Chapter 3: Point-to-Point Connections

Connecting Networks

Cisco | Networking Academy®
Mind Wide Open™

Chapter 3

3.1 Serial Point-to-Point Overview

3.2 PPP Operation

3.3 Configuring PPP

3.4 Troubleshooting WAN Connectivity

3.5 Summary

Chapter 3: Objectives

In this chapter, you will be able to:

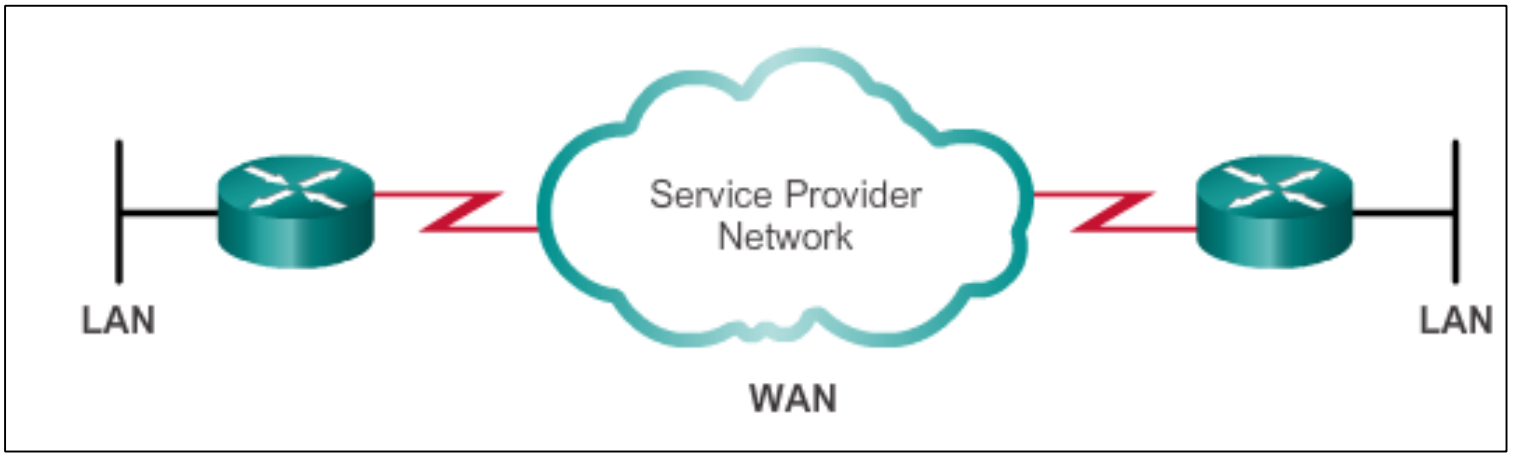
- Explain the fundamentals of point-to-point serial communication across a WAN.
- Configure HDLC encapsulation on a point-to-point serial link.
- Describe the benefits of using PPP over HDLC in a WAN.
- Describe the PPP layered architecture and the functions of LCP and NCP.
- Explain how a PPP session is established.
- Configure PPP encapsulation on a point-to-point serial link.
- Configure PPP authentication protocols.
- Use show and debug commands to troubleshoot PPP.

3.1 Serial Point-to-Point Overview

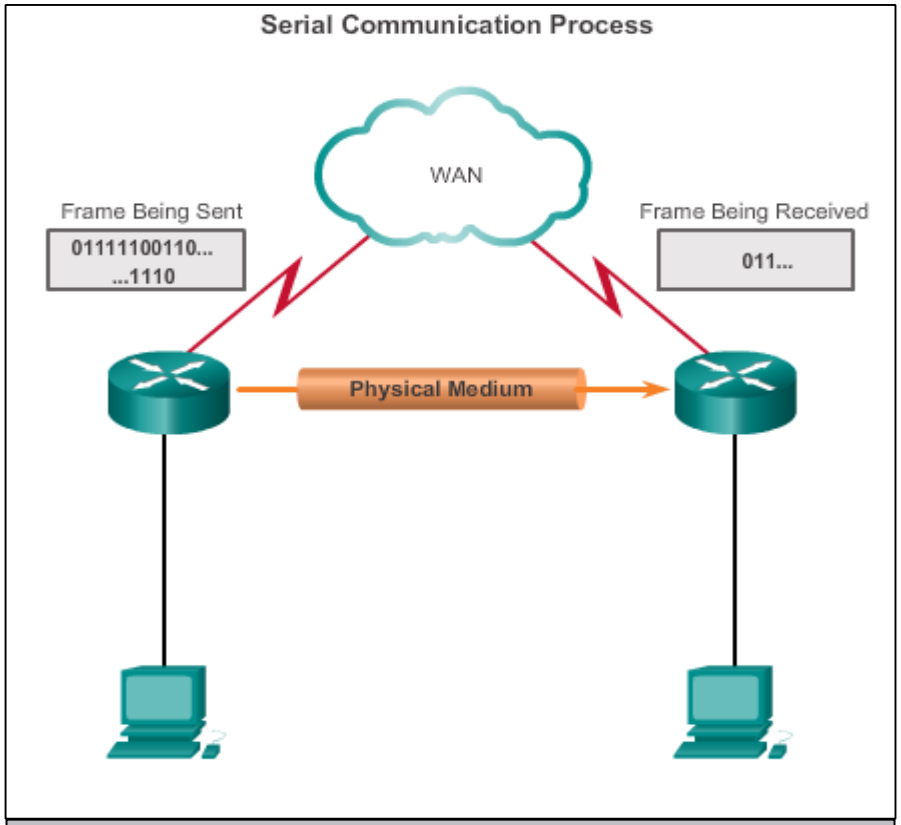
Cisco | Networking Academy®
Mind Wide Open™

Serial and Parallel Ports

- Point-to-point connections are used to connect LANs to service provider WANs.
  - Also referred to as a serial connection or leased-line connection.
- Communications across a serial connection is a method of data transmissions in which the bits are transmitted sequentially over a single channel.
- In parallel communications, bits can be transmitted simultaneously over multiple wires.



Serial Communication

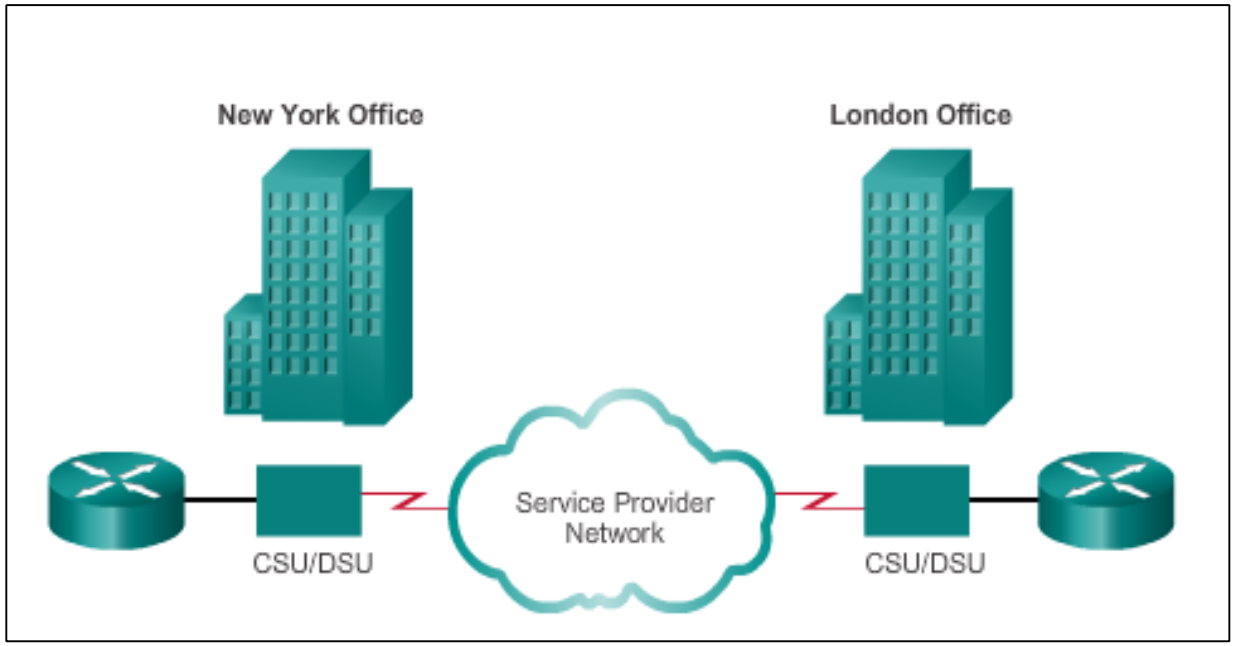


Three serial communication standards for LAN-to-WAN connections: RS-232, V.35, HSSI

- On the WAN link, data is encapsulated by the protocol used by the sending router.
- Encapsulated frame is sent on a physical medium to the WAN.
- Receiving router uses the same communications protocol to de-encapsulate the frame when it arrives.

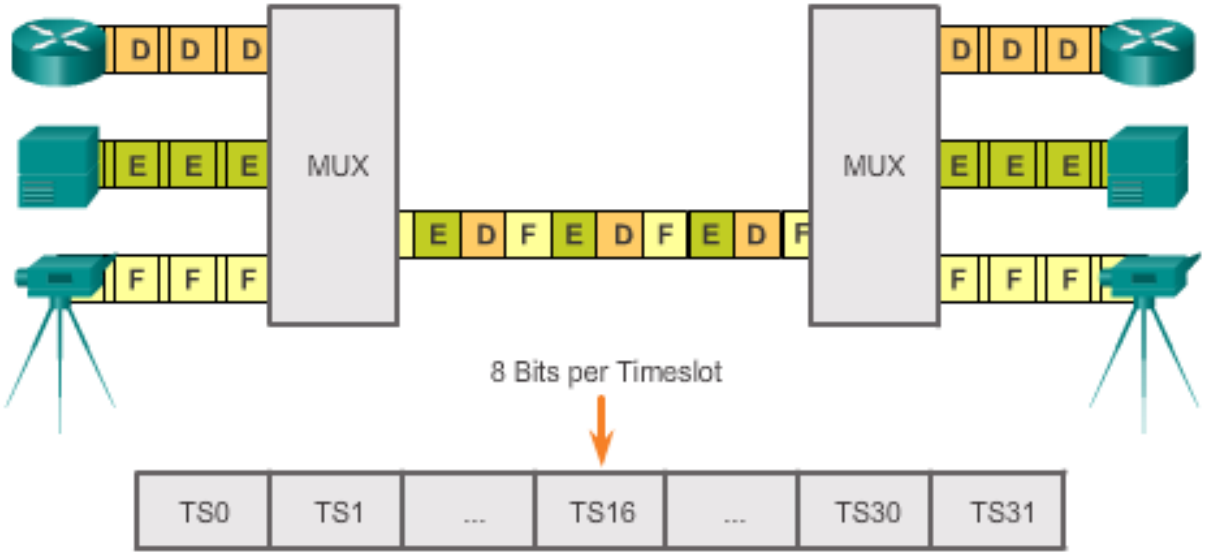
Point-to-Point Communication Links

- Point-to-point links can connect two geographically distant sites.
- Carrier dedicates specific resources for a line leased by the customer (leased-line).
- Point-to-point links are usually more expensive than shared services.



Time-Division Multiplexing

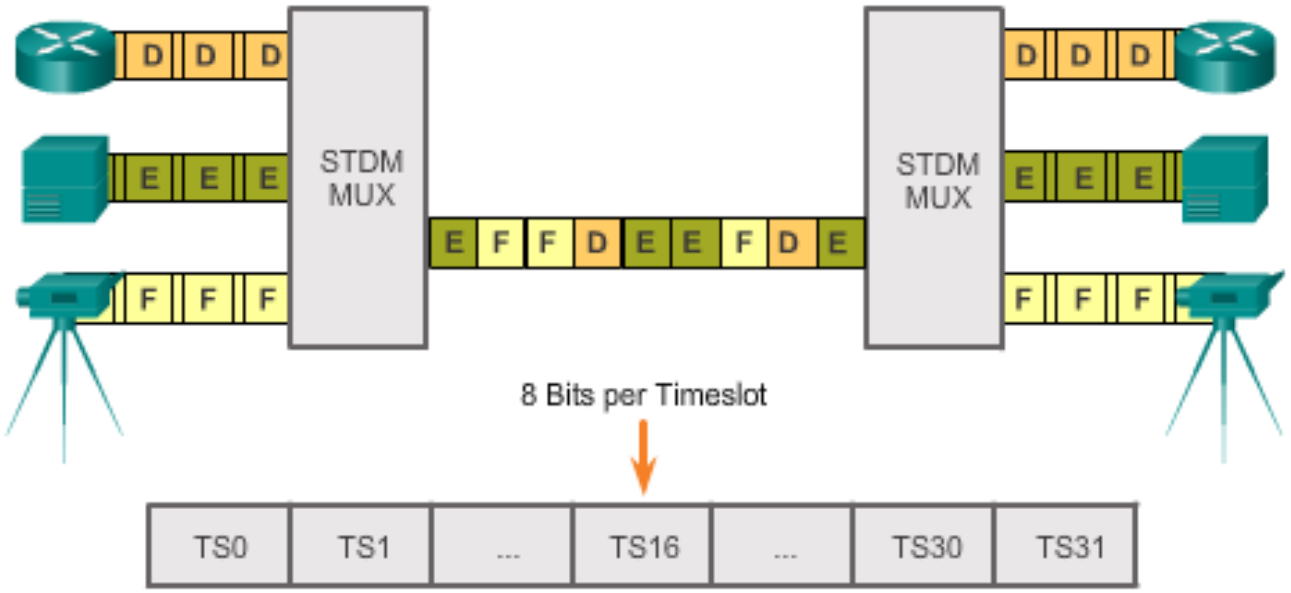
Multiplexing – A scheme that allows multiple logical signals to share a single physical channel.



