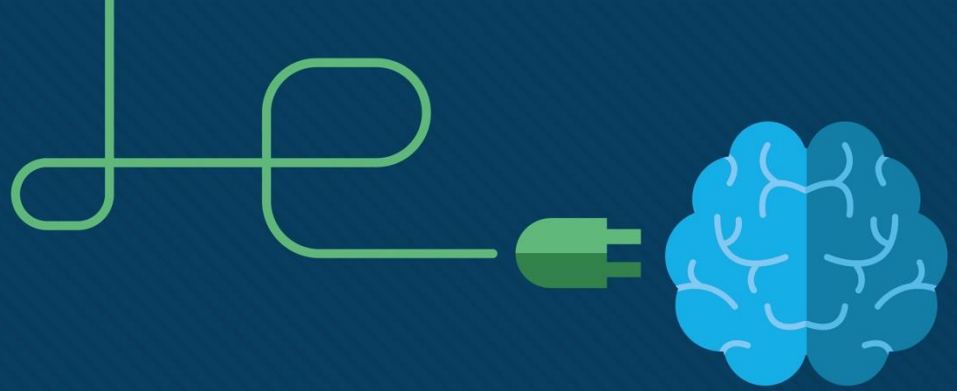


24 Point-to-Point Connections

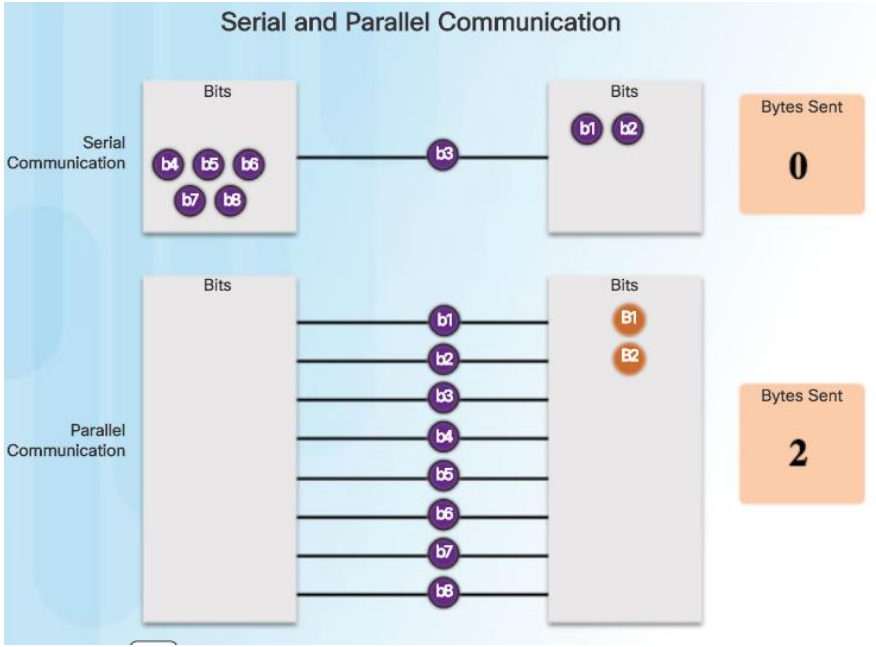
24.1 Serial Point-to-Point Overview

Serial and Parallel Ports

Serial Point-to-Point Connection

- A WAN is owned by a service provider and a LAN is typically owned by an organization.
- Point-to-point connections connect LANs to service provider WANs and connect LAN segments.
- A LAN-to-WAN point-to-point connection is also referred to as a serial connection or leased-line connection.
- Lines are leased from a carrier.
- Companies pay for a continuous connection between two remote sites, and the line is continuously active and available.

Serial and Parallel Ports (Cont.)

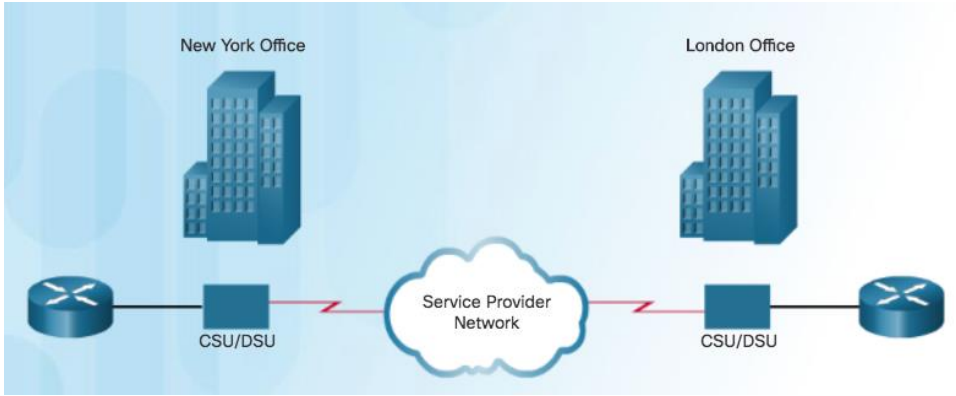


- On most PCs, parallel ports and RS-232 serial ports have been replaced by the higher speed serial Universal Serial Bus (USB) interfaces.

- Serial Communication
  - Method of data transmissions in which the bits are transmitted sequentially over a single channel.
  - Equivalent to a pipe only wide enough to fit one ball at a time. Multiple balls can go into the pipe, but only one at a time, and they only have one exit point, the other end of the pipe.
- Parallel communications
  - Bits can be transmitted simultaneously over multiple wires.
  - Sends a byte (eight bits) in the time that a serial connection sends a single bit.
  - At one time, most PCs included both serial and parallel ports. Parallel ports were used to connect printers, computers, and other devices that required relatively high bandwidth.

Point-to-Point Communication Links

- Point-to-point link
  - Used when permanent dedicated connections are required
  - Provides a single, pre-established WAN communications path
  - Path goes from the customer premises, through the provider network, to a remote destination, as shown in the figure



- Can connect two geographically distant sites, such as a corporate office in New York and a regional office in London
- Not limited to connections that cross land (undersea fiber-optics)
- Usually more expensive than shared services
- Constant availability is essential for some applications such as VoIP or video over IP.

Serial Bandwidth

- Bandwidth
  - Refers to the rate at which data is transferred over the communication link.
  - Carrier technology will dictate how much bandwidth is available.
    - North American (T-carrier) specification
    - European (E-carrier) system
    - U.S. Optical Carrier (OC) bandwidth points
  - OC transmission rates are a set of standardized specifications for the transmission of digital signals carried on SONET fiber-optic networks.

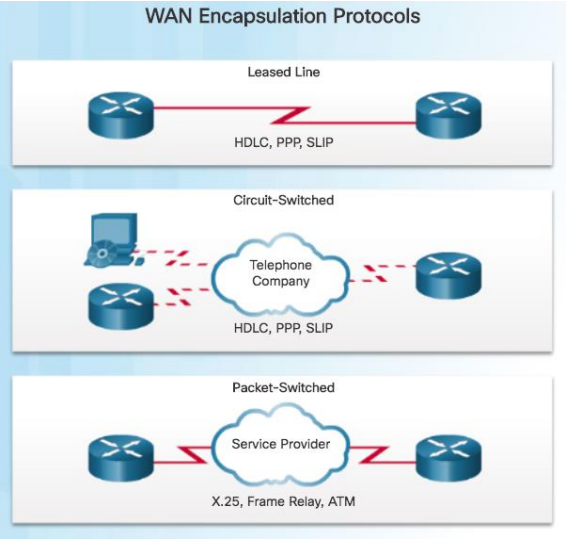
Carrier Transmission Rates

Line Type	Bit Rate Capacity
56	56 kb/s
64	64 kb/s
T1	1.544 Mb/s
E1	2.048 Mb/s
J1	1.544 Mb/s
E3	34.368 Mb/s
T3	44.736 Mb/s
OC-1	51.84 Mb/s
OC-3	155.52 Mb/s
OC-9	466.56 Mb/s
OC-12	622.08 Mb/s
OC-18	933.12 Mb/s
OC-24	1.244 Gb/s
OC-36	1.866 Gb/s
OC-48	2.488 Gb/s
OC-96	4.976 Gb/s
OC-192	9.954 Gb/s
OC-768	39.813 Gb/s

- In North America, expressed as a digital signal level number (DS0, DS1, etc.), which refers to the rate and format of the signal.
  - Most fundamental line speed is 64 kb/s, or DS0.
  - 24 DS0s can be bundled to get a DS1 line (T1 line).
  - 28 DS1s can be bundled to get a DS3 line (T3 line).

WAN Encapsulation Protocols

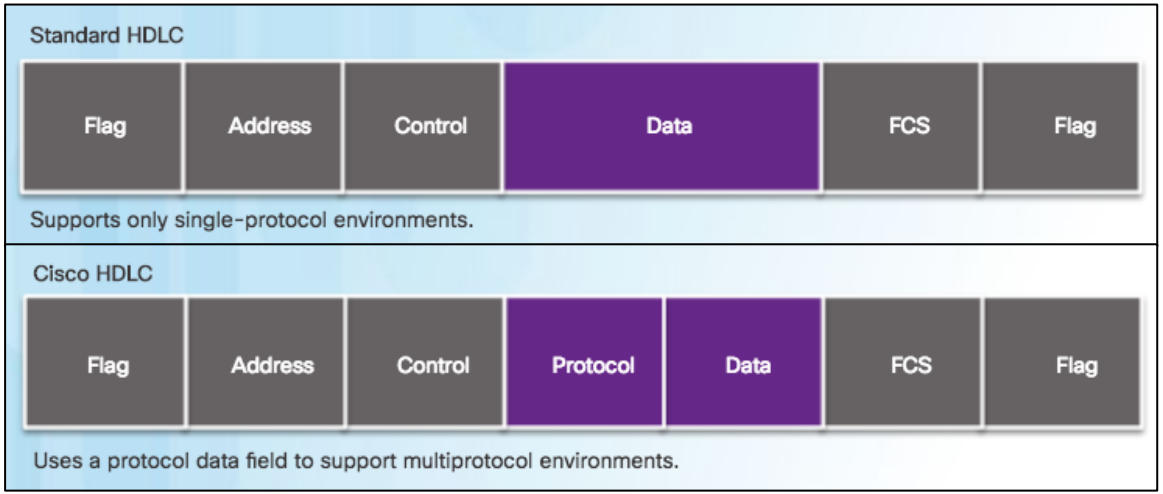
- Data is encapsulated into frames before crossing the WAN link and must be configured for the appropriate Layer 2 protocol.
- Choice of protocol depends on the WAN technology and the communicating equipment.
- WAN protocols (HDLC and PPP are the focus of this course):
  - HDLC - Default encapsulation on point-to-point connections, dedicated links, and circuit-switched connections when the link uses two Cisco devices.
  - PPP - Provides router-to-router and host-to-network connections over synchronous and asynchronous circuits. Has built-in security mechanisms such as PAP and CHAP.



- Serial Line Internet Protocol (SLIP) - Displaced by PPP.
- X.25/Link Access Procedure, Balanced (LAPB) - Predecessor to Frame Relay.
- Frame Relay - Data link layer protocol that handles multiple virtual circuits. After X.25.
- ATM - International standard for cell relay in which devices send multiple service types, such as voice, video, or data, in fixed-length (53-byte) cells. Takes advantage of high-speed transmission media such as E3, SONET, and T3..

HDLC Encapsulation

The figure compares standard HDLC to Cisco HDLC.



Uses a frame delimiter, or flag, to mark beginning and end of each frame.

With an added protocol type field, Cisco HDLC can only work with other Cisco devices.

- HDLC is a synchronous data link layer protocol developed by the International Organization for Standardization (ISO).
- HDLC defines a Layer 2 framing structure that allows flow and error control through acknowledgments.
  - Default serial encapsulation method when connecting two Cisco routers.
  - Cisco's HDLC is a point-to-point protocol that can be used on leased lines between two Cisco devices.
  - Protocol field makes it possible for a single serial link to accommodate multiple network-layer protocols.

