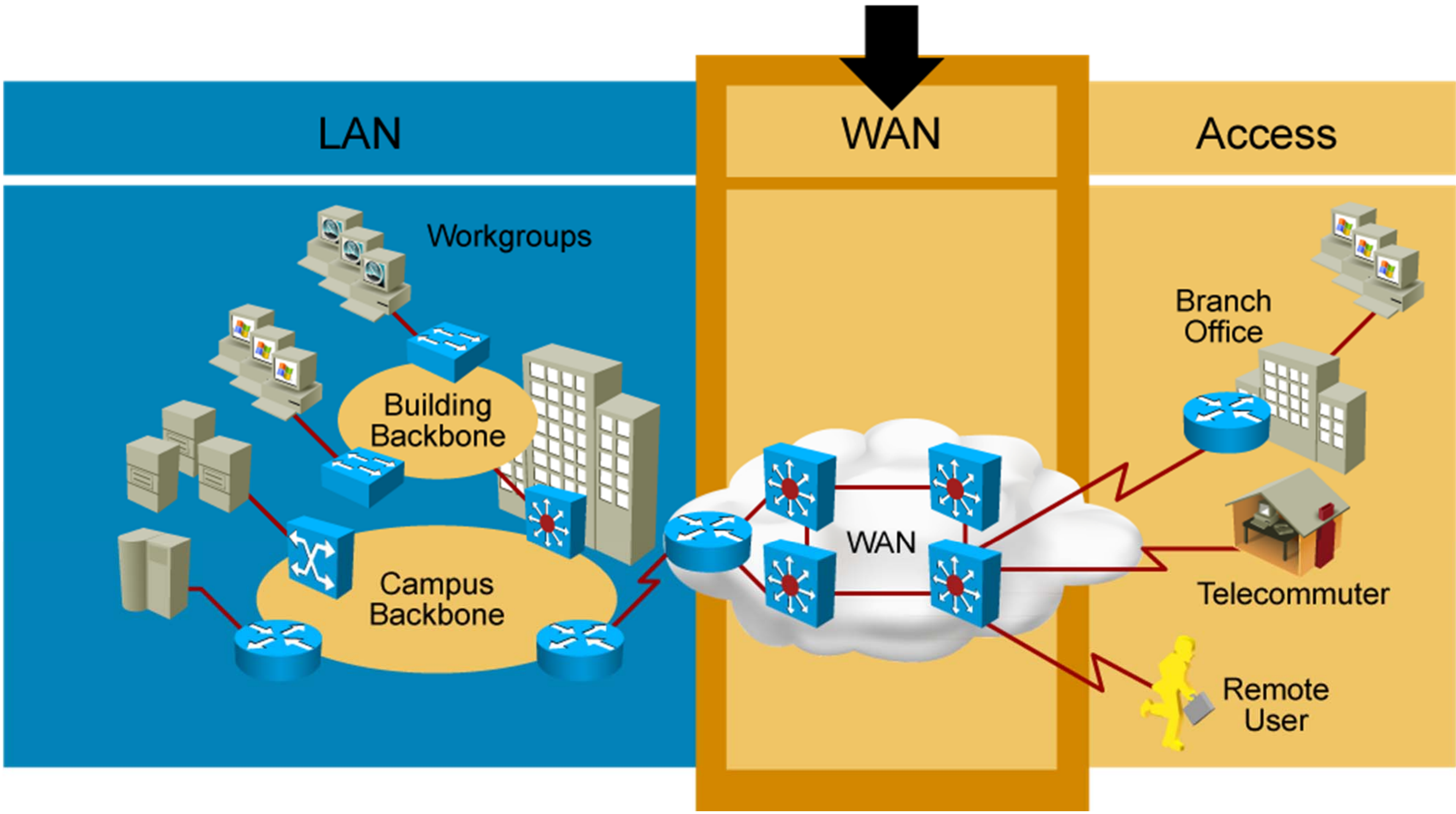
Wide-Area Networks

Interconnecting Cisco Networking Devices, Part 2 (ICND2) v2.0

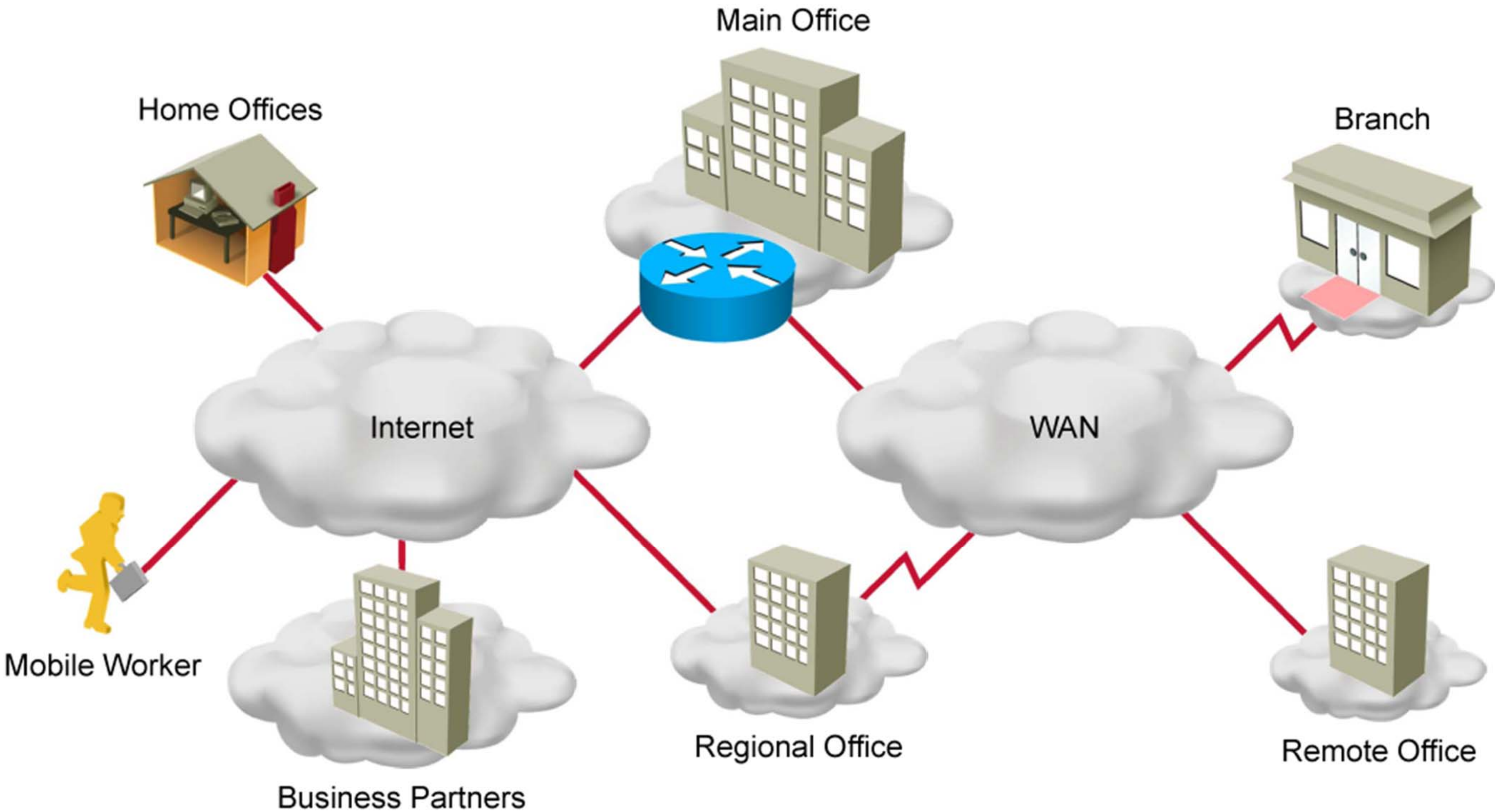
Understanding WAN Technologies

Wide-Area Networks

Introduction to WAN Technologies

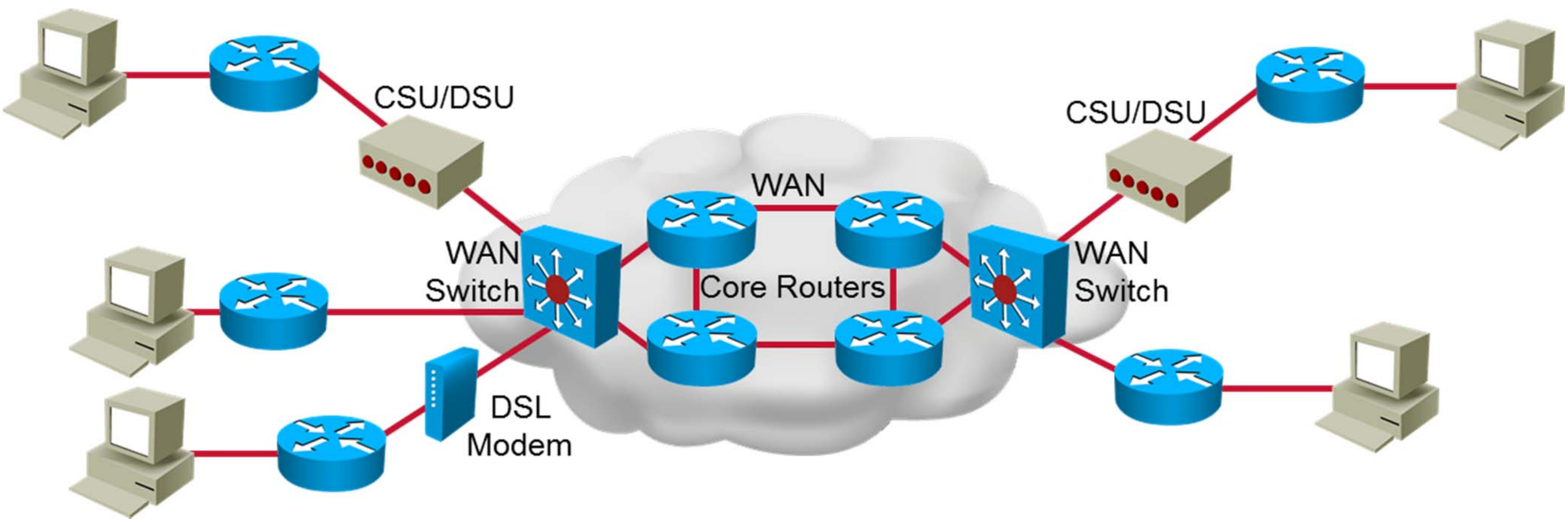


Introduction to WAN Technologies (Cont.)

