (IPCP) negotiates IP address assignments and other parameters when IP is used as network layer.

PPP Link Control Protocol (LCP) Message Exchanges



Name	Direction	Description
Configure-request	I → R	List of proposed options and values
Configure-ack	I ← R	All options are accepted
Configure-nak	I ← R	Some options are not accepted
Configure-reject	I ← R	Some options are not negotiable
Terminate-request	I → R	Request to shut the line down
Terminate-ack	I ← R	OK, line shut down
Code-reject	I ← R	Unknown request received
Protocol-reject	I ← R	Unknown protocol requested
Echo-request	I → R	Please send this frame back
Echo-reply	I ← R	Here is the frame back
Discard-request	I → R	Just discard this frame (for testing)

The LCP frame types.

Three basic methods for logging onto a server:

- Anyone with a computer and a modem can dial into any ISP's modems and negotiate modem protocols to establish a "connection".
- But ISPs offer services only to paying customers or members, so before they let anyone start a TCP/IP session, they ask that each connection to identify itself with a username and password.
- This process is called authentication. There are three basic methods for logging onto a server: manual or scripted logins, PAP, and CHAP.

The exchange of data in manual logins is plain text. For a faster, more secure authentication, most ISP's use Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP).

Manual and scripted logins

- Manual and scripted logins are technically the same thing.
- First, the ISP's server (actually a modem card on the modem chassis rack) sends a text login prompt to the user's terminal.
- The user, or a script running and waiting for the login prompt, sends the username.
- The modem card responds with a password prompt (before actually checking the validity of the username). .
- The user or script responds with the password, and the modem card takes that information and sends it to the RADIUS server (the ISP's database of usernames and passwords) for checking. If something doesn't match up, the modem card sends "Login failed" to the terminal, counts down one, and sends the login prompt again.
- Once the username and password are checked and cleared, the modem card takes an IP from its available pool, packages it with other info like the modem card's IP and the DNS servers, and sends it down the line to the user's computer to establish a PPP connection.

Password Authentication Protocol (PAP)

- **PAP works as follows**:

1. After the link is established, the client sends a password and username to the server bundled as a one Link Control Protocol (LCP) packet.
2. The server (the modem card in the modem racks) recognizes the packet as a PAP authentication request, and sends the data to the RADIUS server (the database of usernames and passwords).
3. RADIUS either validates the request and sends back an acknowledgement to the modem card, terminates the connection, or offers the client another chance.

Passwords are sent as plain text.

The difference between PAP authentication and a manual or scripted login, is that PAP is not interactive.

The username and password are entered in the client's dialing software and sent as one data package as soon as the modems have established a connection, rather than the server sending a login prompt and waiting for a response.

Challenge Handshake Authentication Protocol (CHAP).

CHAP is a more secure procedure for connecting to a system than PAP. Here's how CHAP works:

1. After the link is made, the server sends a challenge message to the client. The client responds with a value obtained by using a one-way hash function.

   A one-way hash function, also known as a message digest, fingerprint or compression function
2. The server checks the response by comparing it its own calculation of the expected hash value.
   All modern hash algorithms produce hash values of 128 bits and higher.
3. If the values match, the authentication is acknowledged; otherwise the connection is terminated.

   At any time, the server can request the connected party to send a new challenge message. Because CHAP identifiers are changed frequently and because authentication can be requested by the server at any time, CHAP provides more security than PAP.