Configuring HDLC Encapsulation

```
Router(config)# interface s0/0/0
Router(config-if)# encapsulation hdlc
```

- Enable HDLC encapsulation
- HDLC is the default encapsulation on synchronous serial interfaces

- Use Cisco HDLC as a point-to-point protocol on leased lines between two Cisco devices.
- If connecting non-Cisco devices, use synchronous PPP.
- If the default encapsulation method has been changed, use the **encapsulation hdlc** command in interface configuration mode to re-enable HDLC.

Troubleshooting a Serial Interface

```
R1# show interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 172.16.0.1/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  CRC checking enabled
  Last input 00:00:05, output 00:00:04, output hang
  never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total
  output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold
  /drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     5 packets input, 1017 bytes, 0 no buffer
     Received 5 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun,
         0 ignored, 0 abort
     4 packets output, 395 bytes, 0 underruns
```

- The **show interfaces serial *x/x/x*** command displays information specific to serial interfaces.
- When HDLC is configured, “encapsulation HDLC” should be reflected in the output as highlighted in the figure.
- “Serial 0/0/0 is up, line protocol is up”, indicates that the line is up and functioning.

Troubleshooting a Serial Interface (Cont.)

- Five possible problem states can be identified in the interface status line of the **`show interface serial`** display:

  Serial *x* is down, line protocol is down.

  Serial *x* is up, line protocol is down.

  Serial *x* is administratively down, line protocol is down.

Troubleshooting a Serial Interface (Cont.)

Serial interface issues associated with state, and how to troubleshoot the issue.

Status Line	Possible Condition	Problem / Solution
Serial x is up, line protocol is up	This is the proper status line condition.	No action is required.
Serial x is down, line protocol is down (DTE mode)	The router is not sensing a carrier detect (CD) signal, which means the CD is not active. A WAN carrier service provider problem has occurred, which means the line is down or is not connected to CSU/DSU. Cabling is faulty or incorrect. Hardware failure has occurred (CSU/DSU).	1. Check the LEDs on the CSU/DSU to see whether the CD is active, or insert a breakout box on the line to check for the CD signal. 2. Verify that the proper cable and interface are being used by looking at the hardware installation documentation. 3. Insert a breakout box and check all control leads. 4. Contact the leased-line or other carrier service to see whether there is a problem. 5. Swap faulty parts. 6. If faulty router hardware is suspected, change the serial line to another port. If the connection comes up, the previously connected interface has a problem.
Serial x is up, line protocol is down (DTE mode)	A local or remote router is misconfigured.	1. Put the modem, CSU, or DSU in local loopback mode and use the `show interfaces serial` command to determine whether the line protocol comes up. If the line protocol comes up, a WAN carrier service provider

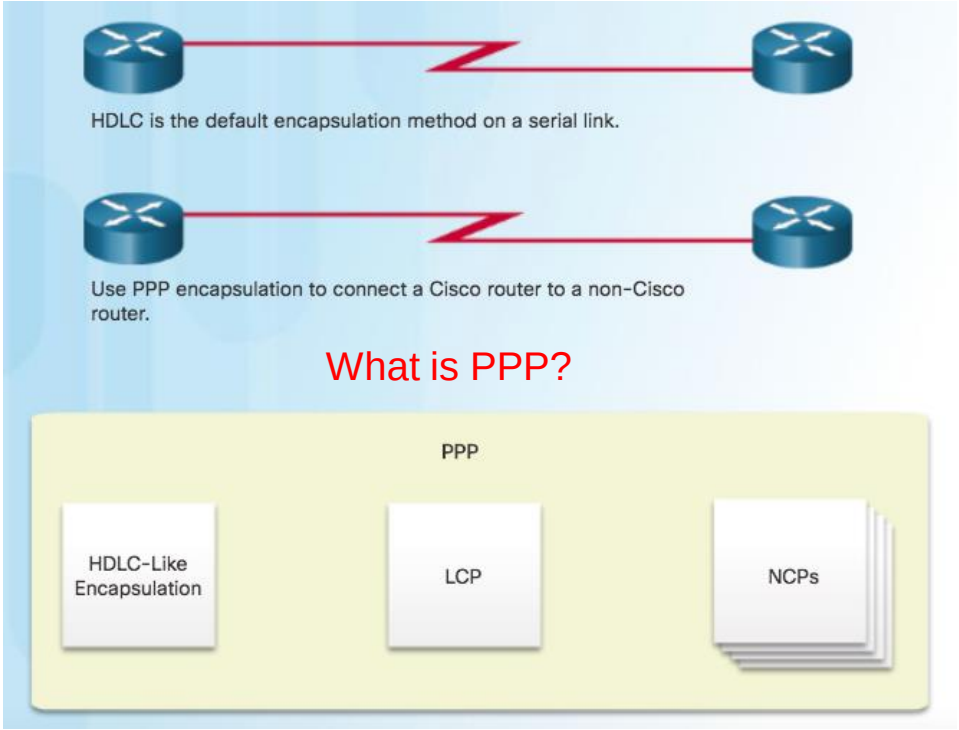
Troubleshooting a Serial Interface (Cont.)

Show controllers command output indicates the state of the interface channels and whether a cable is attached to the interface. In the figure, interface serial 0/0/0 has a V.35 DCE cable attached.

```
R1# show controllers serial 0/0/0
Interface Serial0/0/0
Hardware is GT96K
DCE V.35, clock rate 64000
idb at 0x66855120, driver data structure at 0x6685C93C
wic_info 0x6685CF68
Physical Port 0, SCC Num 0
MPSC Registers:
MMCR_L=0x000304C0, MMCR_H=0x00000000, MPCR=0x00000000
CHR1=0x00FE007E, CHR2=0x00000000, CHR3=0x0000064A,
CHR4=0x00000000
CHR5=0x00000000, CHR6=0x00000000, CHR7=0x00000000,
CHR8=0x00000000
CHR9=0x00000000, CHR10=0x00003008
SDMA Registers:
SDC=0x00002201, SDCM=0x00000080, SGC=0x0000C000
CRDP=0x0DBD2DB0, CTDP=0x0DBD31D0, FTDB=0x0DBD31D0
Main Routing Register=0x0003FE38 BRG Conf
Register=0x0005023F
Rx Clk Routing Register=0x76543818 Tx Clk
Routing Register=0x76543910
GPP Registers:
Conf=0x430002   , Io=0x46C050   , Data=0x7F4BBFAD,
Level=0x80004
Conf0=0x430002   , Io0=0x46C050   , Data0=0x7F4BBFAD,
Level0=0x80004
0 input aborts on receiving flag sequence
0 throttles, 0 enables
```

24.2 PPP Operation

Introducing PPP

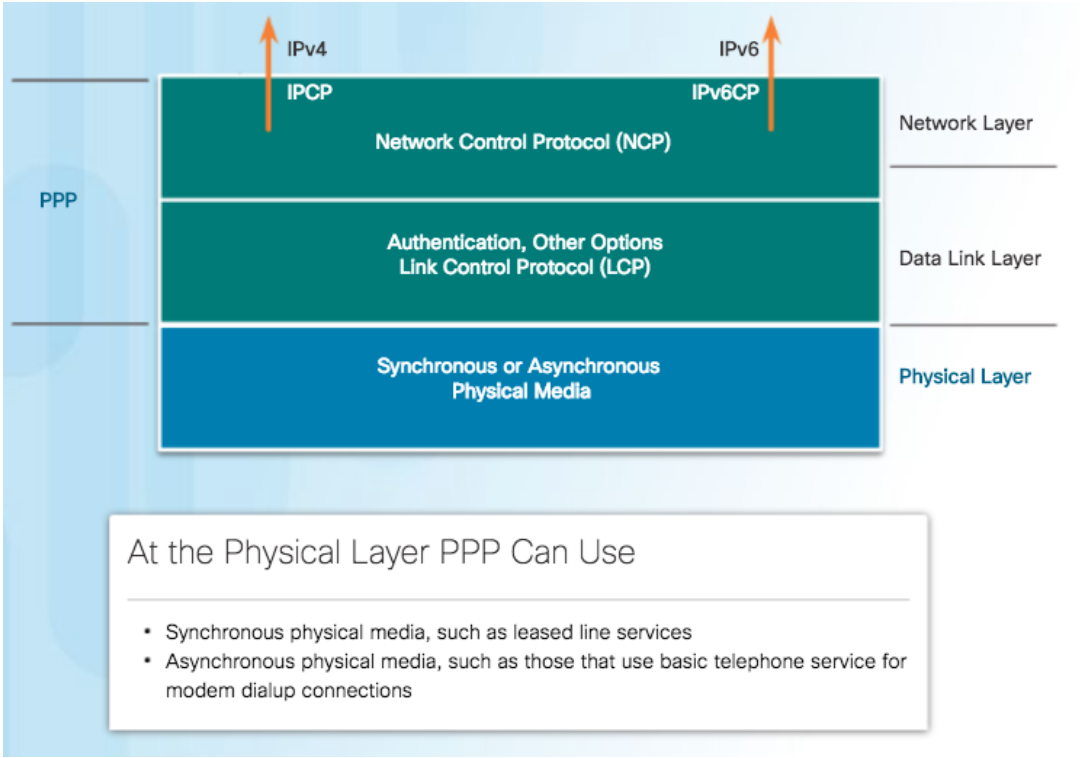


- PPP encapsulation should be used when there is a need to connect to a non-Cisco router.
- PPP encapsulates data frames for transmission over Layer 2 physical links.
- PPP establishes a direct connection using serial cables, phone lines, trunk lines, cellular telephones, specialized radio links, or fiber-optic links.
- PPP contains three main components:
  - HDLC-like framing for transporting multiprotocol packets over point-to-point links.
  - Extensible Link Control Protocol (LCP) for establishing, configuring, and testing the data-link connection.
  - Network Control Protocols (NCPs) for establishing and configuring different network layer protocols (IPv4 and IPv6 Control Protocol).

Advantages of PPP

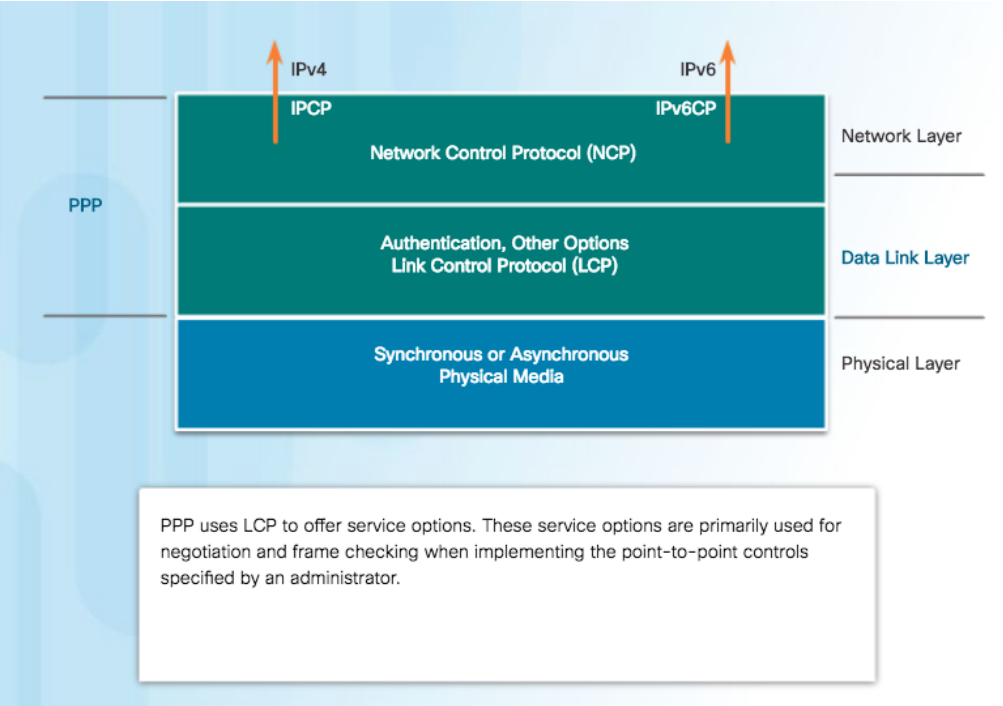
- PPP includes many features not available in HDLC:
  - The link quality management feature (LQM) monitors the quality of the link. LQM can be configured with the interface command **ppp quality** *percentage*. If the error percentage falls below the configured threshold, the link is taken down and packets are rerouted or dropped.
  - PPP supports PAP and CHAP authentication.

