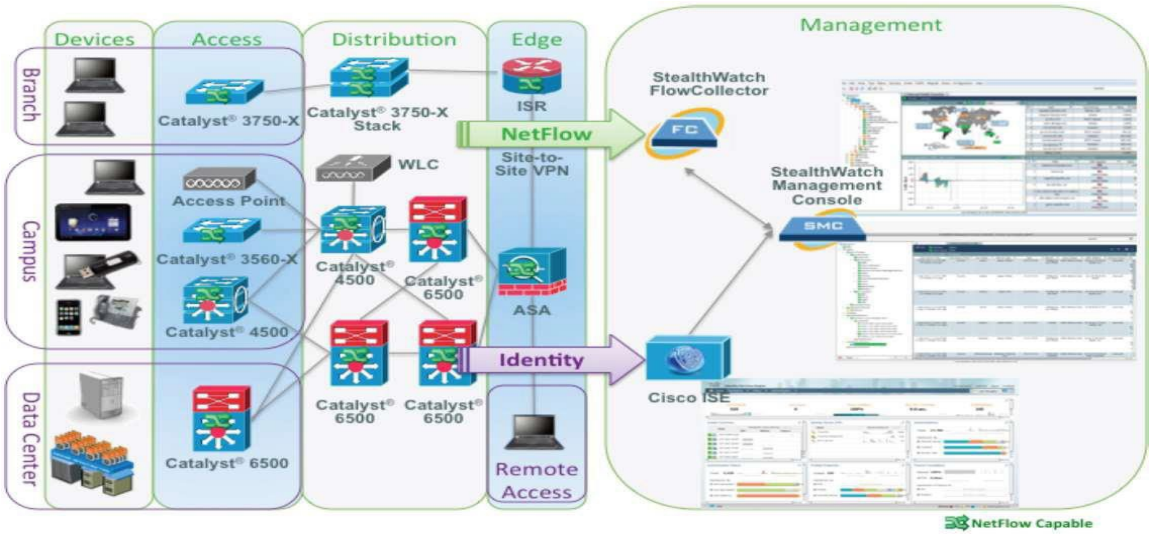
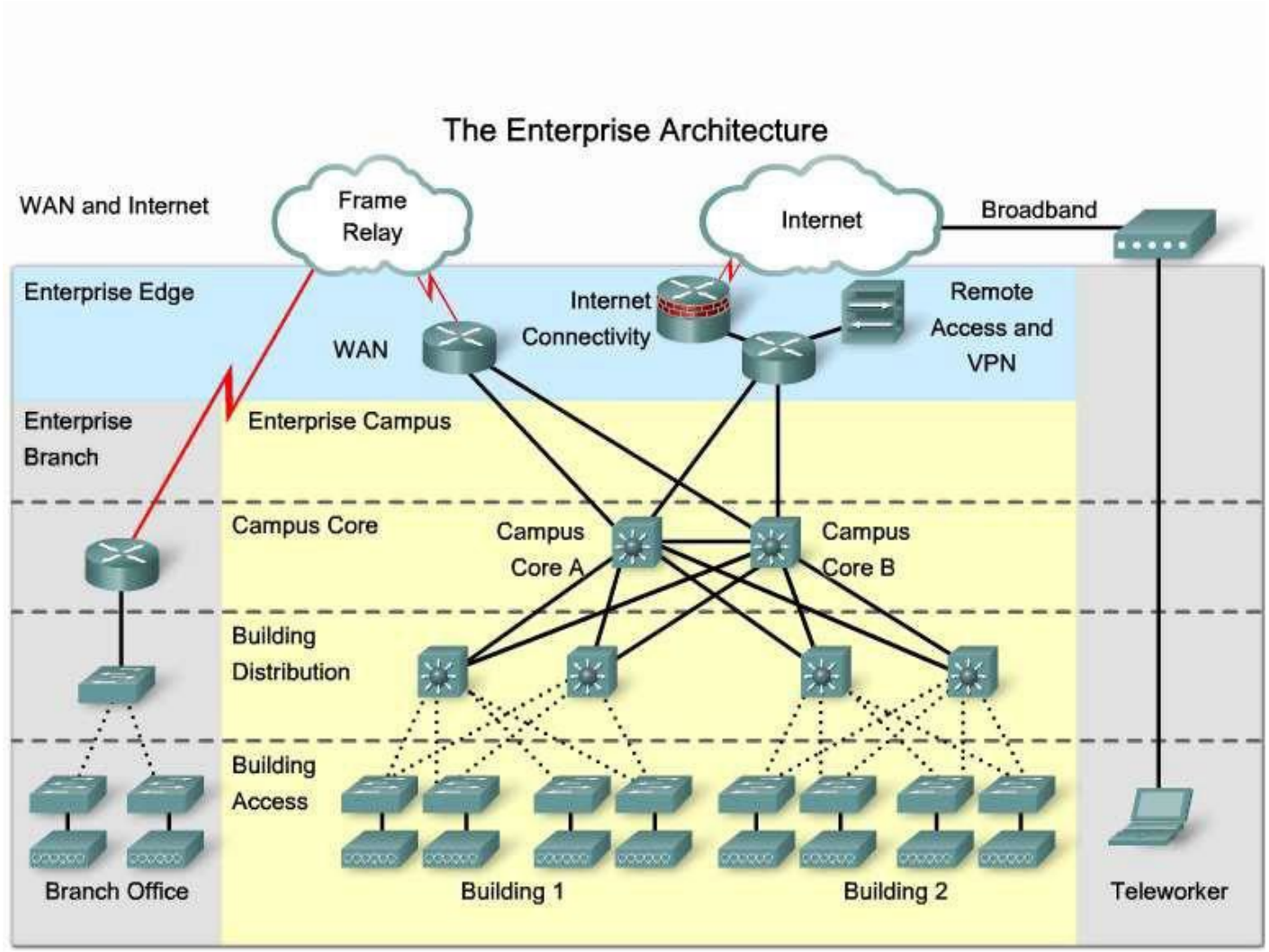
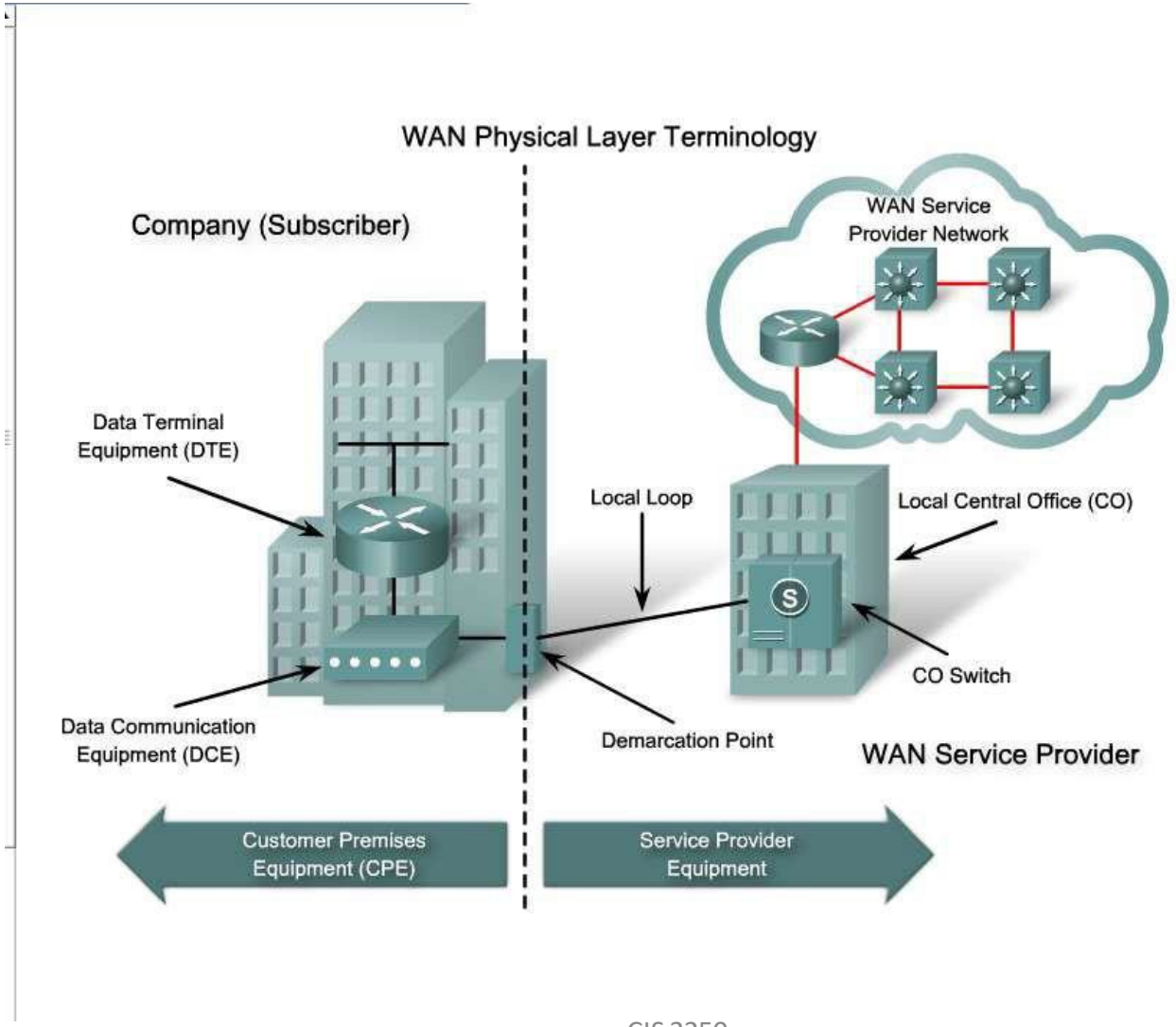
CIS 3250
Accessing the WAN
Point to Point Protocol



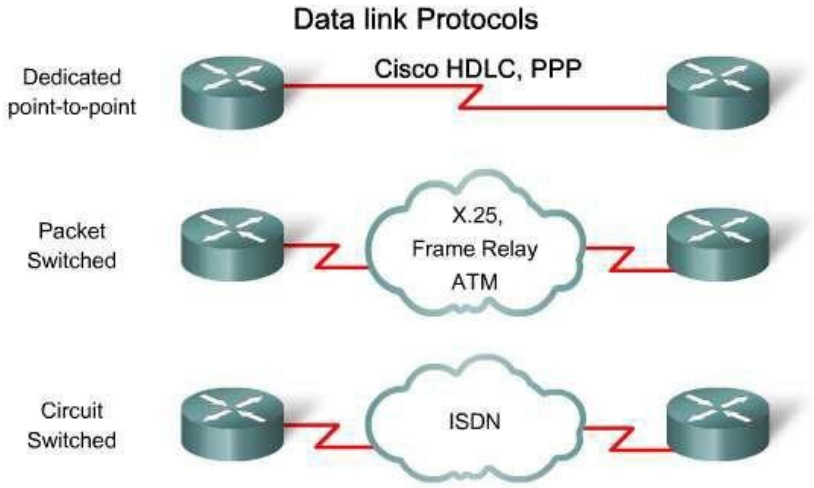
Enterprise Architecture



WAN Layer 1 Terminology



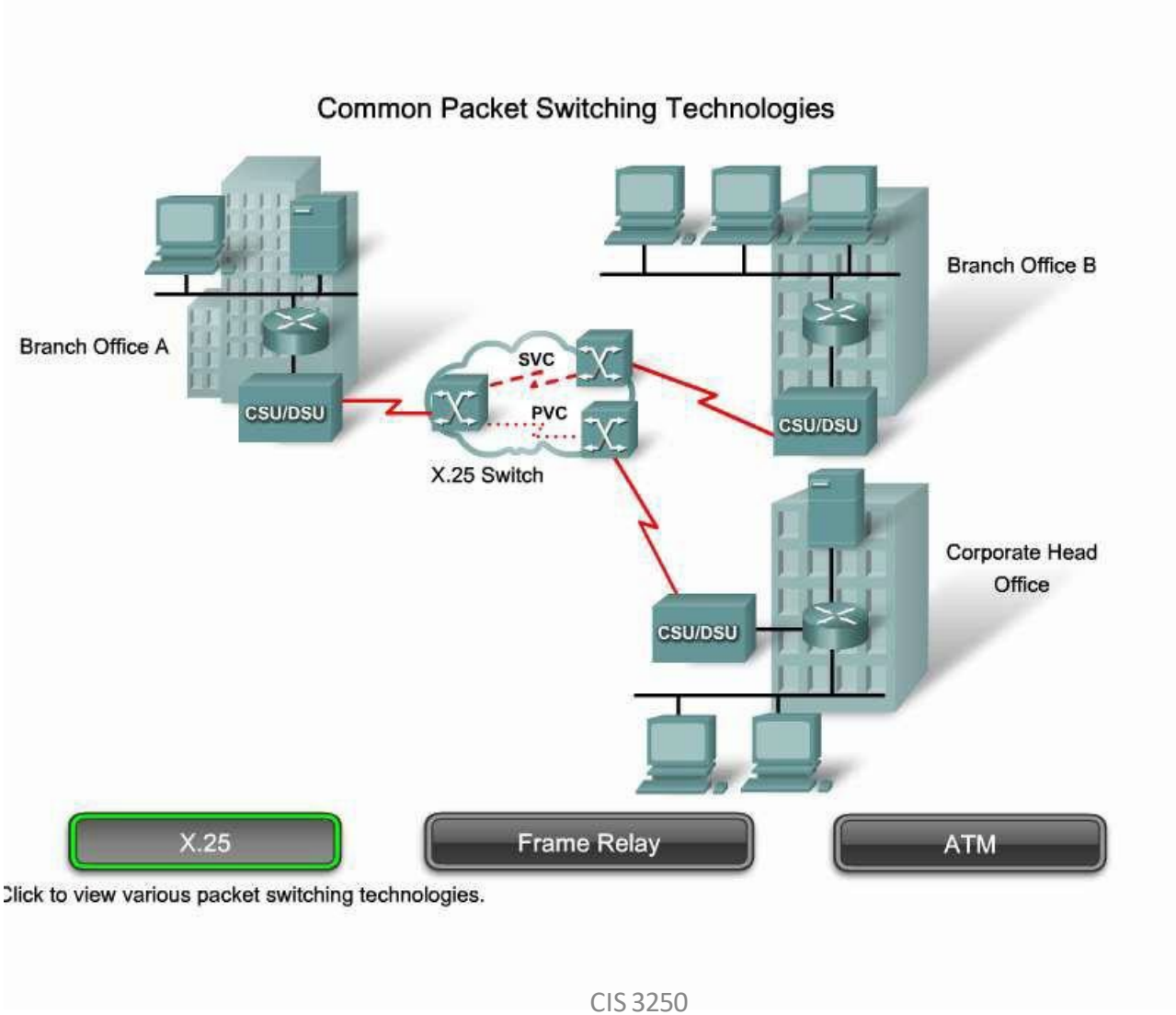
WAN Layer 2 Concepts



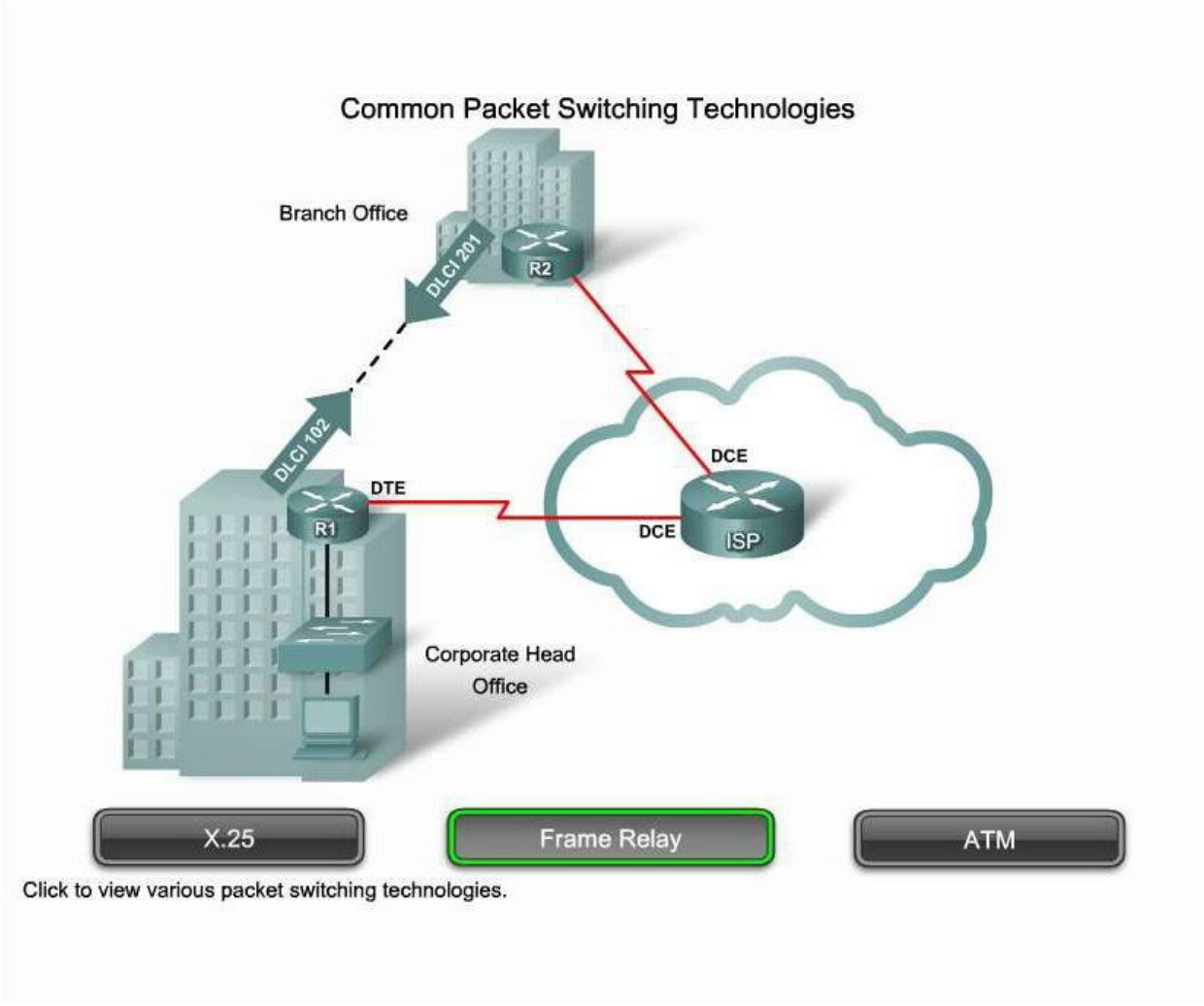
Protocol	Usage
Link Access Procedure Balanced (LAPB)	X.25
Link Access Procedure D Channel (LAPD)	ISDN D channel
Link Access Procedure Frame (LAPF)	Frame Relay
High-Level Data Link Control (HDLC)	Cisco default
Point-to-Point Protocol (PPP)	Serial WAN switched connections

The data link layer protocols define how data is encapsulated for transmission to remote sites and the mechanisms for transferring the resulting frames.

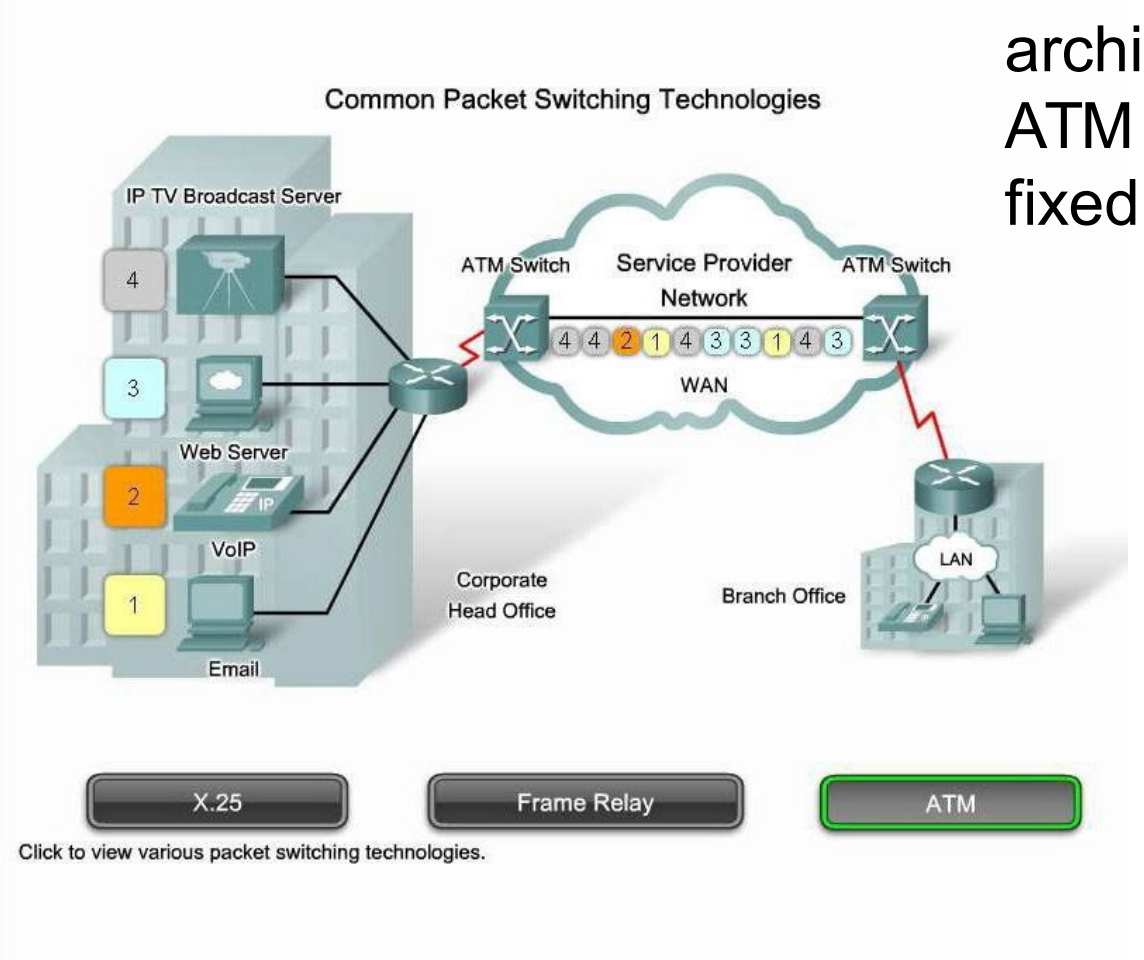
Packet Switching Technologies



Frame Relay


Common Packet Switching Technologies
Branch Office
DLCI 201
R2
DLCI 102
DTE
R1
DCE
DCE
ISP
Corporate Head Office
X.25
Frame Relay
ATM
Click to view various packet switching technologies.

ATM

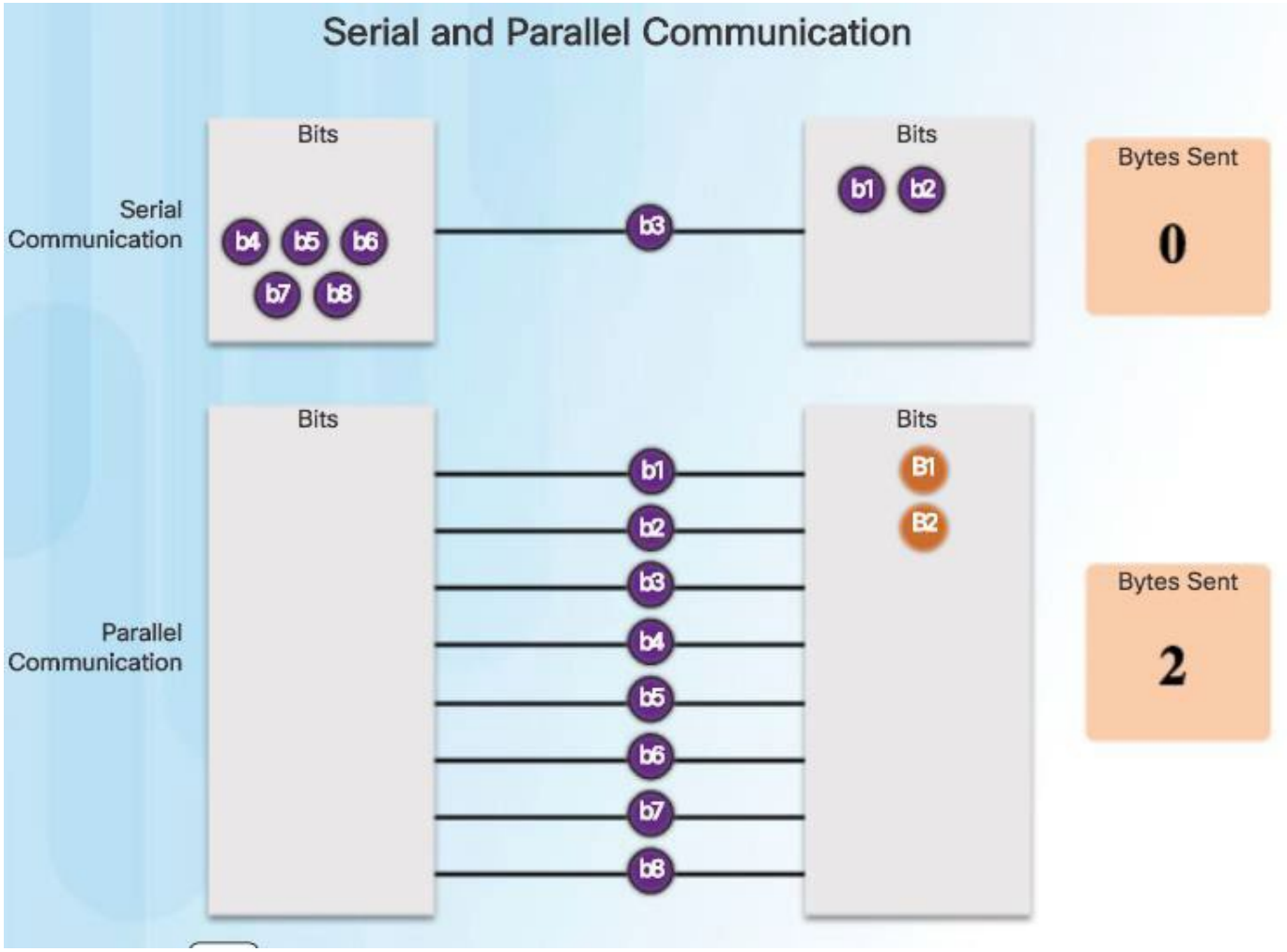


ATM uses cell-based architecture.
ATM cells are always a fixed length of 53 bytes.

Point-to-Point

- One of the most common types of WAN connection is the point-to-point connection.
- Point-to-point connections connect LANs to service provider WANs and LAN segments within an Enterprise network.
- A LAN-to-WAN point-to-point connection is also referred to as a serial connection or leased-line connection because the lines are leased from a carrier (usually a telephone company) and are dedicated for use by the company leasing the lines.
- Companies pay for a continuous connection between two remote sites, and the line is continuously active and available.