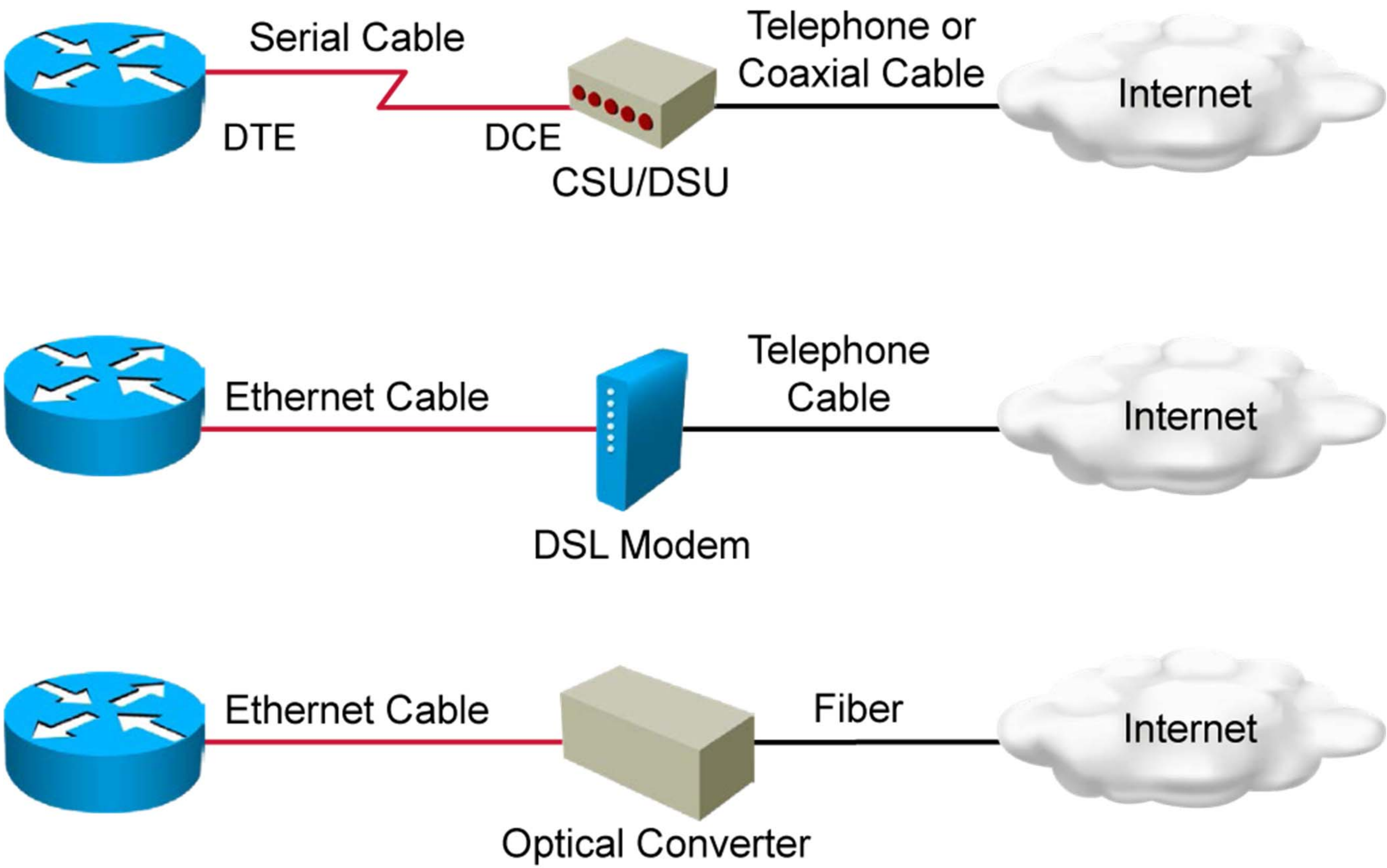


WAN Devices

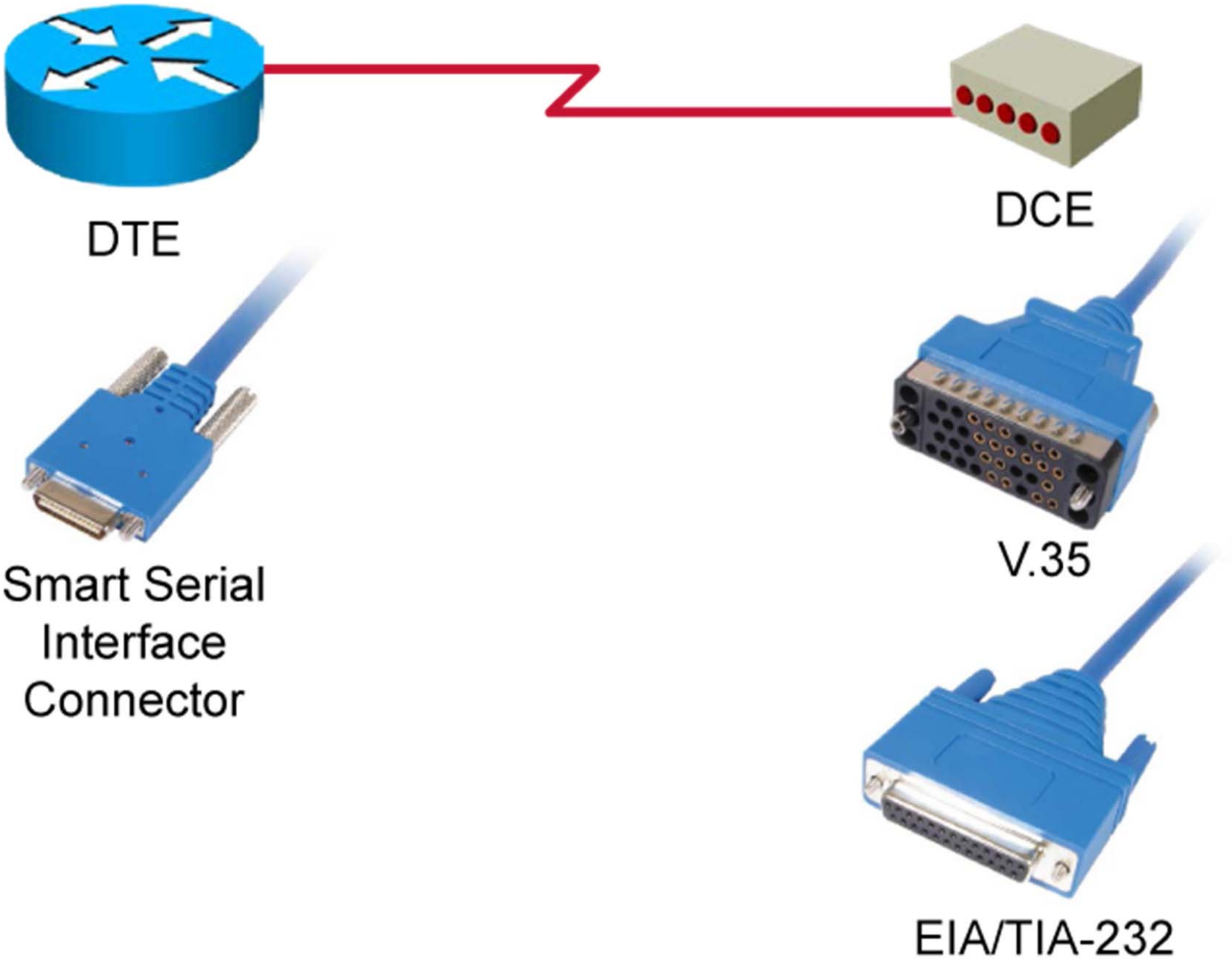
- Routers