PPP Layered Architecture



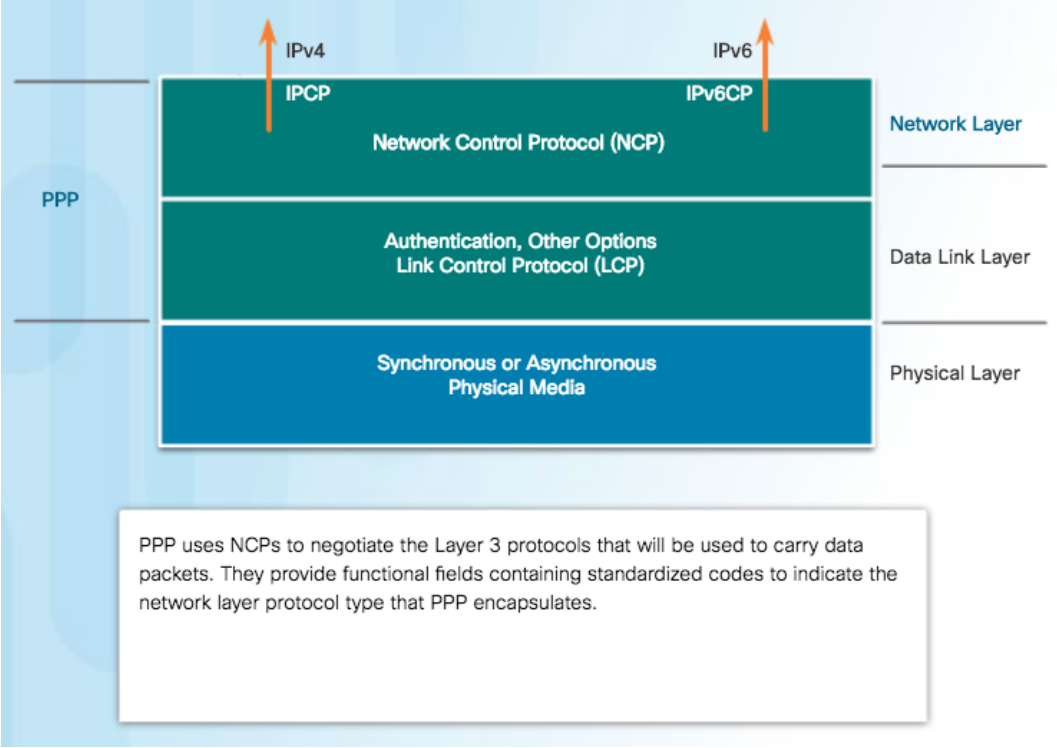
- The figure maps the layered architecture of PPP against the Open System Interconnection (OSI) model.
- PPP and OSI share the same physical layer, but PPP distributes the functions of LCP and NCP differently.
- PPP requires a full-duplex circuit, either dedicated or switched, that can operate in an asynchronous or synchronous bit-serial mode.
- Most of the work done by PPP happens at the data link and network layers, by LCP and NCPs.

PPP – Link Control Protocol (LCP)



- LCP functions within the data link layer and has a role in establishing, configuring, and testing the data-link connection.
- LCP establishes the point-to-point link.
- LCP also negotiates and sets up control options on the WAN data link, which are handled by the NCPs.
- After the link is established, PPP also uses LCP to agree automatically on encapsulation formats such as authentication, compression, and error detection.

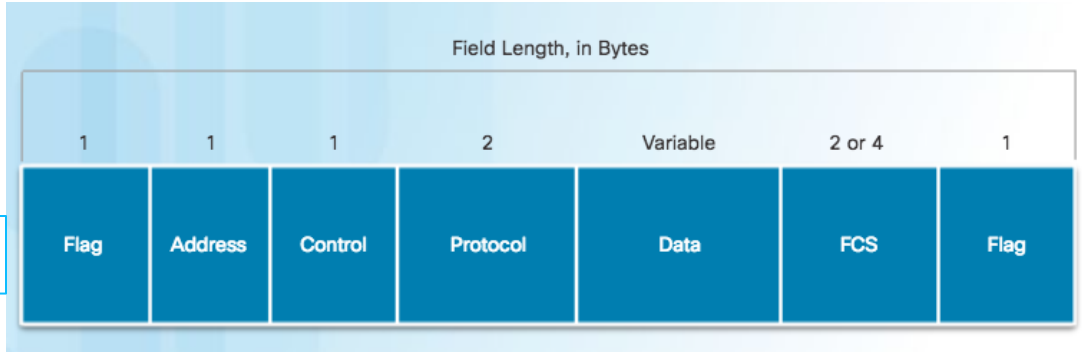
PPP – Network Control Protocol (NCP)



- PPP permits multiple network layer protocols to operate on the same communications link.
- For every network layer protocol used, PPP uses a separate NCP, as shown in the figure. IPv4 uses IP Control Protocol and IPv6 uses IPv6 Control Protocol.
- NCPs include functional fields containing standardized codes to indicate the network layer protocol that PPP encapsulates.
  - Value 8021 = IPCP
  - Value 8057 = IPv6CP

PPP Frame Structure

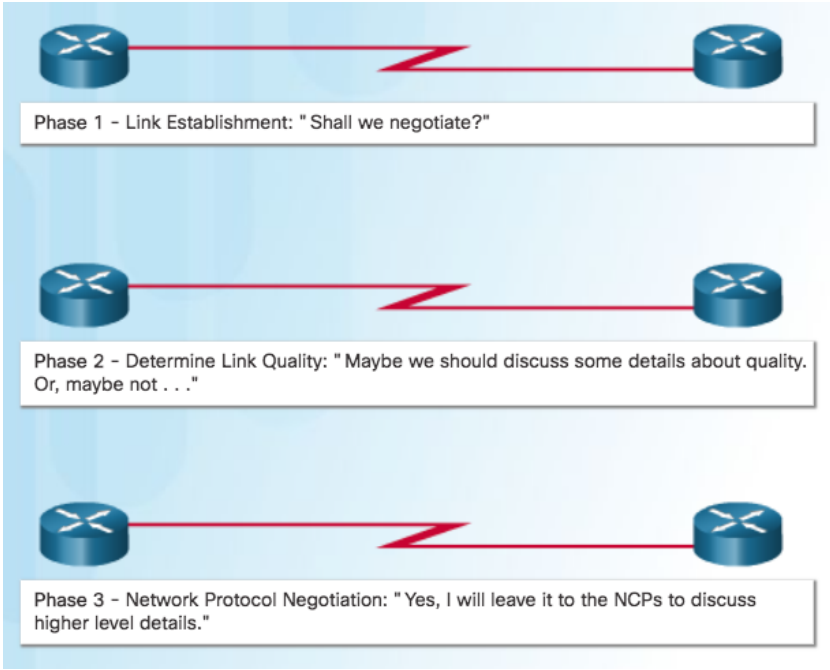
PPP Frame Fields



- **Flag** - A single byte that indicates the beginning or end of a frame. The Flag field consists of the binary sequence 01111110.
- **Address** - A single byte that contains the binary sequence 11111111, the standard broadcast address
- **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.
- **Data** - Zero or more bytes that contain the datagram for the protocol specified in the protocol field.
- **Frame Check Sequence (FCS)** – This is normally 16 bits (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

Establishing a PPP Session

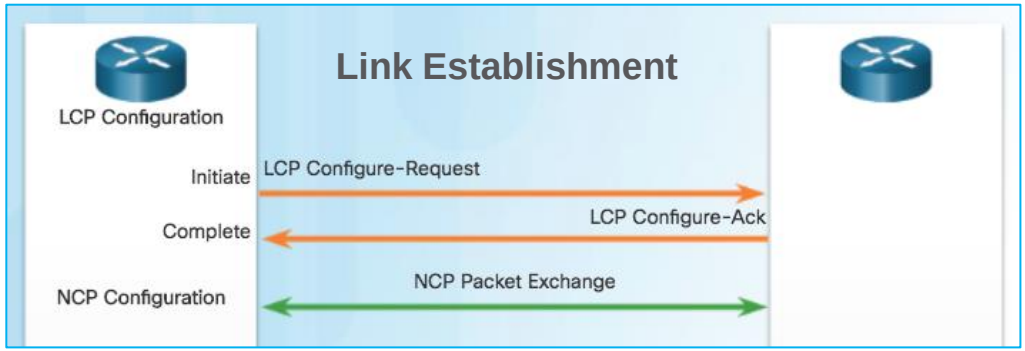
- **Phase 1: Link establishment and configuration negotiation** - Before PPP exchanges any network layer datagrams, such as IP, the LCP must first open the connection and negotiate configuration options. This phase is complete when the receiving router sends a configuration-acknowledgment frame back 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.



- **Phase 3: Network layer protocol configuration negotiation** - After the LCP has finished Phase 2, the appropriate NCP can separately configure the network layer protocols, and bring them up and take them down at any time. If the LCP closes the link, it informs the network layer protocols so that they can take appropriate action.

LCP Operation

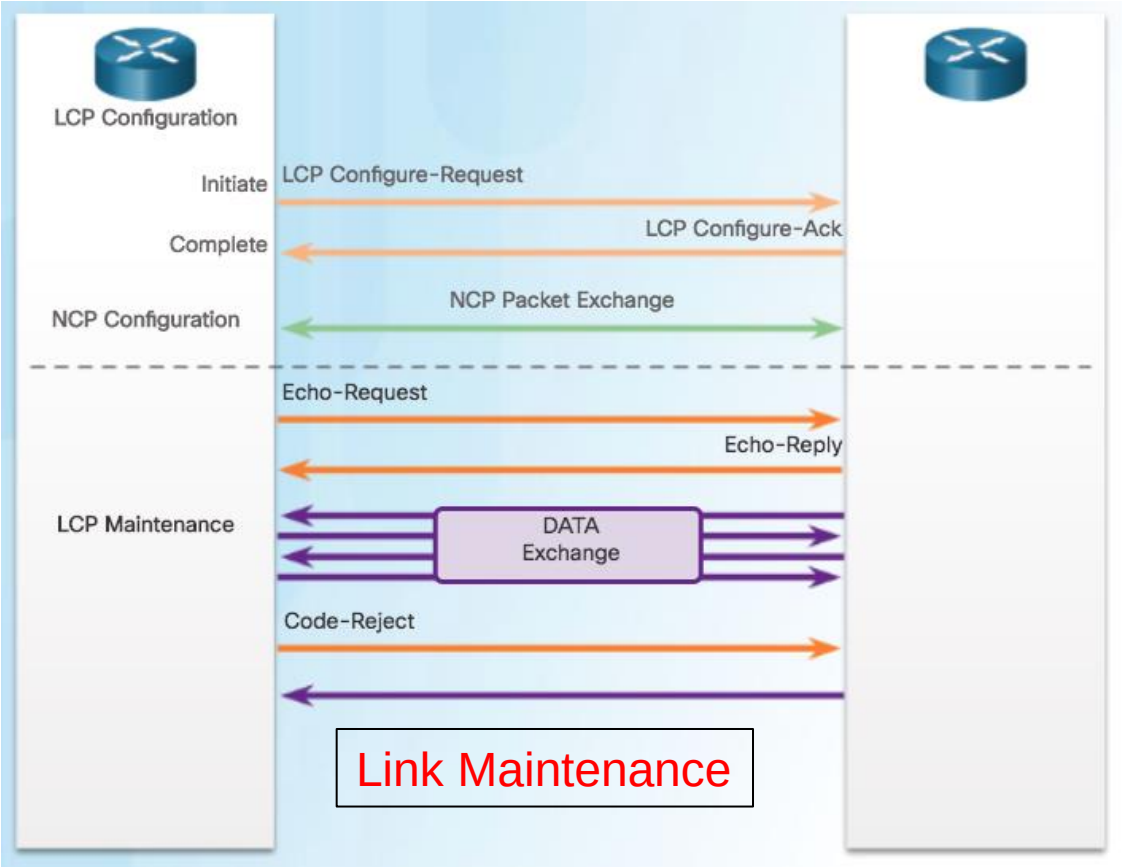
- LCP operation includes provisions for 3 classes of LCP frames:
  - Link-establishment frames
  - Link-maintenance frames
  - Link-termination frames
- During link establishment, the LCP opens the connection and negotiates the configuration parameters. The link establishment process starts with the initiating device sending a Configure-Request frame to the responder.