- TDM shares available transmission time on a medium by assigning timeslots to users.
- The MUX accepts input from attached devices in an alternating sequence (round-robin) and transmits the data in a recurrent pattern.
- T1/E1 and ISDN telephone lines are common examples of synchronous TDM.

Statistical Time-Division Multiplexing

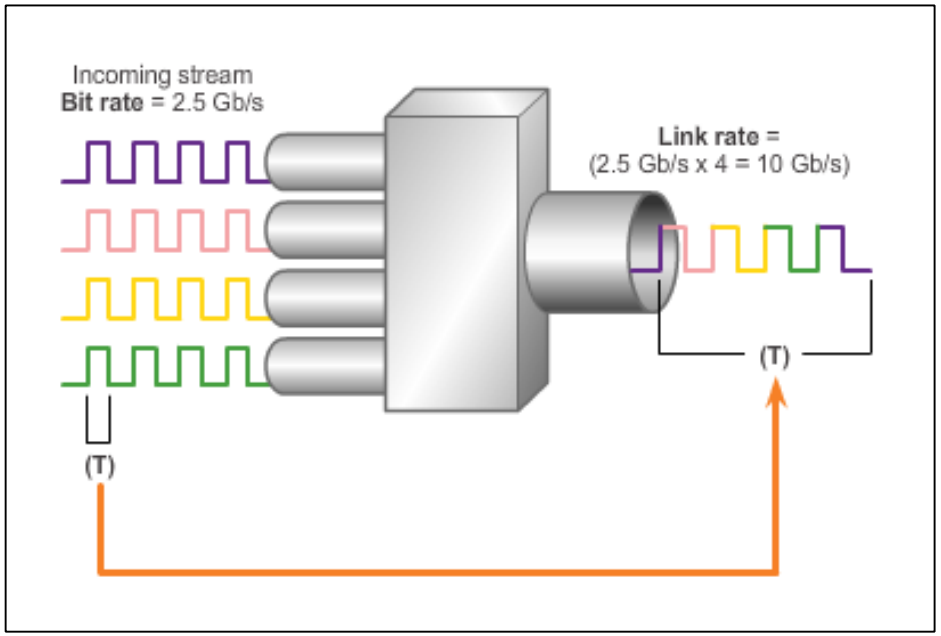
- STDM uses a variable time-slot length, allowing channels to compete for any free slot space.
- STDM does not waste high-speed line time with inactive channels using this scheme.



TDM Examples

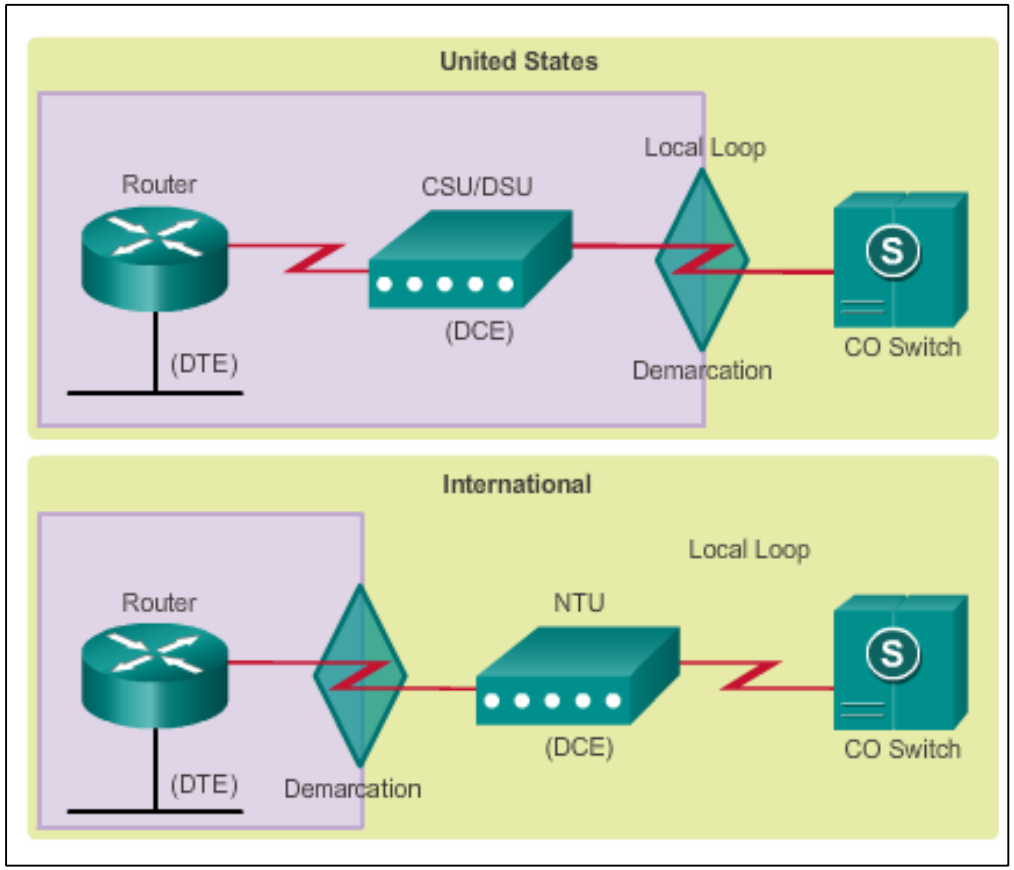
- The industry uses the Synchronous Optical Networking (SONET) or Synchronous Digital Hierarchy (SDH) standard for optical transport of TDM data.
- Traffic arriving at the SONET multiplexer from four places at 2.5 Gb/s goes out as a single stream at 4 x 2.5 Gb/s or 10 Gb/s.

Example:
TDM SONET



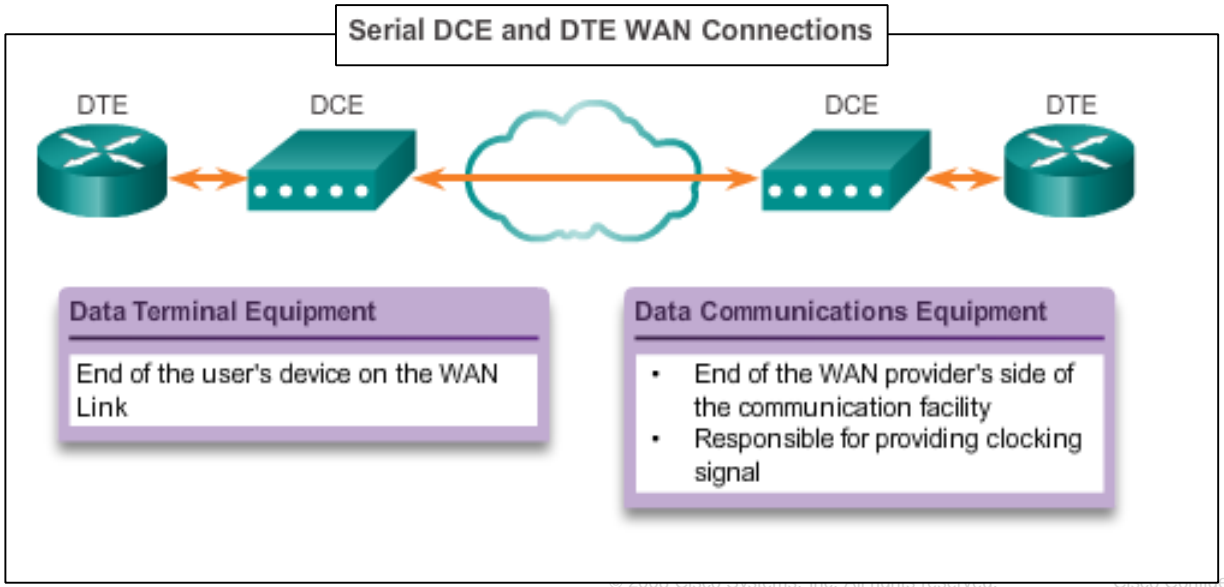
Demarcation Point

- Marks the point where your network interfaces with a network that is owned by another organization
- Interface between CPE and network service provider equipment
- Point in the network where the responsibility of the service provider ends



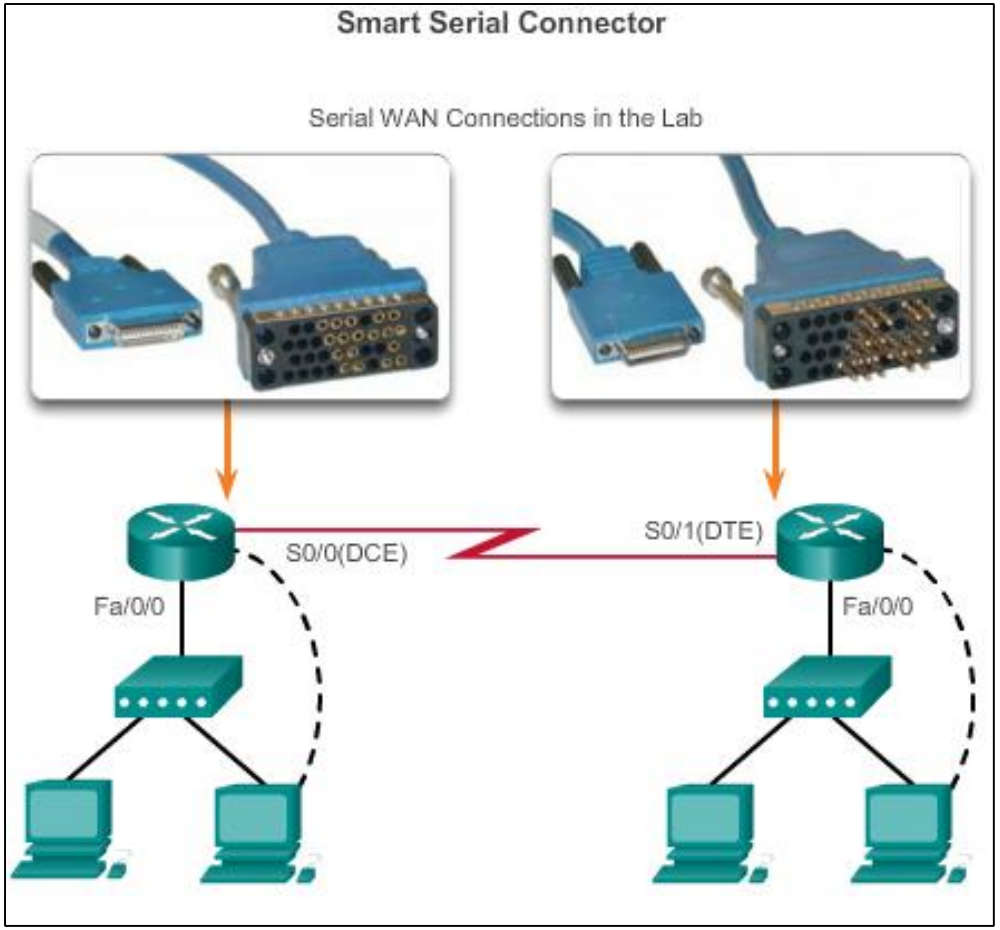
DTE-DCE

- **DTE** – Commonly CPE, generally a router, could also be a terminal, computer, printer, or fax machine if they connect directly to the service provider network.
- **DCE** – Commonly a modem or CSU/DSU, it is a device used to convert the user data from the DTE into a form acceptable to the WAN service provider transmission link. The signal is received at the remote DCE, which decodes the signal back into a sequence of bits; the remote DCE then signals this sequence to the remote DTE.