- CSU/DSU
- WAN switches
- Core routers
- Modems



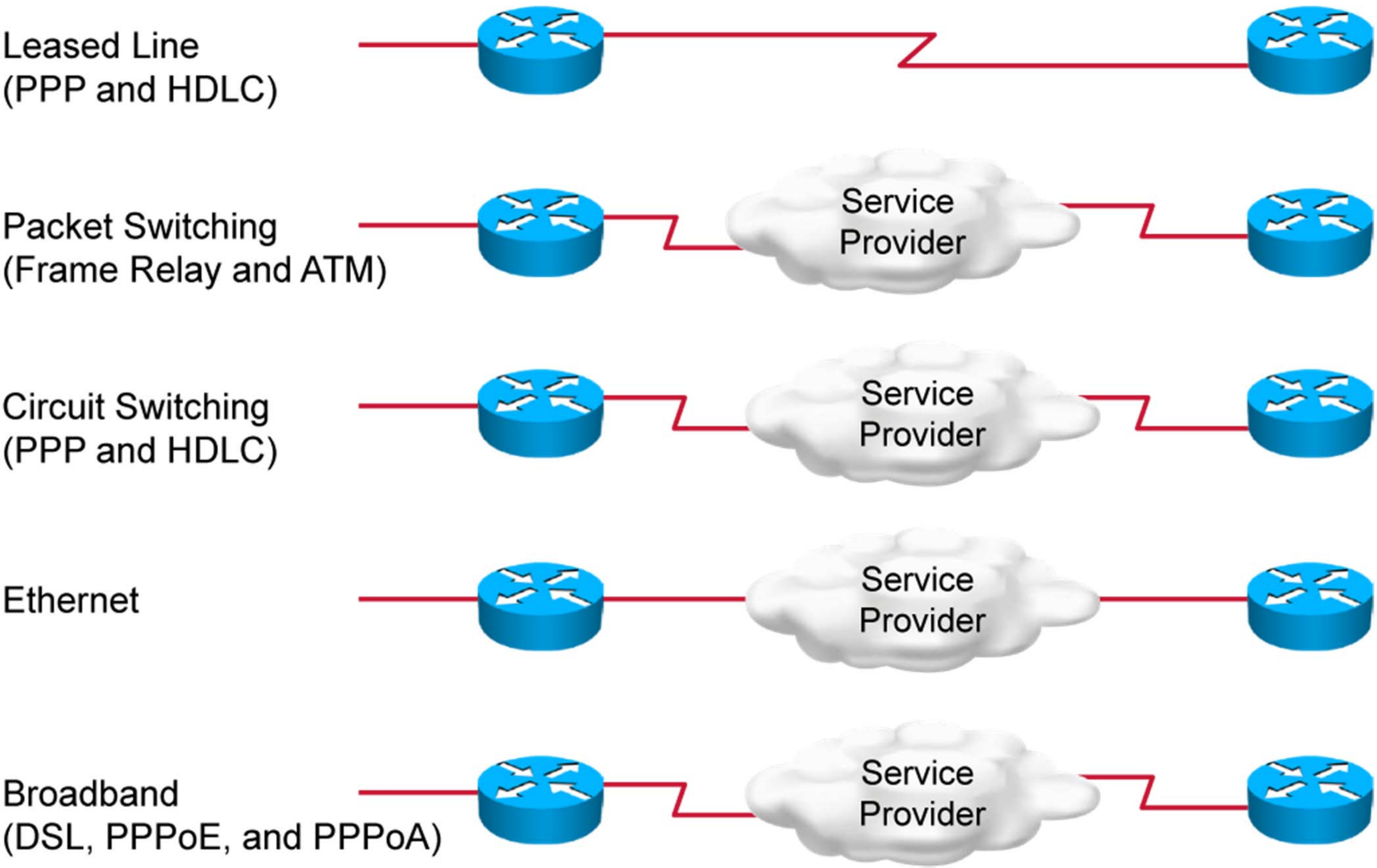
WAN Devices (Cont.)