- Responder processes the request:
  - If the options are not acceptable or not recognized, the responder sends a Configure-Nak or Configure-Reject message.
  - 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.
- When NCP has completed all necessary configurations, including validating authentication, the line is available for data transfer. During the exchange of data, LCP transitions into link maintenance.

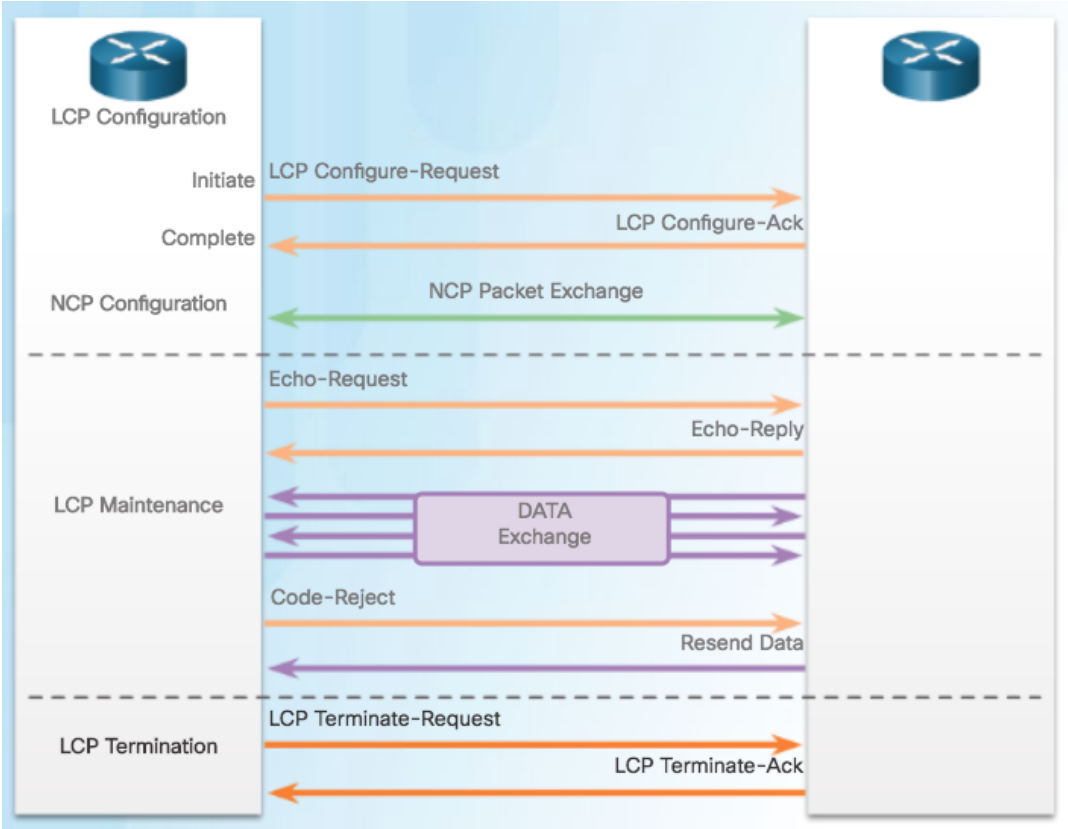
LCP Operation (Cont.)

- During link maintenance, LCP can use messages to provide feedback and test the link.
  - **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.



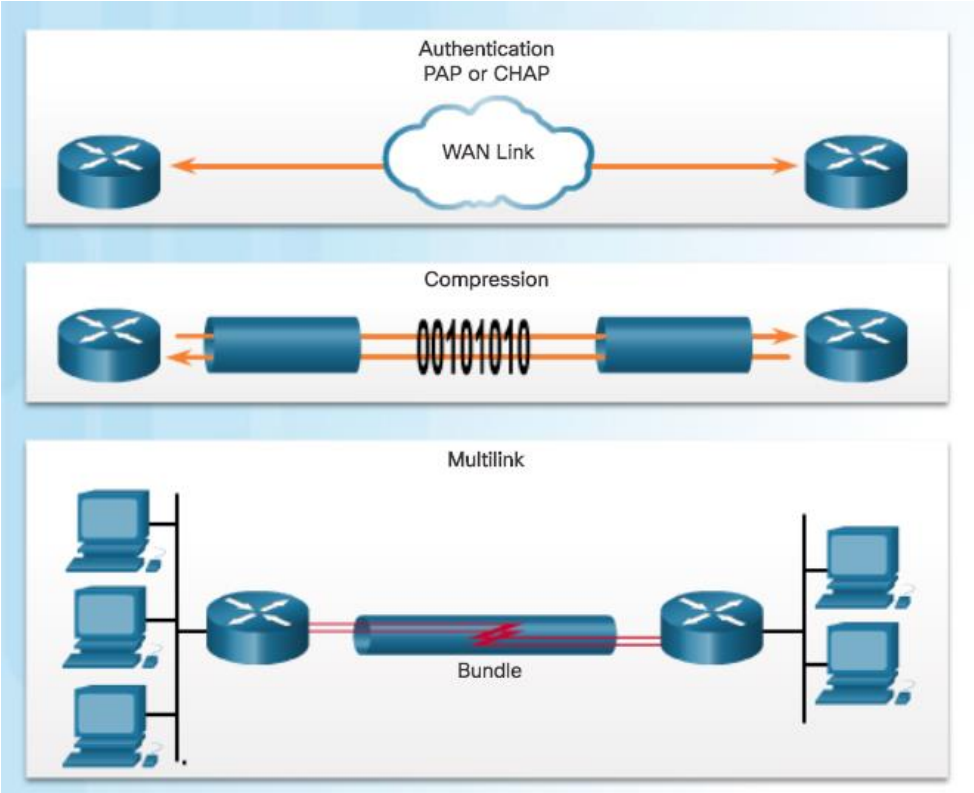
LCP Operation (Cont.)

- Link Termination
  - After the transfer of data at the network layer completes, the LCP terminates the link. NCP only terminates the network layer and NCP link. The link remains open until the LCP terminates it.
  - PPP can terminate the link at any time because of the loss of the carrier, authentication failure, link quality failure, the expiration of an idle-period timer, or the administrative closing of the link.
  - The LCP closes the link by exchanging Terminate packets.



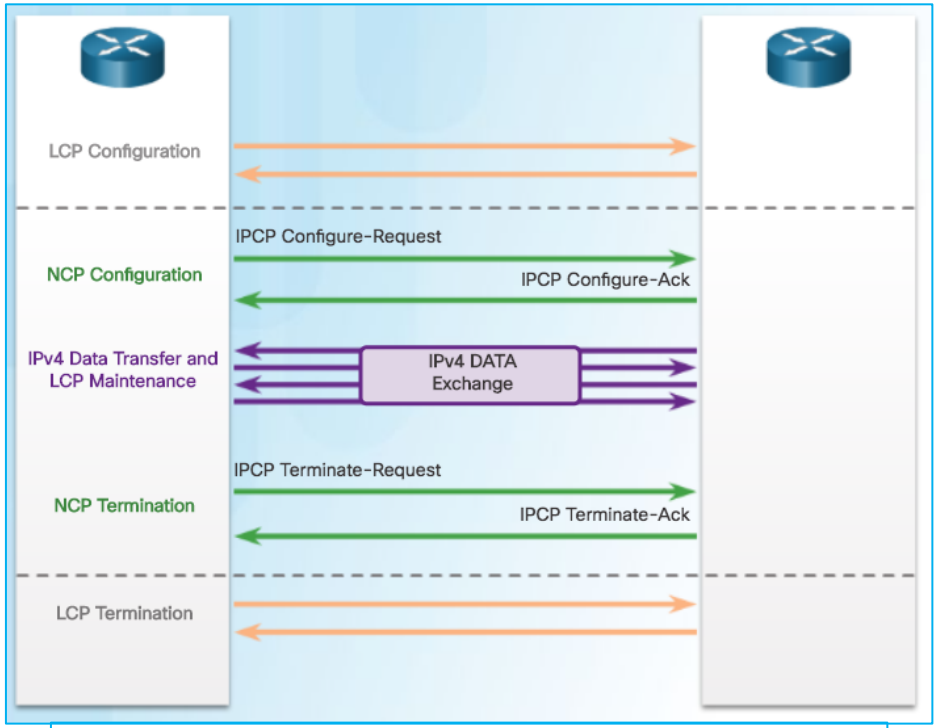
Device initiating the shutdown sends a Terminate-Request message. Other device replies with a Terminate-Ack.

PPP Configuration Options



- Authentication using either PAP or CHAP
- Compression using either Stacker or Predictor
- Multilink that combines two or more channels to increase the WAN bandwidth

NCP Explained



When data transfer is complete, NCP terminates the protocol link and LCP terminates the PPP connection.

- After LCP has established the link, the routers exchange IPCP messages, negotiating options specific to IPv4.
- 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.
- After the NCP process is complete, the link goes into the open state and LCP takes over again in a link maintenance phase.

24.3 PPP Implementation

PPP Configuration Options

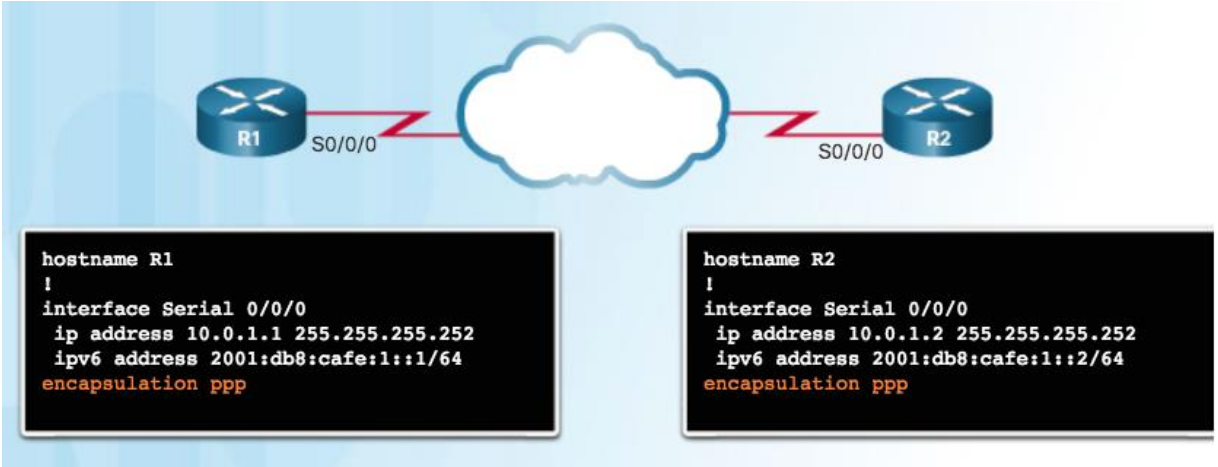
- Compression - Two compression protocols available in Cisco routers are Stacker and Predictor.
- Error detection - Identifies fault conditions. The Quality and Magic Number options help ensure a reliable, loop-free data link.
- PPP Callback - PPP callback is used to enhance security. With this LCP option, a Cisco router can act as a callback client or a callback server.