Serial Communications

Serial Cables



Serial Communications

Serial Bandwidth

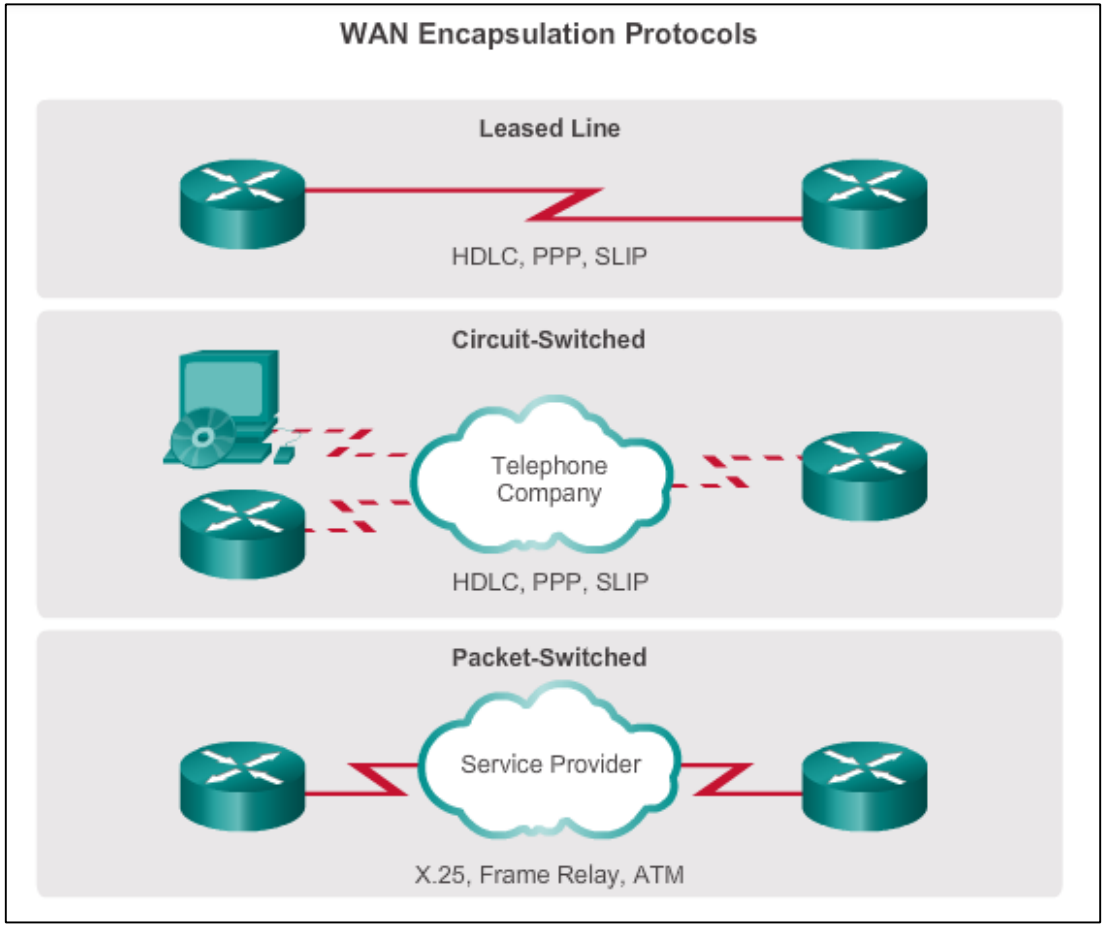
Bandwidth refers to the rate at which data is transferred over the communication link.

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	2.048 Mb/s
E3	34.064 Mb/s
T3	44.736 Mb/s
OC-1	51.84 Mb/s
OC-3	155.54 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

WAN Encapsulation Protocols

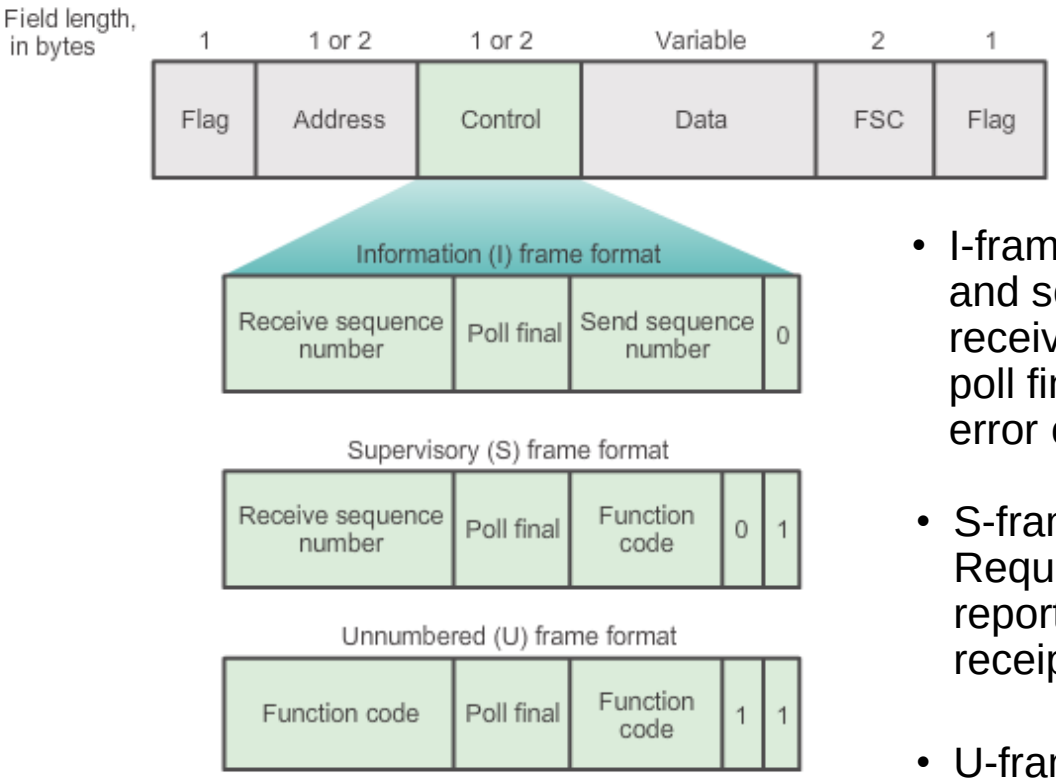
Data is encapsulated into frames before crossing the WAN link; an appropriate Layer 2 encapsulation type must be configured.



HDLC Encapsulation

- Bit-oriented, synchronous data link layer protocol developed by the International Organization for Standardization (ISO).
- Uses synchronous serial transmission to provide error-free communication between two points.
- Defines a Layer 2 framing structure that allows for flow control and error control through the use of acknowledgments.
- Cisco has developed an extension to the HLDC protocol to solve the inability to provide multiprotocol support (Cisco HLDC also referred to as cHDLC).

HDLC Frame Types



- The **Flag** field initiates and terminates error checking, and the frame always starts and ends with an 8-bit flag field, 01111110.

- I-frames carry upper layer information and some control information; sends and receives sequence numbers, and the poll final (P/F) bit performs flow and error control.

- S-frames provide control information – Request and suspend transmission, report on status, and acknowledge receipt of I-frame.

- U-frames support control purposes and are not sequenced.

Configuring HDLC Encapsulation

- Default encapsulation method used by Cisco devices on synchronous serial lines
- Point-to-point protocol on leased lines between two Cisco devices
- Connecting to a non-Cisco device, use synchronous PPP