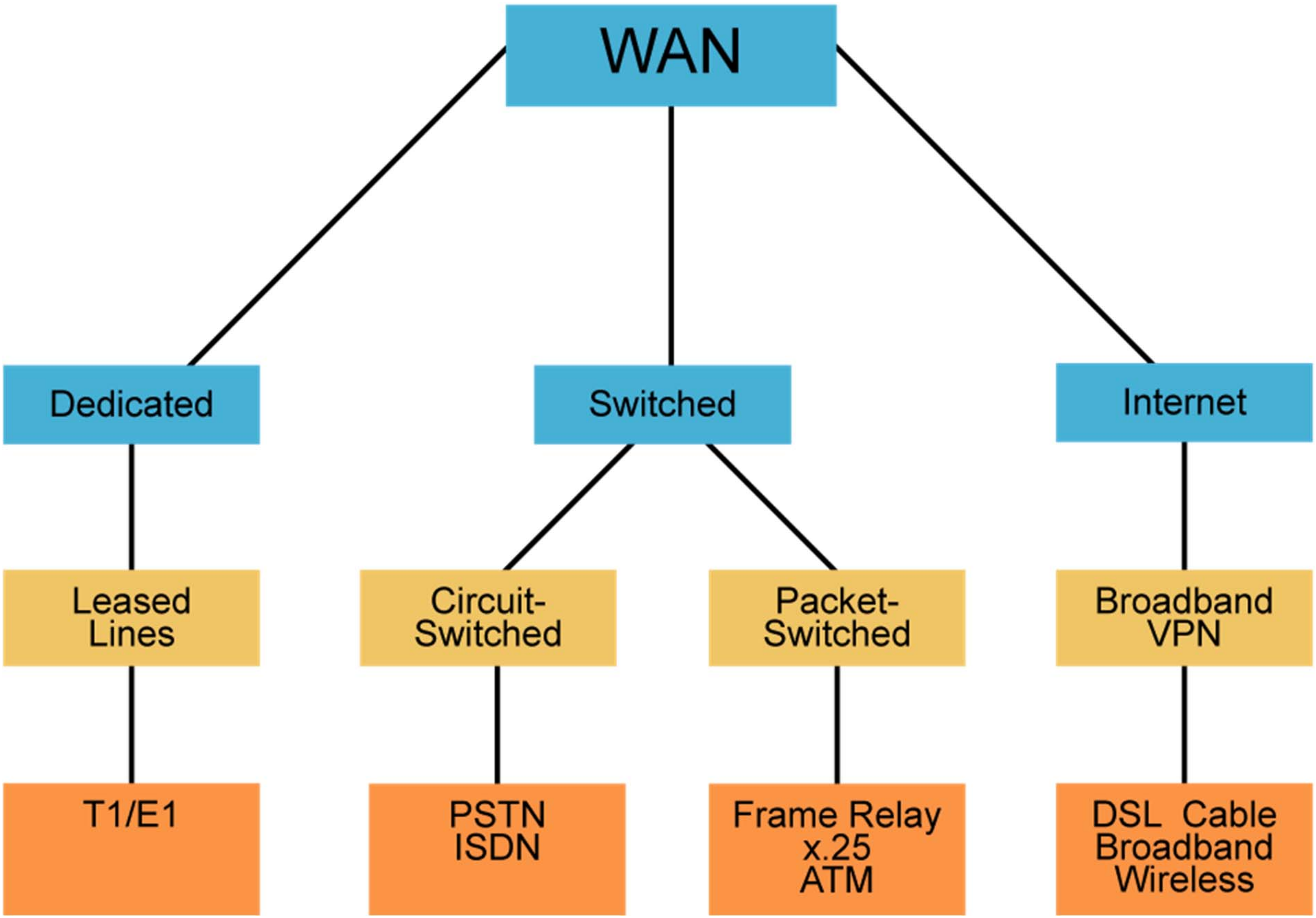
Serial WAN Cabling



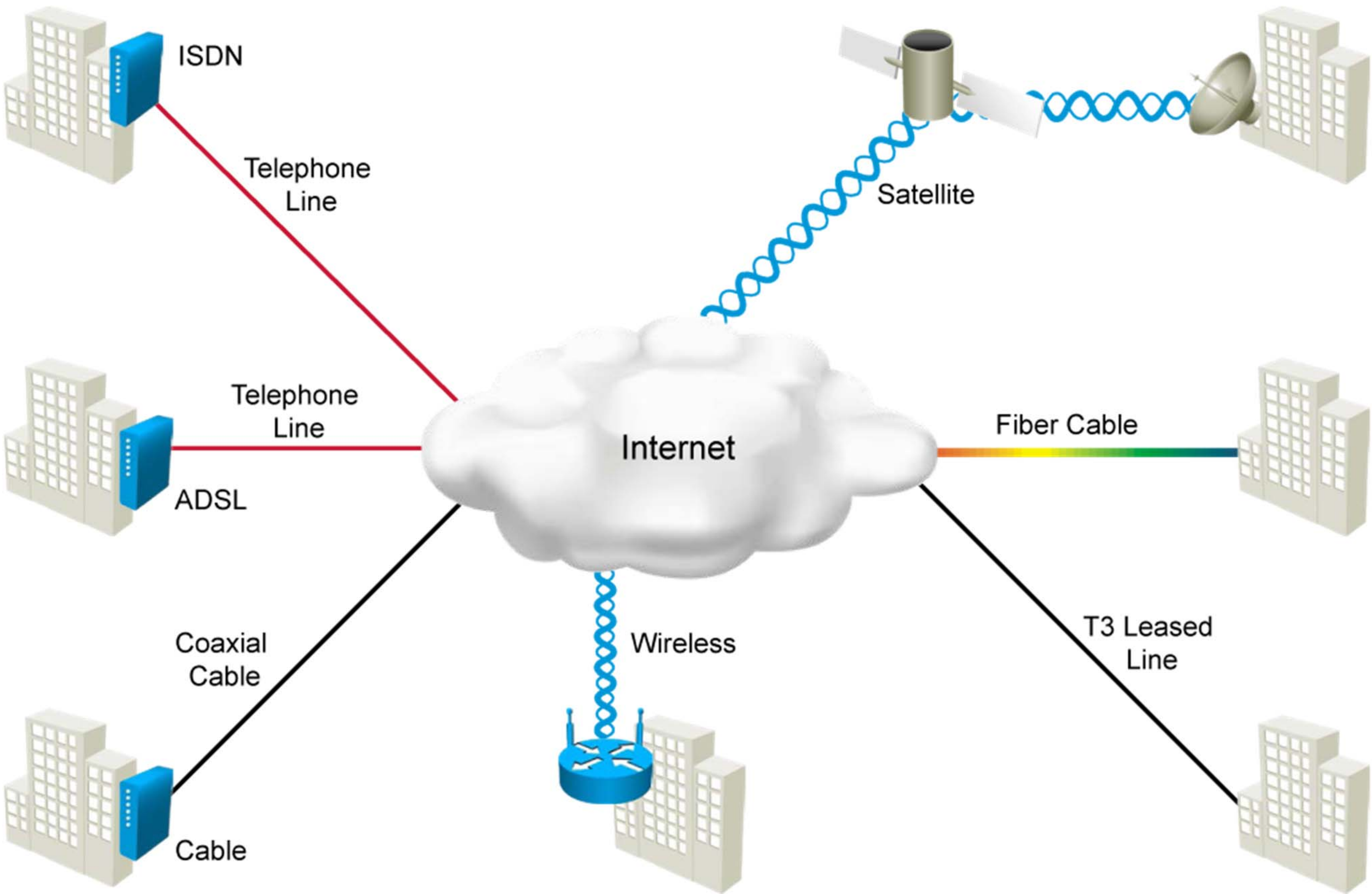
WAN Layer 2 Protocols



WAN Link Options



WAN Link Options (Cont.)