Configurable Options Field Codes

Option Name	Option Type	Option Length	Description
Authentication Protocol	3	5 or 6	This field indicates the authentication protocol, either PAP or CHAP.
Protocol Compression	7	2	A flag indicating that the PPP protocol ID be compressed to a single octet when the 2-byte protocol ID is in the range 0x00-00 to 0x00-FF.
Address and Control Field Compression	8	2	A flag indicating that the PPP Address field (always set to 0xFF) and the PPP Control field (always set to 0x03) be removed from the PPP header.
Magic Number (Error Detection)	5	6	This is a random number chosen to distinguish a peer and detect looped back lines.
Callback	13 or 0x0D	3	A 1-octet indicator of how callback is to be determined.

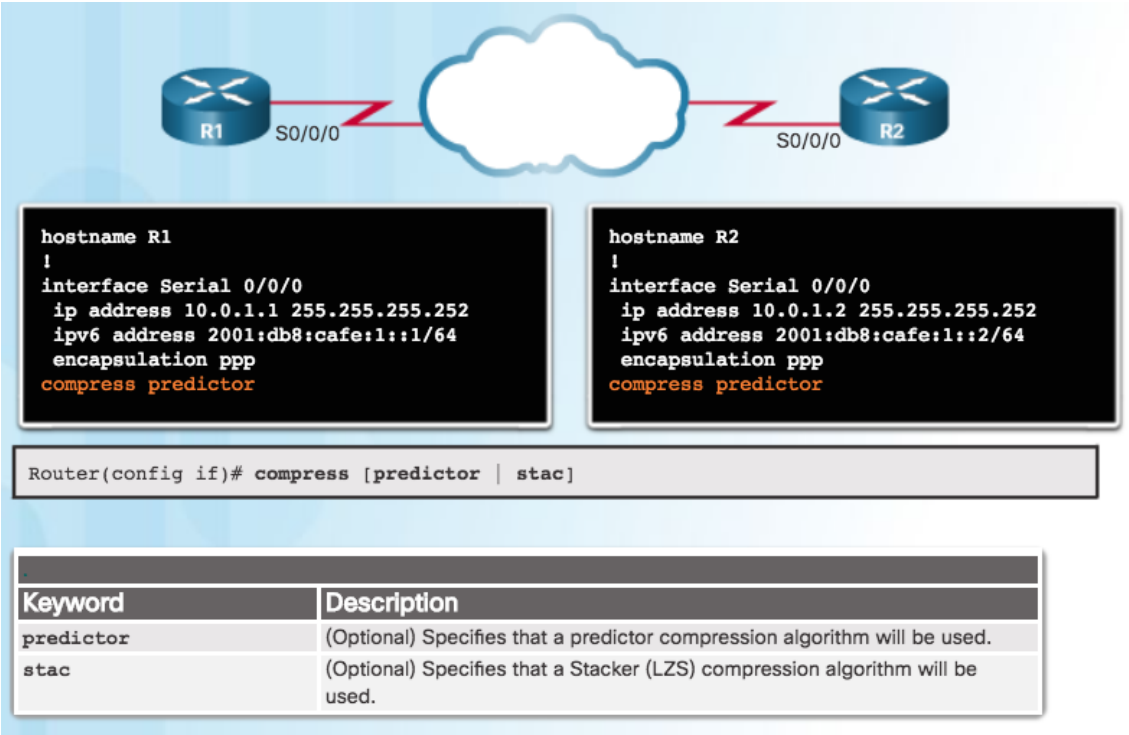
PPP Basic Configuration Command

- Remember that if PPP is not configured on a Cisco router, the default encapsulation for serial interfaces is HDLC.
- PPP is a Layer 2 encapsulation that supports various Layer 3 protocols including IPv4 and IPv6.



PPP Compression Commands

- Point-to-point software compression on serial interfaces can be configured after PPP encapsulation is enabled.
- Because this option invokes a software compression process, it can affect system performance.



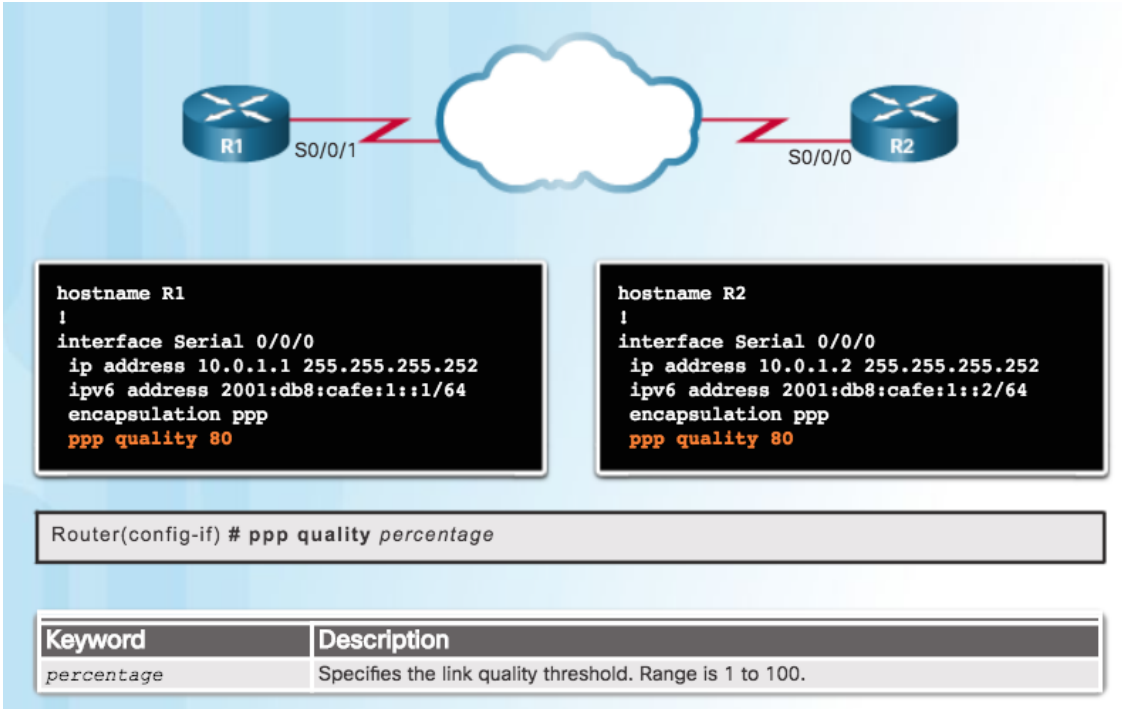
Keyword	Description
predictor	(Optional) Specifies that a predictor compression algorithm will be used.
stac	(Optional) Specifies that a Stacker (LZS) compression algorithm will be used.

predictor 算法是**RAM密集型**的。

stac 算法是**CPU密集型**的。

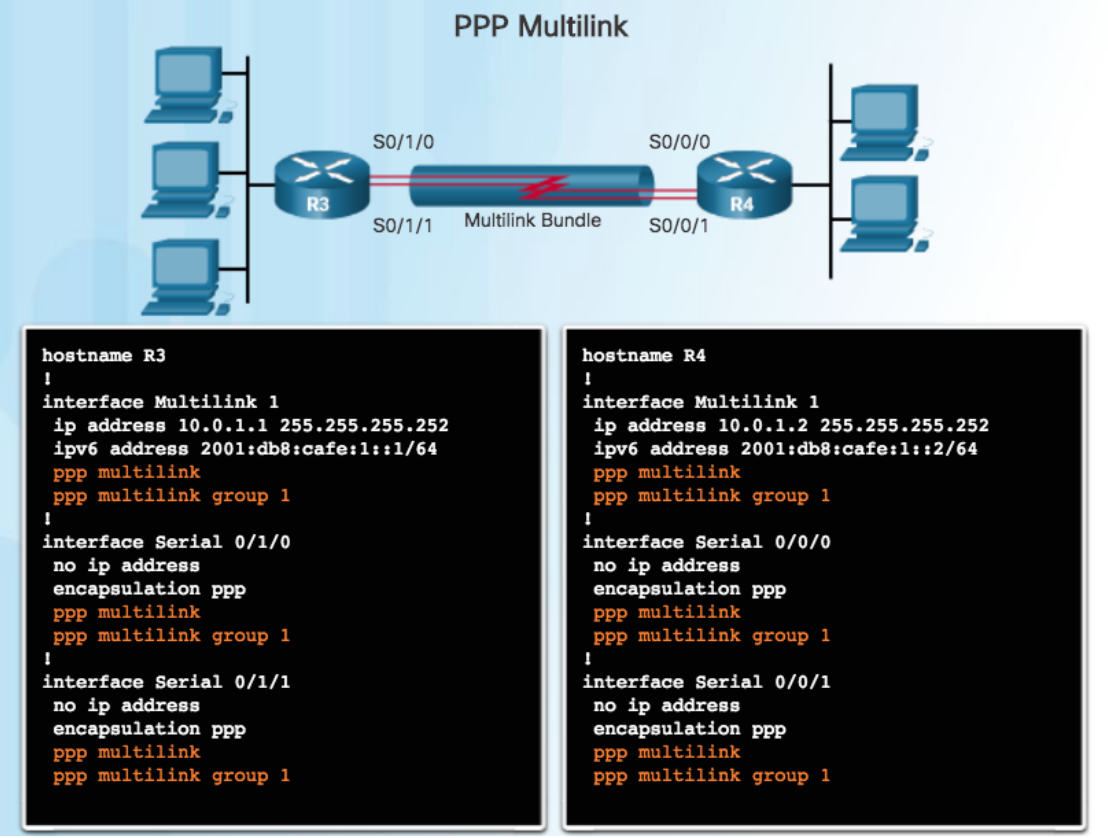
PPP Link Quality Monitoring Command

- The **ppp quality *percentage*** command ensures that the link meets the set quality requirement; otherwise, the link closes down
- Percentages are calculated for both incoming and outgoing directions
- Configuration **ppp quality 80**, shown in the figure, sets minimum quality to 80%



PPP Multilink Commands

- Multilink PPP provides a method for spreading traffic across multiple physical WAN links.
- Configuring MPPP requires two steps, as shown in the figure.
  - Step 1. Create a multilink bundle.
  - Step 2. Assign interfaces to the multilink bundle.
- To disable PPP multilink, use the **no ppp multilink** command on each of the bundled interfaces.



Verifying PPP Configuration

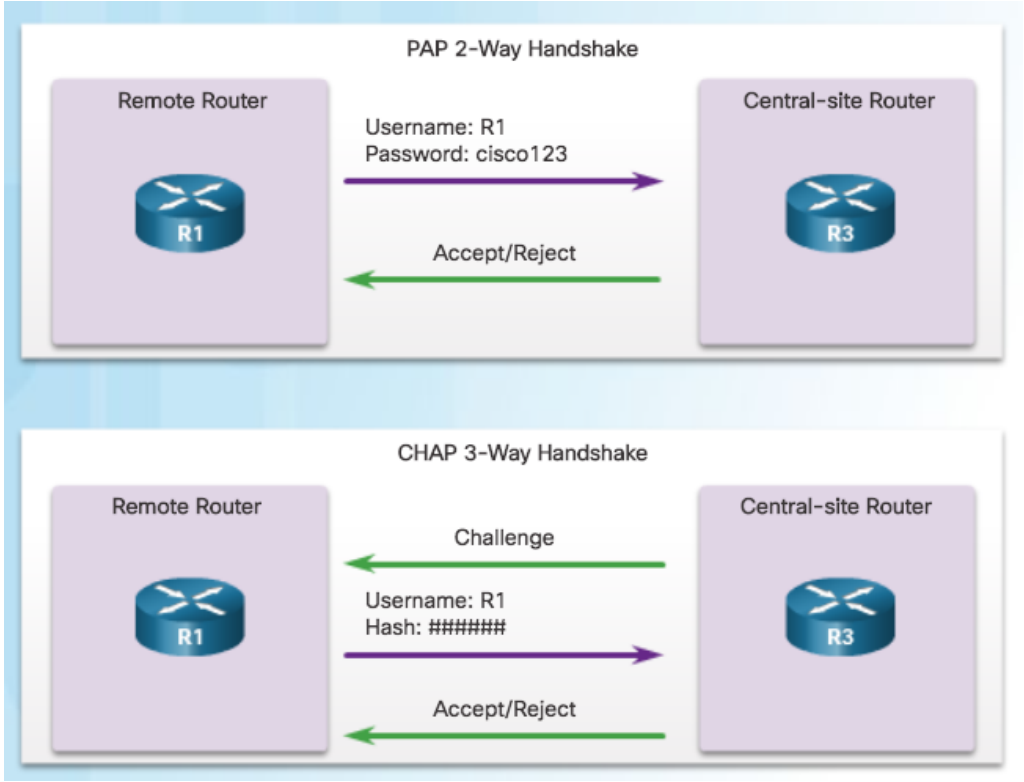
Verifying PPP Serial Encapsulation Configuration

```
R2# show interfaces serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.0.1.2/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, IPV6CP, CCP, CDPCP, loopback not set
  Keepalive set (10 sec)
  CRC checking enabled
  Last input 00:00:02, output 00:00:02, output hang never
  Last clearing of "show interface" counters 01:29:06
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output
drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1944 packets input, 67803 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     1934 packets output, 67718 bytes, 0 underruns
     0 output errors, 0 collisions, 5 interface resets
     1 unknown protocol drops
```

Command	Description
`show interfaces`	Displays statistics for all interfaces configured on the router.
`show interfaces serial`	Displays information about a serial interface.
`show ppp multilink`	Displays information about a PPP multilink interface.