Serial and Parallel Communication



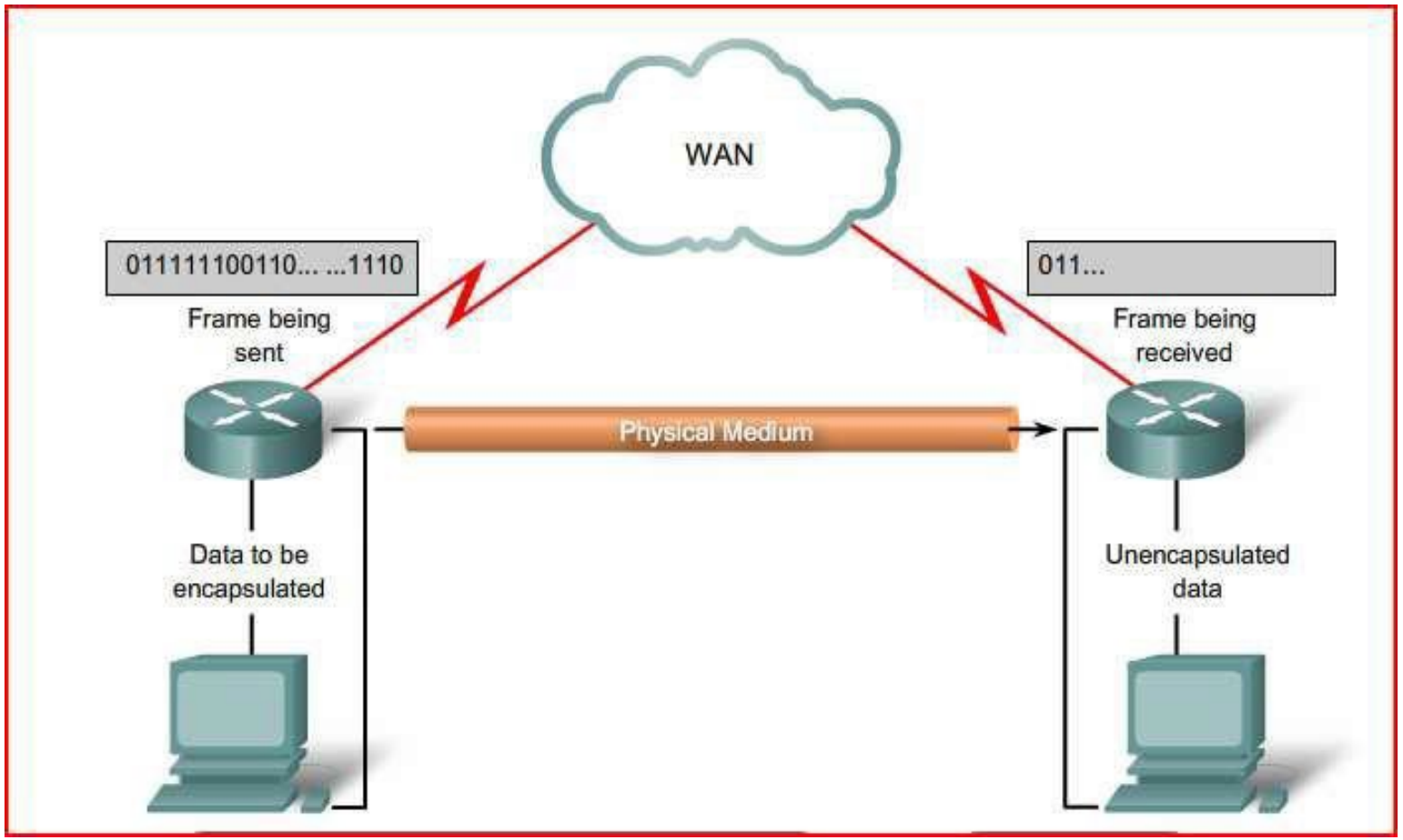
Serial Connections

- With a serial connection, information is sent across one wire, one data bit at a time.
- The 9-pin serial connector on most PCs uses two loops of wire, one in each direction, for data communication.
- Additional wires control the flow of information.
- In any given direction, data still flows over a single wire.

Parallel Connections

- A parallel connection sends the bits over more wires simultaneously.
- The 25-pin parallel port on a PC has eight data-carrying wires that carry 8 bits simultaneously. Because there are eight wires to carry the data, the parallel link theoretically transfers data eight times faster than a serial connection.
- According to this theory, a parallel connection sends a byte in the time a serial connection sends a bit.
- Clock Skew and Crosstalk limit parallel connections to shorter distances.

Serial Communication Standards



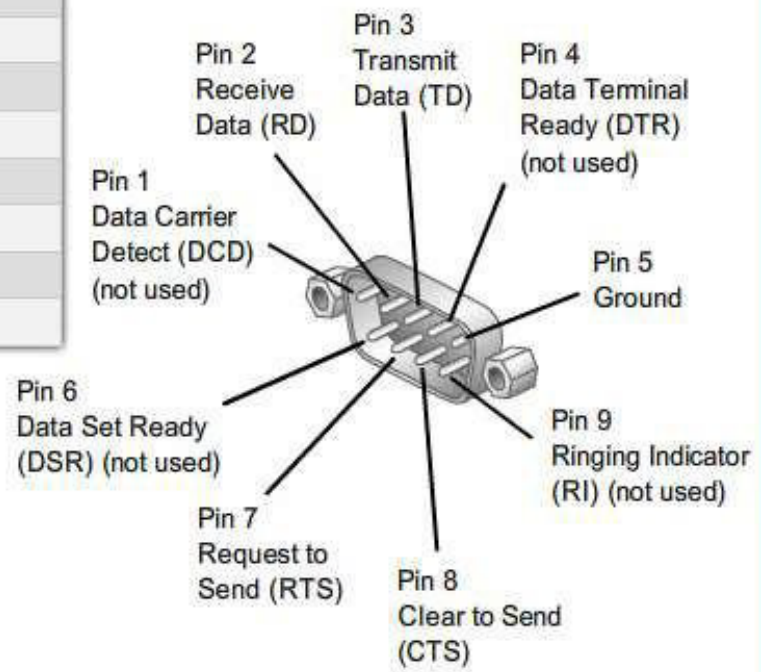
Serial Communication Standards 2

- **RS-232** - Most serial ports on personal computers conform to the RS-232C or newer RS-422 and RS-423 standards. Both 9-pin and 25-pin connectors are used. A serial port is a general-purpose interface that can be used for almost any type of device, including modems, mice, and printers
- **V.35** - Typically used for modem-to-multiplexer communication, this ITU standard for high-speed, synchronous data exchange combines the bandwidth of several telephone circuits. V.35 cables are high-speed serial assemblies designed to support higher
- **HSSI** - A High-Speed Serial Interface (HSSI) supports transmission rates up to 52 Mb/s. Engineers use HSSI to connect routers on LANs with WANs over high-speed lines such as T3 lines. HSSI is a DTE/DCE interface developed by Cisco Systems and T3plus Networking to address the need for high-speed communication over WAN links.

RS-232 Connector

9-Pin RS-232 Connector

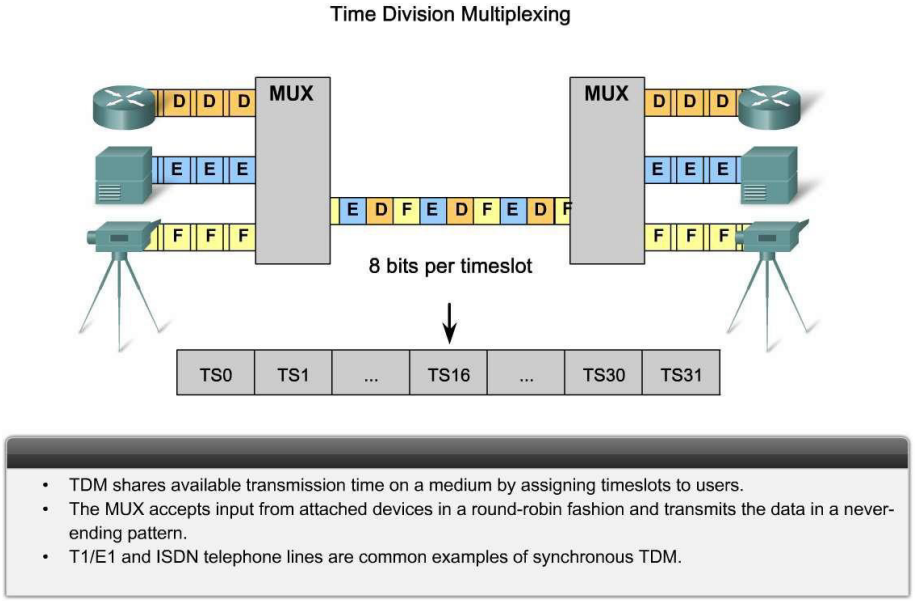
Pin Number	Signal	Description
1	DCD	Data carrier detect
2	RxD	Receive data
3	TxD	Transmit data
4	DTR	Data terminal ready
5	GND	Signal ground
6	DSR	Data set ready
7	RTS	Ready to send
8	CTS	Clear to send
9	RI	Ring indicator

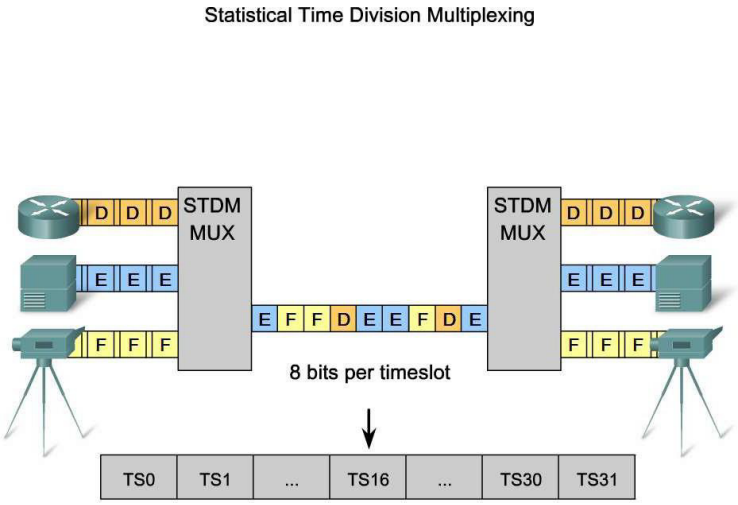


9-pin D-type RS-232 serial connector pin-out

Fundamental Concepts of Point-to-Point Serial Communication

- Two or more data streams are transported across a single physical connection using TDM





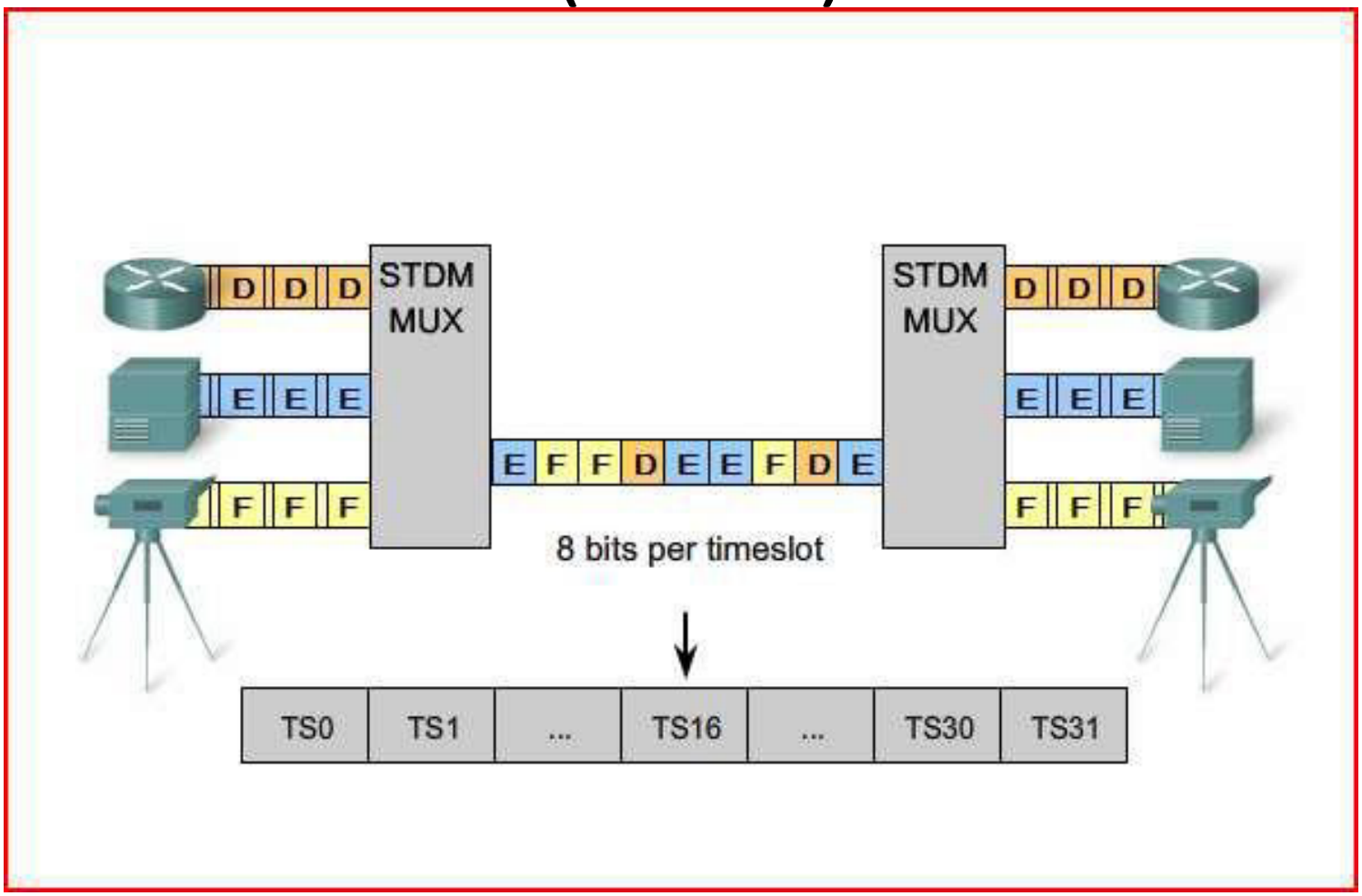
TDM

- Bell Laboratories invented time-division multiplexing (TDM) to maximize the amount of voice traffic carried over a medium.
- Before multiplexing, each telephone call required its own physical link.
- This was expensive and did not scale well. TDM divides the bandwidth of a single link into separate channels or time slots. The channels take turns using the link.
- TDM is a physical layer concept. It has no regard for the nature of the information that is being multiplexed onto the output channel. TDM is independent of the Layer 2 protocol that the input channels use.

TDM Analogy

- TDM can be explained by comparing TDM to a train with 32 railroad cars.
- A different freight company owns each car, and every day the train leaves with the 32 cars attached.
- If one of the companies has cargo to send, the car is loaded.
- If the company has nothing to send, the car remains empty but stays on the train.
- Shipping empty containers is not very efficient.
- TDM shares this inefficiency when traffic is intermittent because the time slot is still allocated even when the channel has no data to transmit.

Statistical Time Division Multiplexing (STDM)

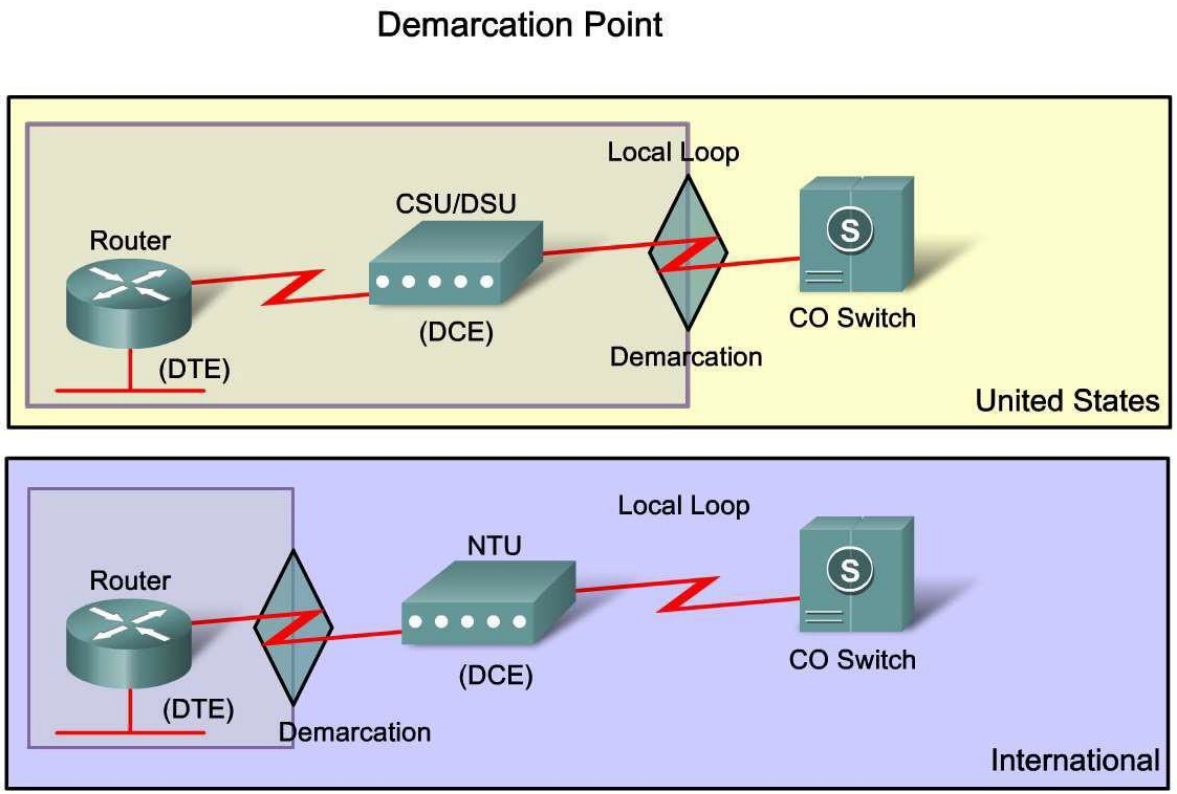


STDM Analogy

- STDM was developed to overcome this inefficiency.
- STDM uses a variable time slot length, allowing channels to compete for any free slot space.
- It employs a buffer memory that temporarily stores the data during periods of peak traffic.
- STDM does not waste high-speed line time with inactive channels using this scheme.
- Allows multiplexed channels to increase their data rate above their share if other stations are not using theirs to the full capacity
- STDM requires each transmission to carry identification information (a channel identifier).

Demarcation Point

- Define the location of the demarcation point relative to customer and service provider networks

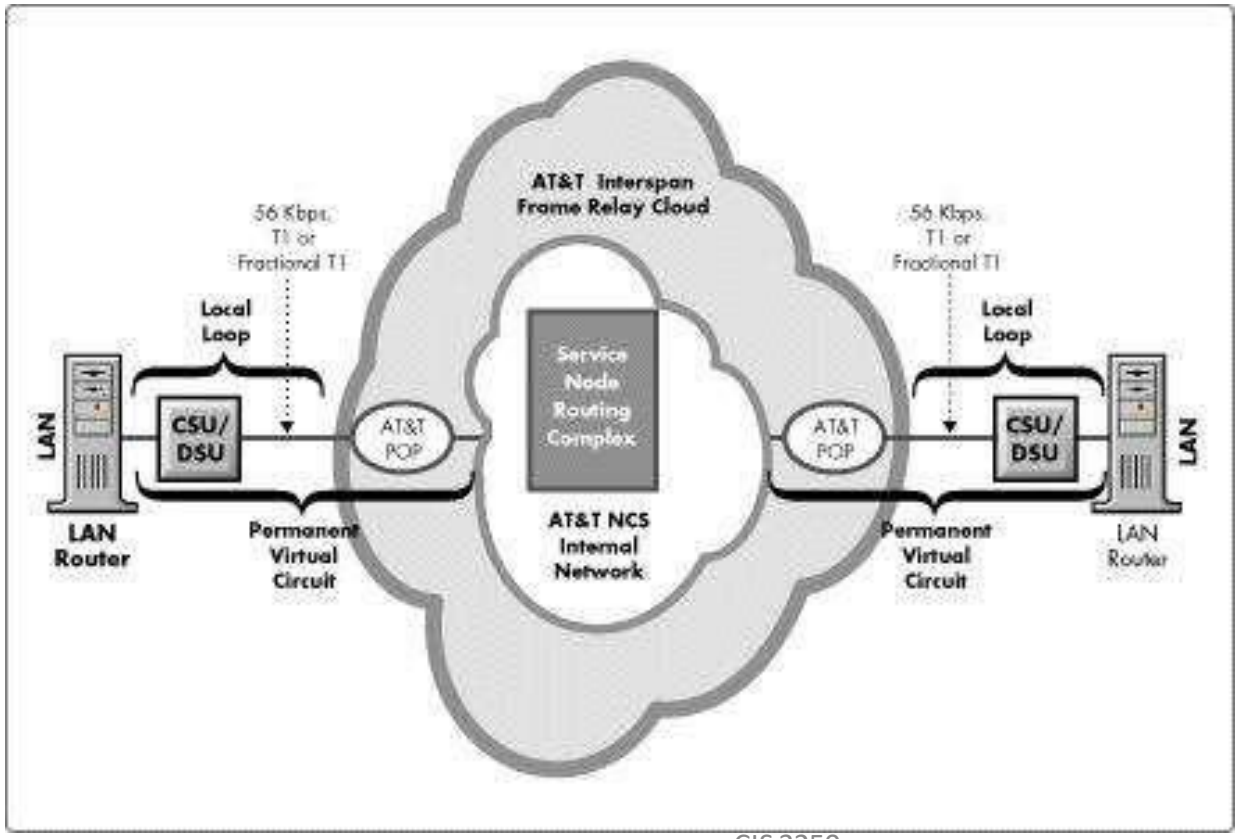


Demarcation

- Prior to deregulation in North America and other countries, telephone companies owned the local loop, including the wiring and equipment on customers' premises.
- Deregulation forced telephone companies to unbundle their local loop infrastructure to allow other suppliers to provide equipment and services.
- This led to a need to delineate which part of the network the telephone company owned and which part the customer owned. This point of delineation is the demarcation point or *demarc*.
- The demarcation point marks the point where your network interfaces with the network owned by another organization. In telephone terminology, this is the interface between customer-premises equipment (CPE) and network service provider equipment

Local Loop

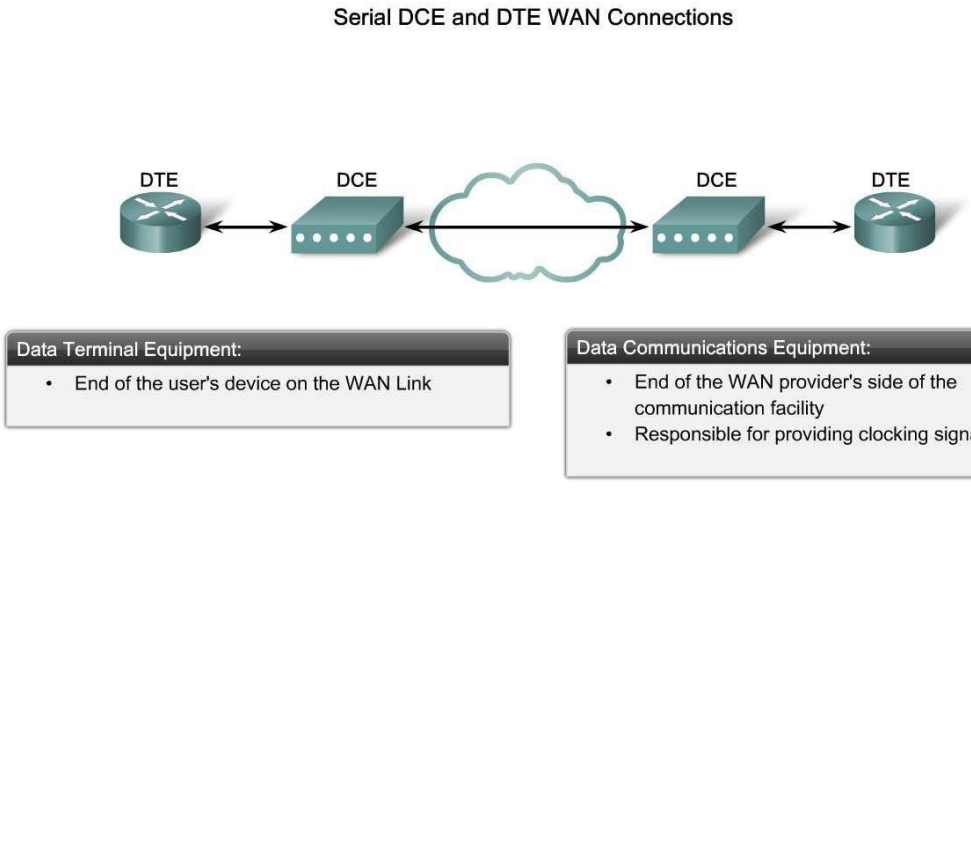
- physical link or circuit that connects from the demarcation point of the customer premises to the edge of the carrier or telecommunications service provider's network