Summary

- There are three major characteristics of a WAN:
  - Connection of devices that are separated by wide geographical distances
  - Use of the services of carriers such as telcos, cable companies, satellite systems, and network providers
  - Use of serial connections of various types to access bandwidth over large geographic areas
- The major types of devices that are used for WAN access environments include routers, modems (CSUs/DSUs), and other networking devices such as WAN switches.
- WAN physical layer protocols establish the codes and electrical parameters that the devices use to communicate with each other. Choosing a protocol is largely determined by the method of facilitation of the service provider.

Summary (Cont.)

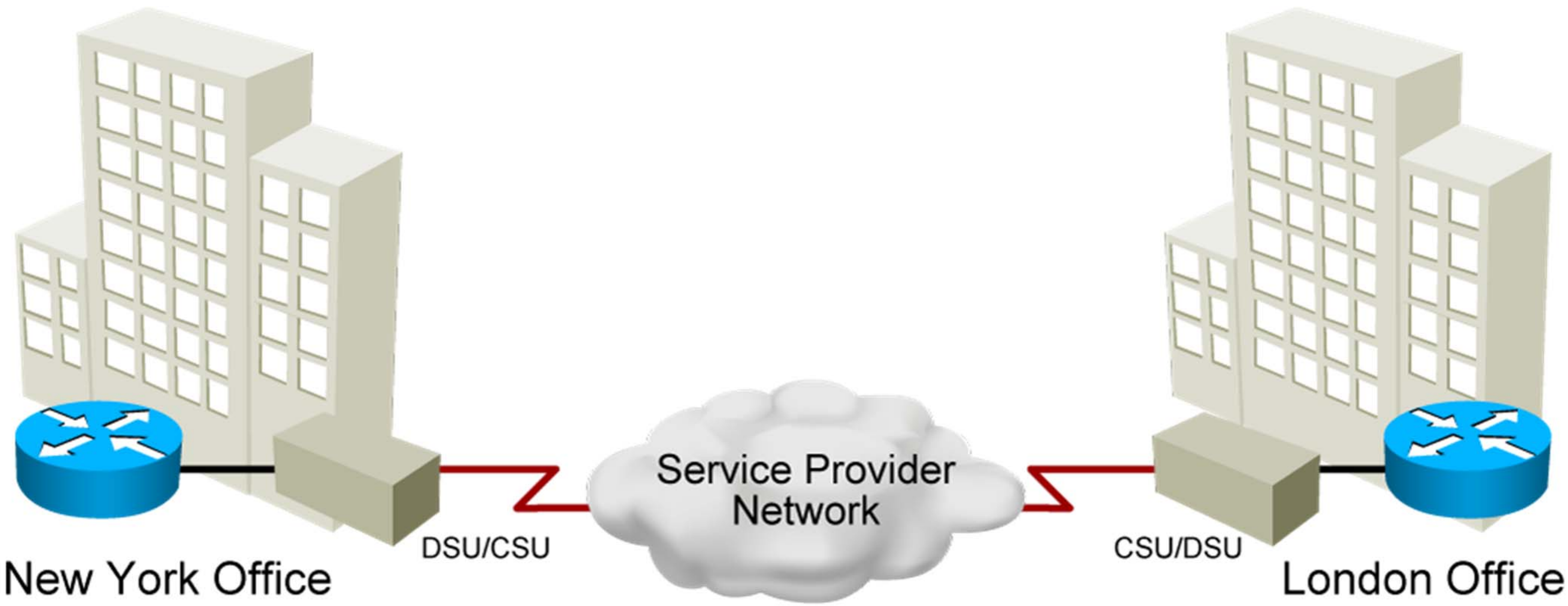
- WANs require data-link layer protocols to establish the link across the communication line from the sending to the receiving device.
- WAN connections can be either over a private infrastructure or over a public infrastructure, such as the Internet. Private WAN connections include both dedicated and switched communication link options.

Configuring Serial Encapsulation

Wide-Area Networks

Serial Communication Links

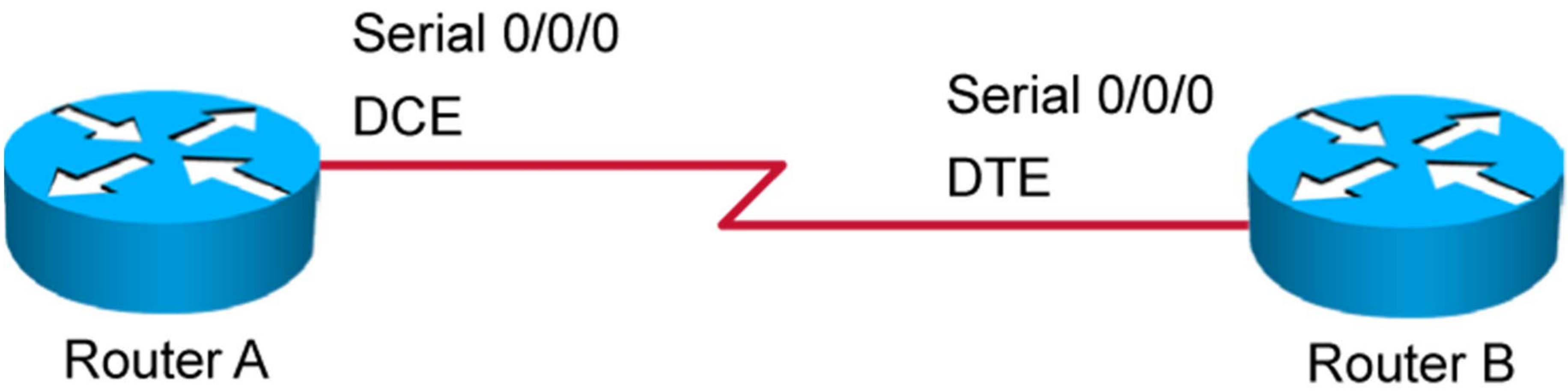
Serial links use leased lines to provide a dedicated connection.



Serial Communication Links (Cont.)