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

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

HDLC Encapsulation

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
```

```
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
```

HDLC Encapsulation

Troubleshooting a Serial Interface (cont.)

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.

HDLC Encapsulation

Troubleshooting a Serial Interface (cont.)

Status Line	Possible Condition	Problem / Solution
Serial x is up, line protocol is down (DCE mode)	The clockrate interface configuration command is missing. The DTE device does not support or is not set up for SCTE mode (terminal timing). The remote CSU or DSU has failed.	1. Add the **clockrate** interface configuration command on the serial interface. Syntax: **clockrate** *bps* Syntax Description:bps - Desired clock rate in bits per second: 1200, 2400, 4800, 9600, 19200, 38400, 56000, 64000, 72000, 125000, 148000, 250000, 500000, 800000, 1000000, 1300000, 2000000, 4000000, or 8000000 2. If the problem appears to be on the remote end, repeat Step 1 on the remote modem, CSU, or DSU. 3. Verify that the correct cable is being used. 4. If the line protocol is still down, there is a possible hardware failure or cabling problem. Insert a breakout box and observe leads.

HDLC Encapsulation

Troubleshooting a Serial Interface (cont.)

Status Line	Possible Condition	Problem / Solution
Serial x is up, line protocol is up (looped)	A loop exists in the circuit. The sequence number in the keepalive packet changes to a random number when a loop is initially detected. If the same random number is returned over the link, a loop exists.	1. Use the **`show running-config`** privileged exec command to look for any **`loopback`** interface configuration command entries. 2. If there is a **`loopback`** interface configuration command entry, use the **`no loopback`** interface configuration command to remove the loop. 3. If there is no **`loopback`** interface configuration command, examine the CSU/DSU to determine whether they are configured in manual loopback mode. If they are, disable manual loopback. 4. After disabling loopback mode on the CSU/DSU, reset the CSU/DSU, and inspect the line status. If the line protocol comes up, no other action is needed. 5. If upon inspection, that the CSU or DSU cannot be manually set, then contact the leased-line or other carrier service for line troubleshooting assistance.

HDLC Encapsulation

Troubleshooting a Serial Interface (cont.)

Status Line	Possible Condition	Problem / Solution
Serial x is up, line protocol is down (disabled)	A high error rate has occurred due to a WAN service provider problem. A CSU or DSU hardware problem has occurred. Router hardware (interface) is bad.	1. Troubleshoot the line with a serial analyzer and breakout box. Look for toggling CTS and DSR signals. 2. Loop CSU/DSU (DTE loop). If the problem continues, it is likely that there is a hardware problem. If the problem does not continue, it is likely that there is a WAN service provider problem. 3. Swap out bad hardware as required (CSU, DSU, switch, local or remote router).

HDLC Encapsulation

Troubleshooting a Serial Interface (cont.)

Status Line	Possible Condition	Problem / Solution
Serial x is administratively down, line protocol is down	The router configuration includes the **shutdown** interface configuration command. A duplicate IP address exists.	1. Check the router configuration for the **shutdown** command. 2. Use the **no shutdown** interface configuration command to remove the **shutdown** command. 3. Verify that there are no identical IP addresses using the **show running-config** privileged exec command or the **show interfaces** exec command. 4. If there are duplicate addresses, resolve the conflict by changing one of the IP addresses.

3.2 PPP Operation

Cisco | Networking Academy®
Mind Wide Open™

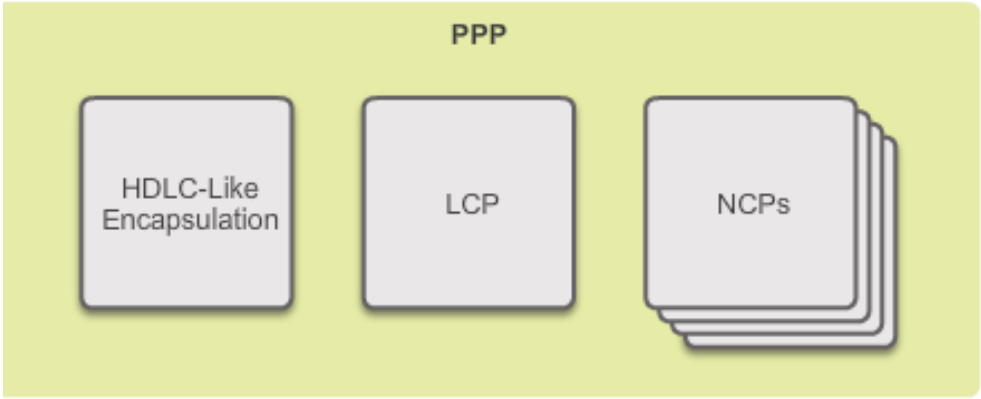
Introducing PPP

PPP contains three main components:

- HDLC protocol for encapsulating datagrams over point-to-point links
- Extensible Link Control Protocol (LCP) to establish, configure, and test the data link connection
- Family of Network Control Protocols (NCPs) to establish and configure different network layer protocols (IPv4, IPv6, AppleTalk, Novell IPX, and SNA Control Protocol)

HDLC is the default encapsulation method on a serial link.

Use PPP encapsulation to connect a Cisco router to a non-Cisco router.

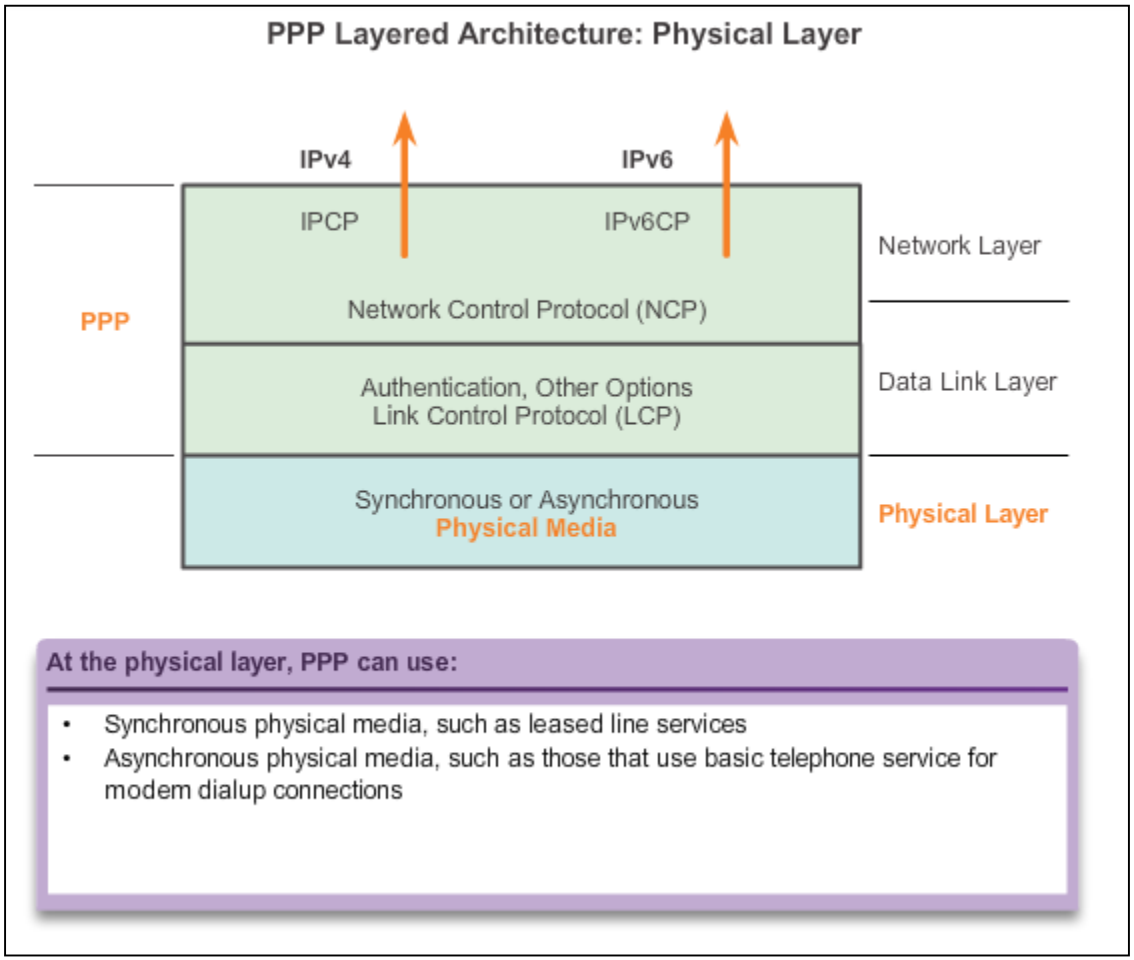


Advantages of PPP

- PPP not proprietary
- PPP includes many features not available in HDLC
  - Link quality management feature monitors the quality of the link. If too many errors are detected, PPP takes down the link
  - Supports PAP and CHAP authentication

PPP Layered Architecture

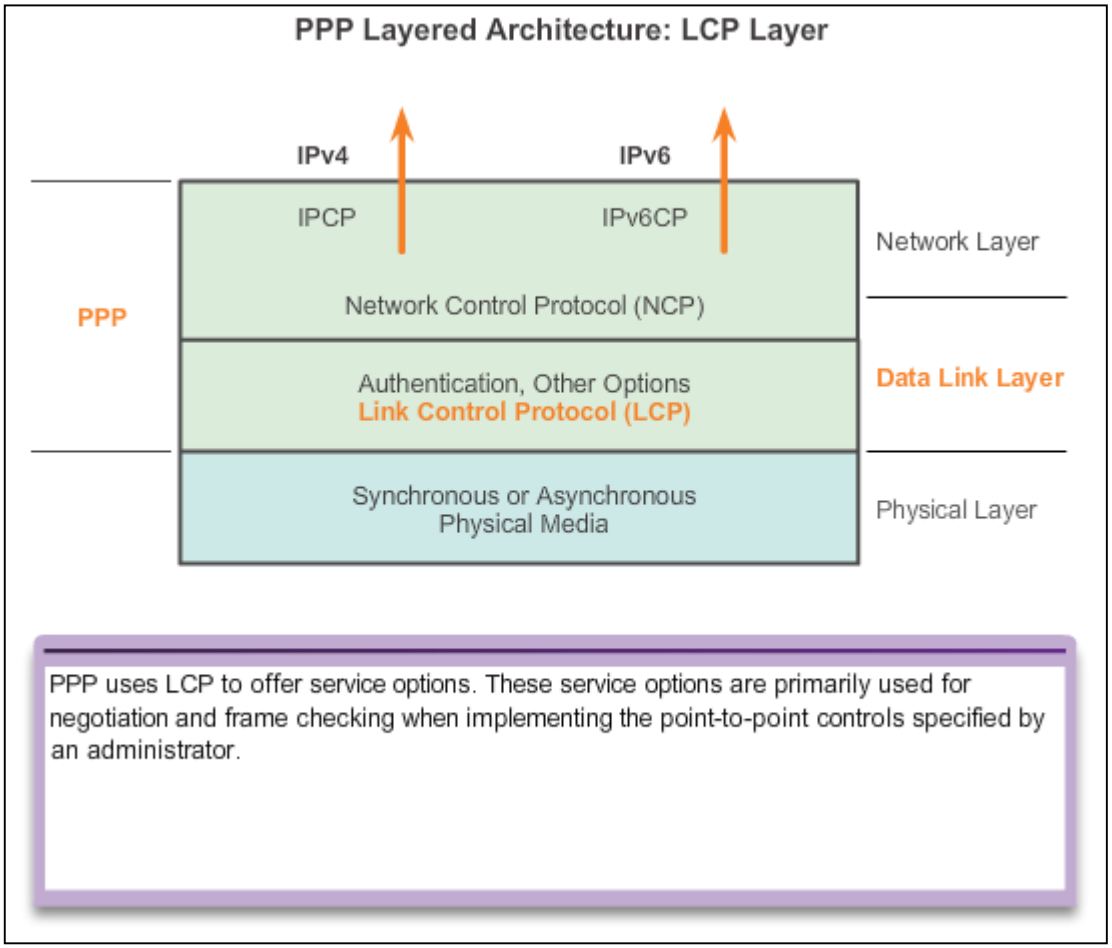
- LCP sets up the PPP connection and its parameters
- NCPs handle higher layer protocol configurations
- LCP terminates the PPP connection



PPP Control Protocol (LCP)

LCP provides automatic configuration of the interfaces at each end, including:

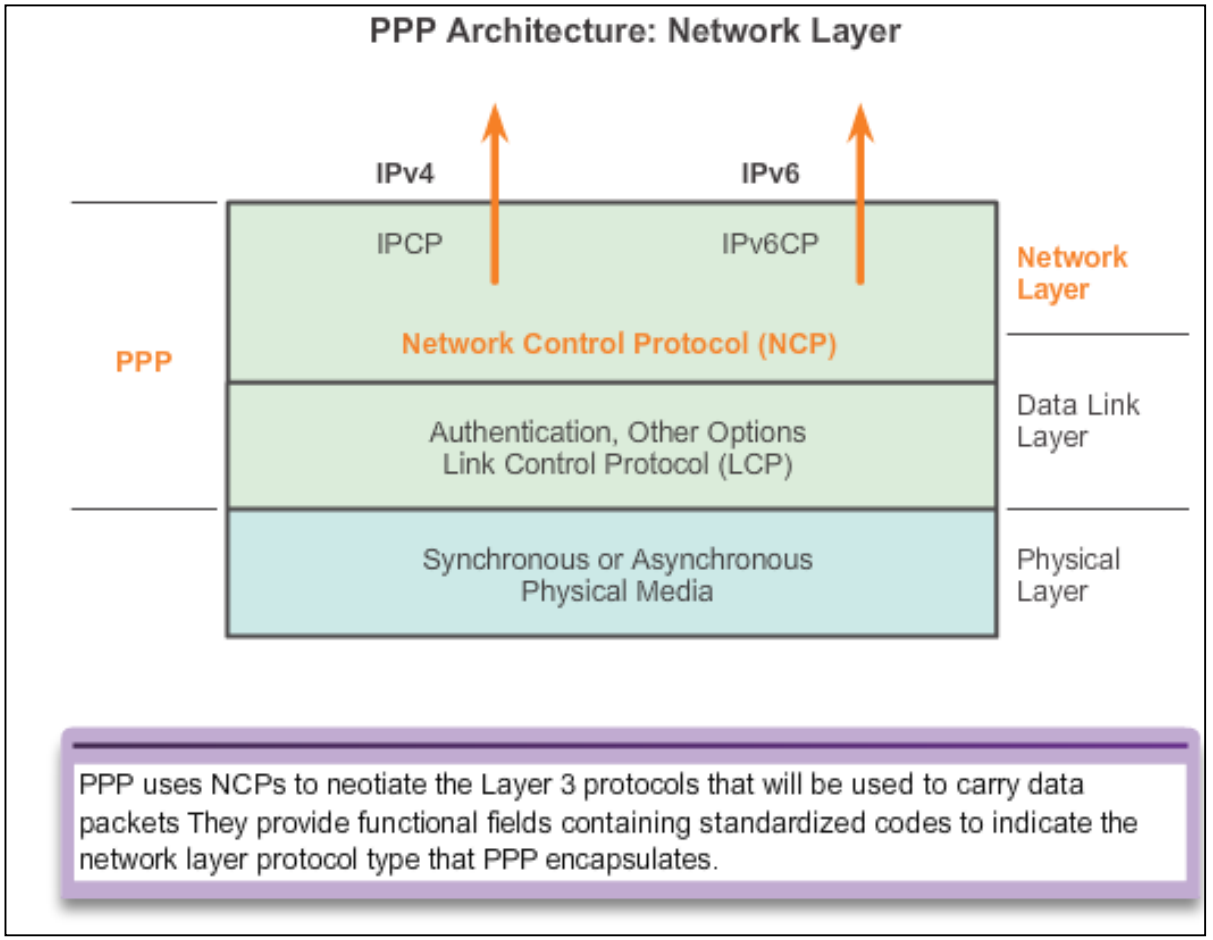
- Handling varying limits on packet size.
- Detecting common misconfiguration errors.
- Terminating the link.
- Determining when a link is functioning properly or when it is failing.



LCP and NCP

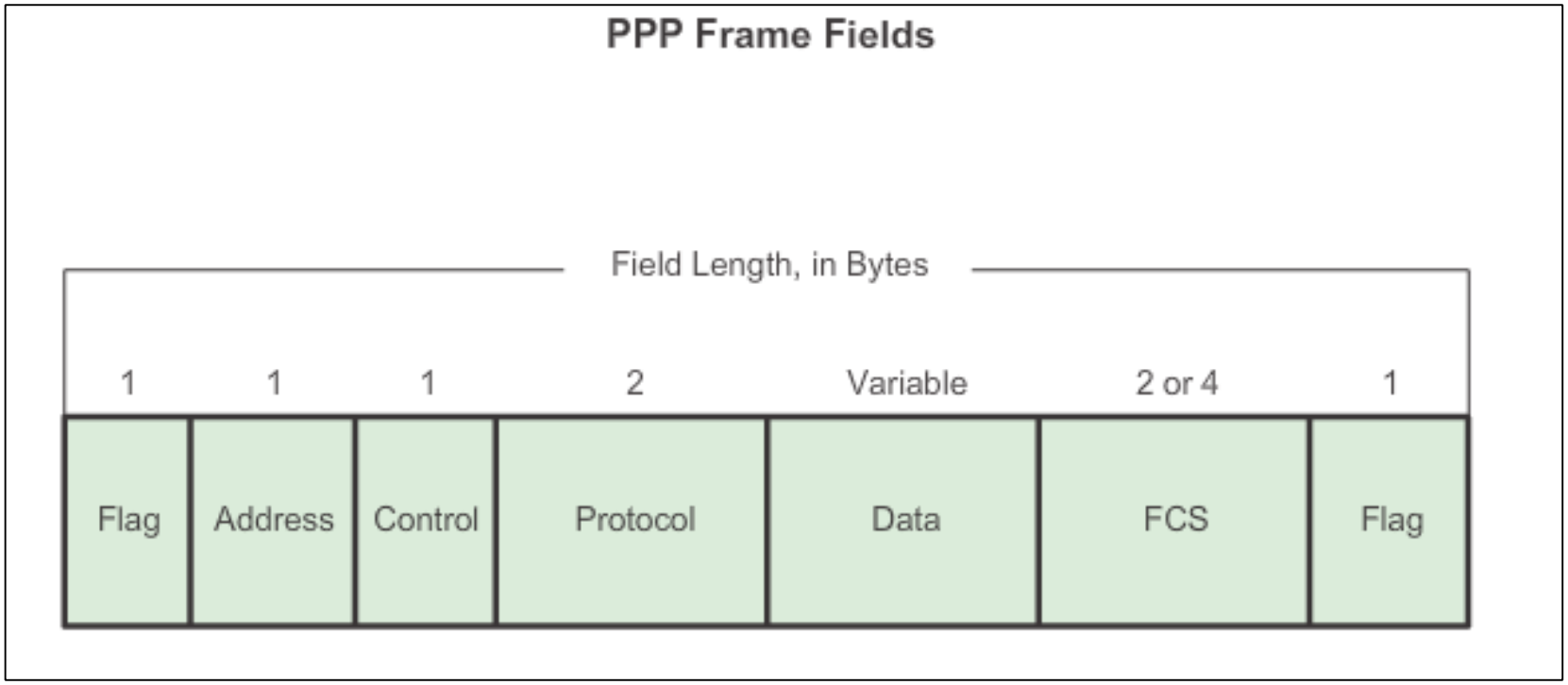
PPP Network Control Protocol (NCP)