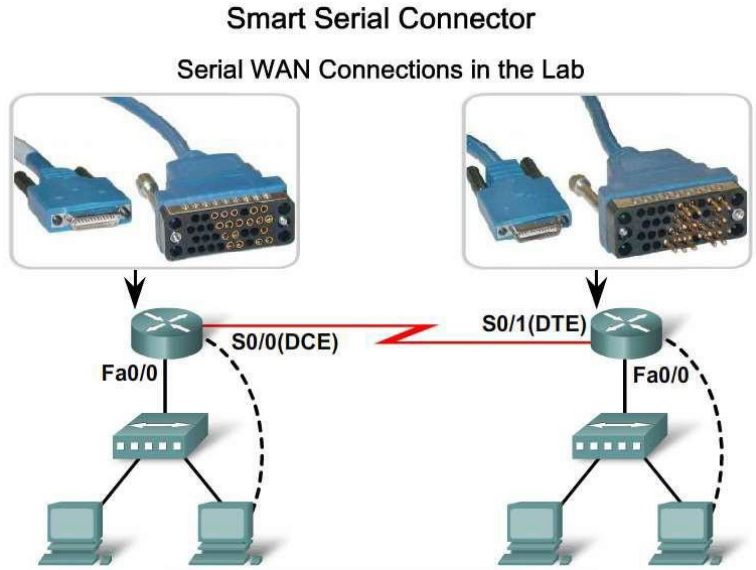


Source:
http://support.novell.com/techcenter/articles/ana19960603.html

Fundamental Concepts of Point-to-Point Serial Communication

- DTE and DCE with relative to the location of devices in a network

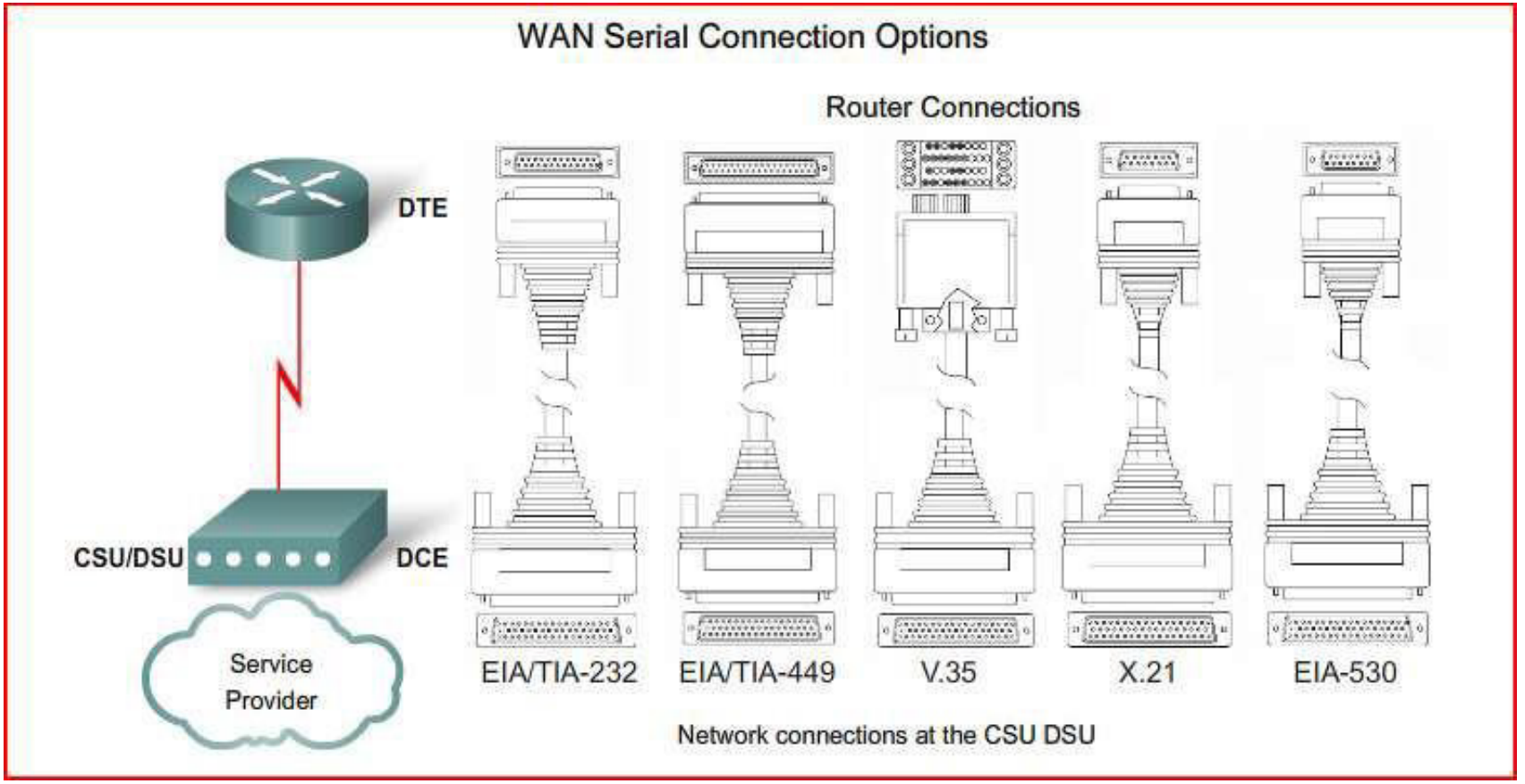




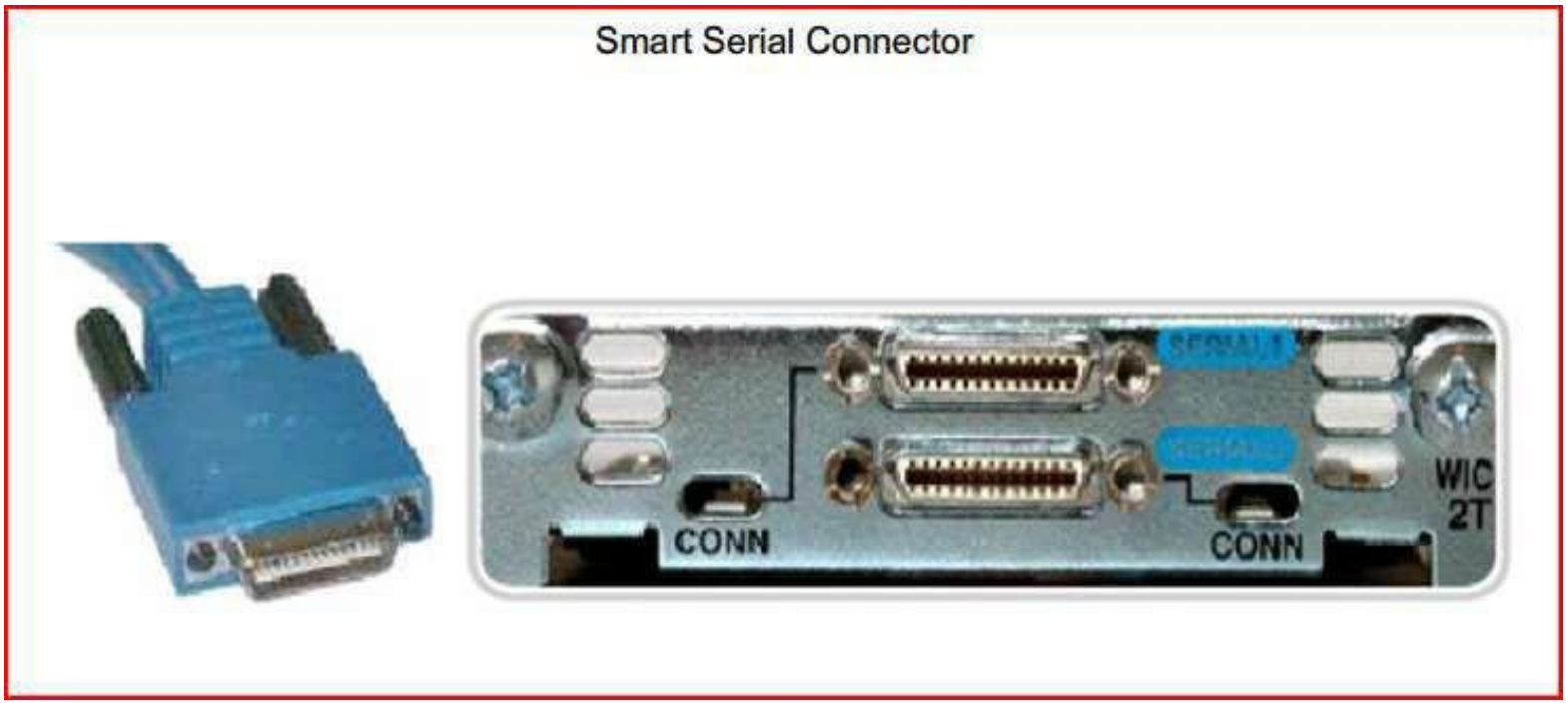
DTE - DCE

- From the point of view of connecting to the WAN, a serial connection has a DTE device at one end of the connection and a DCE device at the other end. The connection between the two DCE devices is the WAN service provider transmission network. In this case:
- The Customer Premises Equipment (CPE), which is generally a router, is the DTE. If it connects directly to the service provider network, the DTE could also be a terminal, computer, printer, or fax machine.
- The DCE, commonly a modem or CSU/DSU, is the device used to convert the user data from the DTE into a form acceptable to the WAN service provider transmission link. This 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.

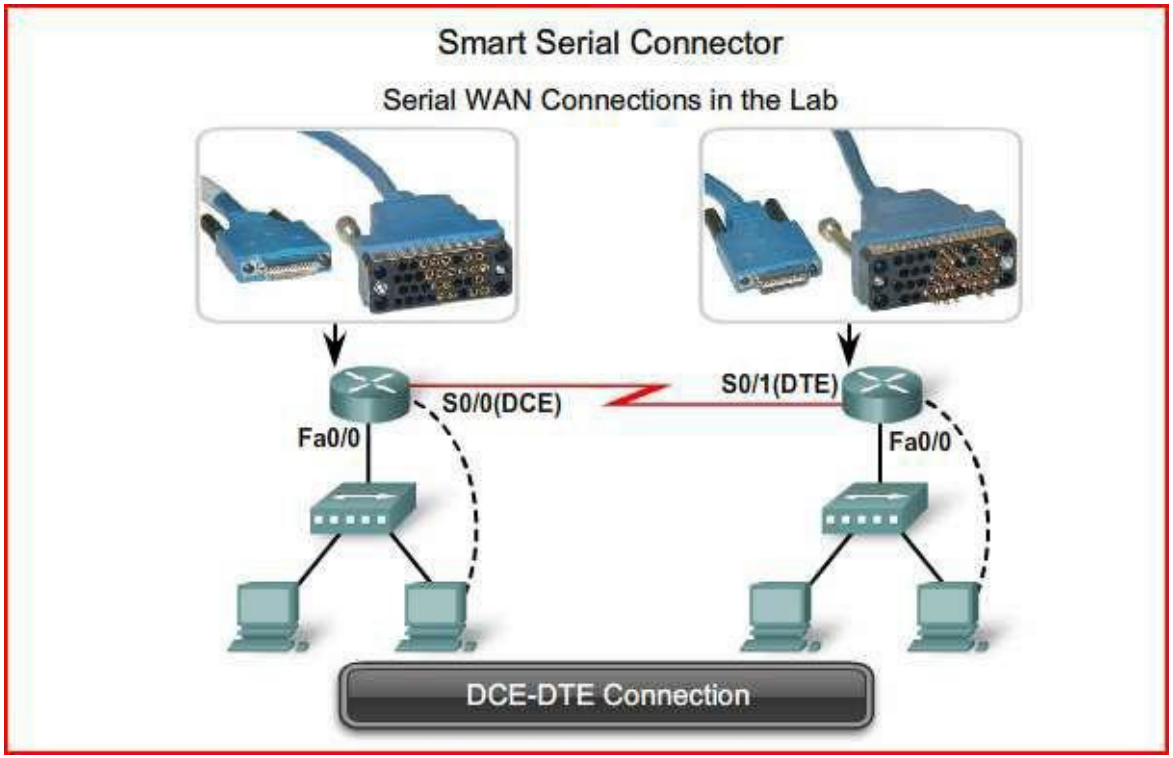
WAN Serial Connections



HSSI



DTE – DCE Connections in the Lab



Encapsulation

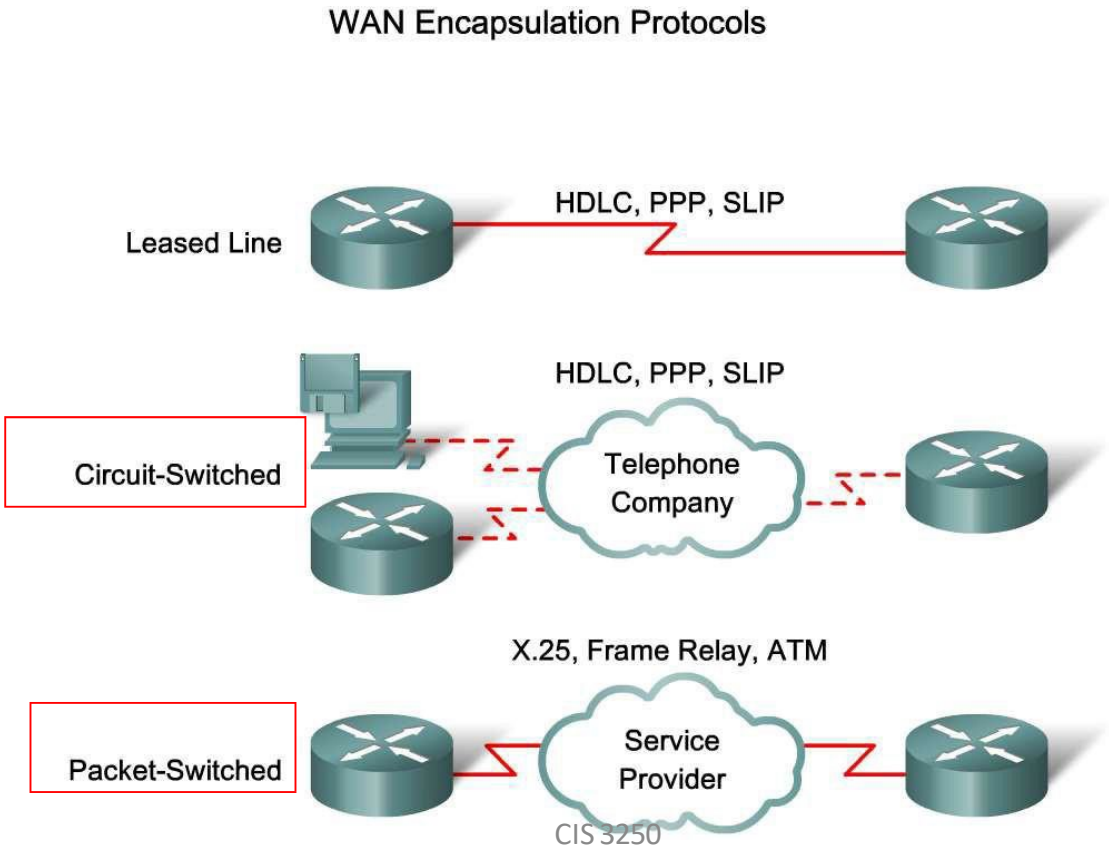
- **High-Level Data Link Control (HDLC):** This is the default encapsulation type on point-to-point connections, dedicated links, and circuit-switched connections when the link uses two Cisco devices. HDLC is now the basis for synchronous PPP, which many servers use to connect to a WAN, most commonly the Internet.
- **Point-to-Point Protocol (PPP):** Provides router-to-router and host-to-network connections over **synchronous** and **asynchronous** circuits. PPP works with several network layer protocols, such as IP and Internetwork Packet Exchange (IPX). PPP also has built-in security mechanisms such as PAP and CHAP. Most of this chapter deals with PPP.
- **Serial Line Internet Protocol (SLIP):** A standard protocol (legacy) for point-to-point serial connections using TCP/IP. PPP has largely displaced SLIP.

Encapsulation Continued

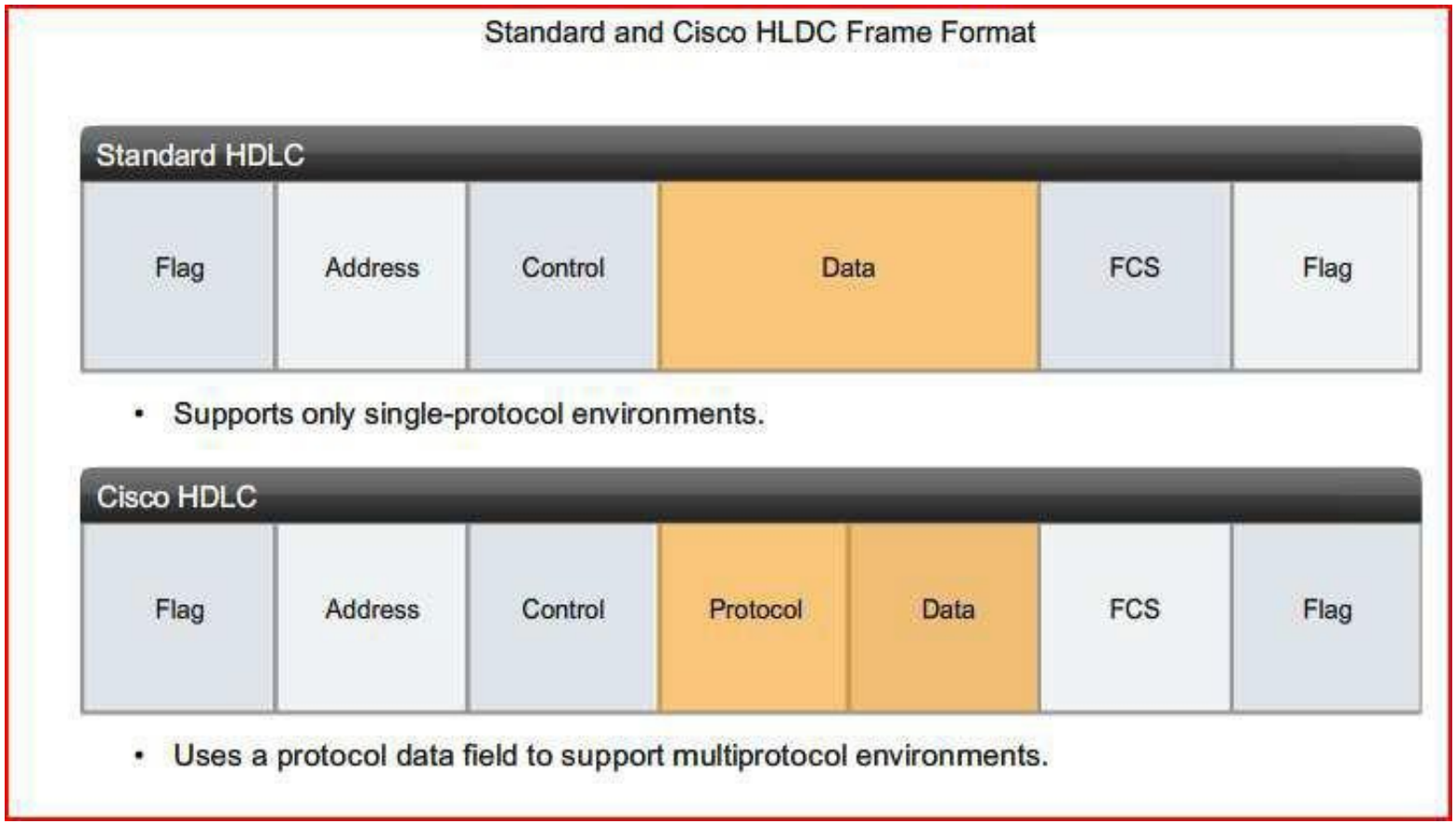
- **X.25/Link Access Procedure, Balanced** (LAPB): ITU-T standard that defines how connections between a DTE and DCE are maintained for remote terminal access and computer communications in public data networks. X.25 specifies LAPB, a data link layer protocol. X.25 is a predecessor to Frame Relay.
- **Frame Relay:** Industry standard, switched, data link layer protocol that handles multiple virtual circuits. Frame Relay is a next-generation protocol after X.25. Frame Relay eliminates some of the time-consuming processes (such as error correction and flow control) employed in X.25. The next chapter covers Frame Relay.
- **ATM:** The international standard for cell relay in which devices send multiple service types (such as voice, video, or data) in fixed-length (53-byte) cells. ATM takes advantage of high-speed transmission media such as E3, SONET, and T3.

Describe the Fundamental Concepts of Point-to-Point Serial Communication

high-level data link control (HDLC) uses one of three frame types to encapsulate data



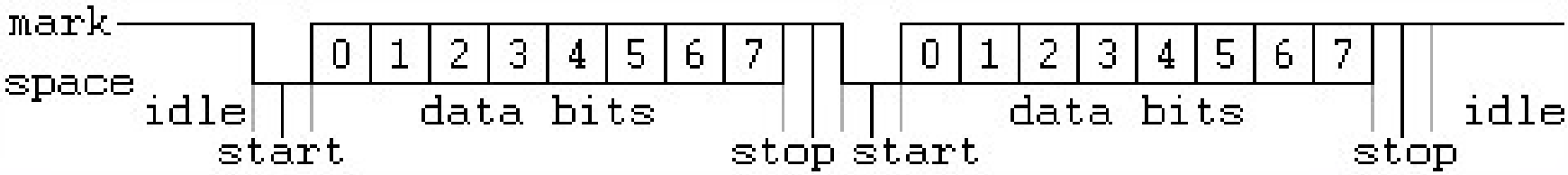
HDLC Frame Format



HDLC Encapsulation

- HDLC is a data link layer protocol developed by the International Organization for Standardization (ISO). The current standard for HDLC is ISO 13239. HDLC provides both connection-oriented and connectionless services.
- HDLC uses synchronous serial transmission to provide error-free communication between two points. The HDLC Layer 2 framing structure allows for flow and error control through the use of acknowledgments. All frame types have the same format.
- HDLC uses a frame delimiter, or flag, to mark the beginning and the end of each frame.
- Cisco has developed an extension to the HLDC protocol to solve the inability to provide multiprotocol support. Although Cisco HLDC (also referred to as cHDLC) is proprietary, Cisco has allowed many other network equipment vendors to implement it. Cisco HDLC frames contain a field for identifying the network protocol being encapsulated.

Asynchronous



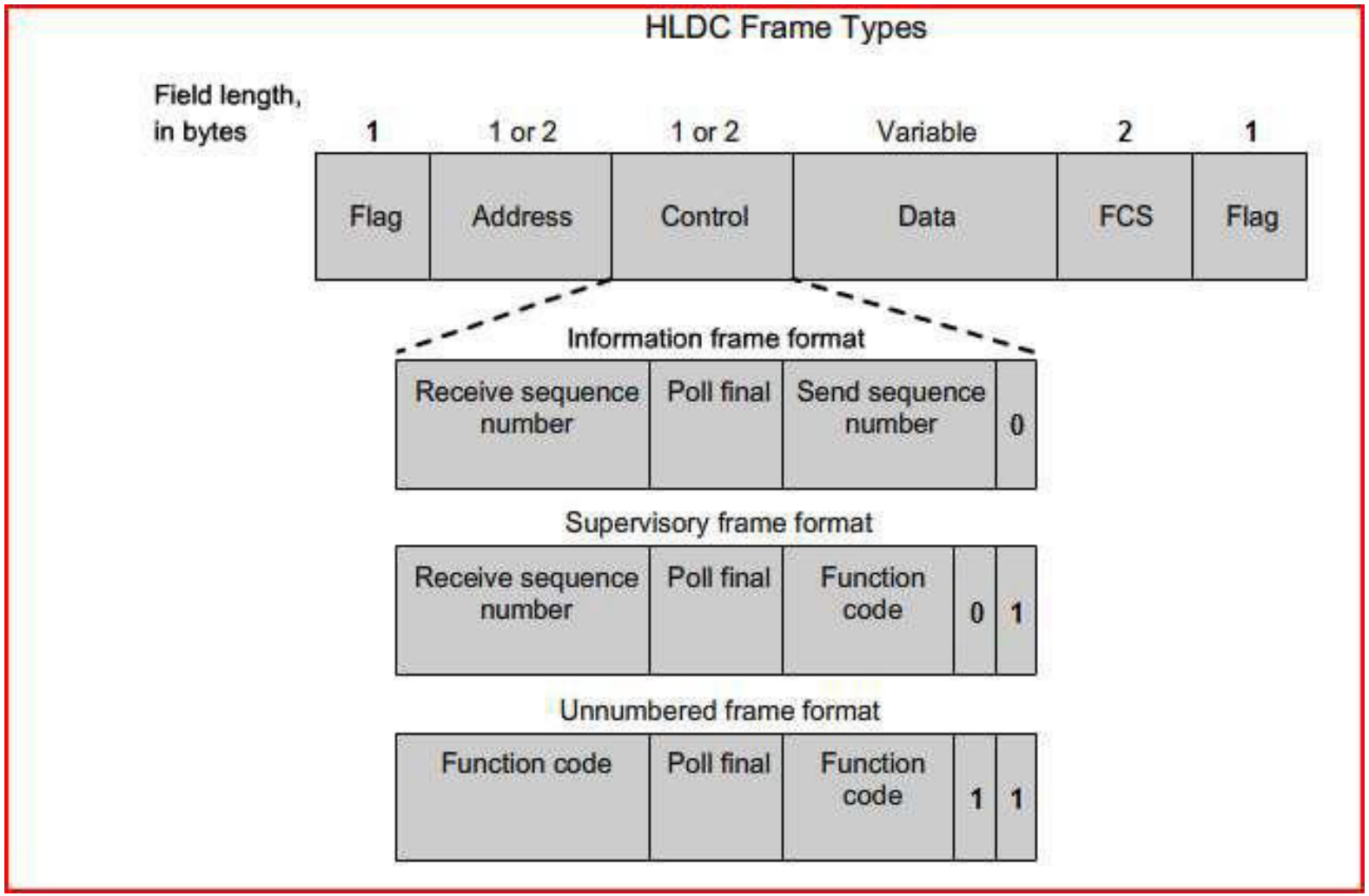
- Asynchronously transmitted data is preceded with a start bit which indicates to the receiver that a word (a chunk of data broken up into individual bits) is about to begin.
- To avoid confusion with other bits, the start bit is twice the size of any other bit in the transmission.
- The end of a word is followed by a stop bit, which tells the receiver that the word has come to an end, that it should begin looking for the next start bit, and that any bits it receives before getting the start bit should be ignored

Source: http://www.quatech.com/support/comm-over-asyncserial.php

Synchronous

- Synchronous communication takes place between a transmitter and a receiver operating on synchronized clocks.
- In a synchronous system, the communication partners have a short conversation before data exchange begins.
- In this conversation, they align their clocks and agree upon the parameters of the data transfer, including the time interval between bits of data.
- Any data that falls outside these parameters will be assumed to be either in error or a placeholder used to maintain synchronization.
- (Synchronous lines are constantly active in order to maintain synchronization, thus the need for placeholders between valid data.)

HDLC Frame Types



HDLC Frame Fields

- HDLC defines three types of frames, each with a different control field format.
- **Flag** - The flag field initiates and terminates error checking. The frame always starts and ends with an 8-bit flag field. The bit pattern is 01111110. Because there is a likelihood that this pattern occurs in the actual data, the sending HDLC system always inserts a 0 bit after every five 1s in the data field, so in practice the flag sequence can only occur at the frame ends. The receiving system strips out the inserted bits. When frames are transmitted consecutively, the end flag of the first frame is used as the start flag of the next frame.
- **Address** - The address field contains the HDLC address of the secondary station. This address can contain a specific address, a group address, or a broadcast address. A primary address is either a communication source or a destination, which eliminates the need to include the address of the primary.

HDLC Frame Types

- **Control** - The control field uses three different formats, depending on the type of HDLC frame used:
- **Information** (I) frame: carry upper layer information and some control information. This frame sends and receives sequence numbers, and the poll final (P/F) bit performs flow and error control. The send sequence number refers to the number of the frame to be sent next. The receive sequence number provides the number of the frame to be received next. Both sender and receiver maintain send and receive sequence numbers. A primary station uses the P/F bit to tell the secondary whether it requires an immediate response. A secondary station uses the P/F bit to tell the primary whether the current frame is the last in its current response.
- **Supervisory** (S) frame: provide control information. An S-frame can request and suspend transmission, report on status, and acknowledge receipt of I-frames. S-frames do not have an information field.
- **Unnumbered** (U) frame: support control purposes and are not sequenced. A U-frame can be used to initialize secondaries. Depending on the function of the U-frame, its control field is 1 or 2 bytes. Some U-frames have an information field.