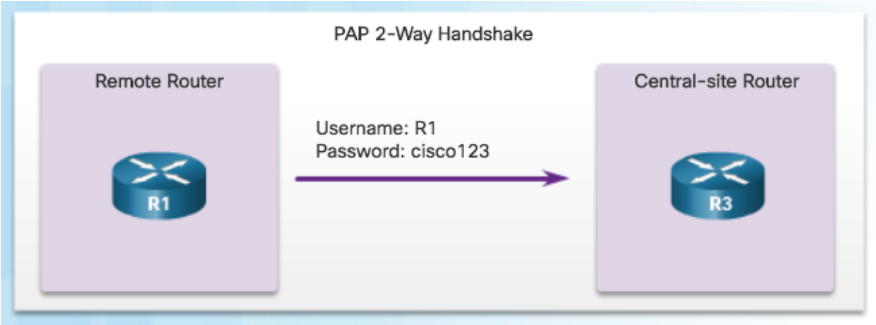
```
R3# show ppp multilink

Multilink1
  Bundle name: R4
  Remote Endpoint Discriminator: [1] R4
  Local Endpoint Discriminator: [1] R3
  Bundle up for 00:01:20, total bandwidth 3088, load 1/255
  Receive buffer limit 24000 bytes, frag timeout 1000 ms
    0/0 fragments/bytes in reassembly list
    0 lost fragments, 0 reordered
    0/0 discarded fragments/bytes, 0 lost received
    0x2 received sequence, 0x2 sent sequence
  Member links: 2 active, 0 inactive (max 255, min not set)
    Se0/1/1, since 00:01:20
    Se0/1/0, since 00:01:06
No inactive multilink interfaces
R3#
```

PPP Authentication Protocols



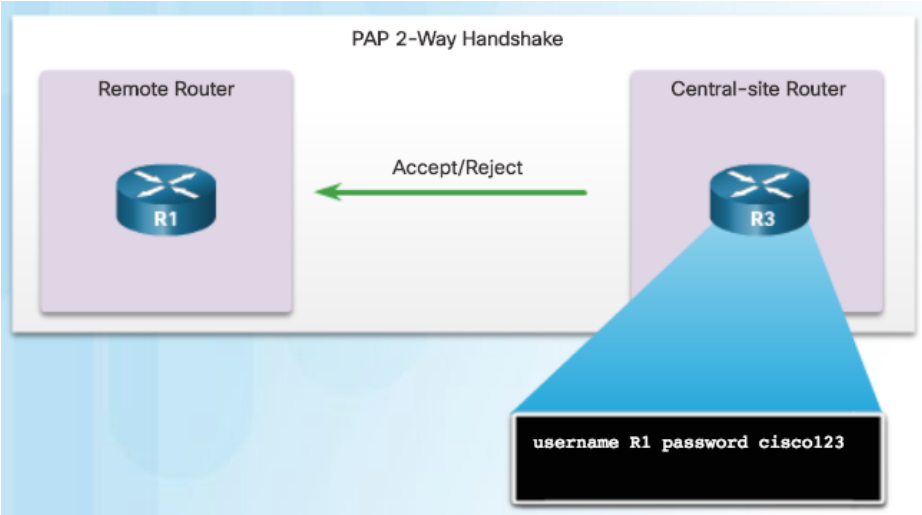
- PAP is a very basic two-way process with no encryption. The username and password are sent in plaintext. If it is accepted, the connection is allowed.
- CHAP is more secure than PAP. It involves a three-way exchange of a shared secret.
- The authentication phase of a PPP session is optional. If used, the peer is authenticated after LCP establishes the link and chooses the authentication protocol.
- Authentication takes place before the network layer protocol configuration phase begins.

Password Authentication Protocol (PAP)



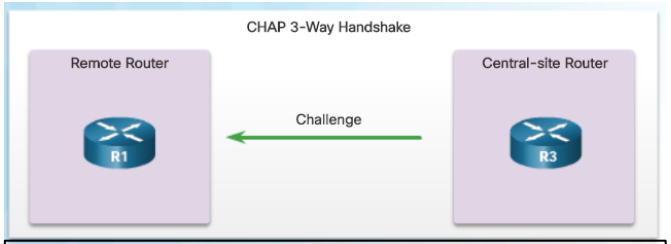
Initiating PAP – R1 Sends its PAP username and password to R3.

Note: PAP is not a strong authentication protocol. Using PAP, passwords are sent across the link in plaintext and there is no protection from playback or repeated trial-and-error attacks.

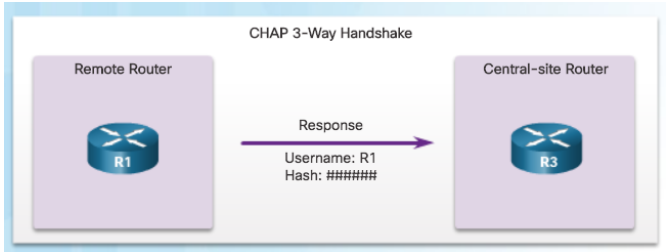


Completing PAP – R3 Evaluates R1's username and password against its local database. If it matches, it accepts the connection. If not, it rejects the connection.

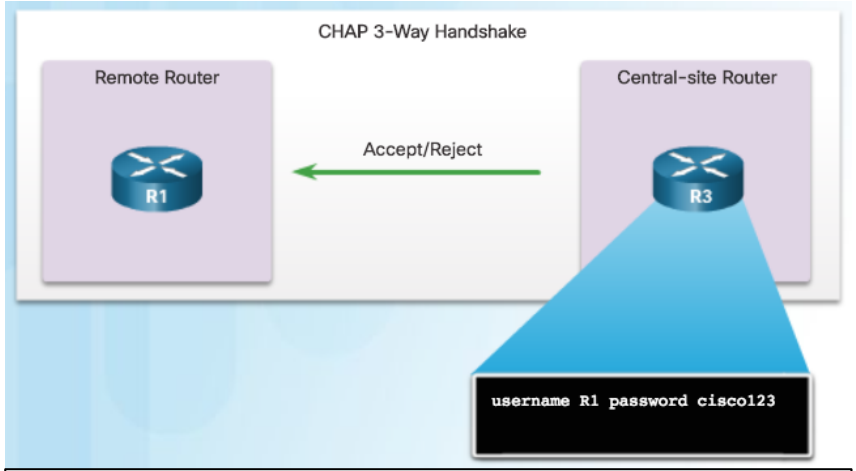
Challenge Handshake Authentication Protocol (CHAP)



#1 R3 initiates the 3-way handshake and sends a challenge message to R1.



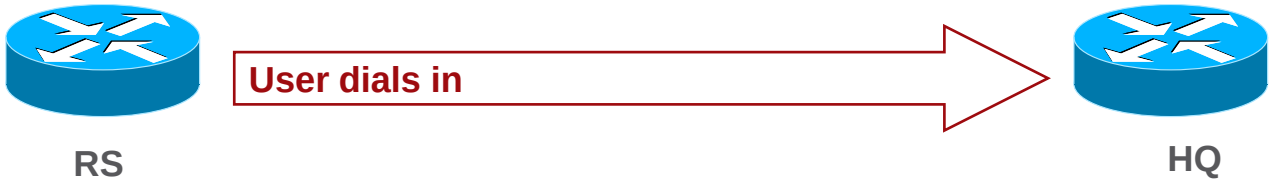
#2 The remote node responds with a value that is calculated using a one-way hash function.



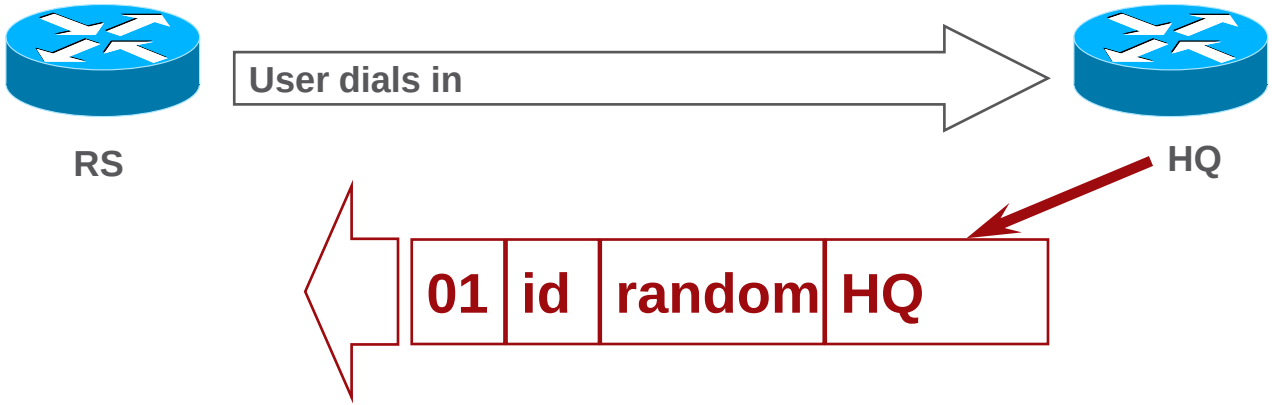
#3 The local router checks the response against its own calculation of the expected hash value. If the values match, the initiating node acknowledges the authentication.

Note: CHAP conducts periodic challenges to make sure that the remote node still has a valid password value.