- Typical WAN speeds for the U.S.:
  - T1 = (1.544 Mb/s)
  - T2 = 4 T1 lines (6 Mb/s)
  - T3 = 28 T1 lines (45 Mb/s)
  - T4 = 168 T1 lines (275 Mb/s)
- Typical WAN speeds for Europe:
  - E1 = (2 Mb/s)
  - E2 = 128 E0 lines (8 Mb/s)
  - E3 = 16 E1 lines (34 Mb/s)
  - E4 = 64 E1 lines (140 Mb/s)

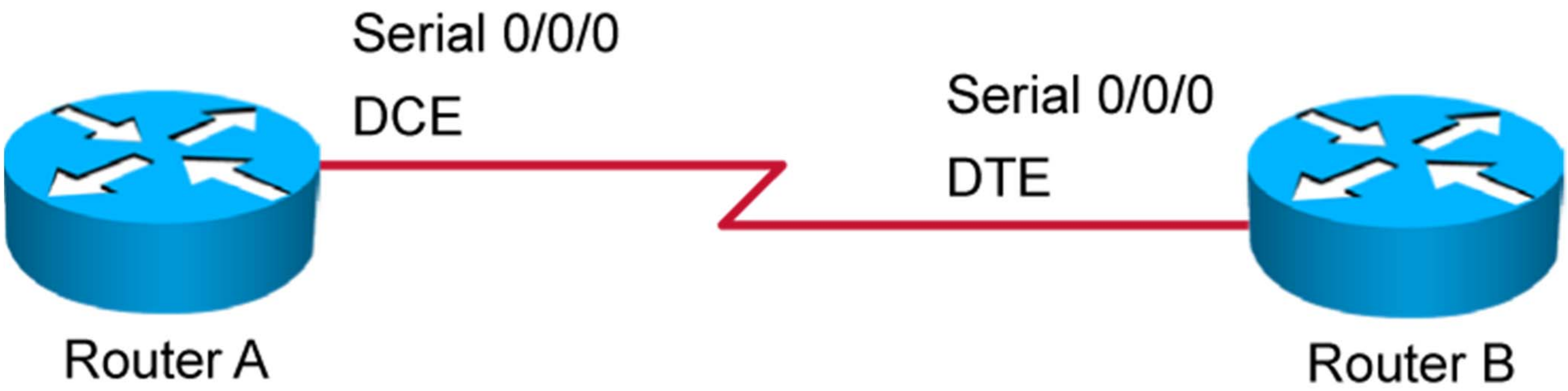
Configuration of a Serial Interface




```
RouterA(config)#interface Serial 0/0/0
RouterA(config-if)#clockrate 64000
RouterA(config-if)#bandwidth 64
RouterA(config-if)#no shutdown
```

Configuration of serial interface on Router A

Configuration of a Serial Interface (Cont.)




```
RouterB(config)#interface Serial 0/0/0
RouterB(config-if)#bandwidth 64
RouterB(config-if)#no shutdown
```

Configuration of serial interface on Router B

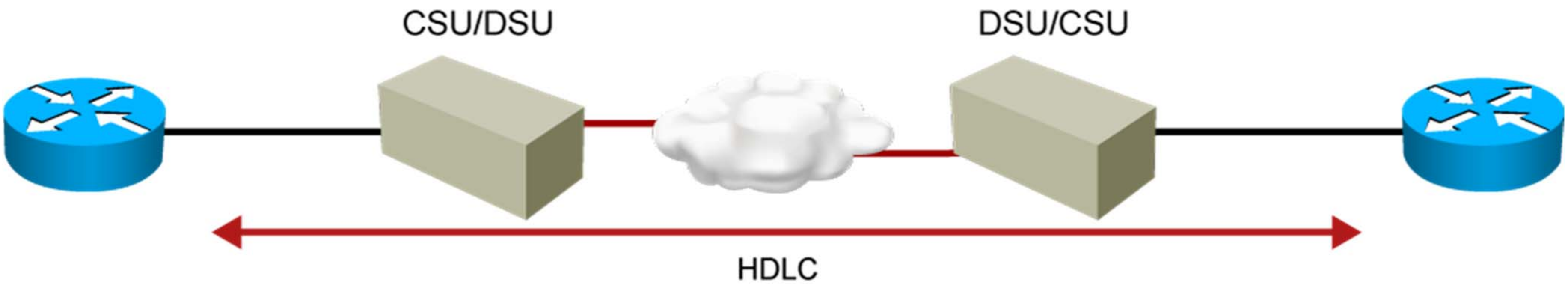
Configuration of a Serial Interface (Cont.)

```
RouterB#show controllers Serial 0/0/0
Interface Serial0/0/0
Hardware is GT96K
DTE V.35idb at 0x4753C1F4, driver data structure at 0x47543900
wic_info 0x47543F2C
Physical Port 1, SCC Num 1
<text omitted>
```

Configuration of serial interface on Router B

HDLC Protocol

HDLC specifies an encapsulation method for data on synchronous serial data links.



HDLC

Flag	Address	Control	Data	FCS	Flag

Cisco HDLC

Flag	Address	Control	Proprietary	Data	FCS	Flag

FCS = Frame Check Sequence

HDLC Protocol (Cont.)

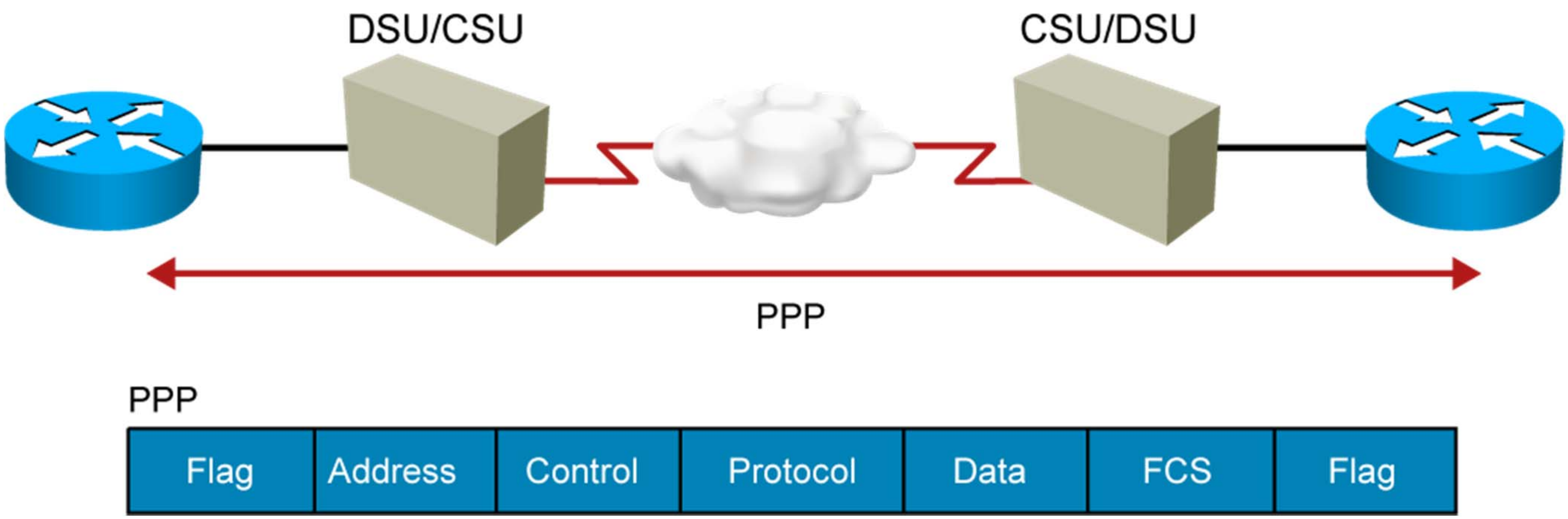
```
RouterA#show interfaces Serial 0/0/0
Serial0/0/0 is up, line protocol is up
 Hardware is GT96K Serial
  Description: Link to HQ
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  CRC checking enabled
  Last input 00:00:02, output 00:00:05, 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
<output omitted>
```

- Verifies correct configuration of HDLC encapsulation on RouterA Serial 0/0/0 interface. By default, Cisco devices use the Cisco HDLC serial encapsulation method on synchronous serial lines.