Describe the Fundamental Concepts of Point-to-Point Serial Communication

Configuring HLDC Encapsulation

```
Router(config-if)#encapsulation hdlc
```

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

Serial Interface Configuration

- IP Address and Subnet Mask
- Clockrate on the DCE end
- No shutdown

Show Interface Command

```
R1#show interfaces 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 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:03, output 00:00:04, output hang never
  Last clearing of "show interface" counters 1w0d
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     219 packets input, 15632 bytes, 0 no buffer
     Received 218 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     217 packets output, 14919 bytes, 0 underruns
     0 output errors, 0 collisions, 107 interface resets
     0 output buffer failures, 0 output buffers swapped out
     12 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Serial Interface States

- The show interface serial command returns one of five possible states.
- **Serial x is up, line protocol is up**
- Serial x is up, line protocol is down
- Serial x is down, line protocol is down
- Serial x is up, line protocol is down (disabled)
- Serial x is administratively down, line protocol is down

Troubleshooting a serial Interface

- http://www.cisco.com/en/US/docs/internetworking/troubleshooting/guide/tr1915.html
- http://www.thebryantadvantage.com/CCENTCCNACiscoExamTrainingLineProtocolTroubleshooting.htm

Serial X Down – Line Protocol Down

Troubleshooting a Serial Interface

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 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.

Protocol Down

R3#sho ip int brief

Interface	IP-Address	OK? Method Status	Protocol
Serial0/0	unassigned	YES unset administratively down	down
Serial0/1	192.168.1.129	YES manual up	down
Serial0/2	unassigned	YES unset administratively down	down
Serial0/3	unassigned	YES unset administratively down	down

R2#show ip interface brief

Interface	IP-Address	OK? Method Status	Protocol
Serial0/0	192.168.1.2	YES manual up	up
Serial0/1	192.168.1.130	YES manual up	down

Show Controllers serial R3

R3#show controllers serial 0/1
Interface Serial0/1
Hardware is PowerQUICC MPC860
DTE V.35 clocks stopped.
idb at 0x81D427D8, driver data structure at 0x81D4ABD4
SCC Registers:
General [GSMR]=0x2:0x00000030, Protocol-specific [PSMR]=0x8
Events [SCCE]=0x0000, Mask [SCCM]=0x001F, Status [SCCS]=0x00
Transmit on Demand [TODR]=0x0, Data Sync [DSR]=0x7E7E
Interrupt Registers:
Config [CICR]=0x00367F80, Pending [CIPR]=0x00008804
Mask [CIMR]=0x08200002, In-srv [CISR]=0x00000000
Command register [CR]=0x6C0

Show Controllers Serial R2

R2#show controllers serial 0/1

Interface Serial0/1

Hardware is PowerQUICC MPC860

DCE V.35, no clock

idb at 0x81D427D8, driver data structure at 0x81D4ABD4

SCC Registers:

General [GSMR]=0x2:0x00000030, Protocol-specific [PSMR]=0x8

Events [SCCE]=0x0000, Mask [SCCM]=0x001F, Status [SCCS]=0x00

Transmit on Demand [TODR]=0x0, Data Sync [DSR]=0x7E7E

Interrupt Registers:

Config [CICR]=0x00367F80, Pending [CIPR]=0x00008004

Mask [CIMR]=0x48204002, In-srv [CISR]=0x00000000

Command register [CR]=0x6C0

Show Controllers