- PPP permits multiple network layer protocols to operate on the same communications link.
- For every network layer protocol used, PPP uses a separate NCP.



LCP and NCP

PPP Frame Structure



Establishing a PPP Session

Phase 1 - Link Establishment: "Shall we negotiate?"

Phase 1 – LCP must first open the connection and negotiate configuration options; it completes when the receiving router sends a configuration-acknowledgment frame back to the router initiating the connection.

Establishing a PPP Session (cont.)

Phase 2 - Determine Link Quality: "Maybe we should discuss some details about quality. Or, maybe not . . ."

Phase 2 – LCP tests the link to determine whether the link quality is sufficient to bring up network layer protocols.

Establishing a PPP Session (cont.)

Phase 3 - Network Protocol Negotiation: "Yes, I will leave it to the NCPs to discuss higher level details."

Phase 3 – After the LCP has finished the link quality determination phase, the appropriate NCP can separately configure the network layer protocols, and bring them up and take them down at any time.

LCP Operation

- LCP operation includes provisions for link establishment, link maintenance, and link termination.
- LCP operation uses three classes of LCP frames to accomplish the work of each of the LCP phases:
  - Link-establishment frames establish and configure a link.
    - Configure-Request, Configure-Ack, Configure-Nak, and Configure-Reject
  - Link-maintenance frames manage and debug a link.
    - Code-Reject, Protocol-Reject, Echo-Request, Echo-Reply, and Discard-Request
  - Link-termination frames terminate a link.
    - Terminate-Request and Terminate-Ack

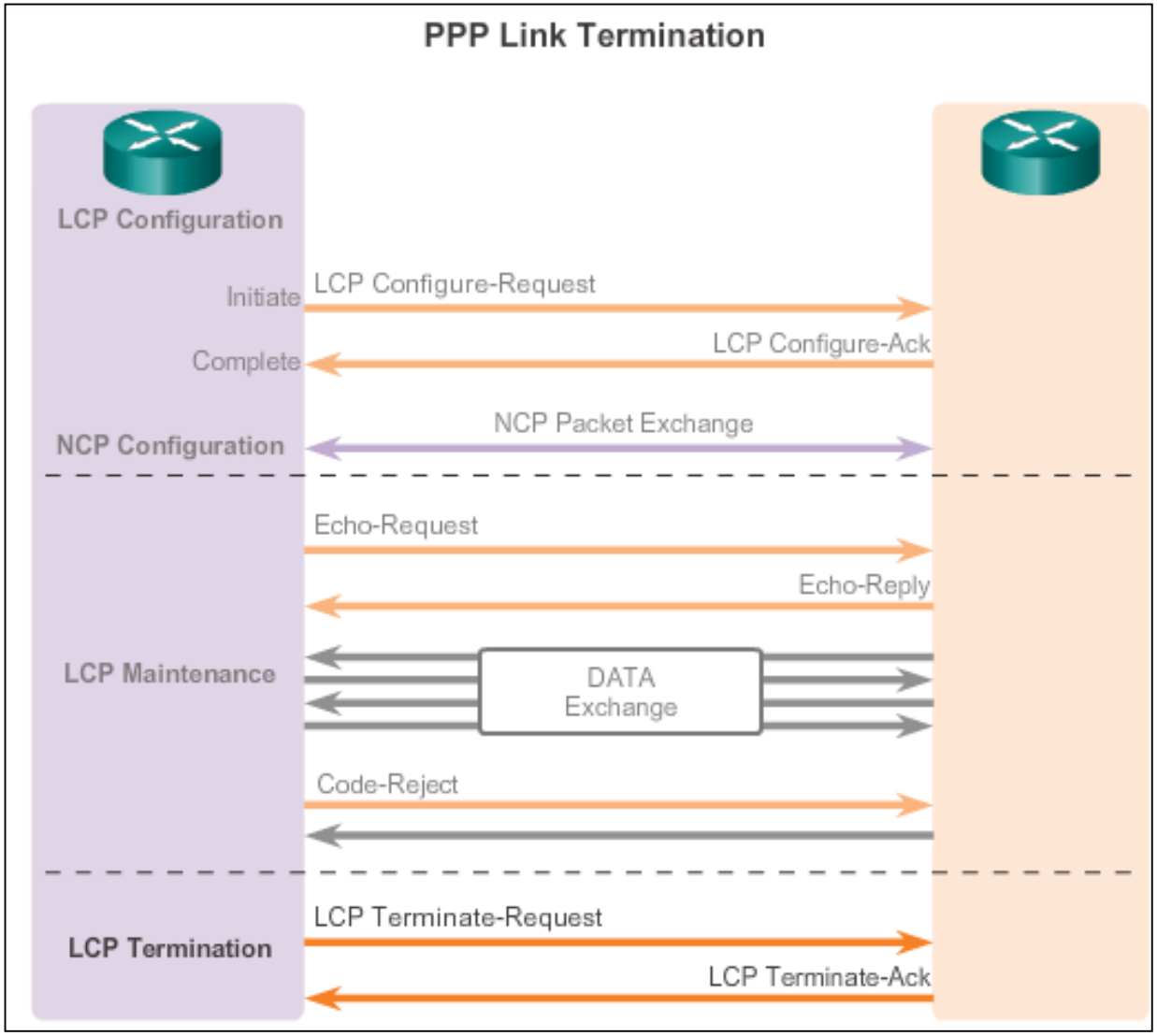
LCP Operation (cont.)

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

- Echo-Request, Echo-Reply, and Discard-Request can be used to test the link.
- Code-Reject and Protocol-Reject provides feedback when one device receives an invalid frame due to either an unrecognized LCP code (LCP frame type) or a bad protocol identifier.

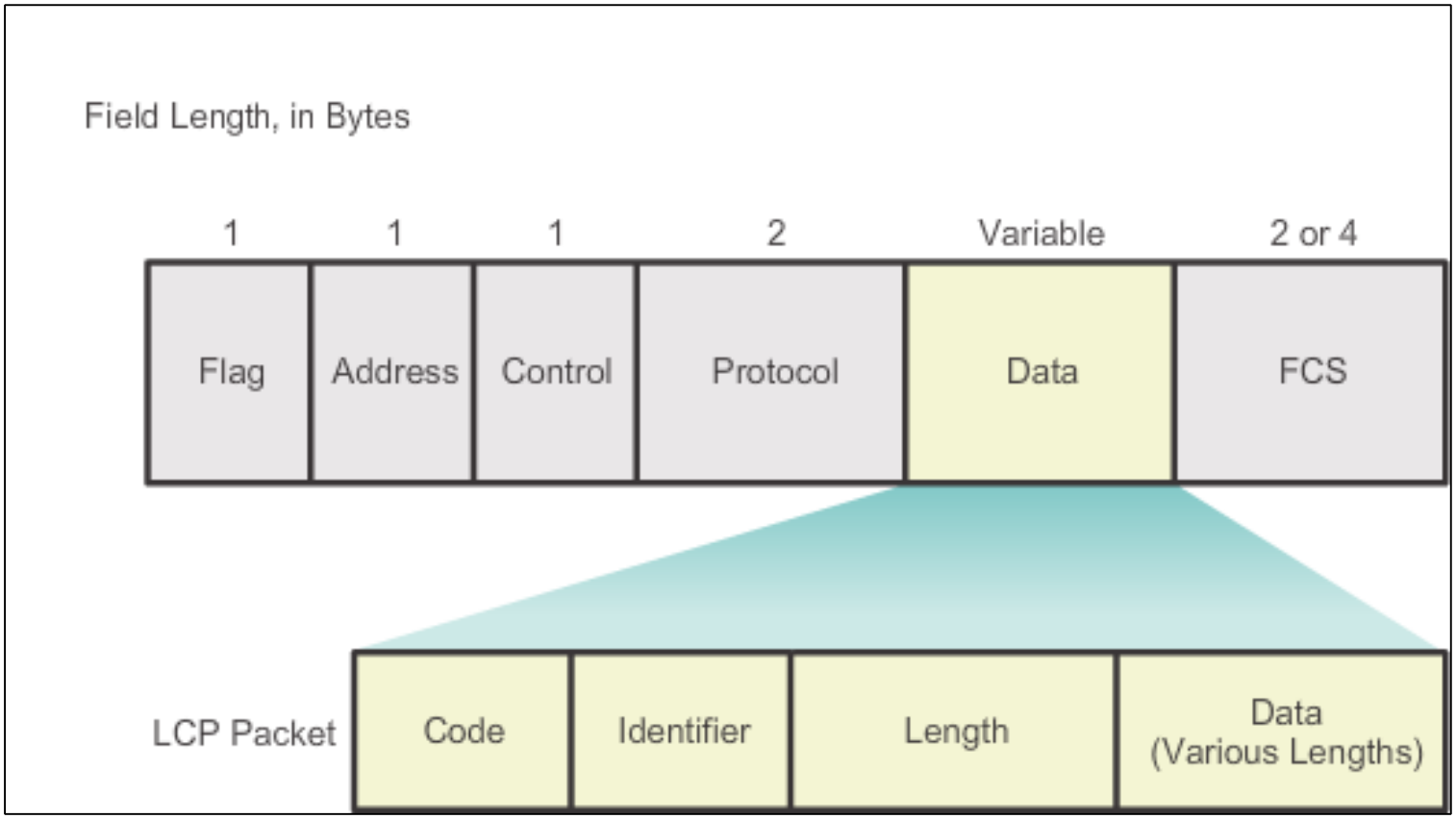
PPP Sessions

LCP Operation (cont.)



PPP Sessions

LCP Packet



PPP Sessions

LCP Packet

LCP Code	LCP Packet Type	Description
1	**Configure-Request**	Sent to open or reset a PPP connection. Configure-Request contains a list of LCP options with changes to default option values.
2	**Configure-Ack**	Sent when all of the values of all of the LCP options in the last Configure-Request received are recognized and acceptable. When both PPP peers send and receive Configure-Acks, the LCP negotiation is complete.
3	**Configure-Nak**	Sent when all the LCP options are recognized, but the values of some options are not acceptable. Configure-Nak includes the mismatching options and their acceptable values.
4	**Configure-Reject**	Sent when LCP options are not recognized or not acceptable for negotiation. Configure-Reject includes the unrecognized or non-negotiable options.
5	**Terminate-Request**	Optionally sent to close the PPP connection.
6	**Terminate-Ack**	Sent in response to the Terminate-Request.

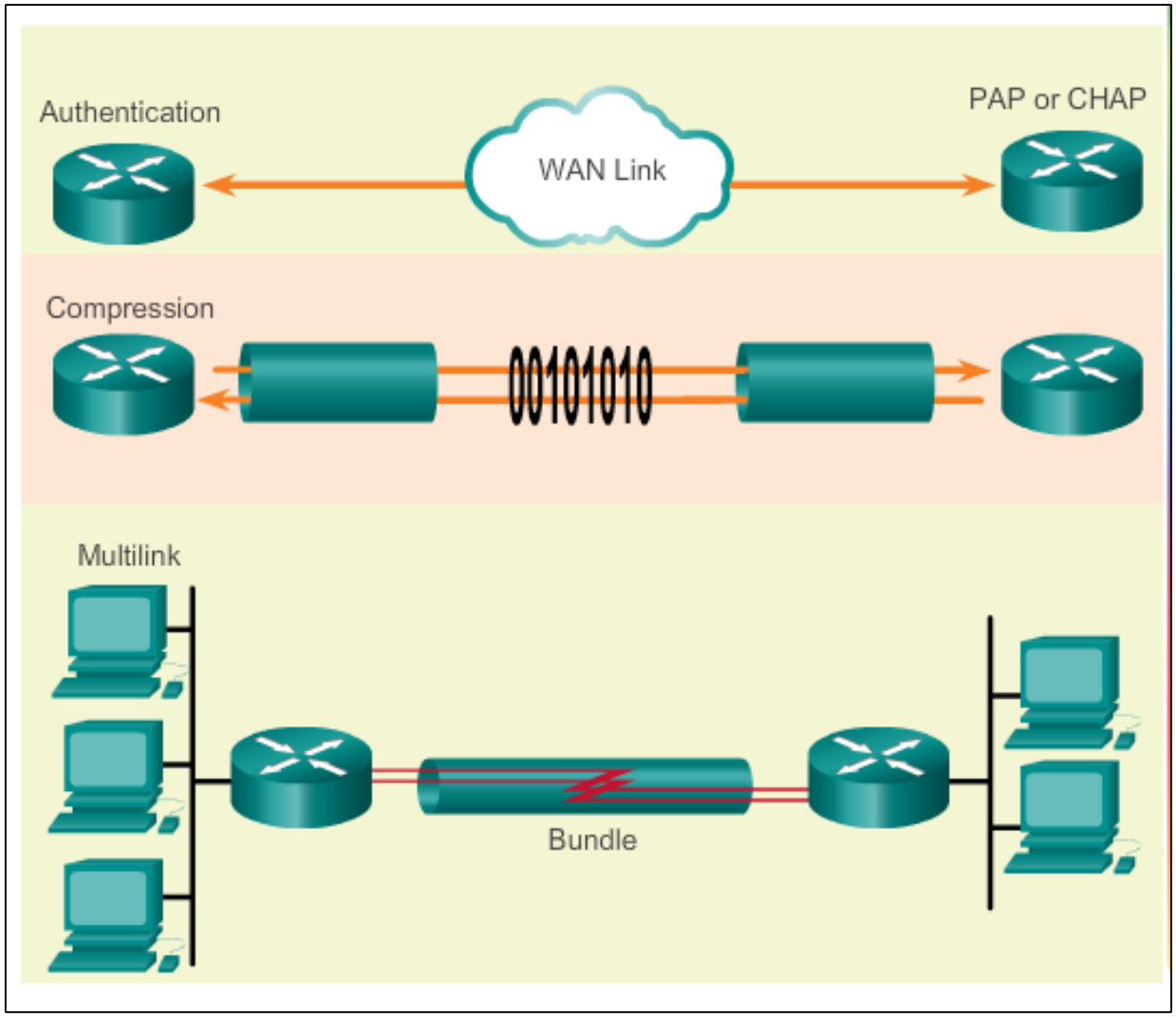
LCP Packet (cont.)

LCP Code	LCP Packet Type	Description
7	**Code-Reject**	Sent when the LCP code is unknown. The Code-Reject message includes the rejected LCP packet.
8	**Protocol-Reject**	Sent when the PPP frame contains an unknown Protocol ID. The Protocol-Reject message includes the rejected LCP packet. Protocol-Reject is typically sent by a PPP peer in response to a PPP NCP for a LAN protocol not enabled on the PPP peer.
9	**Echo-Request**	Optionally sent to test the PPP connection.
10	**Echo-Reply**	Sent in response to an Echo-Request. The PPP Echo-Request and Echo-Reply are not related to the ICMP Echo Request and Echo Reply messages.
11	**Discard-Request**	Optionally sent to exercise the link in the outbound direction.

PPP Configuration Options

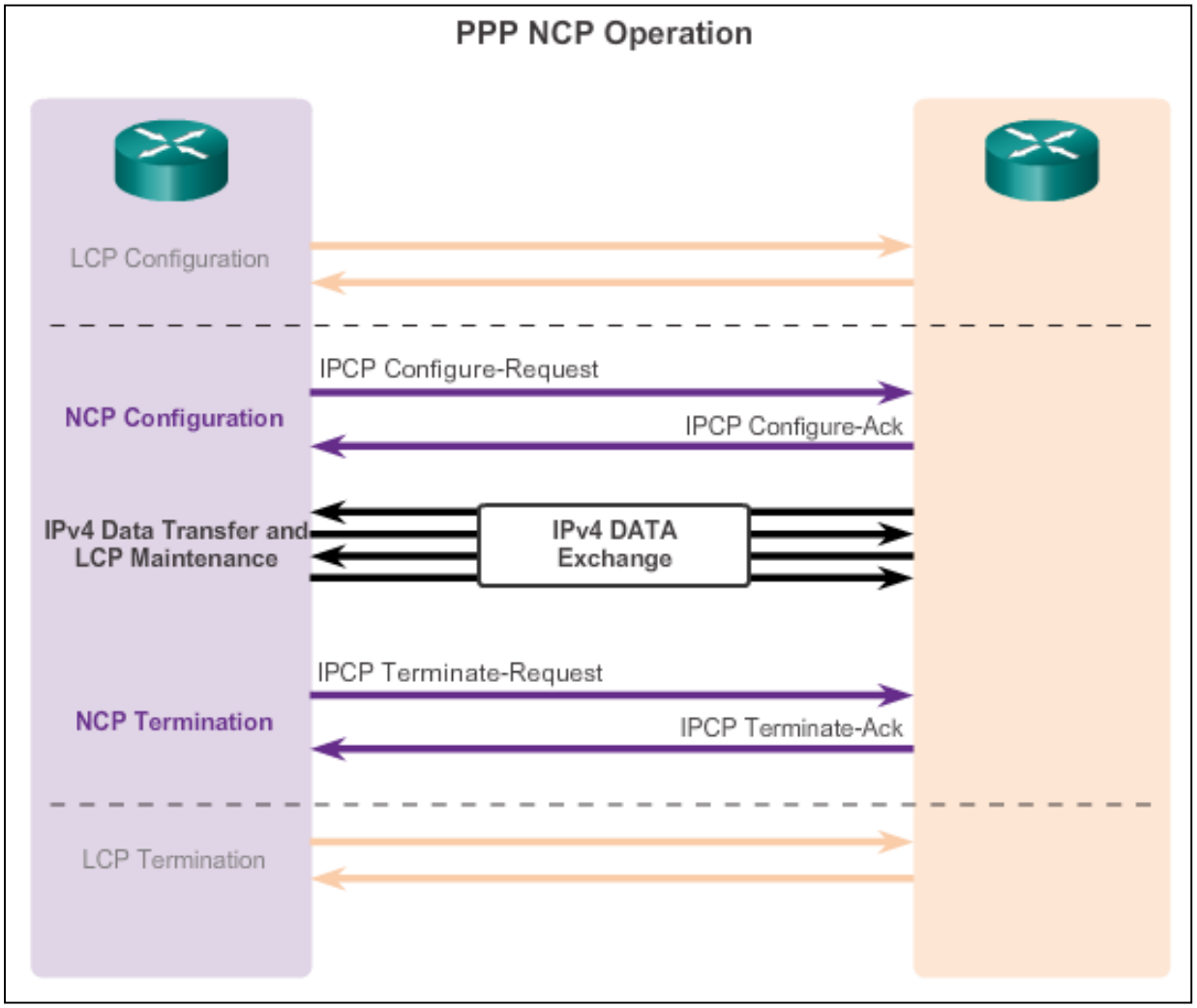
Optional functions include:

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



PPP Sessions

NCP Explained



3.3 Configuring PPP

Cisco | Networking Academy®
Mind Wide Open™

PPP Configuration Options

- **Authentication** – Two authentication choices are Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP).
- **Compression** – Increases the effective throughput on PPP connections by reducing the amount of data in the frame that must travel across the link. The protocol decompresses the frame at its destination. 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. The Magic Number field helps in detecting links that are in a looped-back condition. Magic numbers are generated randomly at each end of the connection.

PPP Configuration Options

- **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. The client makes the initial call, requests that the server call it back, and terminates its initial call. The callback router answers the initial call and makes the return call to the client based on its configuration statements. The command is **`ppp callback [accept | request]`**.
- **Multilink** – This alternative provides load balancing over the router interfaces that PPP uses. Multilink PPP provides a method for spreading traffic across multiple physical WAN links while providing packet fragmentation and reassembly, proper sequencing, multivendor interoperability, and load balancing on inbound and outbound traffic.

Configure PPP

PPP Basic Configuration Command