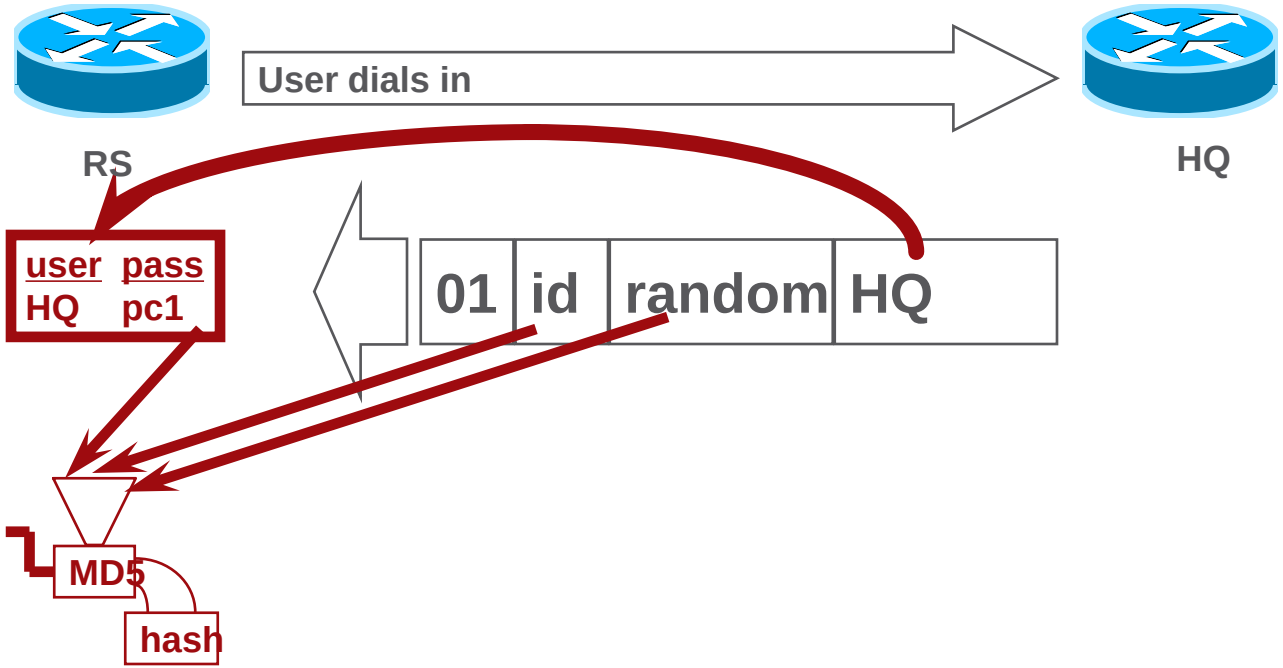
CHAP in Action—Call



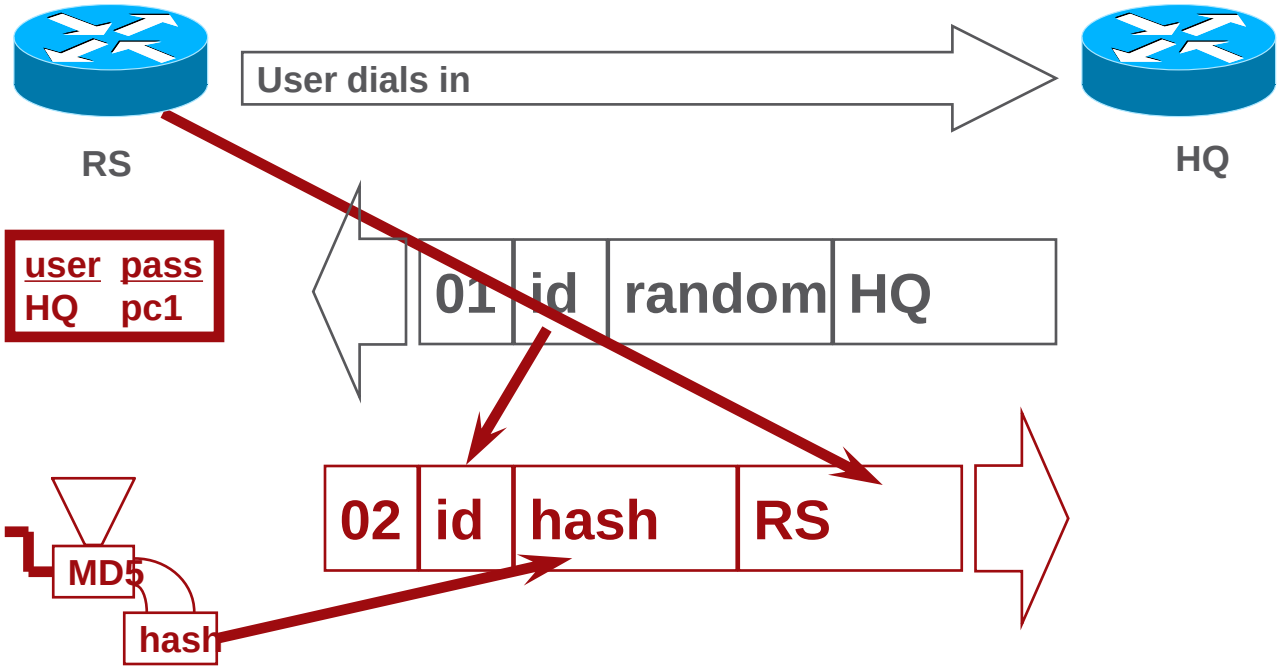
CHAP in Action—Challenge



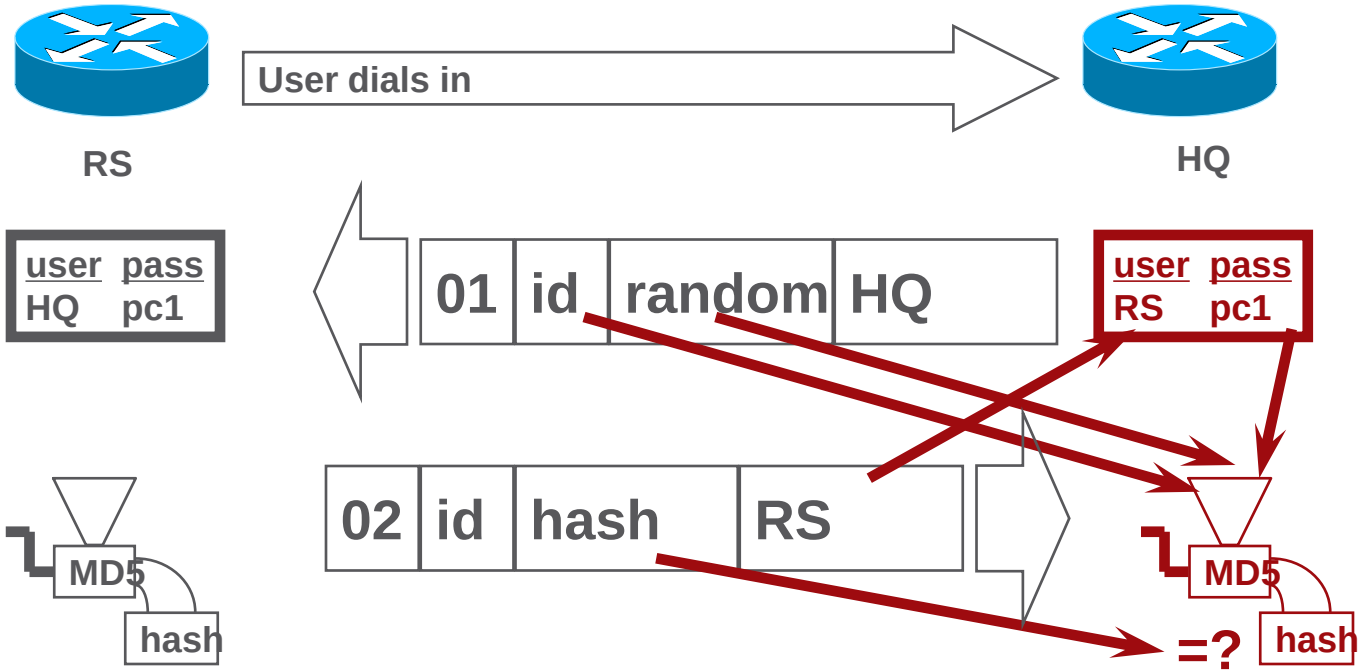
CHAP in Action—Response



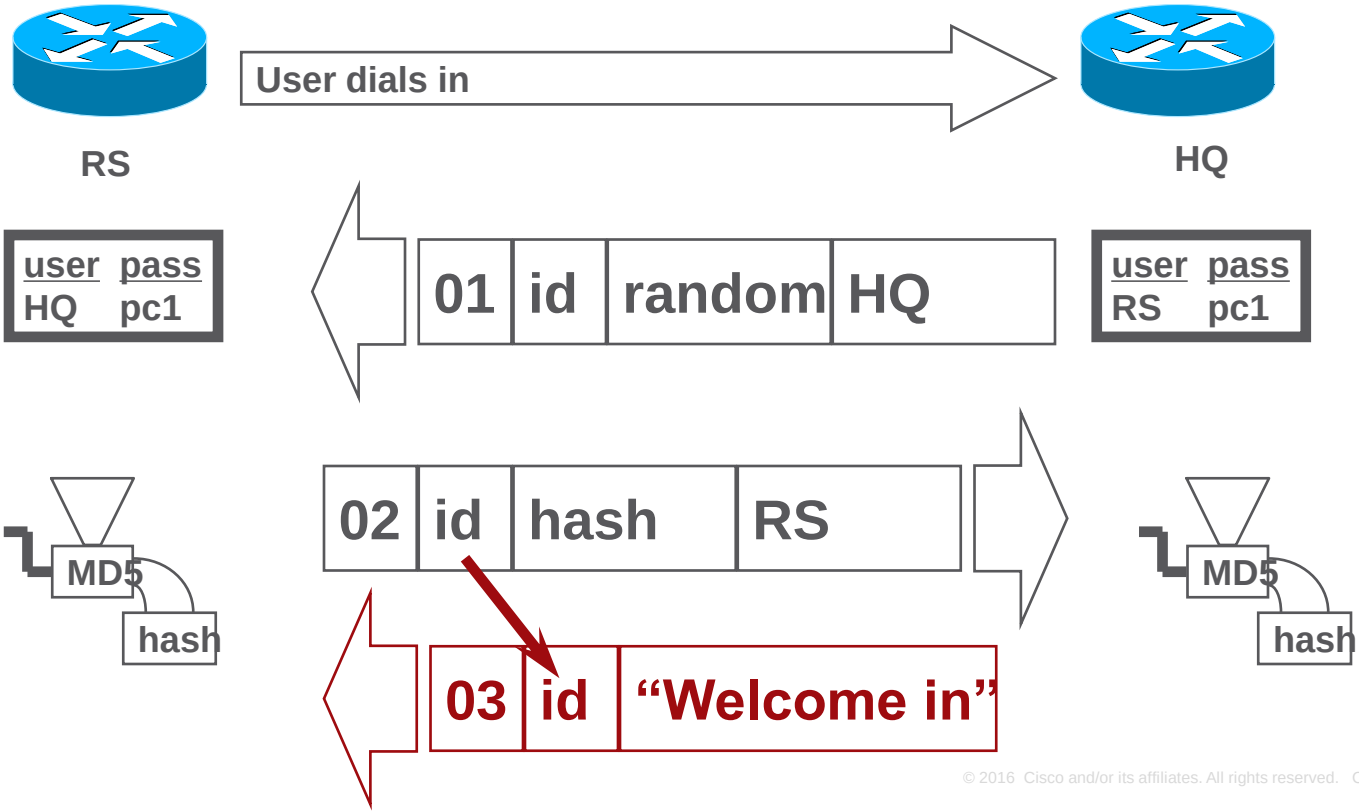
CHAP in Action—Response



CHAP in Action—Verification



CHAP in Action—Result



PPP Authentication Command

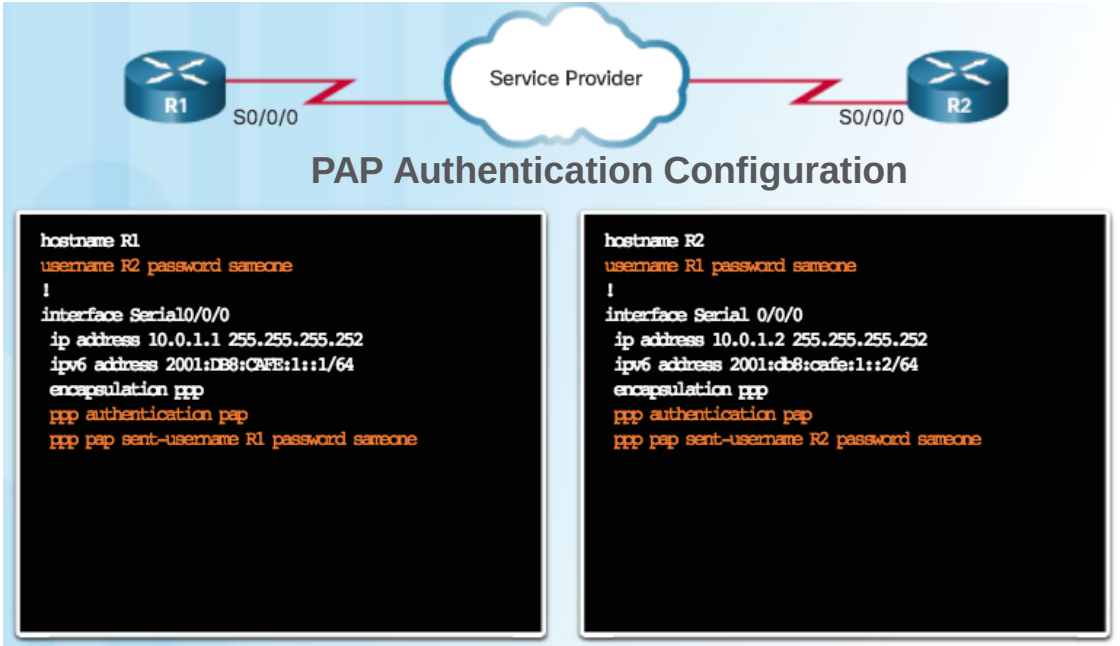
```
ppp authentication {chap | chap pap | pap chap | pap}
```

The **ppp authentication** Command

chap	Enables CHAP on a serial interface.
pap	Enables PAP on a serial interface.
chap pap	Enables both CHAP and PAP, and performs CHAP authentication before PAP.
pap chap	Enables both CHAP and PAP, and performs PAP authentication before CHAP.