```
R1#show controllers serial 0/0/0
Interface Serial0/0/0
Hardware is GT96K
DCE V.35, clock rate 64000
idb at 0x62938244, driver data structure at 0x6293A608
wic_info 0x6293AC04
Physical Port 0, SCC Num 0
MPSC Registers:
MMCR_L=0x000304C0, MMCR_H=0x00000000, MPCR=0x00000000
CHR1=0x00FE007E, CHR2=0x00000000, CHR3=0x000005F4, CHR4=0x00000000
CHR5=0x00000000, CHR6=0x00000000, CHR7=0x00000000, CHR8=0x00000000
CHR9=0x00000000, CHR10=0x00003008
SDMA Registers:
SDC=0x00002201, SDCM=0x00000080, SGC=0x0000C000
CRDP=0x073BD020, CTDP=0x073BD450, FTDB=0x073BD450
Main Routing Register=0x00038E00 BRG Conf Register=0x0005023F
Rx Clk Routing Register=0x76583888 Tx Clk Routing Register=0x76593910
GPP Registers:
Conf=0x43430002, Io=0x4646CA50, Data=0x7F6B3FAD, Level=0x80004
Conf0=0x43430002, Io0=0x4646CA50, Data0=0x7F6B3FAD, Level0=0x80004
0 input aborts on receiving flag sequence
0 throttles, 0 enables
0 overruns
0 transmitter underruns
 --More--
```

Clock Rate – What does it do?

R2#show interface serial 0/1 | include BW

MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,

R2#show controllers serial 0/1 | include clock

DCE V.35, clock rate 115200

R2#show controllers serial 0/0 | include clock

DTE V.35 TX and RX clocks detected.<clock rate 19200>

R2#show interface serial 0/0 | include BW

MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec

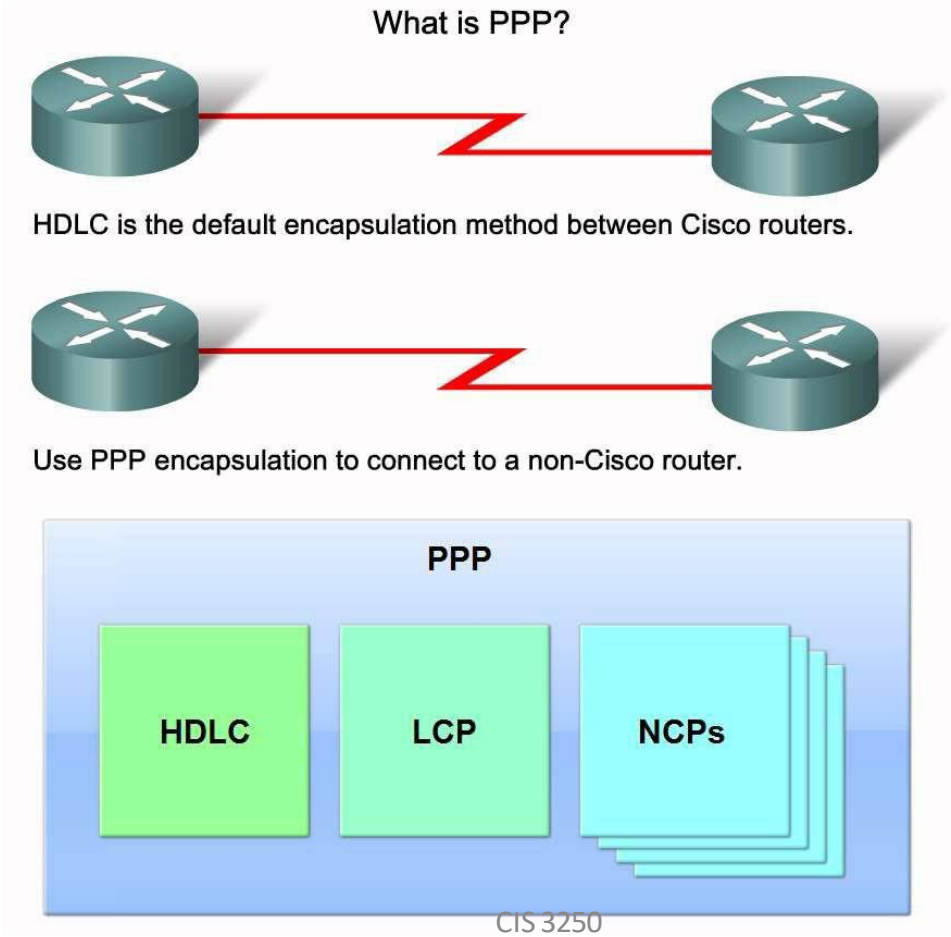
Effect of Clock Rate

R2#ping 192.168.1.1 <clock rate 19200 >
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 92/92/96 ms

R2#ping 192.168.1.130 <clock rate 115200 >
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.130, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/16/20 ms

Describe Point-to-Point Concepts

- Describe PPP in terms of its use in WAN links



What is PPP

- HDLC is the default serial encapsulation method between two Cisco routers. With an added protocol type field, the Cisco version of HDLC is proprietary. Thus, Cisco HDLC can only work with other Cisco devices. Connections to a non-Cisco router require PPP encapsulation.
- PPP encapsulation has been designed to retain compatibility with the most commonly used supporting hardware.
- 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 includes many features not available in HDLC:
    - The link quality management feature monitors the quality of the link. If too many errors are detected, PPP takes the link down.
    - PPP supports PAP and CHAP authentication.

PPP Components

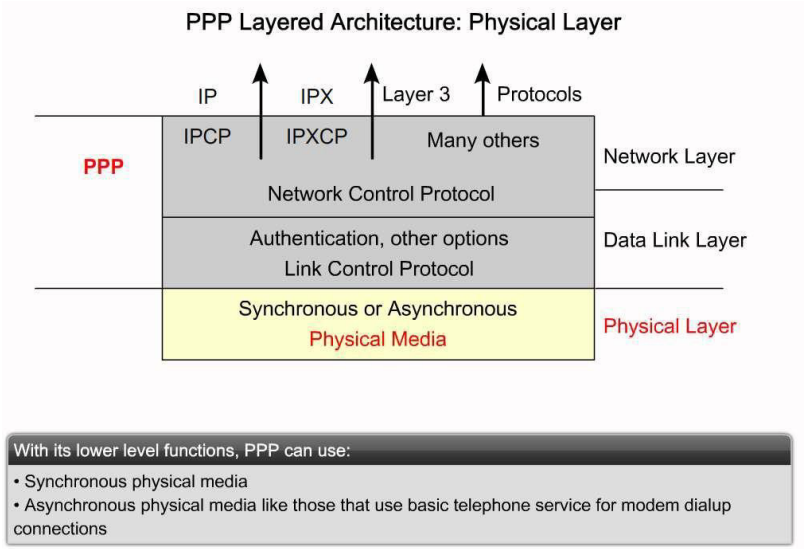
- PPP contains three main components:
- HDLC protocol for encapsulating datagrams over point-to-point links.
- Extensible Link Control Protocol (LCP) to establish, configure, and test the data link connection.
- Family of Network Control Protocols (NCPs) for establishing and configuring different network layer protocols.
- PPP allows the simultaneous use of multiple network layer protocols. Some of the more common NCPs are Internet Protocol Control Protocol, Appletalk Control Protocol, Novell IPX Control Protocol, Cisco Systems Control Protocol, SNA Control Protocol, and Compression Control Protocol.

PPP Operation

- PPP operates across any DTE/DCE interface (RS-232-C, RS-422, RS-423, or V.35).
- The only absolute requirement imposed by PPP is a duplex circuit, either dedicated or switched, that can operate in either an asynchronous or synchronous bit-serial mode, transparent to PPP link layer frames.
- PPP does not impose any restrictions regarding transmission rate other than those imposed by the particular DTE/DCE interface in use.
- Most of the work done by PPP is at the data link and network layers by the LCP and NCPs.
- The LCP sets up the PPP connection and its parameters, the NCPs handle higher layer protocol configurations, and the LCP terminates the PPP connection.

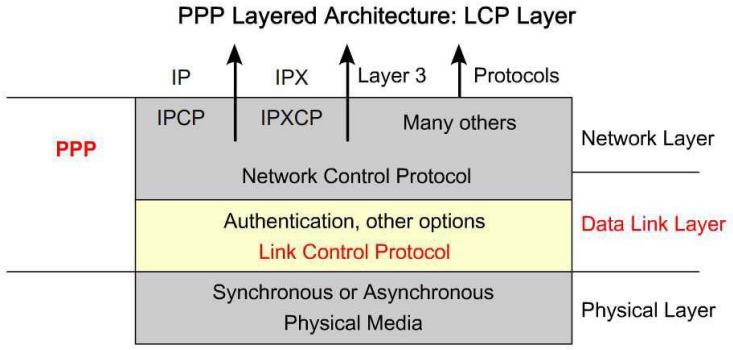
Describe Point-to-Point Concepts

- Describe the general function of each layer of PPP architecture



With its lower level functions, PPP can use:

- Synchronous physical media
- Asynchronous physical media like those that use basic telephone service for modem dialup connections

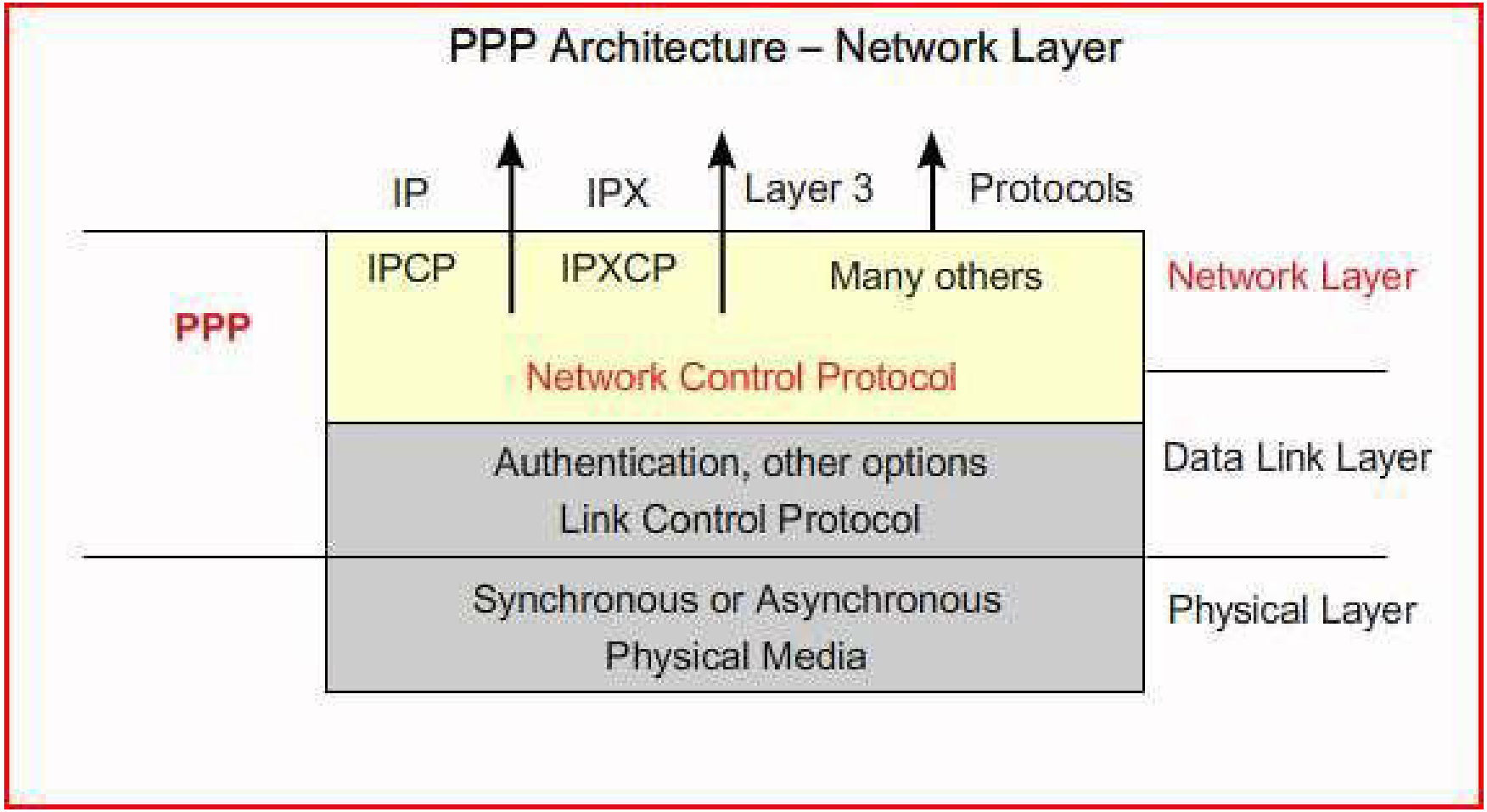


PPP offers service options in LCP and is primarily used for negotiation and frame checking when implementing the point-to-point controls specified by an administrator.

Link Control Protocol - LCP

- The LCP is the real working part of PPP. It sits on top of the physical layer and establishes, configures, and tests the data link connection. The LCP also negotiates and sets up control options on the WAN data link, which are handled by the NCPs.
- The 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
- PPP also uses the LCP to agree automatically on encapsulation formats (authentication, compression, error detection) as soon as the link is established.

Network Control Protocol

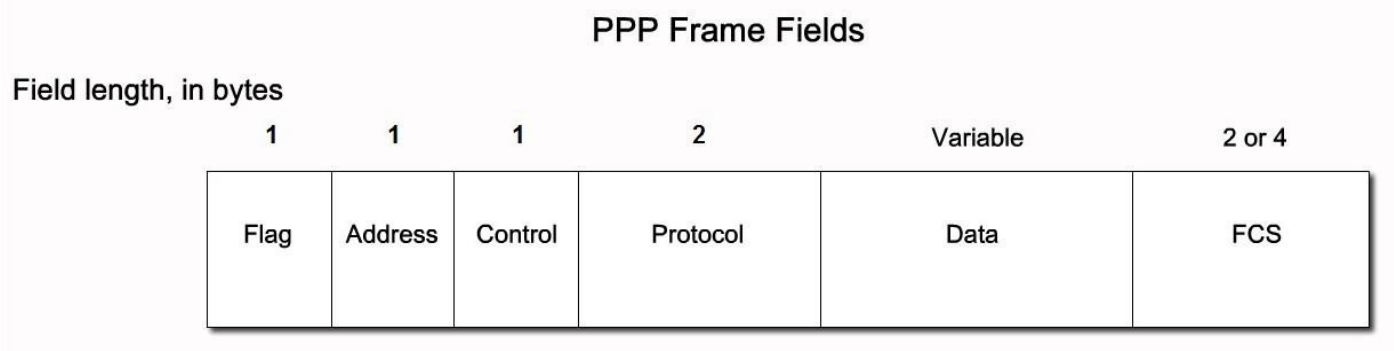


Network Control Protocol - NCP

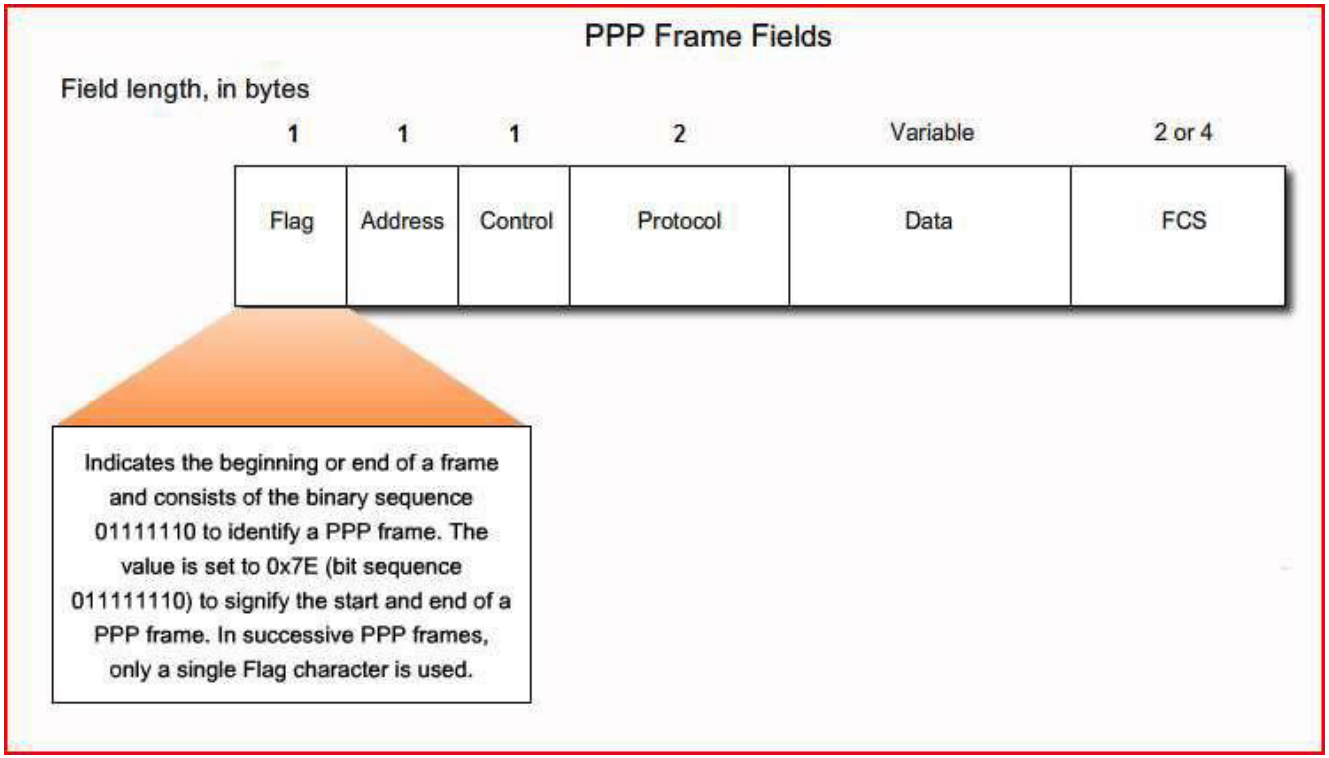
- PPP permits multiple network layer protocols to operate on the same communications link. For every network layer protocol used, PPP uses a separate NCP. For example, IP uses the IP Control Protocol (IPCP), and IPX uses the Novell IPX Control Protocol (IPXCP).
- NCPs include functional fields containing standardized codes (PPP protocol field numbers) to indicate the network layer protocol that PPP encapsulates.
- Each NCP manages the specific needs required by its respective network layer protocols. The various NCP components encapsulate and negotiate options for multiple network layer protocols.
- Using NCPs to configure the various network layer protocols is explained and practiced later.

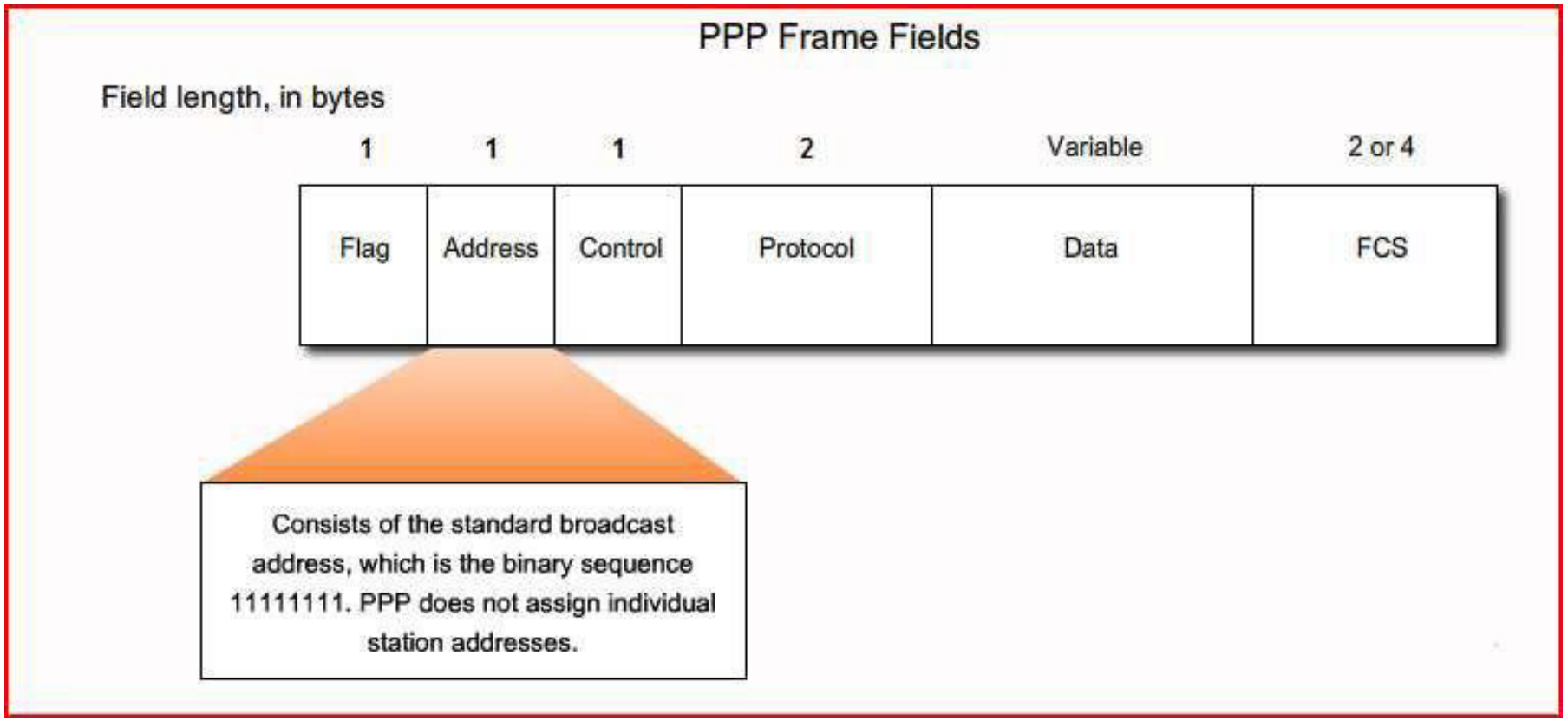
Describe Point-to-Point Concepts

- Describe the purpose and format of each of the fields in a PPP frame

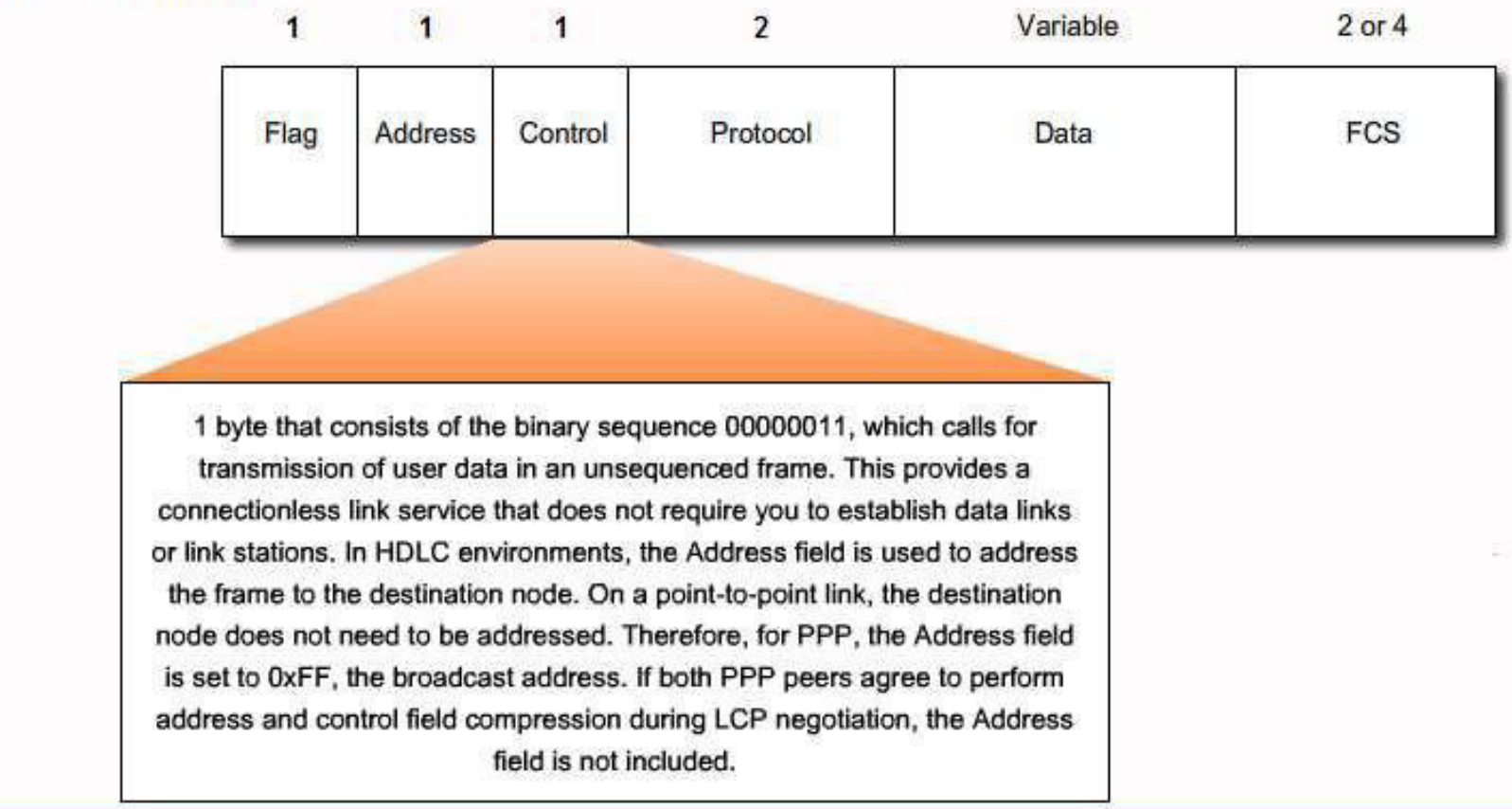


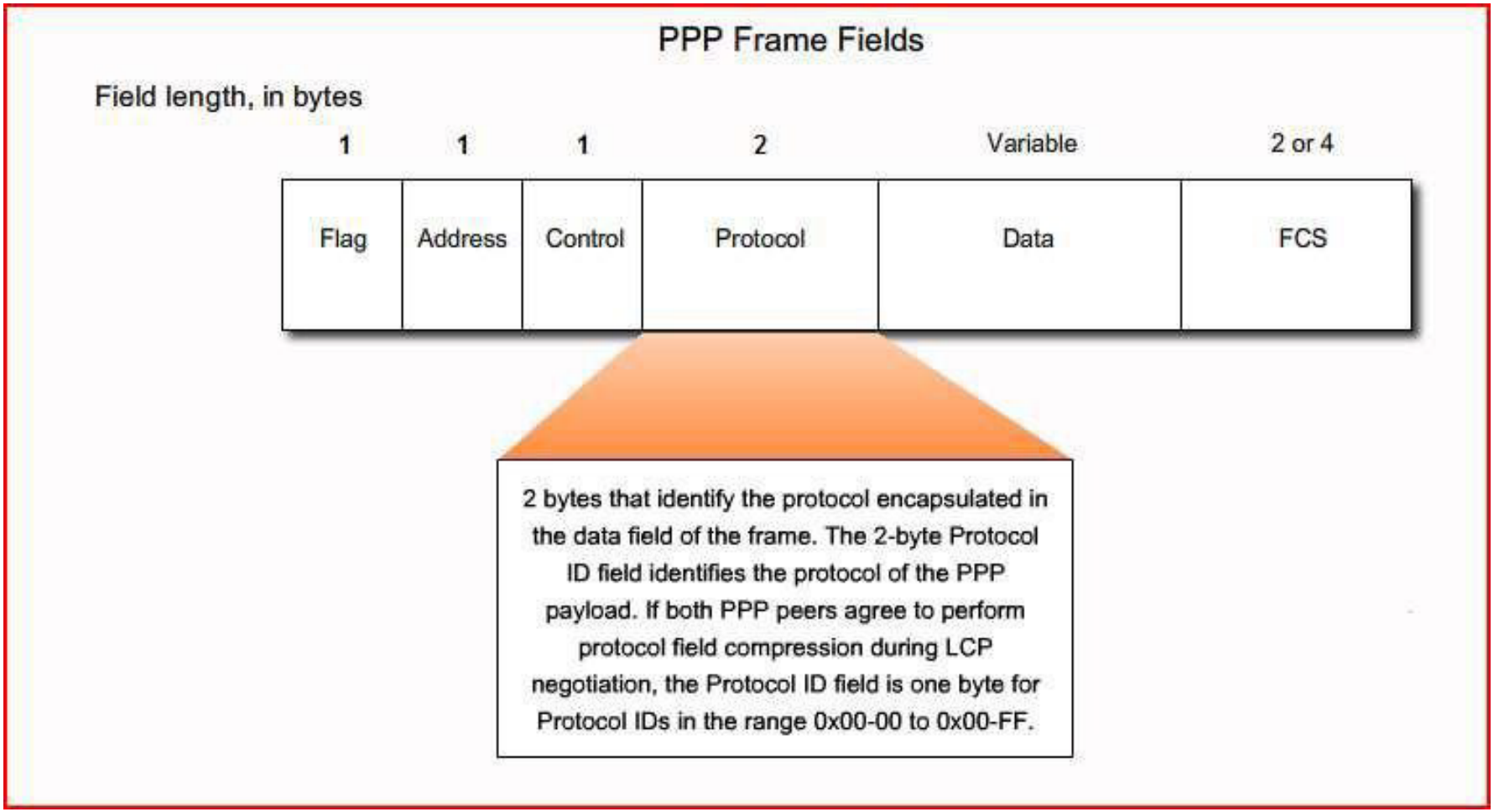
PPP Frame Fields

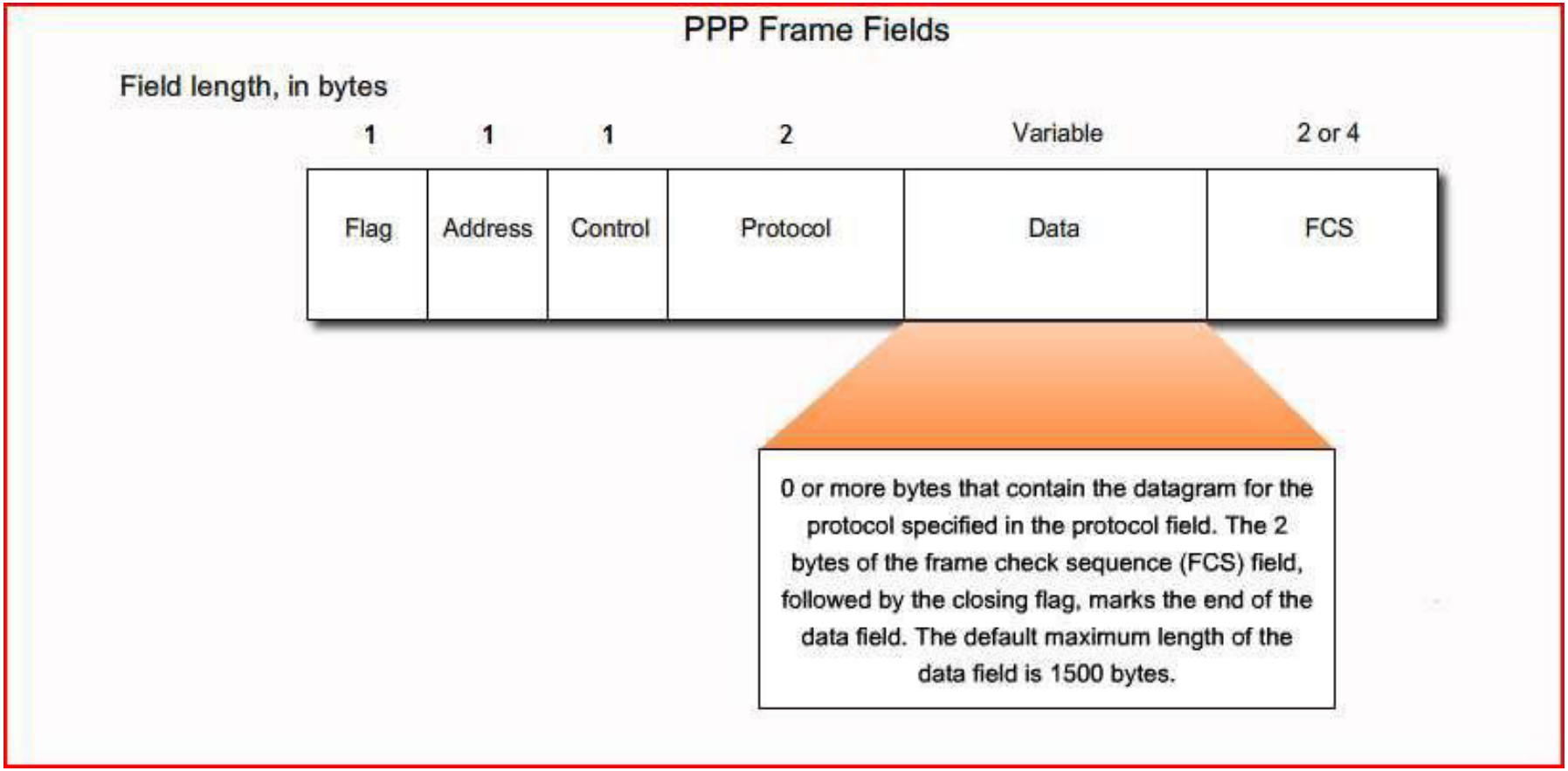



PPP Frame Fields
Field length, in bytes
1
1
1
2
Variable
2 or 4
Flag
Address
Control
Protocol
Data
FCS
Consists of the standard broadcast address, which is the binary sequence 11111111. PPP does not assign individual station addresses.

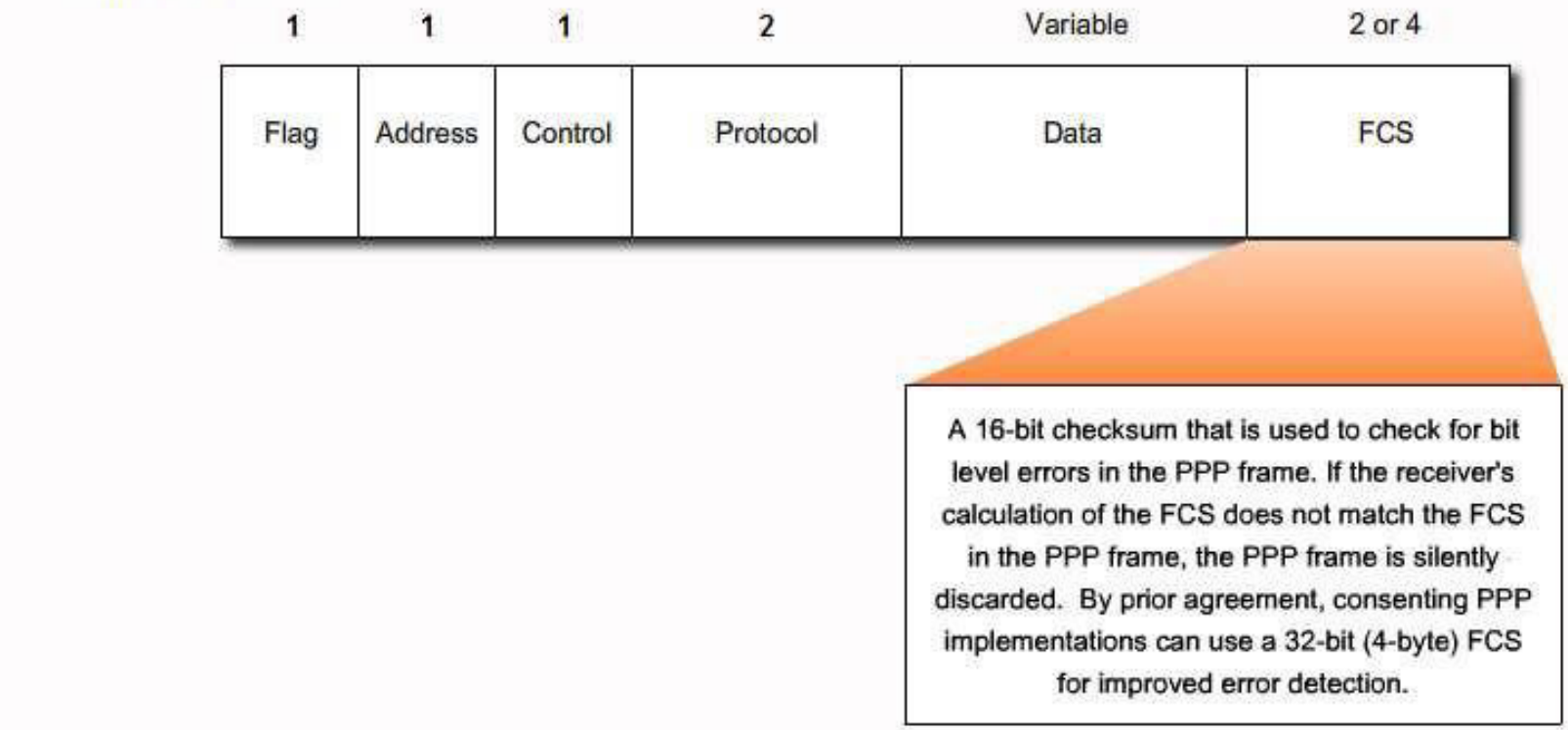
PPP Frame Fields




PPP Frame Fields
Field length, in bytes
1
1
1
2
Variable
2 or 4
Flag
Address
Control
Protocol
Data
FCS
2 bytes that identify the protocol encapsulated in the data field of the frame. The 2-byte Protocol ID field identifies the protocol of the PPP payload. If both PPP peers agree to perform protocol field compression during LCP negotiation, the Protocol ID field is one byte for Protocol IDs in the range 0x00-00 to 0x00-FF.

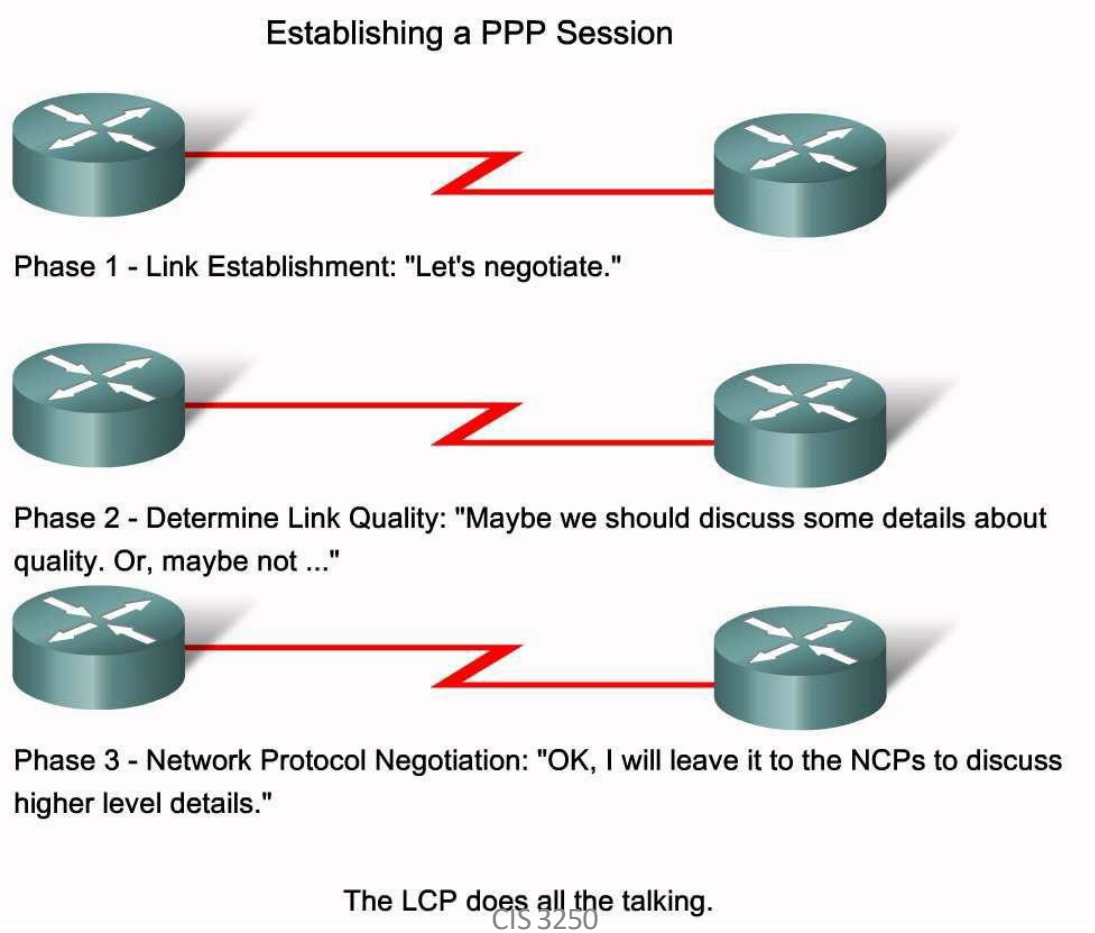

PPP Frame Fields
Field length, in bytes
1
1
1
2
Variable
2 or 4
Flag
Address
Control
Protocol
Data
FCS
0 or more bytes that contain the datagram for the protocol specified in the protocol field. The 2 bytes of the frame check sequence (FCS) field, followed by the closing flag, marks the end of the data field. The default maximum length of the data field is 1500 bytes.

PPP Frame Fields



Describe Point-to-Point Concepts

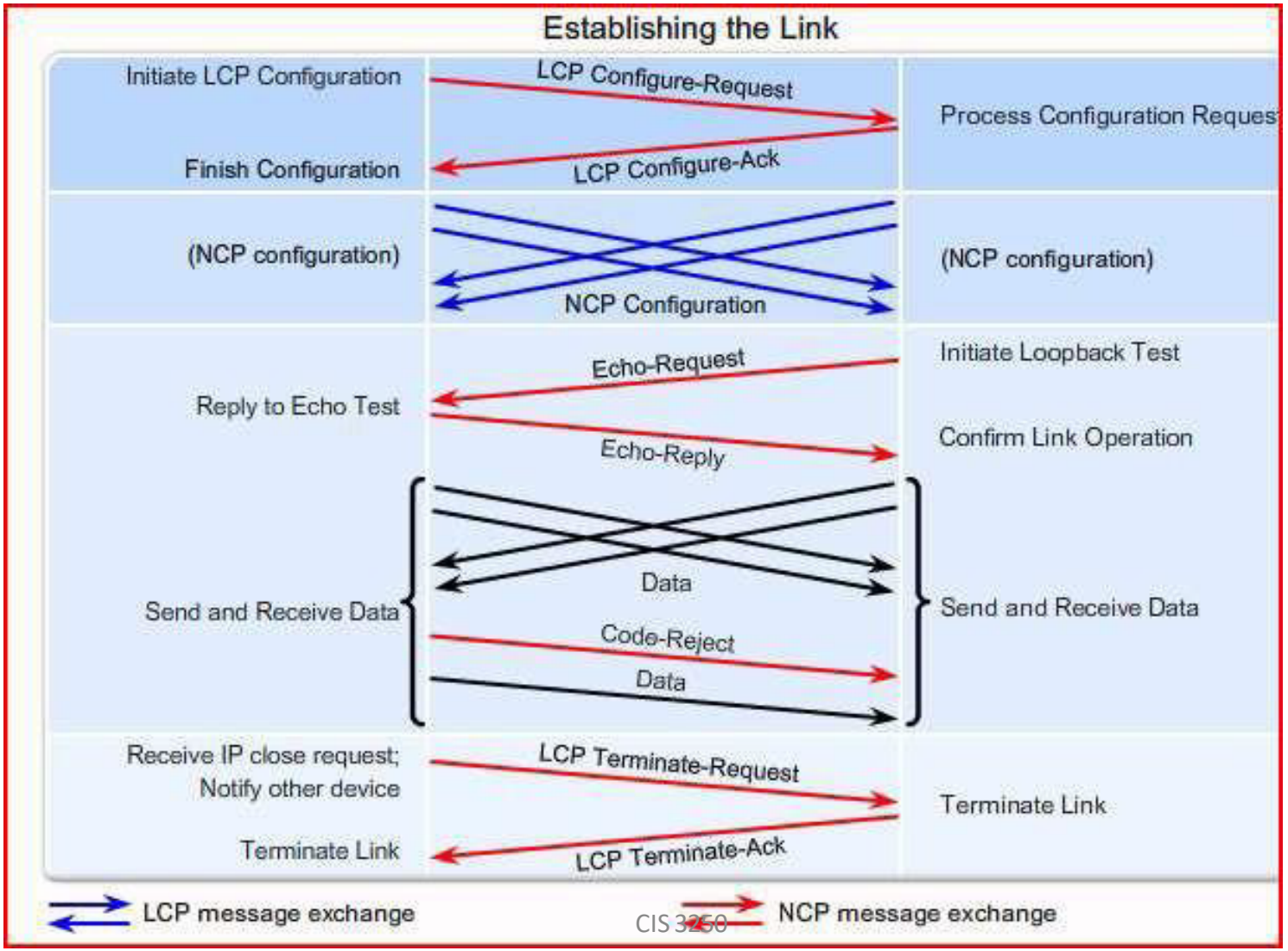
- Define the three phases of PPP session establishment



Link Establishment Phases

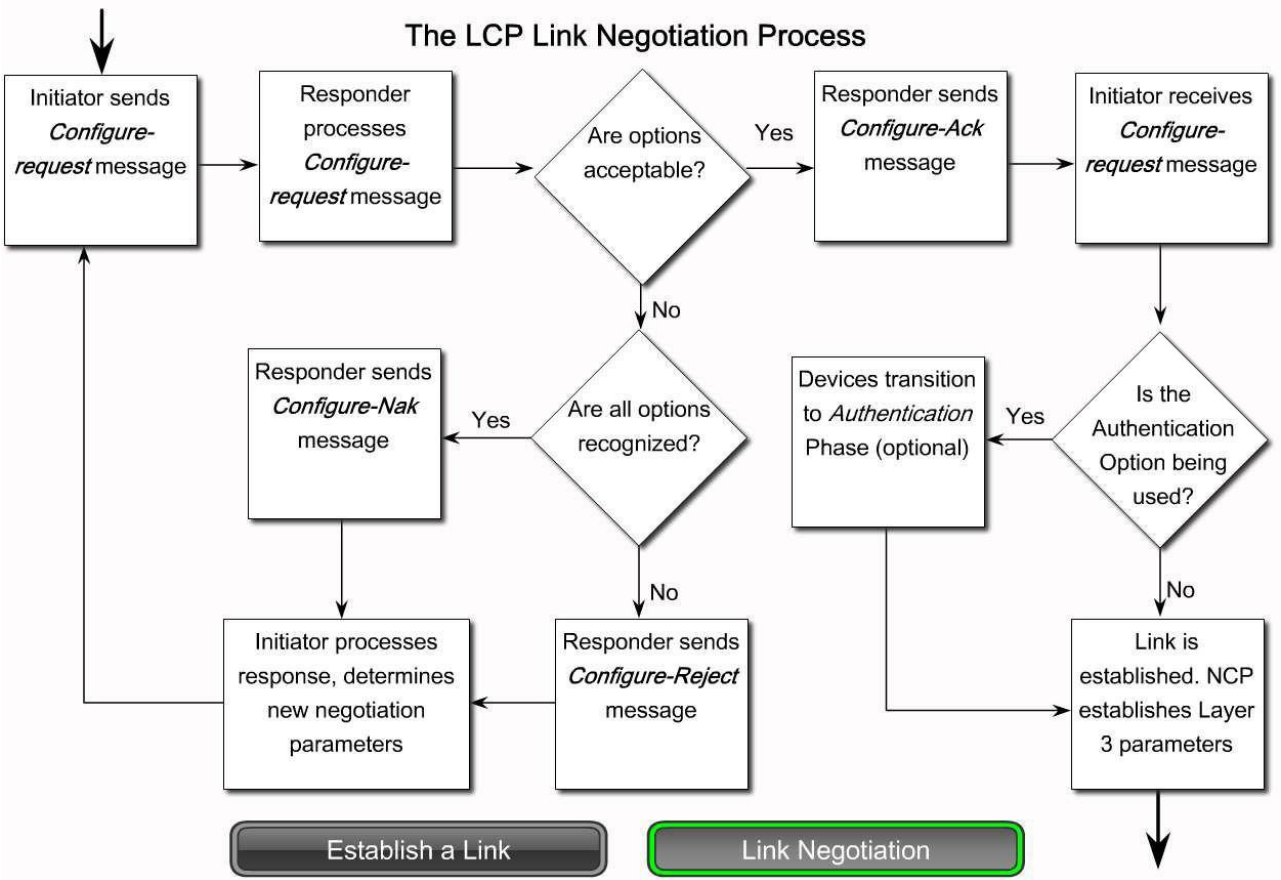
- **Phase 1**: Link establishment and configuration negotiation— Before PPP exchanges any network layer datagrams (for example, IP), the LCP must first open the connection and negotiate configuration options. This phase is complete when the receiving router sends a configuration-acknowledgment frame 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. The LCP can delay transmission of network layer protocol information until this phase is complete.
- **Phase 3**: Network layer protocol configuration negotiation — 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 down at any time. If the LCP closes the link, it informs the network layer protocols so that they can take appropriate action.

Link Establishment



Describe Point-to-Point Concepts

- Explain the role of the LCP in PPP

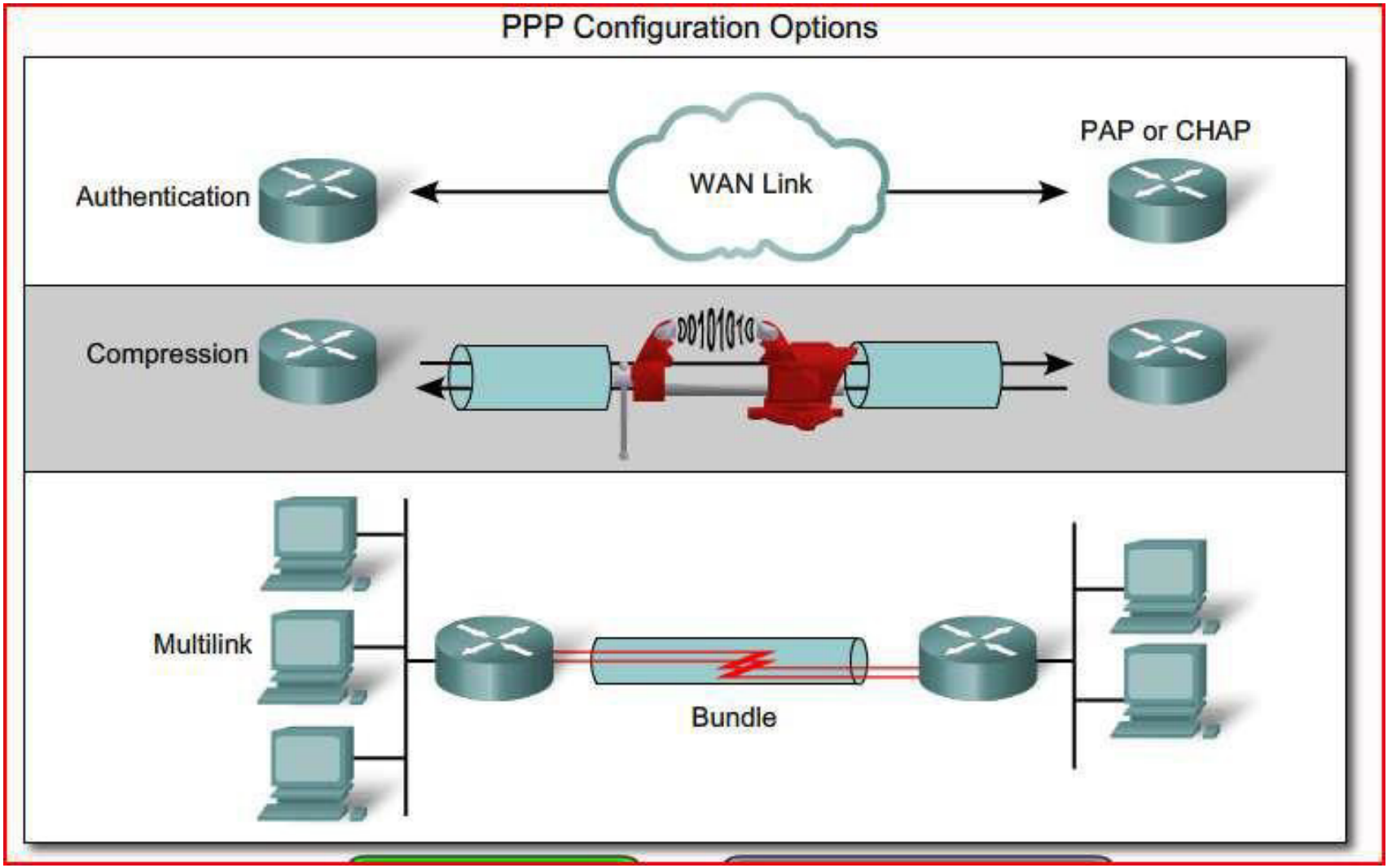


Configure PPP on a Serial Interface

- Describe how configuration options are communicated in the LCP frame

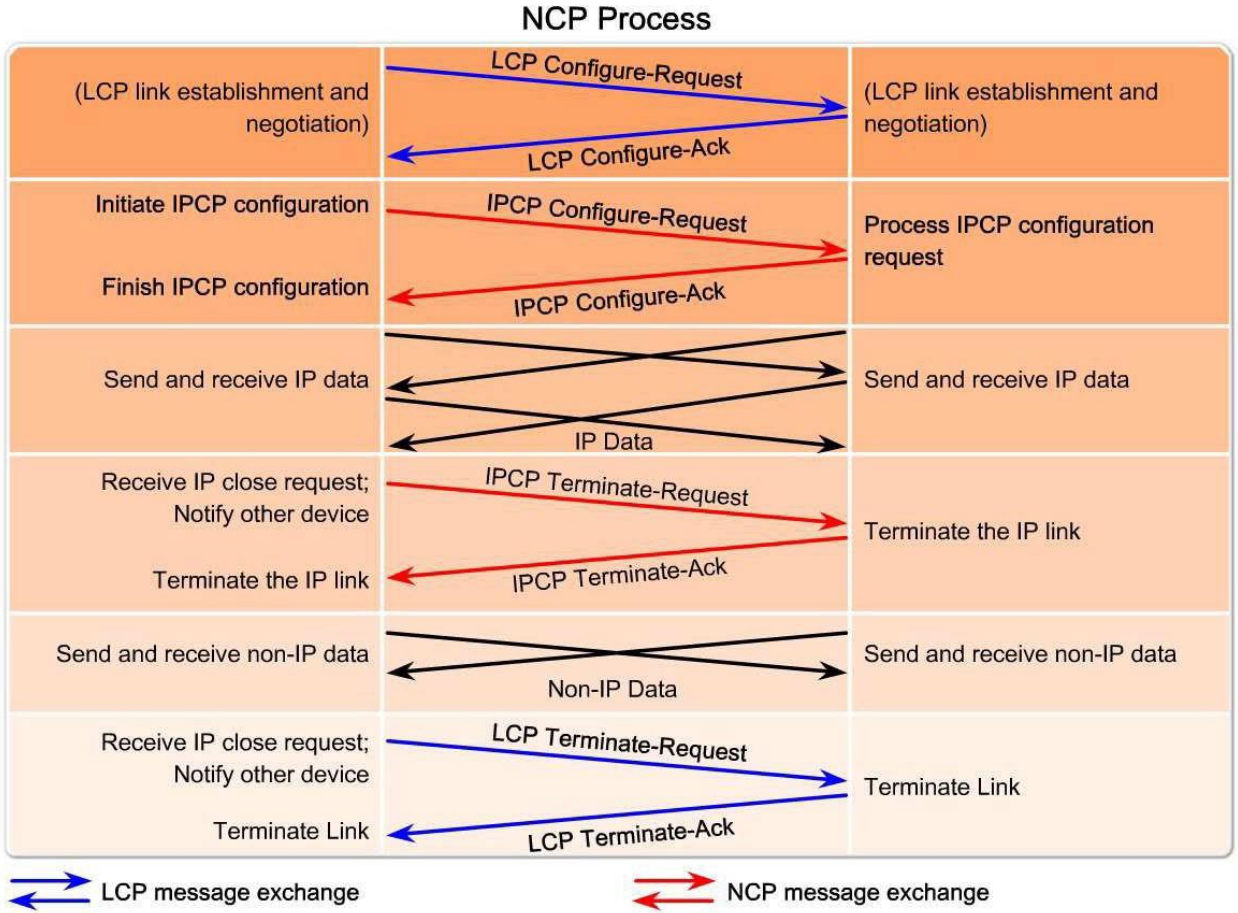
Configurable Options Field Codes

Option Name	Option Type	Option Length	Description
Maximum Receive Unit (MRU)	1	4	MRU is the maximum size of a PPP frame and cannot exceed 65,535. The default is 1,500 and if neither peer is changing the default, it is not negotiated.
Asynchronous Control Character Map (ACCM)	2	6	This is a bit map that enables character escapes for asynchronous links. By default, character escapes are used.
Authentication Protocol	3	5 or 6	This field indicates the authentication protocol, either PAP or CHAP.
Magic Number	5	6	This is a random number chosen to distinguish a peer and detect looped back lines.
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.
Callback	13 or 0x0D	3	A 1-octet indicator of how callback is to be determined.


PPP Configuration Options
Authentication
WAN Link
PAP or CHAP
Compression
0010101
Multilink
Bundle

Describe Point-to-Point Concepts

- Describe the characteristics of NCP



NCP Process

- After the link has been initiated, the LCP passes control to the appropriate NCP.
- PPP can carry data from many types of network layer protocols (at the same time) by using a modular approach in its implementation.
- Its modular model allows the LCP to set up the link and then hand the details of a network protocol to a specific NCP. Each network protocol has a corresponding NCP. There are NCPs for IP, IPX, AppleTalk, etc. NCPs use the same packet format as the LCPs.
- After the LCP has configured and authenticated the basic link, the appropriate NCP completes the specific configuration of the network layer protocol being used.
- When the NCP successfully configures the network layer protocol, it is in the open, and PPP can carry the corresponding network layer protocol packets.

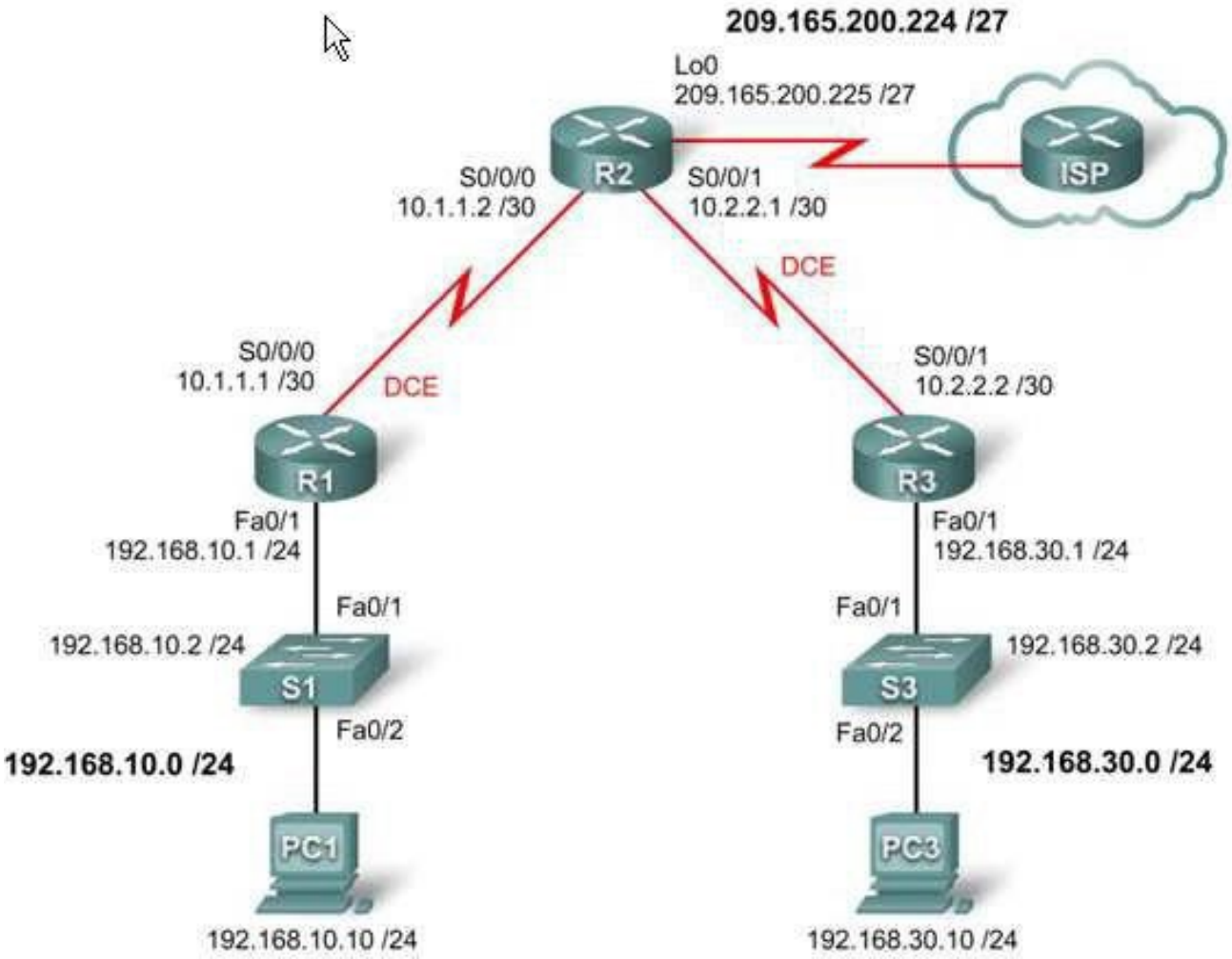
IPCP

- After LCP has established the link, the routers exchange IPCP messages, negotiating options specific to the protocol. IPCP is responsible for configuring, enabling, and disabling the IP 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. Van Jacobson TCP/IP header compression reduces the size of the TCP/IP headers to as few as 3 bytes. This can be a significant improvement on slow serial lines, particularly for interactive traffic.
- **IP-Address** - Allows the initiating device to specify an IP address to use for routing IP over the PPP link, or to request an IP address for the responder. Dialup network links commonly use the IP address option.
- When the NCP process is complete, the link goes into the open state and LCP takes over again. Link traffic consists of any possible combination of LCP, NCP, and network layer protocol packets.

LCP Options

- **Authentication** - Peer routers exchange authentication messages. 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.
- **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. Until the Magic-Number Configuration Option has been successfully negotiated, the Magic-Number must be transmitted as zero. Magic numbers are generated randomly at each end of the connection.
- **Multilink** - Cisco IOS Release 11.1 and later supports multilink PPP. This alternative provides load balancing over the router interfaces that PPP uses. Multilink is not covered in this course.

PPP Demo


209.165.200.224 /27
Lo0
209.165.200.225 /27
R2
ISP
S0/0/0
10.1.1.2 /30
S0/0/1
10.2.2.1 /30
DCE
S0/0/0
10.1.1.1 /30
DCE
S0/0/1
10.2.2.2 /30
R1
R3
Fa0/1
192.168.10.1 /24
Fa0/1
192.168.30.1 /24
Fa0/1
192.168.10.2 /24
S1
Fa0/1
192.168.30.2 /24
S3
Fa0/2
192.168.10.0 /24
Fa0/2
192.168.30.0 /24
PC1
PC3
192.168.10.10 /24
192.168.30.10 /24

LCP Options Continued

- **PPP Callback** - To enhance security, Cisco IOS Release 11.1 and later offers callback over PPP.
- 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].**

Configure PPP on a Serial Interface

- Explain the purpose of the commands used to configure and verify PPP connections

PPP Configuration Commands