```
hostname R1
!
interface Serial 0/0/0
 ip address 10.0.1.1 255.255.255.252
 ipv6 address 2001:db8:cafe:1::1/64
 encapsulation ppp
```

```
hostname R2
!
interface Serial 0/0/0
 ip address 10.0.1.2 255.255.255.252
 ipv6 address 2001:db8:cafe:1::2/64
 encapsulation ppp
```

PPP Compression Commands


```
hostname R1
!
interface Serial 0/0/0
 ip address 10.0.1.1 255.255.255.252
 ipv6 address 2001:db8:cafe:1::1/64
 encapsulation ppp
 compress predictor
```

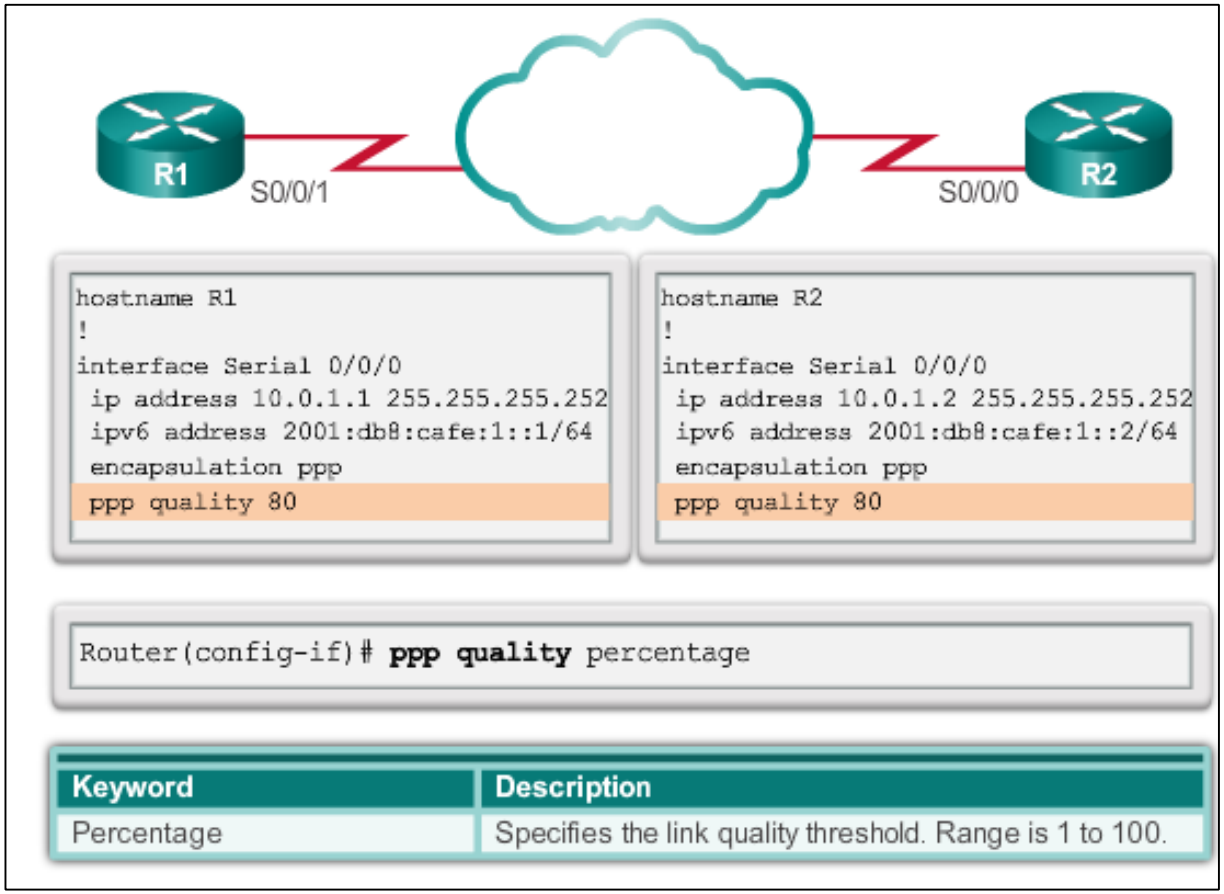
```
hostname R2
!
interface Serial 0/0/0
 ip address 10.0.1.2 255.255.255.252
 ipv6 address 2001:db8:cafe:1::2/64
 encapsulation ppp
 compress predictor
```

```
Router(config if)# compress [predictor | stac]
```

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.

PPP Link Quality Monitoring Command

The **ppp quality *percentage*** command ensures that the link meets the quality requirement set; otherwise, the link closes down.



Keyword	Description
Percentage	Specifies the link quality threshold. Range is 1 to 100.

PPP Multilink Commands


```
hostname R3
!
interface Multilink 1
 ip address 10.0.1.1 255.255.255.252
 ipv6 address 2001:db8:cafe:1::1/64
 ppp multilink
 ppp multilink group 1
!
interface Serial 0/1/0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
!
interface Serial 0/1/1
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
```

```
hostname R4
!
interface Multilink 1
 ip address 10.0.1.2 255.255.255.252
 ipv6 address 2001:db8:cafe:1::2/64
 ppp multilink
 ppp multilink group 1
!
interface Serial 0/0/0
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
!
interface Serial 0/0/1
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
```

Configure PPP

Verifying PPP Configuration

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.