Point-to-Point Protocol

Overview of PPP:

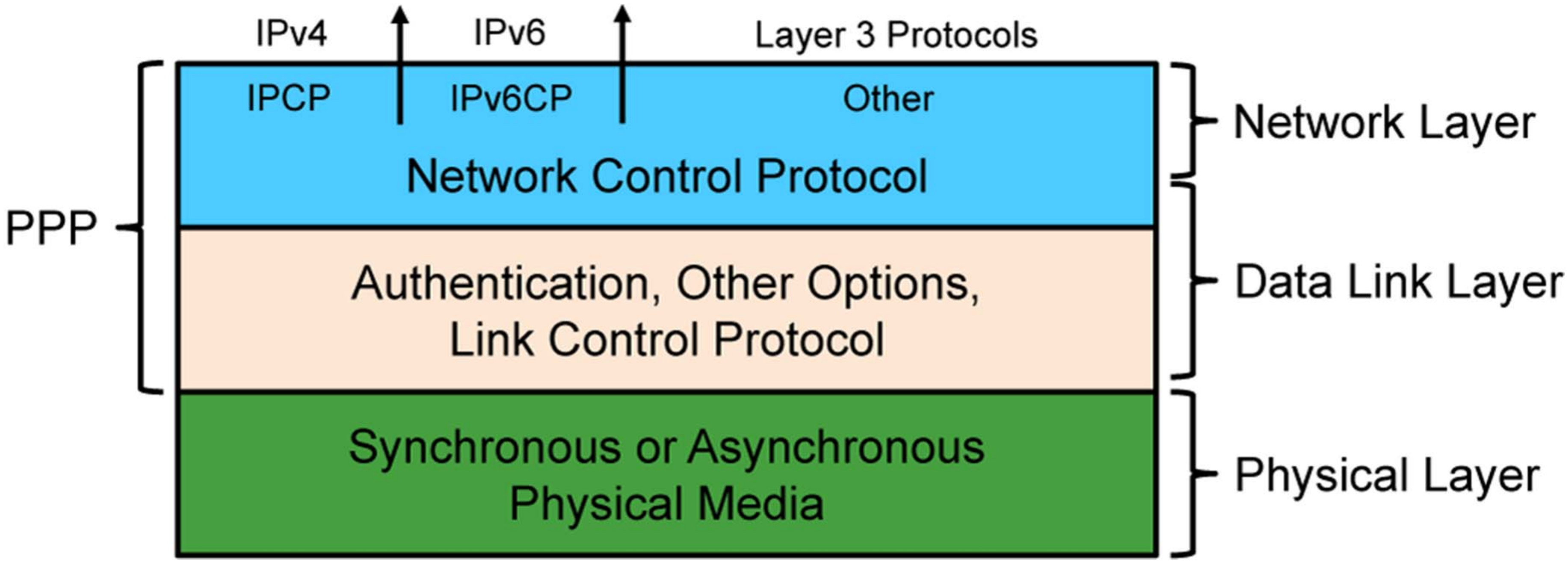
- PPP provides a standard method for transporting datagrams over point-to-point links.
- PPP supports authentication.



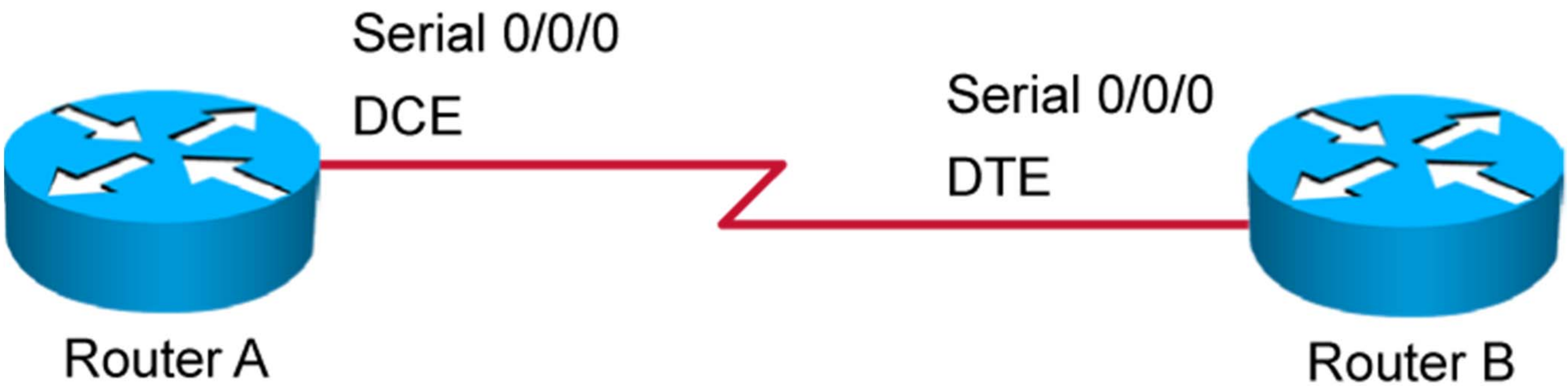
Point-to-Point Protocol (Cont.)

PPP is a layered architecture:

- PPP can carry packets from several protocol suites using NCP.
- PPP controls the setup of several link options using LCP.



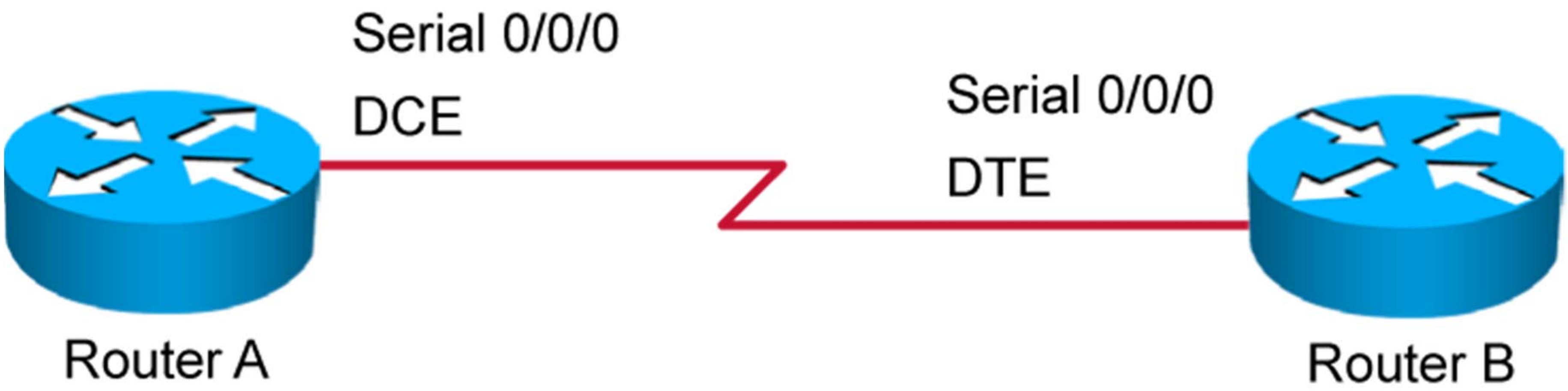
PPP Configuration




```
RouterA(config)#interface Serial 0/0/0
RouterA(config-if)#ip address 10.0.1.1 255.255.255.0
RouterA(config-if)#encapsulation ppp
RouterA(config-if)#bandwidth 512
RouterA(config-if)#clockrate 64000
RouterA(config-if)#no shutdown
```