```
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.

```
Router(config-if)#ppp quality percentage
```

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

Verifying a Serial PPP Encapsulation Configuration

```
R2#show interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:07, output 00:00:07, output hang never
  Last clearing of "show interface" counters 00:00:11
  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  0/1/32 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 96 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     6 packets input, 76 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     7 packets output, 84 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Enabling PPP on a Serial Interface

- The following example enables PPP encapsulation on serial interface 0/0:
- R3#configure terminal
- R3(config)#interface serial 0/0
- R3(config-if)#encapsulation ppp

PPP Compression

- You can configure point-to-point software compression on serial interfaces after you have enabled PPP encapsulation. Because this option invokes a software compression process, it can affect system performance. If the traffic already consists of compressed files (.zip, .tar, or .mpeg, for example), do not use this option.
- To configure compression over PPP, enter the following commands:

- R3(config)#interface serial 0/0

- R3(config-if)#encapsulation ppp

- R3(config-if)#compress [predictor | stac]

Link Quality

- LCP provides an optional link quality determination phase. In this phase, LCP tests the link to determine whether the link quality is sufficient to use Layer 3 protocols. The command ppp quality percentage ensures that the link meets the quality requirement you set; otherwise, the link closes down.
- The percentages are calculated for both incoming and outgoing directions. The outgoing quality is calculated by comparing the total number of packets and bytes sent to the total number of packets and bytes received by the destination node. The incoming quality is calculated by comparing the total number of packets and bytes received to the total number of packets and bytes sent by the destination node.
- If the link quality percentage is not maintained, the link is deemed to be of poor quality and is taken down. Link Quality Monitoring (LQM) implements a time lag so that the link does not bounce up and down.

Link Quality Configuration

- R3(config)#interface serial 0/0
- R3(config-if)#encapsulation ppp
- R3(config-if)#ppp quality 80
- Use the <no ppp quality> command to disable LQM.

Load Balancing

- Multilink PPP (also referred to as MP, MPPP, MLP, or Multilink) 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.
- MPPP allows packets to be **fragmented** and sends these fragments simultaneously over multiple point-to-point links to the same remote address.
- The multiple physical links come up in response to a user-defined load threshold. MPPP can measure the load on just inbound traffic, or on just outbound traffic, but not on the combined load of both inbound and outbound traffic.

Multilink Configuration

- Router(config)#interface serial 0/0
- Router(config-if)#encapsulation ppp
- Router(config-if)#ppp multilink
- The multilink command has no arguments. To disable PPP multilink, use the <no ppp multilink> command.

Verifying PPP

Practice: Verifying and Debugging Commands

Command	Description
`show interfaces`	Displays statistics for all interfaces configured on the router or access server
`show interfaces serial`	Displays information about a serial interface
`debug ppp`	Debugs PPP
`undebug all`	Turns off all debugging displays

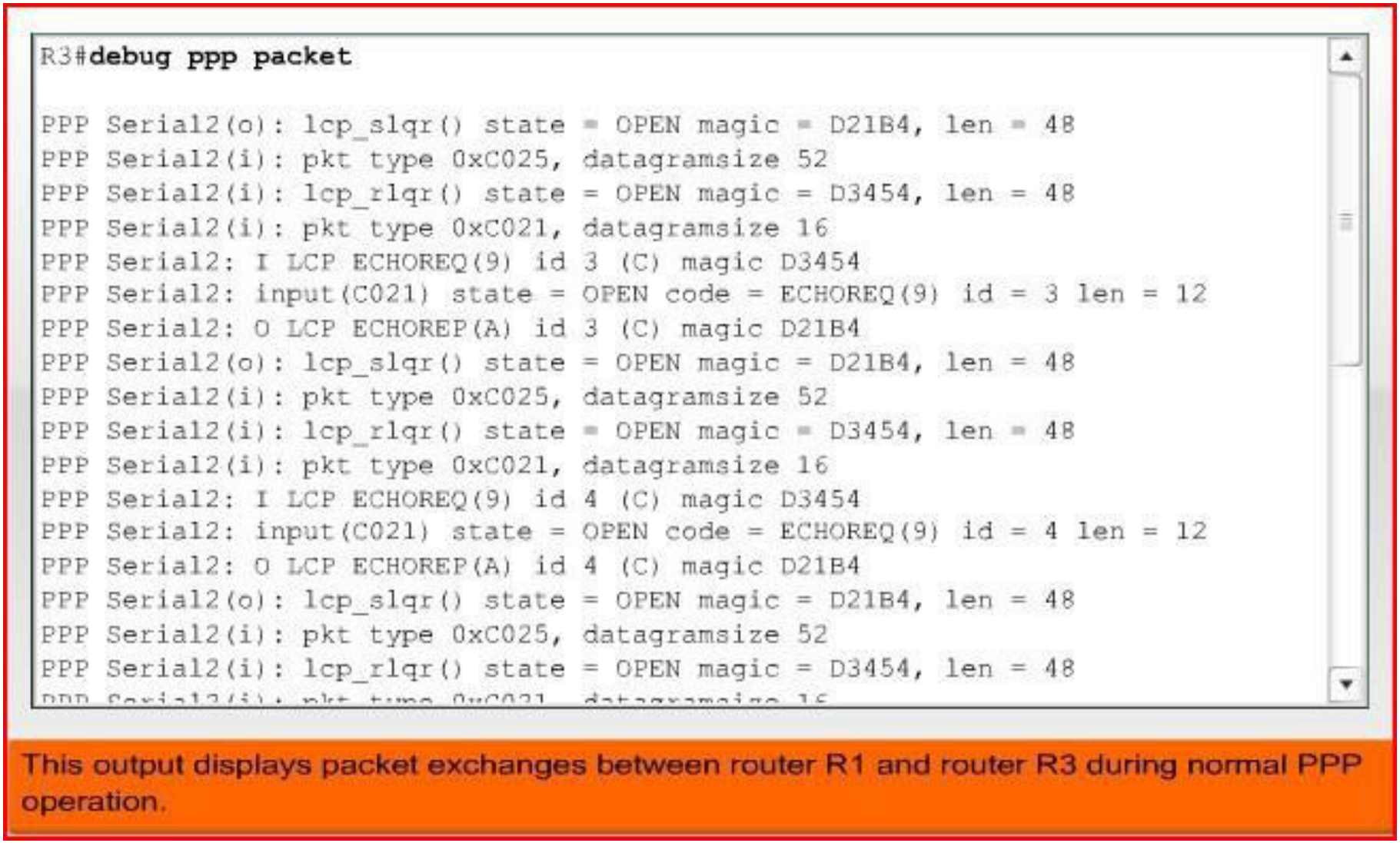
```
R2#show interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:07, output 00:00:07, output hang never
  Last clearing of "show interface" counters 00:00:11
  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  0/1/32 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 96 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     6 packets input, 76 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     7 packets output, 84 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Troubleshooting PPP

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 incorrect packet sequence number information where MPPC compression is enabled.
cbcp	Displays protocol errors and statistics associated with PPP connection negotiations using MSCB.



This output displays packet exchanges between router R1 and router R3 during normal PPP operation.

```
R1# debug ppp negotiation

ppp: sending CONFREQ, type = 4 (CI_QUALITYTYPE), value = C025/3E8
ppp: sending CONFREQ, type = 5 (CI_MAGICNUMBER), value = 3D56CAC
ppp: received config for type = 4 (QUALITYTYPE) acked
ppp: received config for type = 5 (MAGICNUMBER) value = 3D567F8 acked (ok)
PPP Serial2: state = ACKSENT fsm_rconfack(C021): rcvd id 5
ppp: config ACK received, type = 4 (CI_QUALITYTYPE), value = C025
ppp: config ACK received, type = 5 (CI_MAGICNUMBER), value = 3D56CAC
ppp: ipcp_reqci: returning CONFACK.
(ok)
PPP Serial2: state = ACKSENT fsm_rconfack(8021): rcvd id 4
```

This output displays packet exchanges between router R1 and router R3 during the initial PPP negotiation.

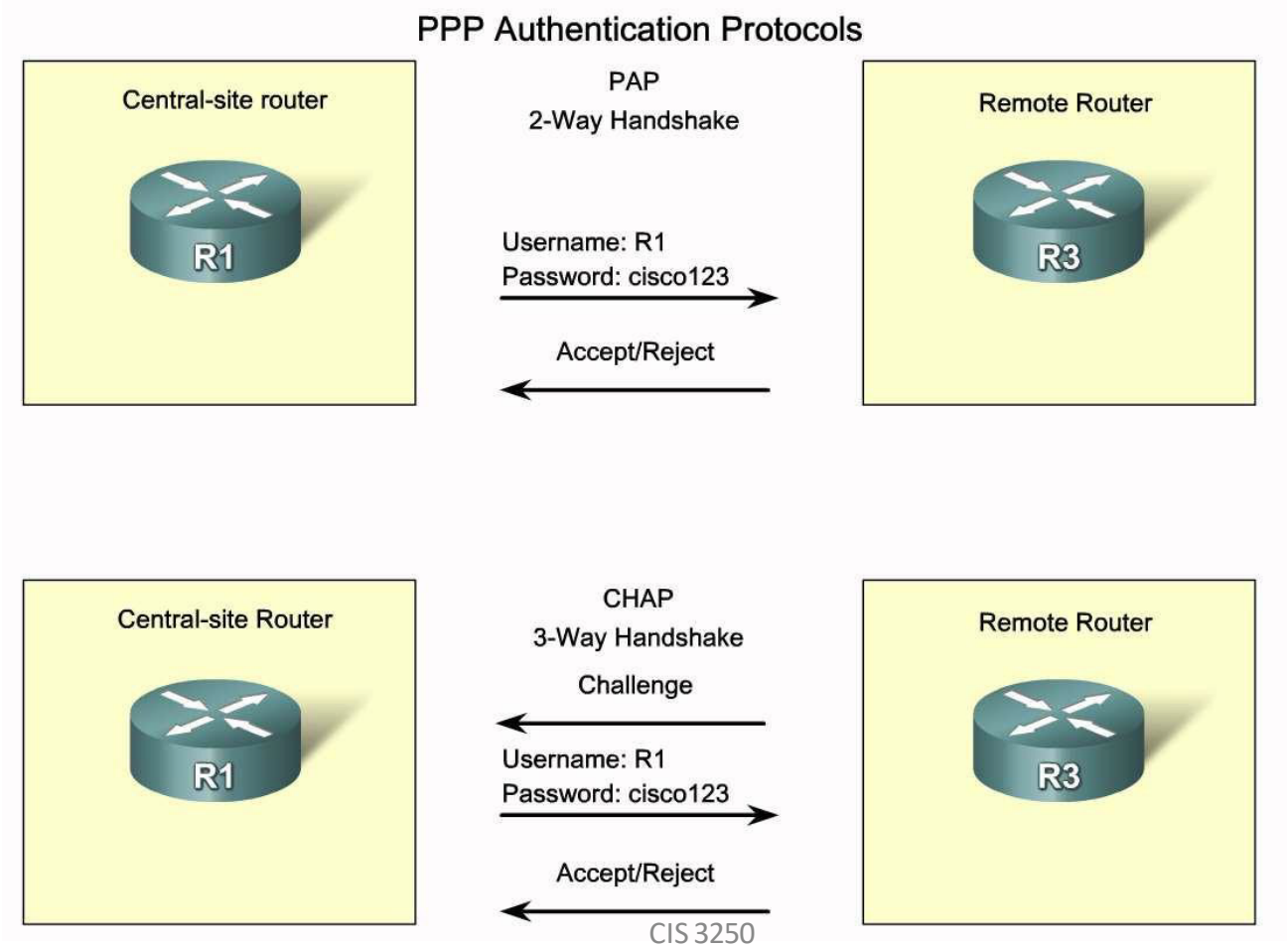
```
R1# debug ppp error
PPP Serial3(i): rlqr receive failure. successes = 15
PPP: myrcvdiffp = 159 peerxmitdiffp = 41091
PPP: myrcvdiffo = 2183 peerxmitdiffo = 1714439
PPP: threshold = 25
PPP Serial2(i): rlqr transmit failure. successes = 15
PPP: myxmitdiffp = 41091 peerrcvdiffp = 159
PPP: myxmitdiffo = 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.
```

PPP debugging Output

- Serial3(i) - Interface number associated with this debugging information; indicates that this is an input packet.
- rlqr receive failure - Receiver does not accept the request to negotiate the Quality Protocol option.
- myrcvdiffp = 159 - Number of packets received over the time period specified.
- peerxmitdiffp = 41091 - Number of packets sent by the remote node over this period.
- myrcvdiffo = 2183 - Number of octets received over this period.
- peerxmitdiffo = 1714439 - Number of octets sent by the remote node over this period.
- threshold = 25 - Maximum error percentage acceptable on this interface. You calculate this percentage using the threshold value entered in the ppp quality percentage interface configuration command. A value of 100 minus number is the maximum error percentage. In this case, a number of 75 was entered. This means that the local router must maintain a minimum 75 percent non-error percentage, or the PPP link closes down.
- OutLQRs = 1 - Current send LQR sequence number of the local router.
- LastOutLQRs = 1 - Last sequence number that the remote node side has seen from the local node.