```
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
```

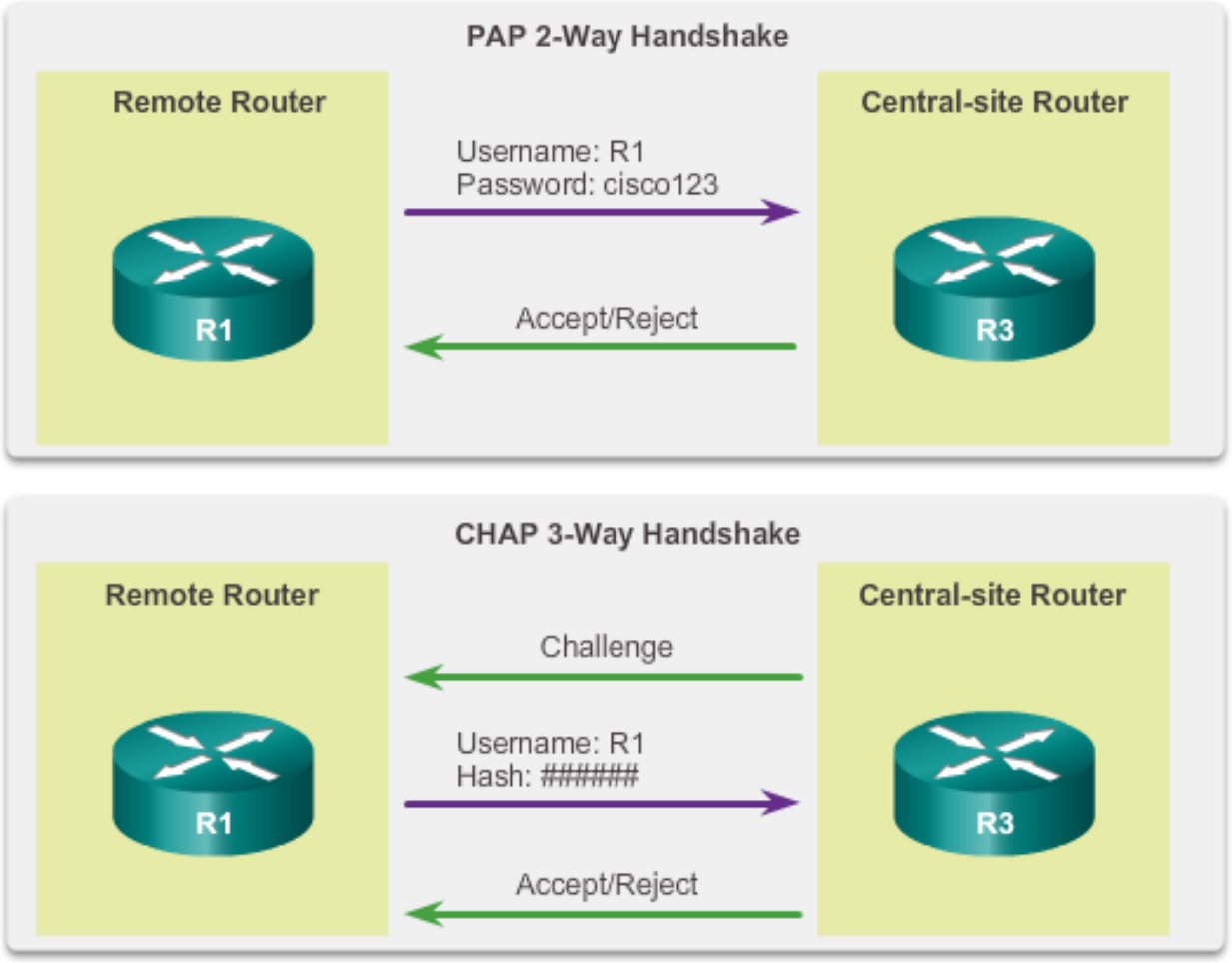
Verifying PPP Configuration (cont.)

The output indicates the interface Multilink 1, the hostnames of both the local and remote endpoints, and the serial interfaces assigned to the multilink bundle.

```
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#
```

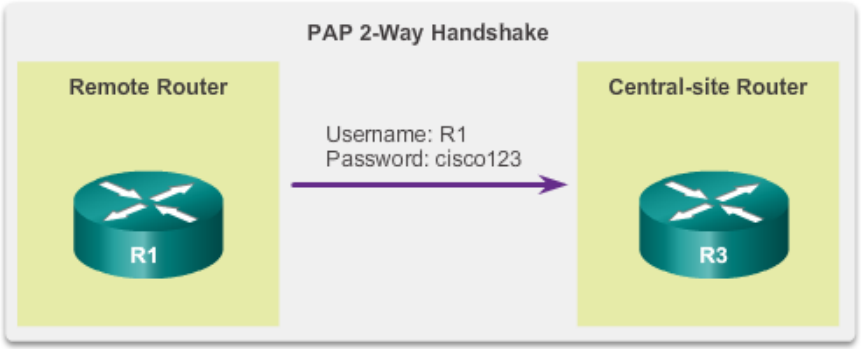
PPP Authentication Protocols



Password Authentication Protocol (PAP)

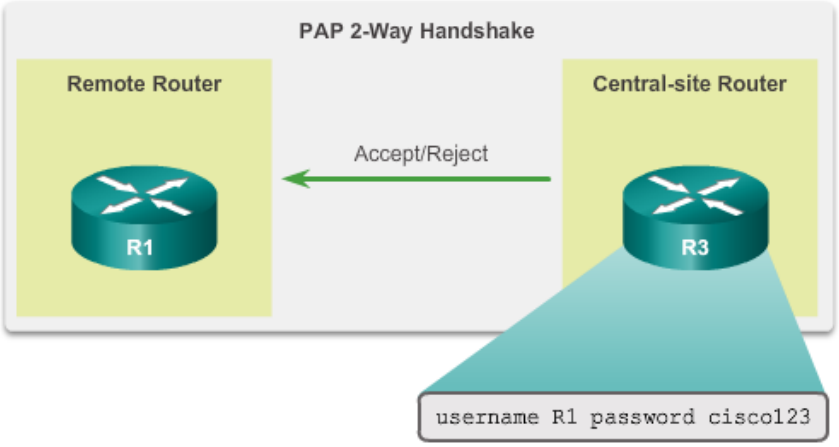
Initiating PAP

R1 sends its PAP username and password to R3.



Completing PAP

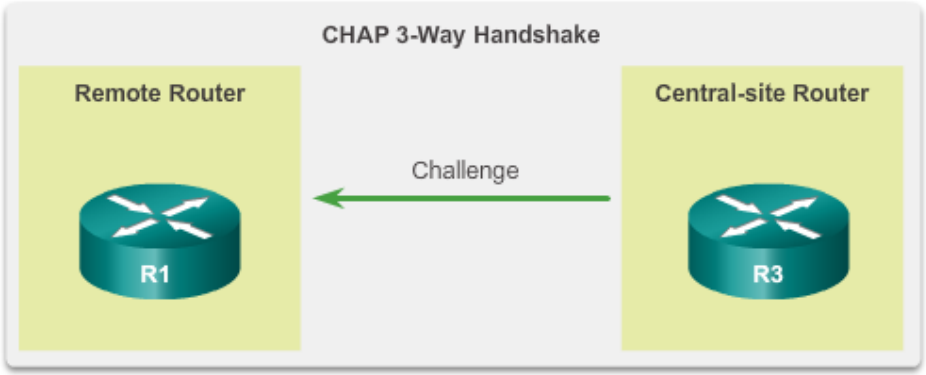
R3 evaluates R1's username and password against its local database. If it matches, it accepts the connection. If not, it rejects the connection.



PPP Authentication
Challenge Handshake Authentication Protocol

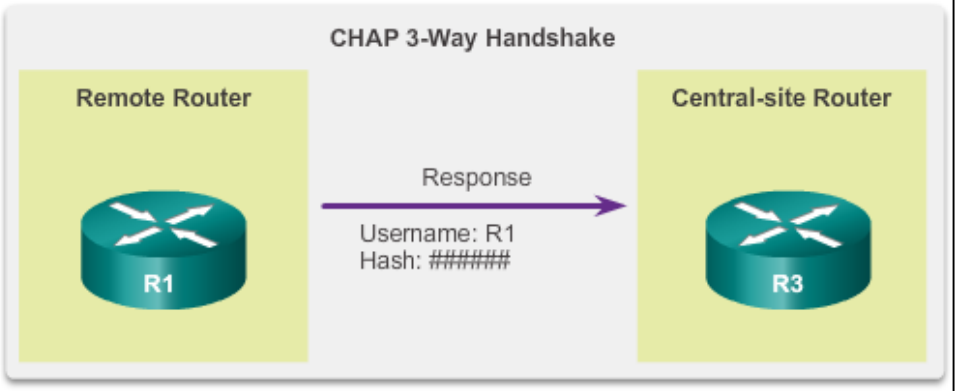
Initiating CHAP

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



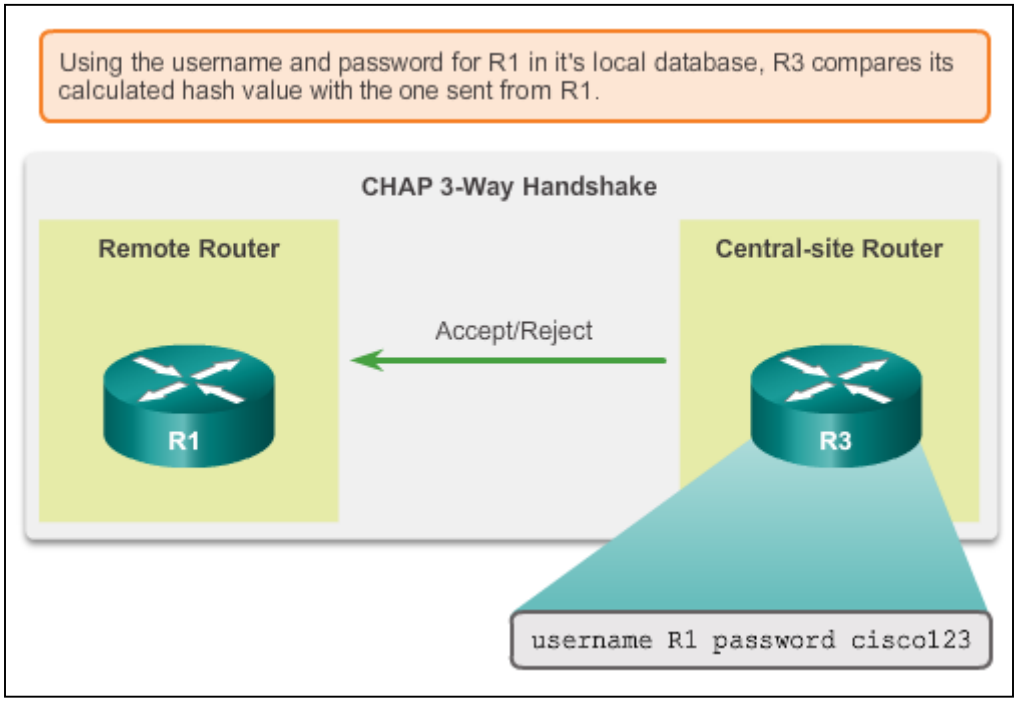
Responding CHAP

R1 responds to R3's CHAP challenge by sending its CHAP username and a hash value that is based on the CHAP password.

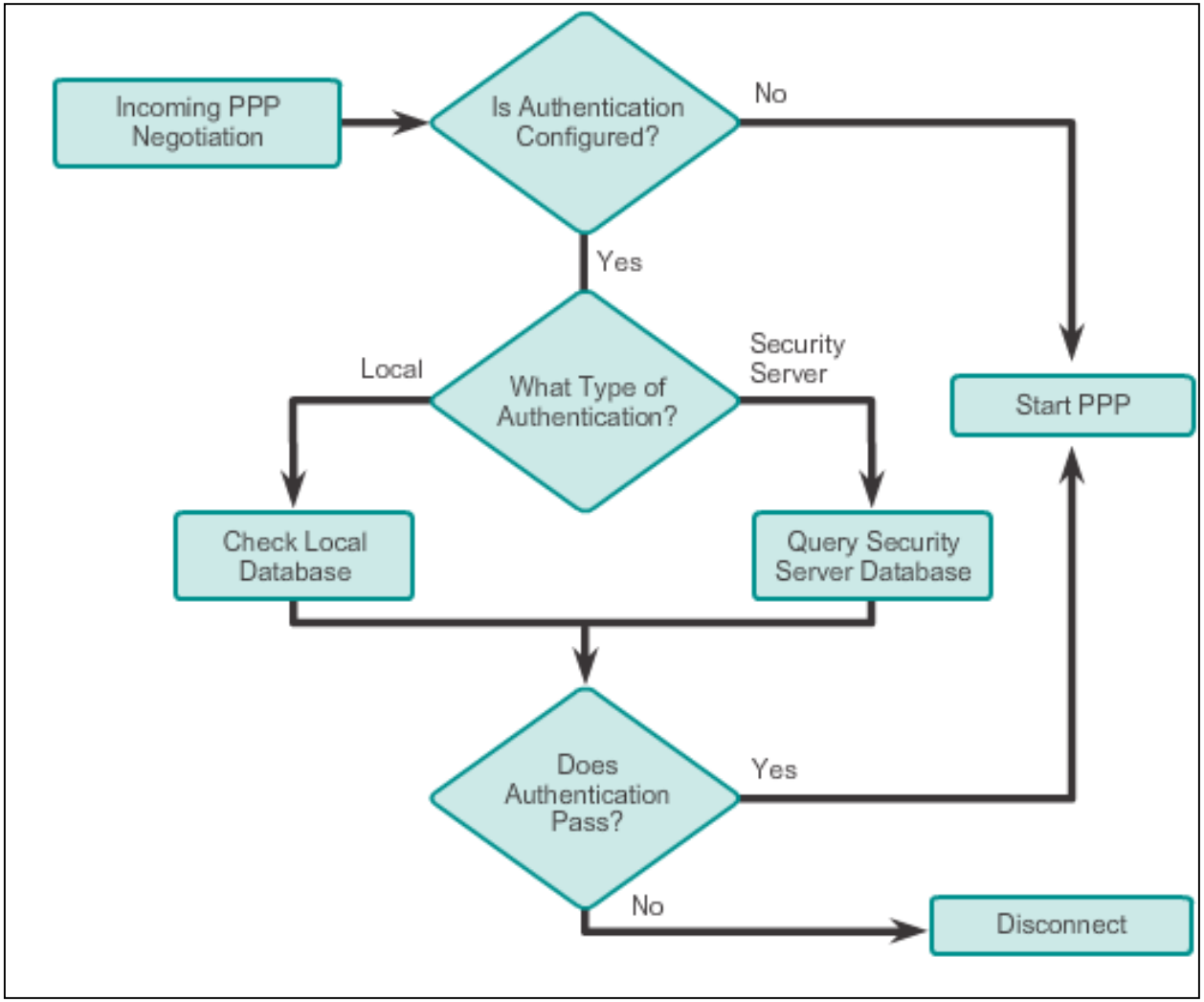


CHAP (cont.)

Completing CHAP



PPP Encapsulation and Authentication Process



Configuring PPP Authentication

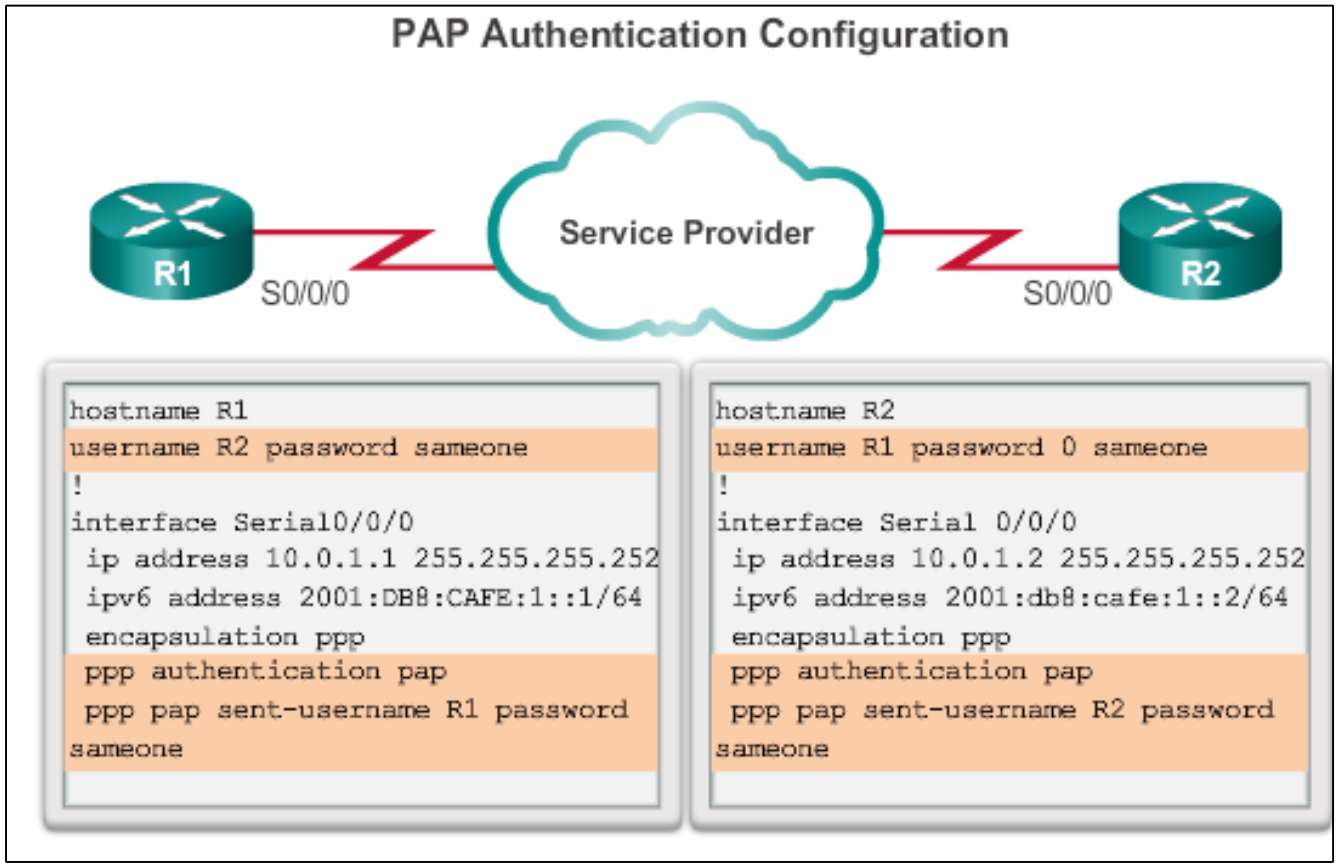
The ppp authentication Command