- To specify the order in which the CHAP or PAP protocols are requested on the interface, use the **ppp authentication** interface configuration command. Use the **no** form of the command to disable this authentication.
- PAP, CHAP, or both can be enabled. If both methods are enabled, the first method specified is requested during link negotiation. If the peer suggests using the second method or simply refuses the first method, the second method should be tried.

Configuring PPP with Authentication



PAP: Hostname on one router must match the username the other router has configured for PPP. The passwords must also match.

Configuring PPP Authentication (cont.)

- Configuring CHAP Authentication Example


```
  hostname left
* username right password 123
  int serial 0
   encapsulation ppp
*  ppp authentication CHAP
```

```
  hostname right
* username left password 123
  int serial 0
   encapsulation ppp
*  ppp authentication CHAP
```

- **Two-way CHAP**

Configuring CHAP Example


```
   hostname left
*  username ABC password 123
   int serial 0
    encapsulation ppp
*   ppp authentication CHAP
```

```
   hostname right
   int serial 0
    encapsulation ppp
*   ppp chap hostname ABC
*   ppp chap password 123
```

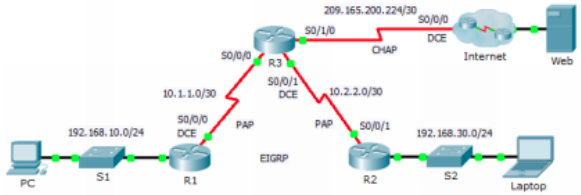
- **One-way CHAP**

Packet Tracer – Configuring PAP and CHAP Authentication

Cisco Networking Academy® Mind Wide Open™

Packet Tracer – Configuring PAP and CHAP Authentication

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.10.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
R2	G0/0	192.168.30.1	255.255.255.0	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
R3	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
	S0/1/0	209.165.200.225	255.255.255.252	N/A
ISP	S0/0/0	209.165.200.226	255.255.255.252	N/A
	G0/0	209.165.200.1	255.255.255.252	N/A
Web	NIC	209.165.200.2	255.255.255.252	209.165.200.1
PC	NIC	192.168.10.10	255.255.255.0	192.168.10.1
Laptop	NIC	192.168.30.10	255.255.255.0	192.168.30.1

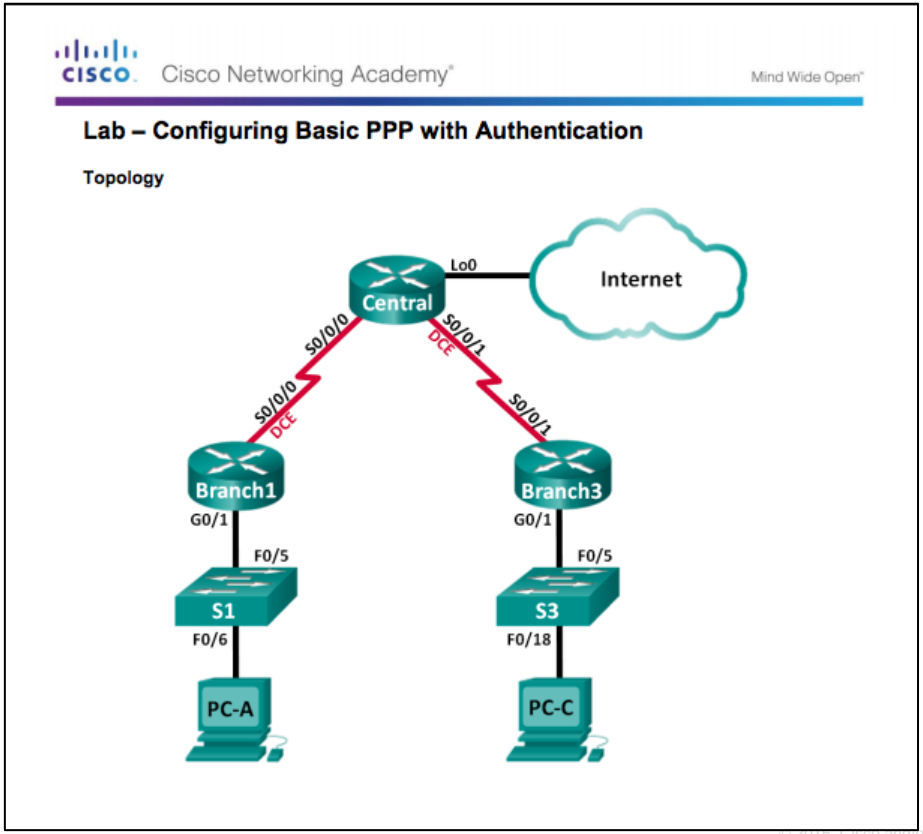
Objectives

Part 1: Review Routing Configurations

Part 2: Configure PPP as the Encapsulation Method

Part 3: Configure PPP Authentication

Lab – Configuring Basic PPP with Authentication



24.4 Troubleshoot WAN Connectivity

Verifying PPP

```
Router#show interfaces serial0/0
Serial0/0 is up, line protocol is up
  Hardware is HD64570
  Internet address is 10.140.1.2/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
rely 255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive
set (10 sec)
  LCP Open                          <-- LCP
  Open: IPCP, CDPCP                 <-- NCP
  Last input 00:00:05, output 00:00:05, output
hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0
drops
  5 minute input rate 0 bits/sec, 0 packets/sec
```

Troubleshooting PPP Serial Encapsulation

debug ppp Command Parameters

```
debug ppp {packet | negotiation | error | authentication | compression | cbcp}
```

The `ppp authentication` Command

Parameter	Usage
`packet`	Displays PPP packets being sent and received. (This command displays low-level packet dumps.)
`negotiation`	Displays PPP packets transmitted during PPP startup, where PPP options are negotiated.
`error`	Displays protocol errors and error statistics associated with PPP connection negotiation and operation.
`authentication`	Displays authentication protocol messages, including Challenge Authentication Protocol (CHAP) packet exchanges and Password Authentication Protocol (PAP) exchanges.
`compression`	Displays information specific to the exchange of PPP connections using MPPC. This command is useful for obtaining incorrect packet sequence number information where MPPC compression is enabled.
`cbcp`	Displays protocol errors and statistics associated with PPP connection negotiations using Microsoft Callback Control (MSCB) protocol.

- **debug** command must not be used as a monitoring tool
- meant to be used for a short period of time for troubleshooting
- can consume a significant amount of resources

Troubleshoot PPP

Debug PPP

Output of debug ppp packet Command


```
R1# debug ppp packet
PPP packet display debugging is on
R1#
*Apr  1 16:15:17.471: Se0/0/0 LQM: O state Open magic 0x1EFC37C3
len 48
*Apr  1 16:15:17.471: Se0/0/0 LQM:    LastOutLQRs 70
LastOutPackets/Octets 194/9735
*Apr  1 16:15:17.471: Se0/0/0 LQM:    PeerInLQRs 70
PeerInPackets/Discards/Errors/Octets 0/0/0/0
*Apr  1 16:15:17.471: Se0/0/0 LQM:    PeerOutLQRs 71
PeerOutPackets/Octets 197/9839
*Apr  1 16:15:17.487: Se0/0/0 PPP: I pkt type 0xC025,
datagramsize 52 link[ppp]
*Apr  1 16:15:17.487: Se0/0/0 LQM: I state Open magic 0xFE83D624
len 48
*Apr  1 16:15:17.487: Se0/0/0 LQM:    LastOutLQRs 71
LastOutPackets/Octets 197/9839
*Apr  1 16:15:17.487: Se0/0/0 LQM:    PeerInLQRs 71
PeerInPackets/Discards/Errors/Octets 0/0/0/0
*Apr  1 16:15:17.487: Se0/0/0 LQM:    PeerOutLQRs 71
PeerOutPackets/Octets 196/9809
*Apr  1 16:15:17.535: Se0/0/0 LCP: O ECHOREQ [Open] id 36 len 12
magic 0x1EFC37C3
```

Output of debug ppp negotiation Command


```
R1# debug ppp negotiation
PPP protocol negotiation debugging is on
R1#
*Apr  1 18:42:29.831: %LINK-3-UPDOWN: Interface Serial0/0/0,
changed state to up
*Apr  1 18:42:29.831: Se0/0/0 PPP: Sending cstate UP notification
*Apr  1 18:42:29.831: Se0/0/0 PPP: Processing CstateUp message
*Apr  1 18:42:29.835: PPP: Alloc Context [66A27824]
*Apr  1 18:42:29.835: ppp2 PPP: Phase is ESTABLISHING
*Apr  1 18:42:29.835: Se0/0/0 PPP: Using default call direction
*Apr  1 18:42:29.835: Se0/0/0 PPP: Treating connection as a
dedicated line
*Apr  1 18:42:29.835: Se0/0/0 PPP: Session handle[4000002]
Session id[2]
*Apr  1 18:42:29.835: Se0/0/0 LCP: Event[OPEN]
State[Initial to Starting]
*Apr  1 18:42:29.835: Se0/0/0 LCP: O CONFREQ [Starting]
id 1 len 23
*Apr  1 18:42:29.835: Se0/0/0 LCP:    AuthProto
CHAP (0x0305C22305)
*Apr  1 18:42:29.835: Se0/0/0 LCP:    QualityType 0xC025
period 1000 (0x0408C025000003E8)
*Apr  1 18:42:29.835: Se0/0/0 LCP:    MagicNumber 0x1F887DD3
```

```
R1# debug ppp error
PPP Serial3(i): rlqr receive failure. successes = 15
PPP: myrcvdiffp = 159 peerxmitdiffp = 41091
PPP: myrcvdiffo = 2183 peerxmitdiffo = 1714439
PPP: threshold = 25
PPP Serial2(i): rlqr transmit failure. successes = 15
PPP: myxmitdiffp = 41091 peerrcvdiffp = 159
PPP: myxmitdiffo = 1714439 peerrcvdiffo = 2183
PPP: l->OutLQRs = 1 LastOutLQRs = 1
PPP: threshold = 25
PPP Serial3(i): lqr_protrej() Stop sending LQRs.
PPP Serial3(i): The link appears to be looped back.
```

Troubleshooting a PPP Configuration with Authentication

```
R2# debug ppp authentication

Serial0: Unable to authenticate. No name received from peer
Serial0: Unable to validate CHAP response. USERNAME pioneer not found.
Serial0: Unable to validate CHAP response. No password defined for USERNAME pioneer
Serial0: Failed CHAP authentication with remote.
Remote message is Unknown name
Serial0: remote passed CHAP authentication.
Serial0: Passed CHAP authentication with remote.
Serial0: CHAP input code = 4 id = 3 len = 48
```

In the last line, the code 4 means that a failure has occurred. Other code values are as follows:

1 – Challenge 2 – Response 3 – Success 4 - Failure

id - 3 is the ID number per LCP packet format len - 48 is the packet length without the header

24.5 Summary

Chapter 2: Point-to-Point Connections

- Configure HDLC encapsulation.
- Explain how PPP operates across a point-to-point serial link.
- Configure PPP encapsulation.
- Troubleshoot PPP


CISCO