Configuring PPP with Authentication

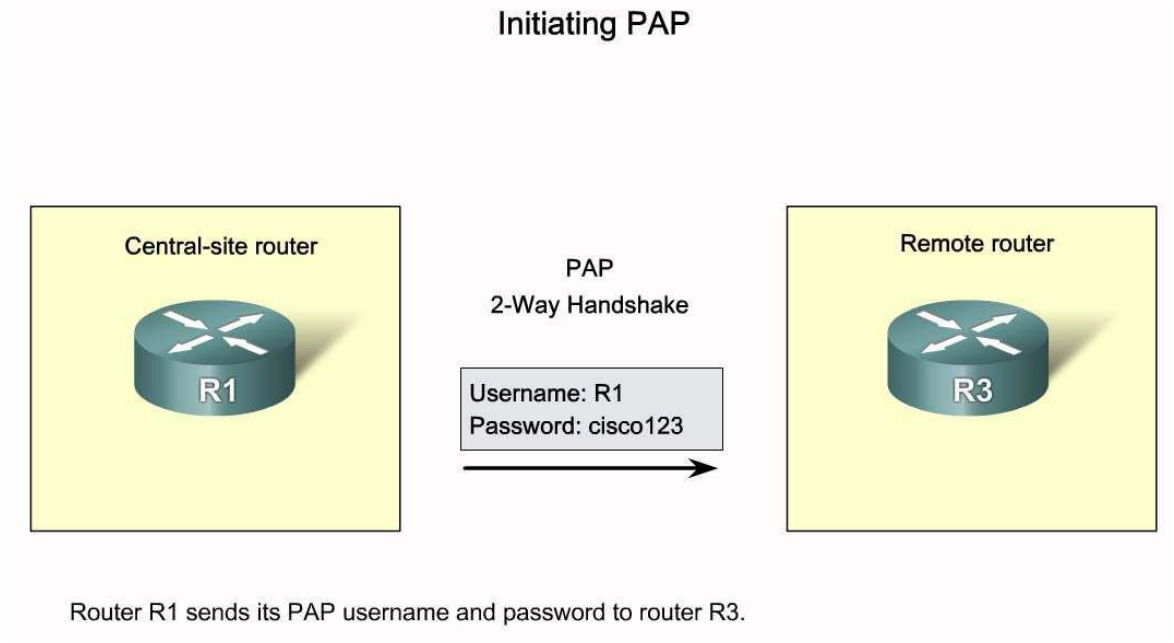
- Differentiate between PAP and CHAP



PPP Authentications Protocols

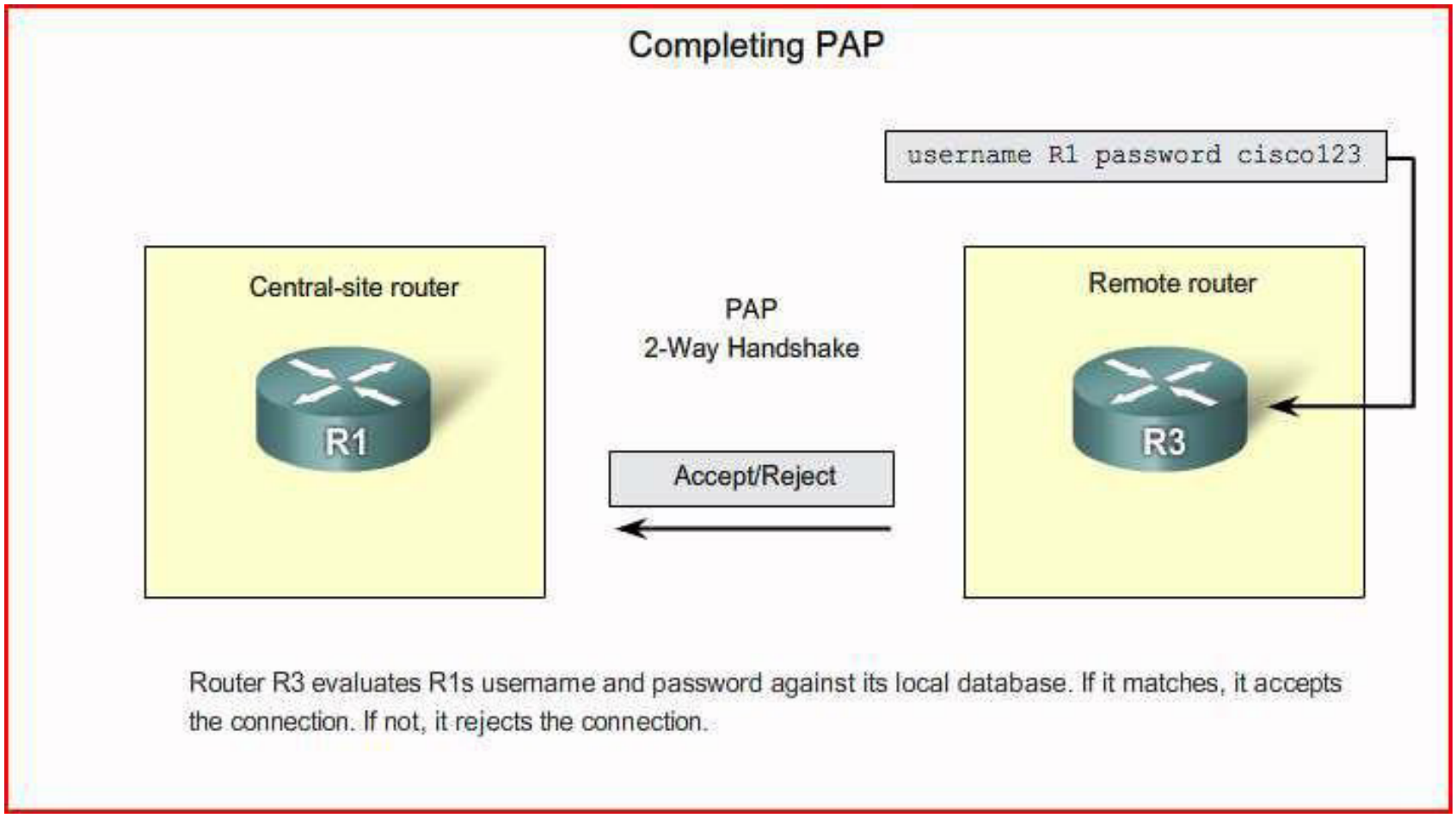
- PPP defines an extensible LCP that allows negotiation of an authentication protocol for authenticating its peer before allowing network layer protocols to transmit over the link.
- **PAP** is a very basic two-way process. There is no encryption-the username and password are sent in plain text. If it is accepted, the connection is allowed.
- **CHAP** is more secure than PAP. It involves a three-way exchange of a shared secret. The process is described later in this section.
- The authentication phase of a PPP session is optional. If used, you can authenticate the peer after the LCP establishes the link and choose the authentication protocol. If it is used, authentication takes place before the network layer protocol configuration phase begins.
- The authentication options require that the calling side of the link enter authentication information. This helps to ensure that the user has the permission of the network administrator to make the call. Peer routers exchange authentication messages.

Configuring PPP with PAP



The username and password are sent as one LCP data package, rather than the server sending a login prompt and waiting for a response. After PPP completes the link establishment phase, the remote node repeatedly sends a username-password pair across the link until the sending node acknowledges it or terminates the connection.

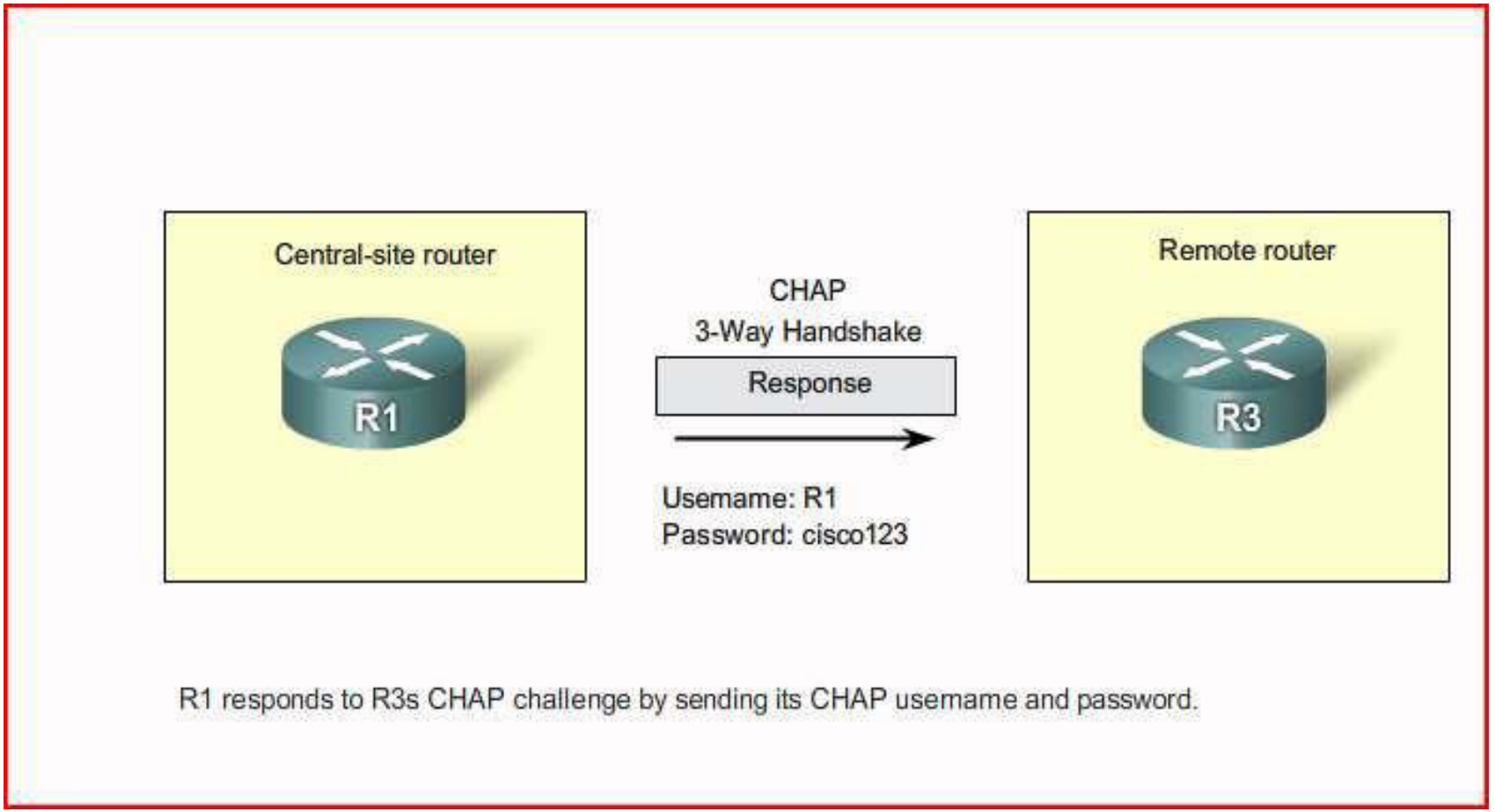
PAP 2-Way Handshake



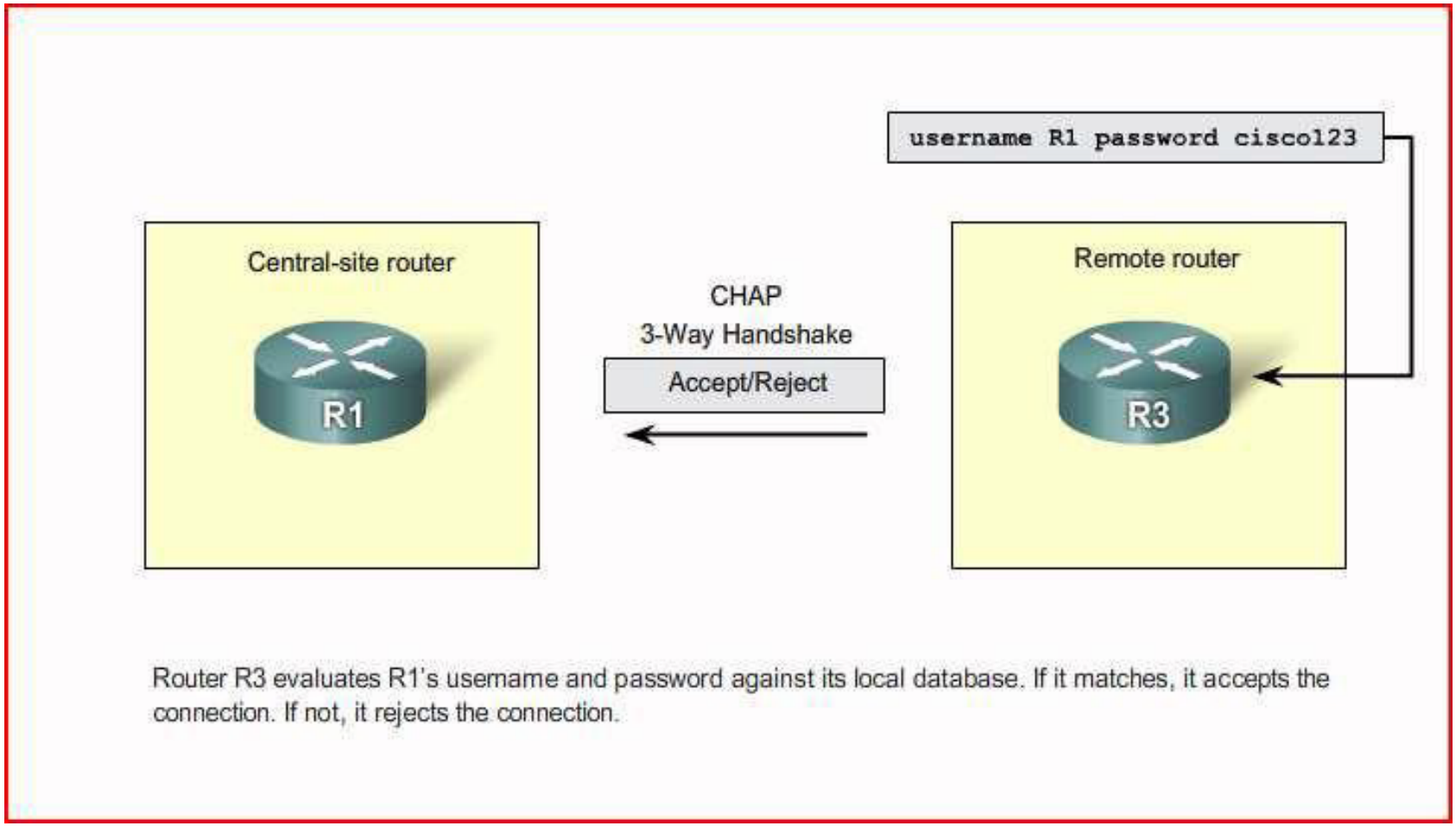
Initiating CHAP

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

Responding CHAP

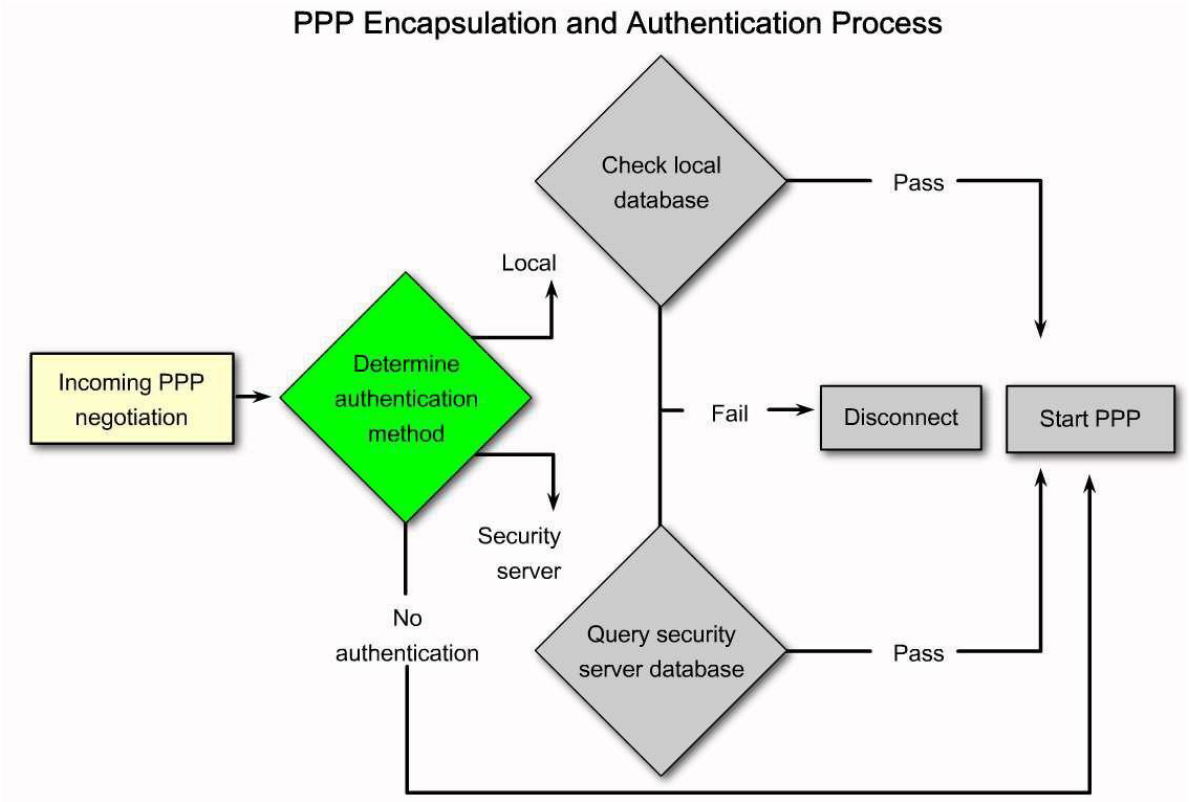


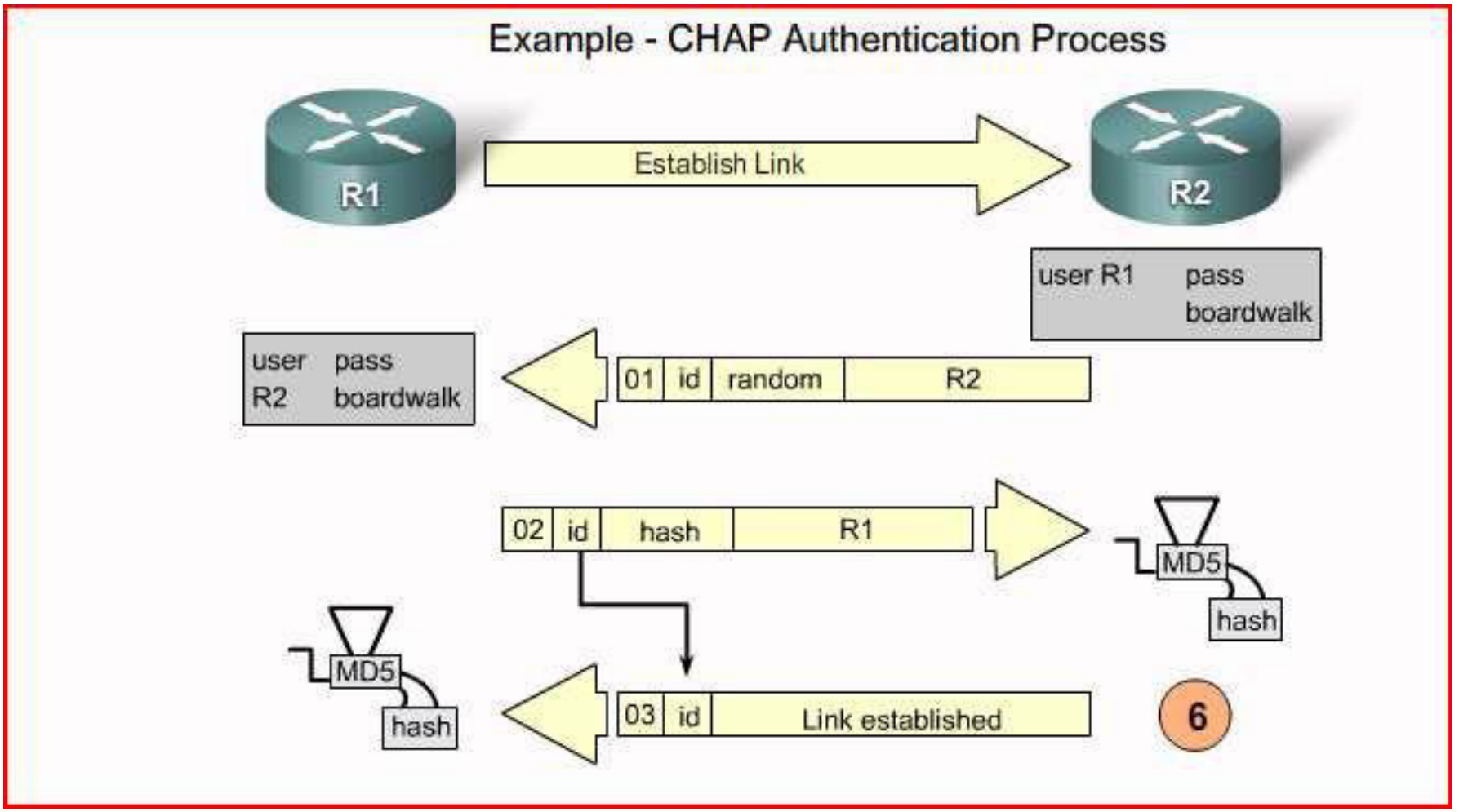
Completing CHAP



Configuring PPP with Authentication

- Outline the PPP encapsulation and authentication process on a flow chart




Example - CHAP Authentication Process
R1
Establish Link
R2
user R1 pass boardwalk
user R2 pass boardwalk
01 id random R2
02 id hash R1
MD5
hash
MD5
hash
03 id Link established
6

CHAP

- **Step 1**. R1 initially negotiates the link connection using LCP with router R2 and the two systems agree to use CHAP authentication during the PPP LCP negotiation.
- **Step 2**. Router R2 generates an ID and a random number and sends that plus its username as a CHAP challenge packet to R1.
- **Step 3**. R1 will use the username of the challenger (R2) and cross reference it with its local database to find its associated password. R1 will then generate a unique MD5 hash number using the R2's username, ID, random number and the shared secret password.
- **Step 4**. Router R1 then sends the challenge ID, the hashed value, and its username (R1) to R2.
- **Step 5**. R2 generates it own hash value using the ID, the shared secret password, and the random number it originally sent to R1.
- **Step 6**. R2 compares its hash value with the hash value sent by R1. If the values are the same, R2 sends a link established response to R1.

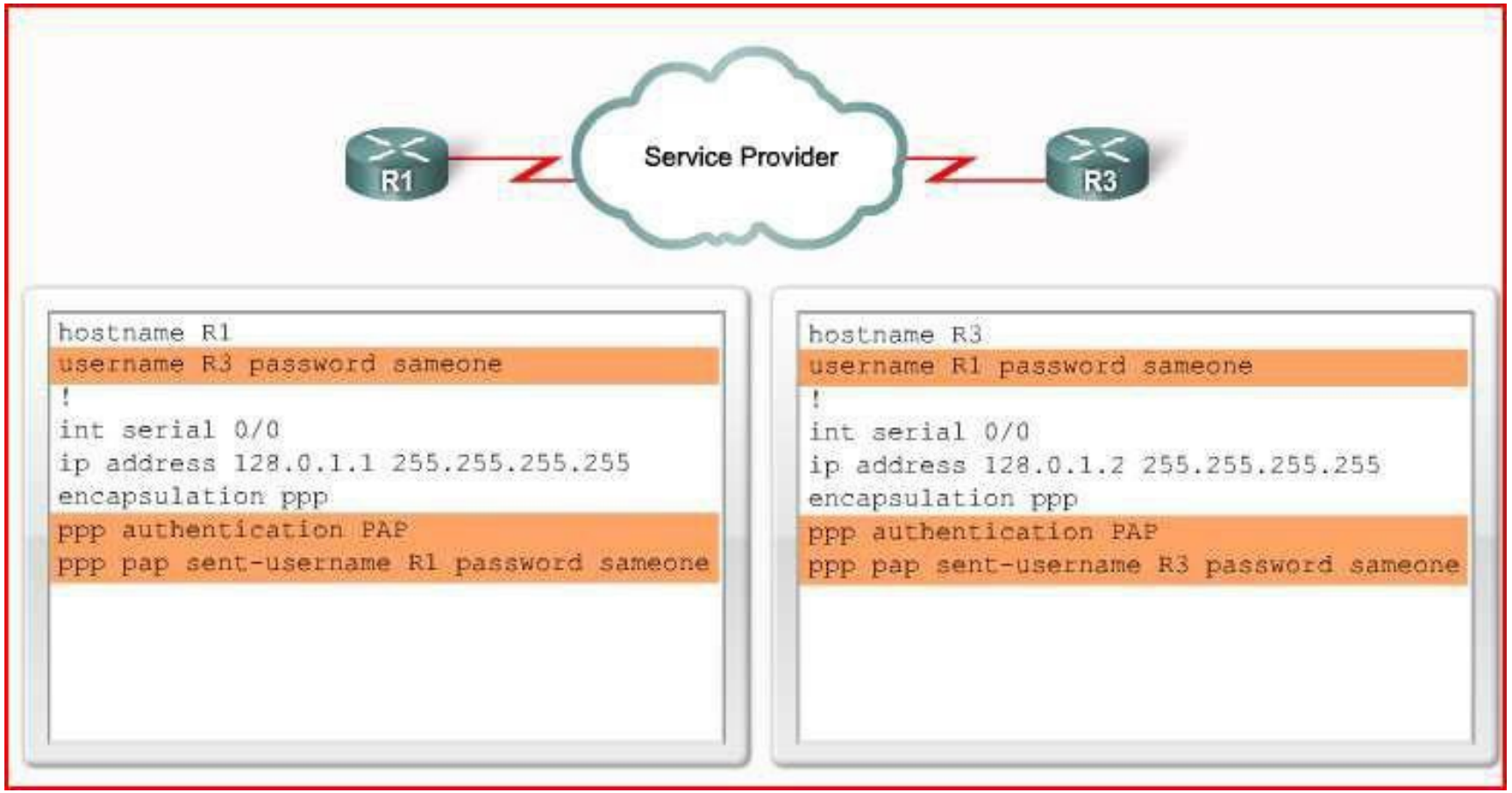
PPP Authentication Command

The **ppp authentication** Command

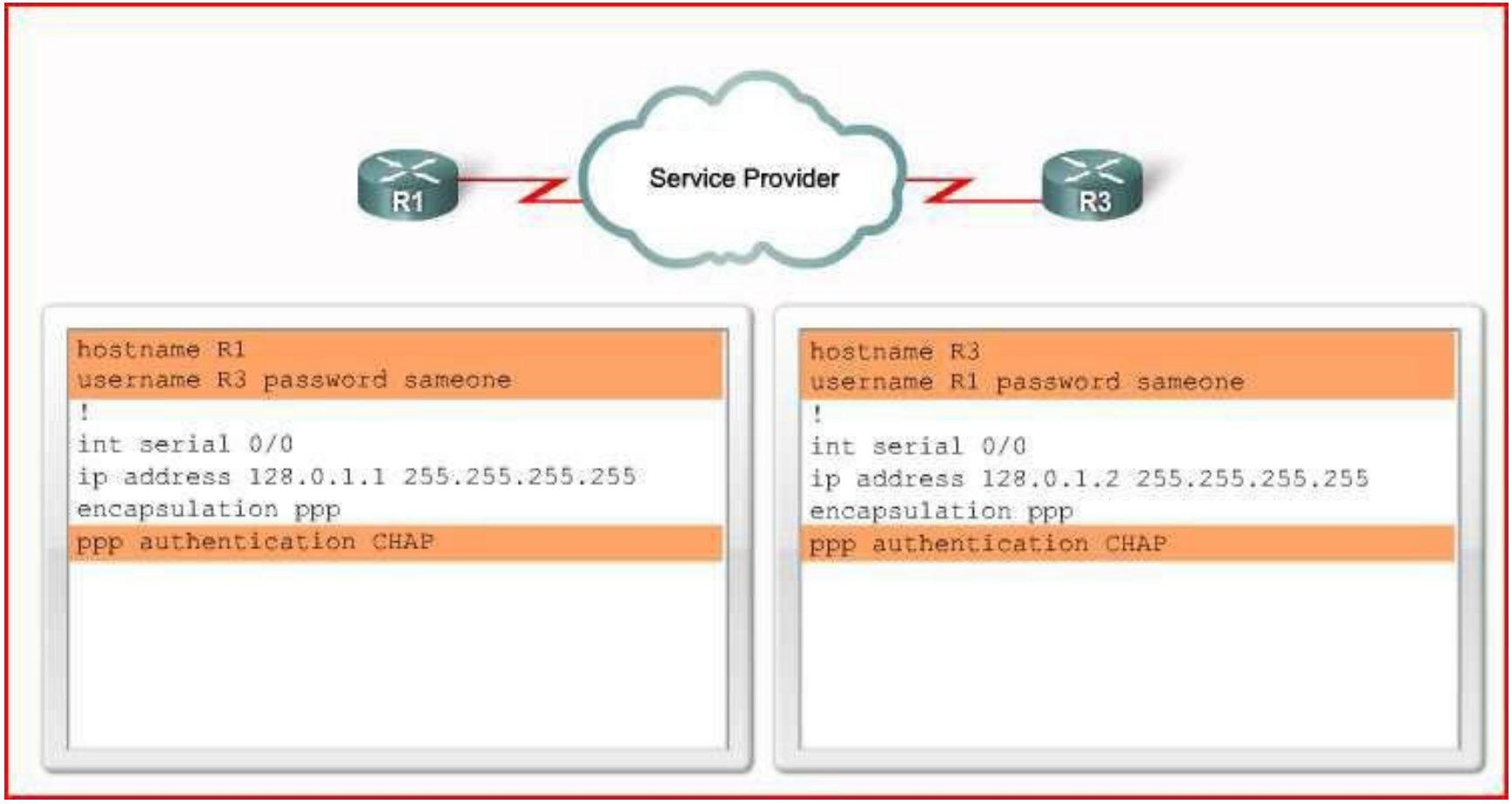
```
ppp authentication {chap | chap pap | pap chap | pap} [if-needed]
[list-name | default] [callin]
```

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 authentic 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.