```
ppp authentication {chap | chap pap | pap chap | pap} [if-needed]
[list-name | default] [callin]
```

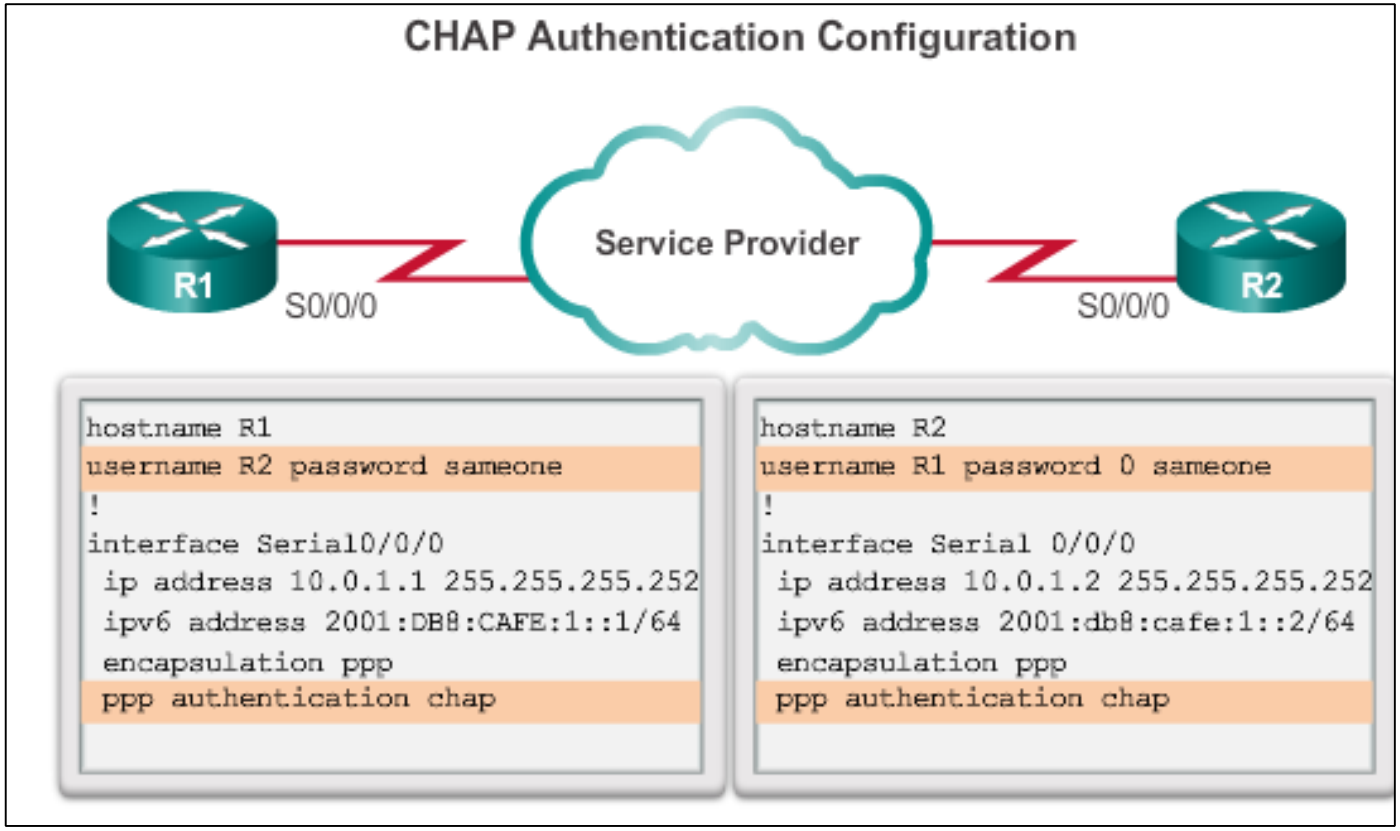
The ppp authentication Command

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.
if-needed (Optional)	Used with TACACS and XTACACS. Do not perform CHAP or PAP authentication if the user has already provided authentication. This option is available only on asynchronous interfaces.
list-name (Optional)	Used with AAA/TACACS+. Specifies the name of a list of TACACS+ methods of authentication to use. If no list name is specified, the system uses the default. Lists are created with the **aaa authentication ppp** command.
default (Optional)	Used with AAA/TACACS+. Created with the **aaa authentication ppp** command.
callin	Specifies authentication on incoming (received) calls only.

Configuring PPP Authentication (cont.)



Configuring PPP Authentication (cont.)



3.4 Troubleshooting WAN Connectivity

Cisco | Networking Academy®
Mind Wide Open™

Troubleshooting PPP Serial Encapsulation

debug ppp Command Parameters

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

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
cbcp	Displays protocol errors and statistics associated with PPP connection negotiations using MSCB.

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
```

Chapter 3: Summary

- Point-to-Point links are usually more expensive than shared services; however, the benefits may outweigh the costs. Constant availability is important for some protocols, such as VoIP.
- SONET is an optical network standard that uses STDM for efficient use of bandwidth.
- The demarcation point is the point in the network where the responsibility of the service provider ends and the responsibility of the customer begins. The CPE, usually a router, is the DTE device. The DCE is usually a modem or CSU/DSU.
- Cisco HDLC is a bit-oriented synchronous data link layer protocol extension of HDLC and is used by many vendors to provide multiprotocol support. This is the default encapsulation method used on Cisco synchronous serial lines.
- Synchronous PPP is used to connect to non-Cisco devices, to monitor link quality, provide authentication, or bundle links for shared use
- LCP is the PPP protocol used to establish, configure, test and terminate the data link connection. LCP can optionally authenticate a peer using PAP or CHAP.