PAP Example


R1
Service Provider
R3
hostname R1
username R3 password sameone
!
int serial 0/0
ip address 128.0.1.1 255.255.255.255
encapsulation ppp
ppp authentication PAP
ppp pap sent-username R1 password sameone
hostname R3
username R1 password sameone
!
int serial 0/0
ip address 128.0.1.2 255.255.255.255
encapsulation ppp
ppp authentication PAP
ppp pap sent-username R3 password sameone

CHAP Example



Troubleshooting PPP Authentication

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
```

Summary

- PPP is a widely used WAN protocol
- PPP provides multi-protocol LAN to WAN connections
- PPP session establishment – 4 phases
  - –Link establishment
  - –Link quality determination
  - –Network layer protocol configuration negotiation
  - –Link termination
- WAN Encapsulation
  - –HDLC default encapsulation
  - –PPP

Summary

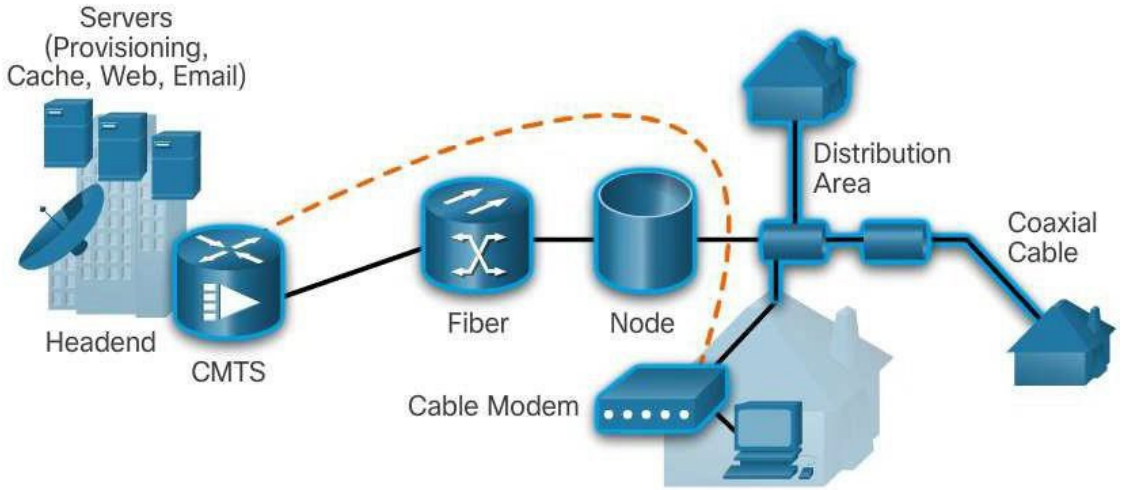
- PPP authentication
  - –PAP
    - 2 way handshake
  - –CHAP
    - 3 way handshake
  - –Use **debug ppp authentication** to confirm authentication configuration
- PPP configuration
  - –Done on a serial interface
- After PPP configuration, use show interfaces command to display:
  - –LCP state
  - –NCP state

Chapter 3- Sections & Objectives

- 3.1 Remote Access Connections
  - Select broadband remote access technologies to support business requirements.
- 3.2 PPPoE
  - Configure a Cisco router with PPPoE.
- 3.3 VPNs
  - Explain how VPNs secure site-to-site and remote access connectivity.
- 3.4 GRE
  - Implement a GRE tunnel.
- 3.5 eBGP
  - Implement eBGP in a single-homed remote access network.

Broadband Connections

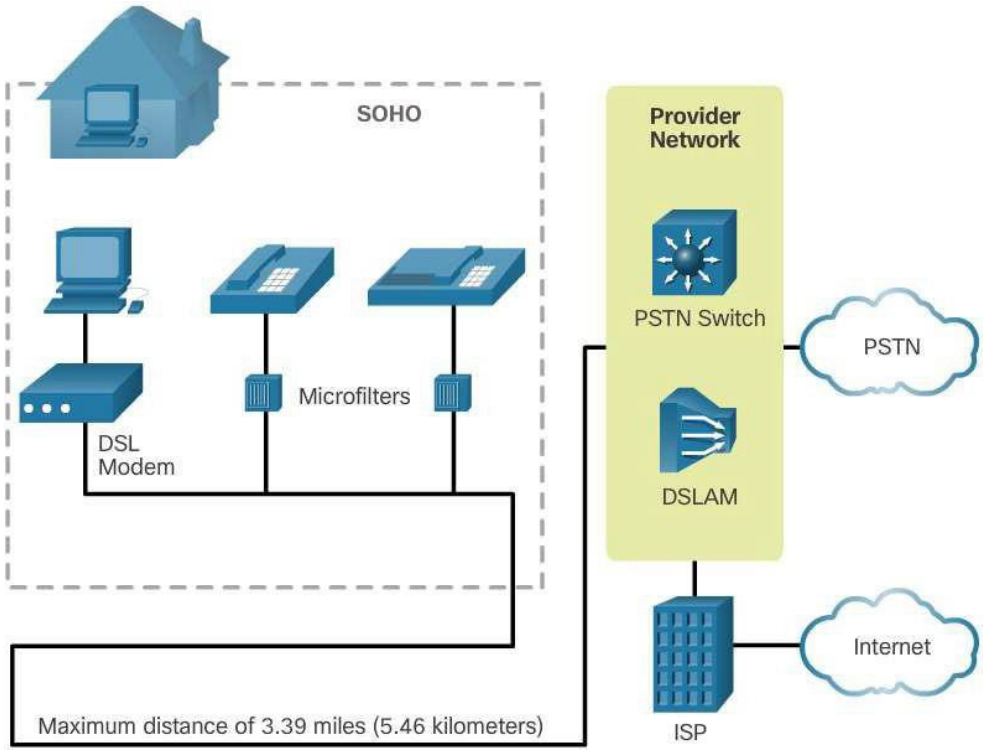
- The cable system uses a coaxial cable that carries radio frequency (RF) signals across the network.
- A headend CMTS communicates with CMs located in subscriber homes.
- The HFC network is a mixed optical-coaxial network in which optical fiber replaces the lower bandwidth coaxial cable.



Remote Access Connections

Broadband Connections

- A Digital Subscriber Line (DSL) is a means of providing high-speed connections over installed copper wires.
- The two important components are the DSL transceiver and the DSLAM
- The advantage that DSL has over cable technology is that DSL is not a shared medium. Each user has a separate direct connection to the DSLAM.



Broadband Connections

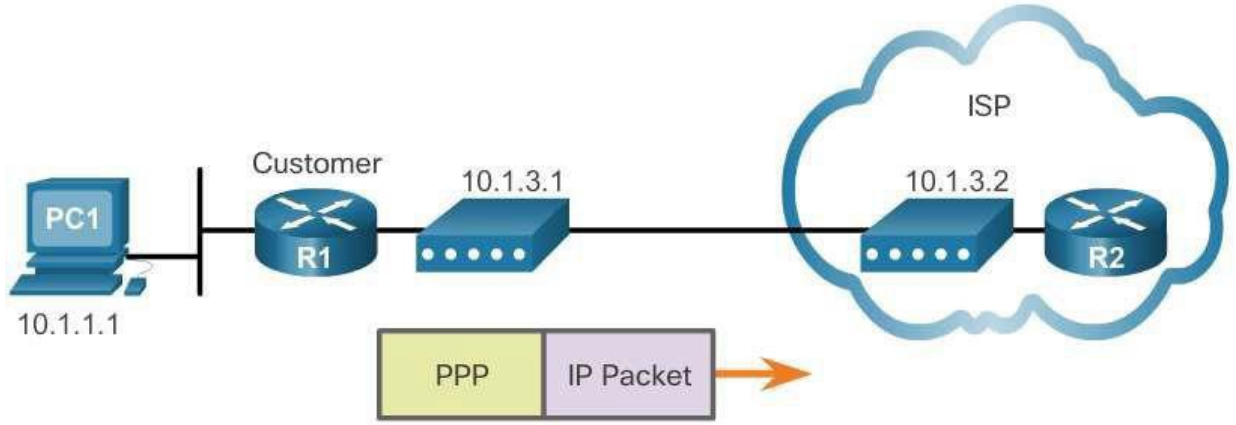
- Developments in broadband wireless technology are increasing wireless availability through three main technologies:
  - **Municipal Wi-Fi** - Most municipal wireless networks use a mesh of interconnected access points. Each access point is in range and can communicate with at least two other access points. The mesh blankets a particular area with radio signals.
  - **Cellular/mobile** - Mobile phones use radio waves to communicate through nearby cell towers. Cellular/mobile broadband access consists of various standards.
  - **Satellite Internet** - Satellite Internet services are used in locations where land-based Internet access is not available, or for temporary installations that are mobile. Internet access using satellites is available worldwide.

Select a Broadband Connection

- Each broadband solution has advantages and disadvantages.
- Some factors to consider in making a decision include:
  - **Cable** - Bandwidth is shared by many users, upstream data rates are often slow during high-usage hours in areas with over-subscription.
  - **DSL** - Limited bandwidth that is distance sensitive (in relation to the ISP's central office), upstream rate is proportionally quite small compared to downstream rate.
  - **Fiber-to-the-Home** - Requires fiber installation directly to the home.
  - **Cellular/Mobile** - Coverage is often an issue, even within a SOHO where bandwidth is relatively limited.
  - **Wi-Fi Mesh** - Most municipalities do not have a mesh network deployed; if it is available and the SOHO is in range, then it is a viable option.
  - **Satellite** - Expensive, limited capacity per subscriber; often provides access where no other access is possible.

PPPoE Overview

- PPP can be used on all serial links including those links created with dial-up analog and ISDN modems.
  - PPP supports the ability to assign IP addresses to remote ends of a PPP link.
  - PPP supports CHAP authentication.
  - Ethernet links do not natively support PPP. PPP over Ethernet (PPPoE) provides a solution to this problem. PPPoE creates a PPP tunnel over an Ethernet connection.



PPPoE

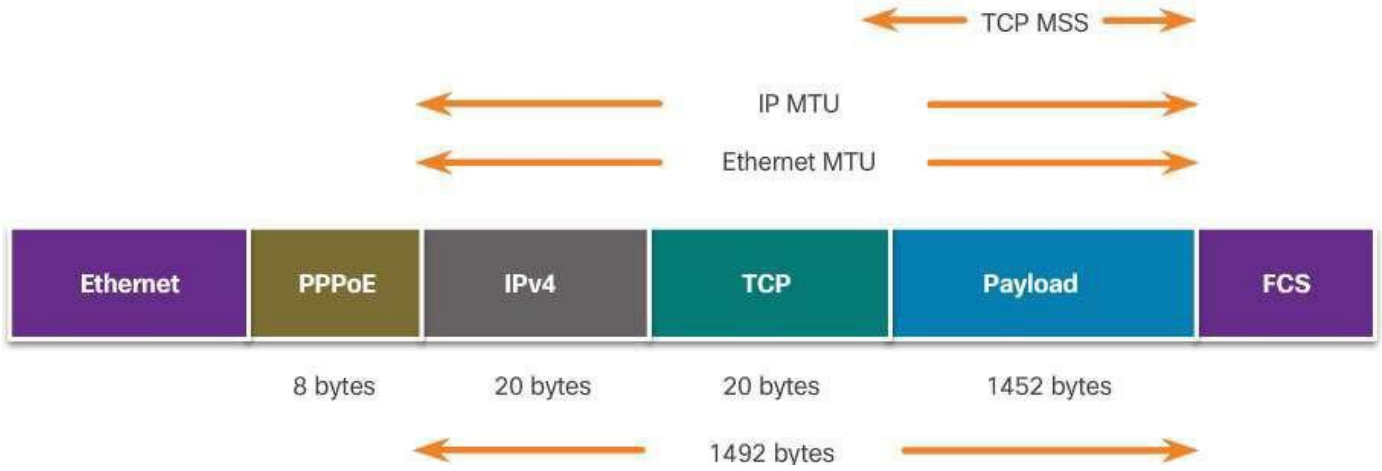
Implement PPPoE

- PPPoE Configuration
  - The dialer interface is created using the **interface dialer** *number* command.
  - The PPP CHAP configuration usually defines one-way authentication; therefore, the ISP authenticates the customer.
  - The physical Ethernet interface that connects to the DSL modem is then enabled with the command **pppoe enable**.
  - The dialer interface is linked to the Ethernet interface with the **dialer pool** and **pppoe-client** commands, using the same number.
  - The maximum transmission unit (MTU) should be set down to 1492, versus the default of 1500, to accommodate the PPPoE headers.
- PPPoE Verification
  - The **show ip interface brief** command is issued to verify the IPv4 address automatically assigned to the dialer interface by the ISP router.
  - The **show interface dialer** command verifies the MTU and PPP encapsulation configured on the dialer interface.
  - The **show pppoe session** command is used to display information about currently active PPPoE sessions.
  - The Ethernet MAC addresses can be verified by using the **show interfaces** command on each router.

PPPoE

Implement PPPoE

- PPPoE Troubleshooting
  - Verify PPP negotiation using the **debug ppp negotiation** command.
  - Re-examine the output of the **debug ppp negotiation** command.
  - PPPoE supports an MTU of only 1492 bytes in order to accommodate the additional 8-byte PPPoE header.
  - The **ip tcp adjust-mss** *max-segment-size* interface command adjusts the MSS value during the TCP 3-way handshake.



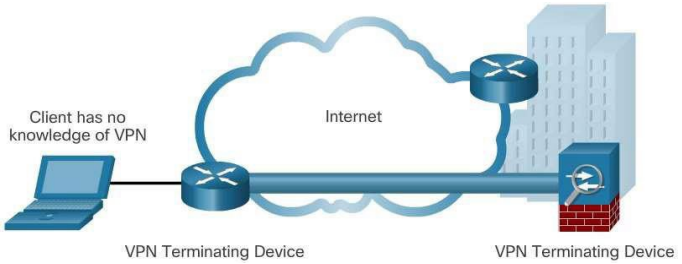
Fundamentals of VPNs

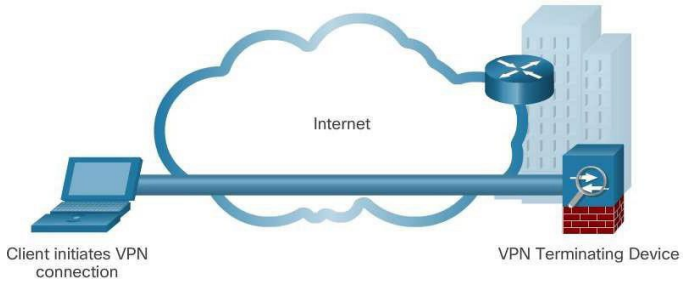
- Introducing VPNs
  - Organizations use VPNs to create an end-to-end private network connection over third-party networks, such as the Internet.
  - Today, a secure implementation of VPN with encryption, such as IPsec VPNs, is what is usually meant by virtual private networking.
  - To implement VPNs, a VPN gateway is necessary. The VPN gateway could be a router, a firewall, or a Cisco Adaptive Security Appliance (ASA).
- Benefits of VPNs
  - Cost savings
  - Scalability
  - Compatibility with broadband technology
  - Security

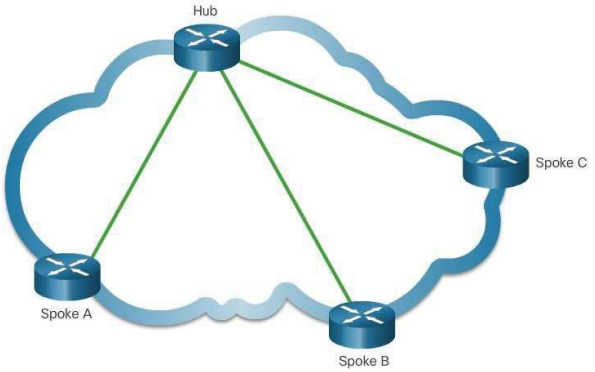
VPNs

Types of VPNs

- Site-to-Site
  - Site-to-site VPNs connect entire networks to each other, for example, they can connect a branch office network to a company headquarters network.
- Remote Access
  - Remote-access VPNs are used to connect individual hosts that must access their company network securely over the Internet.
- DMVPN
  - Dynamic Multipoint VPN (DMVPN) is a Cisco software solution for building multiple VPNs in an easy, dynamic, and scalable manner.





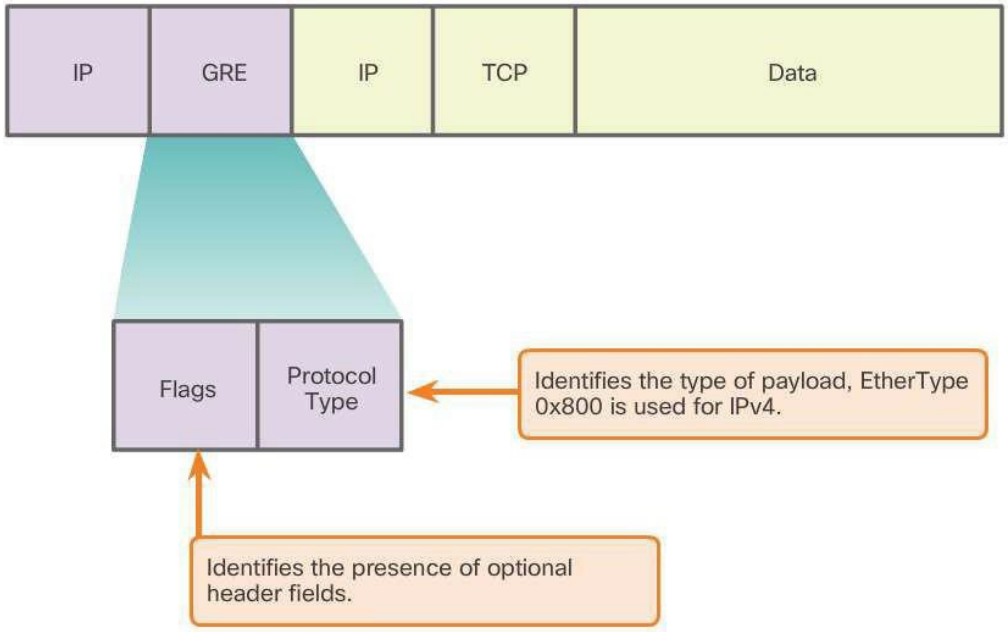


GRE

GRE Overview

- GRE Introduction
  - Generic Routing Encapsulation (GRE) is designed to manage the transportation of multiprotocol and IP multicast traffic between two or more sites, that may only have IP connectivity.

- GRE Characteristics
  - IP tunneling using GRE enables network expansion across a single-protocol backbone environment.



GRE

Implement GRE

- There are five steps to configuring a GRE tunnel:
  - **Step 1.** Create a tunnel interface using the **interface tunnel number** command.
  - **Step 2.** Configure an IP address for the tunnel interface. This is normally a private IP address.
  - **Step 3.** Specify the tunnel source IP address.
  - **Step 4.** Specify the tunnel destination IP address.
  - **Step 5.** (Optional) Specify GRE tunnel mode as the tunnel interface mode.

Command	Description
`tunnel mode gre ip`	Specifies that the mode of the tunnel interface is GRE over IP.
`tunnel source` *ip_address*	Specifies the tunnel source address.
`tunnel destination` *ip_address*	Specifies the tunnel destination address.
`ip address` *ip_address mask*	Specifies the IP address of the tunnel interface.

GRE

Implement GRE

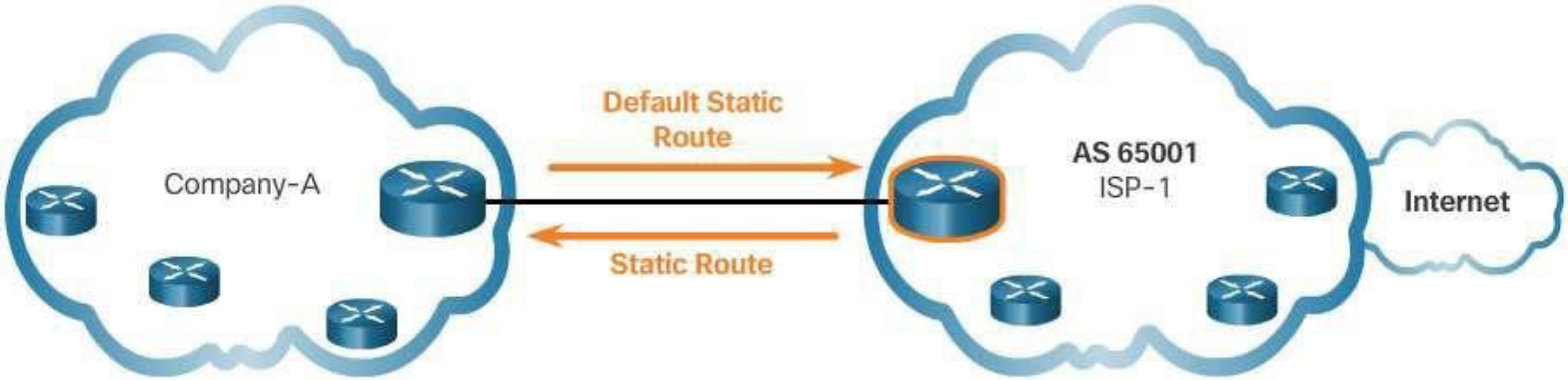
- Verify GRE
  - To determine whether the tunnel interface is up or down, use the **show ip interface brief** command.
  - To verify the state of a GRE tunnel, use the **show interface tunnel** command.
  - Verify that an OSPF adjacency has been established over the tunnel interface using the **show ip ospf neighbor** command.
- Troubleshoot GRE
  - Use the **show ip interface brief** command on both routers to verify that the tunnel interface is up and configured with the correct IP addresses for the physical interface and the tunnel interface.
  - Use the **show ip ospf neighbor** command to verify neighbor adjacency.
  - Use **show ip route** to verify that networks are being passed between the two routers

BGP Overview

- IGP and EGP
  - Interior Gateway Protocols (IGPs) are used to exchange routing information within a company network or an autonomous system (AS).
  - Exterior Gateway Protocols (EGPs) are used for the exchange of routing information between autonomous systems.
- eBGP and iBGP
  - External BGP (eBGP) is the routing protocol used between routers in different autonomous systems.
  - Internal BGP (iBGP) is the routing protocol used between routers in the same AS.
- This course focuses on eBGP only.

BGP Design Considerations

- When to use BGP
  - The use of BGP is most appropriate when an AS has connections to multiple autonomous systems.
  - BGP should not be used when at least one of the following conditions exist:
    - There is a single connection to the Internet or another AS. This is known as single-homed.
    - When there is a limited understanding of BGP.



eBGP

BGP Design Considerations

- BGP Options
  - There are three common ways an organization can choose to implement BGP in a multi-homed environment:
    - Default Route Only - This is the simplest method to implement BGP. However, because the company only receives a default route from both ISPs, sub-optimal routing may occur.
    - Default Route and ISP Routes - This option allows Company-A to forward traffic to the appropriate ISP for networks advertised by that ISP.
    - All Internet Routes - Because Company-A receives all Internet routes from both ISPs, Company-A can determine which ISP to use as the best path to forward traffic for any network. Although this solves the issue of sub-optimal routing, the Company-A's BGP router must contain all Internet routes.

eBGP

BGP Branch Configuration

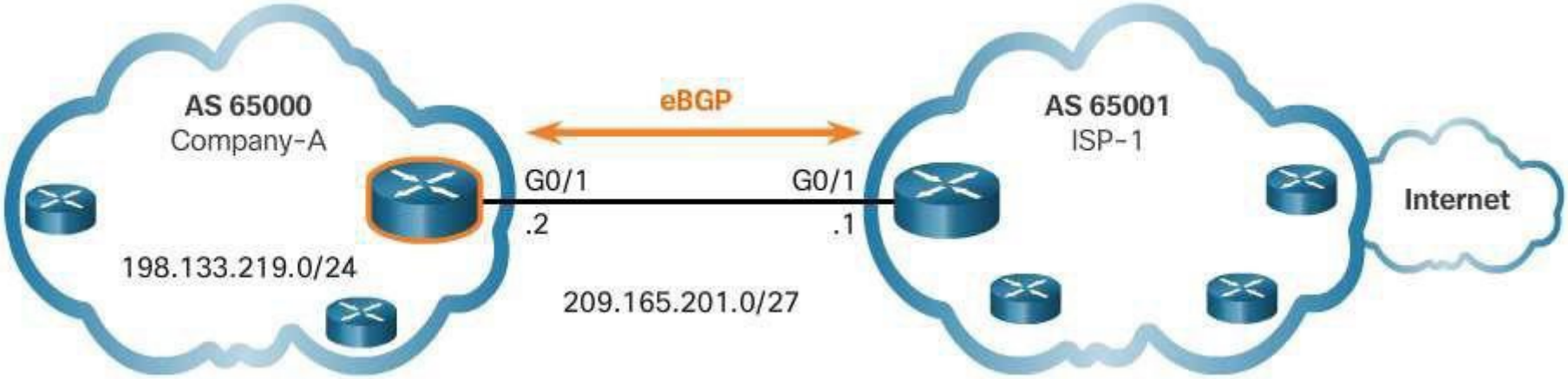
- BGP Configuration Commands
  - There are three steps to implement eBGP:
    - **Step 1**: Enable BGP routing.
    - **Step 2**: Configure BGP neighbor(s) (peering).
    - **Step 3**: Advertise network(s) originating from this AS.

Command	Description
`Router(config)# router bgp as-number`	Enables a BGP routing process, and places the router in router configuration mode.
`Router(config-router)# neighbor ip-address remote-as as-number`	Specifies a BGP neighbor. The as-number is the neighbor's AS number.
`Router(config-router)# network network-address [mask network-mask]`	Advertises a network address to an eBGP neighbor as being originated by this AS. The network-mask is the subnet mask of the network.

BGP Branch Configuration

- Verify eBGP
  - Three commands can be used to verify eBGP

Command	Description
`Router# show ip route`	Verify routes advertised by the BGP neighbor are present in the IPv4 routing table.
`Router# show ip bgp`	Verify that received and advertised IPv4 networks are in the BGP table.
`Router# show ip bgp summary`	Verify IPv4 BGP neighbors and other BGP information.



Chapter Summary

Summary

- Broadband transmission is provided by a wide range of technologies, including DSL, fiber-to-the-home, coaxial cable systems, wireless, and satellite. This transmission requires additional components at the home end and at the corporate end. Broadband wireless solutions include municipal Wi-Fi, cellular/mobile, and satellite Internet. Municipal Wi-Fi mesh networks are not widely deployed. Cellular/mobile coverage can be limited and bandwidth can be an issue. Satellite Internet is relatively expensive and limited, but it may be the only method to provide access.
- If multiple broadband connections are available to a particular location, a cost-benefit analysis should be performed to determine the best solution. The best solution may be to connect to multiple service providers to provide redundancy and reliability.
- PPPoE is a popular data link protocol for connecting remote networks to their ISPs. PPPoE provides the flexibility of PPP and the convenience of Ethernet.

Summary Continued

- VPNs are used to create a secure end-to-end private network connection over a third party network, such as the Internet. GRE is a basic, non-secure site-to-site VPN tunneling protocol that can encapsulate a wide variety of protocol packet types inside IP tunnels, thus allowing an organization to deliver other protocols through an IP-based WAN. Today it is primarily used to deliver IP multicast traffic or IPv6 traffic over an IPv4 unicast-only connection.
- BGP is the routing protocol implemented between autonomous systems. Three basic design options for eBGP are as follows:
- The ISP advertises a default route only to the customer
- The ISP advertises a default route and all of its routes to the customer.
- The ISP advertises all Internet routes to the customer.
- Implementing eBGP in a single-homed network only requires a few commands.