PPP configuration on Router A

PPP Configuration (Cont.)




```
RouterB(config)#interface Serial 0/0/0
RouterB(config-if)#ip address 10.0.1.2 255.255.255.0
RouterB(config-if)#encapsulation ppp
RouterB(config-if)#bandwidth 512
RouterB(config-if)#no shutdown
```

PPP configuration on Router B

PPP Configuration (Cont.)

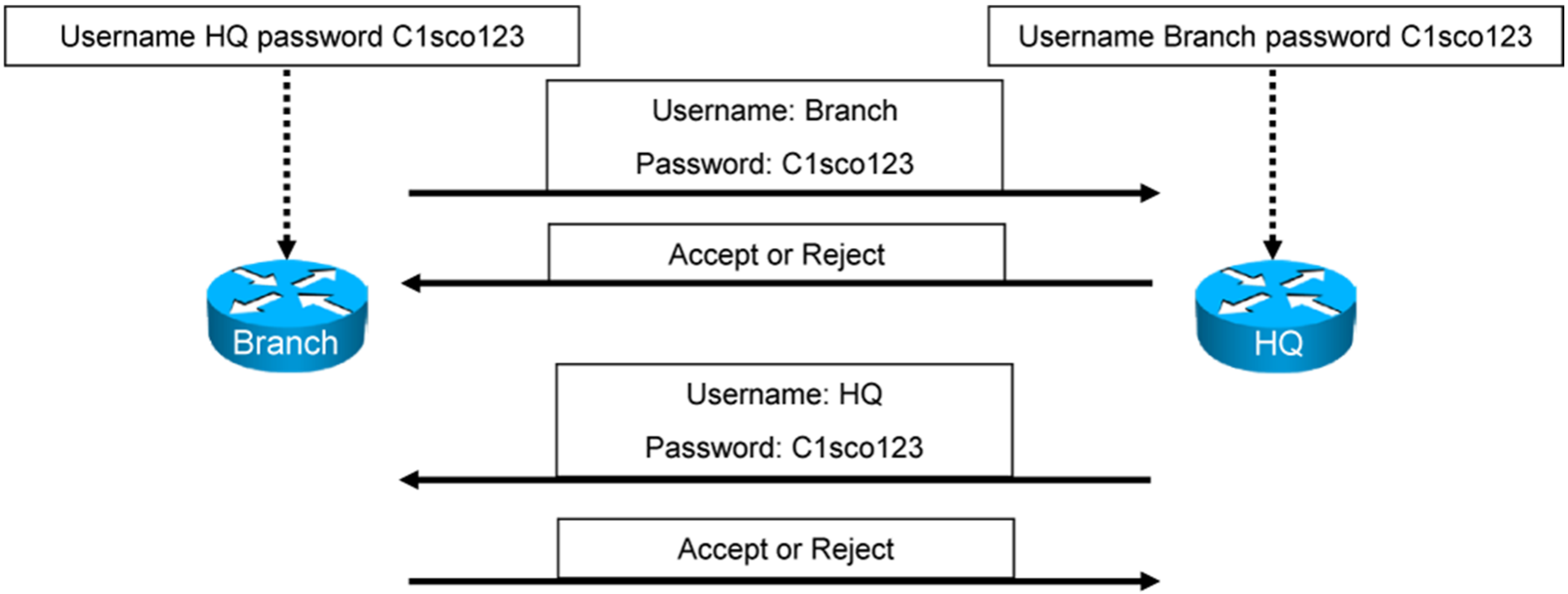
```
RouterA#show interfaces Serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Description: Link to RouterB
  Internet address is 10.0.1.1/24
  MTU 1500 bytes, BW 512 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, CDPCP, loopback not set
  Keepalive set (10 sec)
  CRC checking enabled
  Last input 00:00:36, output 00:00:01, output hang never
  Last clearing of "show interface" counters 00:01:09
  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 384 kilobits/sec
<output omitted>
```

Verifies that proper encapsulation is enabled on the Serial 0/0/0 interface.

PPP Authentication: PAP

Password Authentication Protocol:

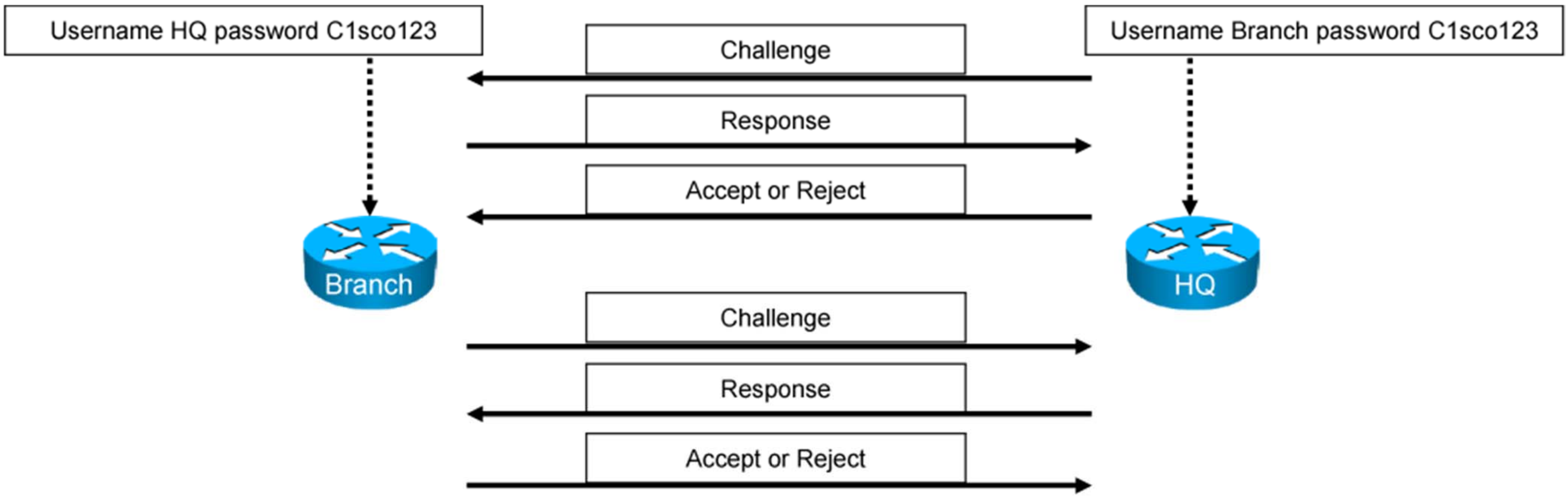
- Passwords are sent in plaintext.
- The peer is in control of attempts.



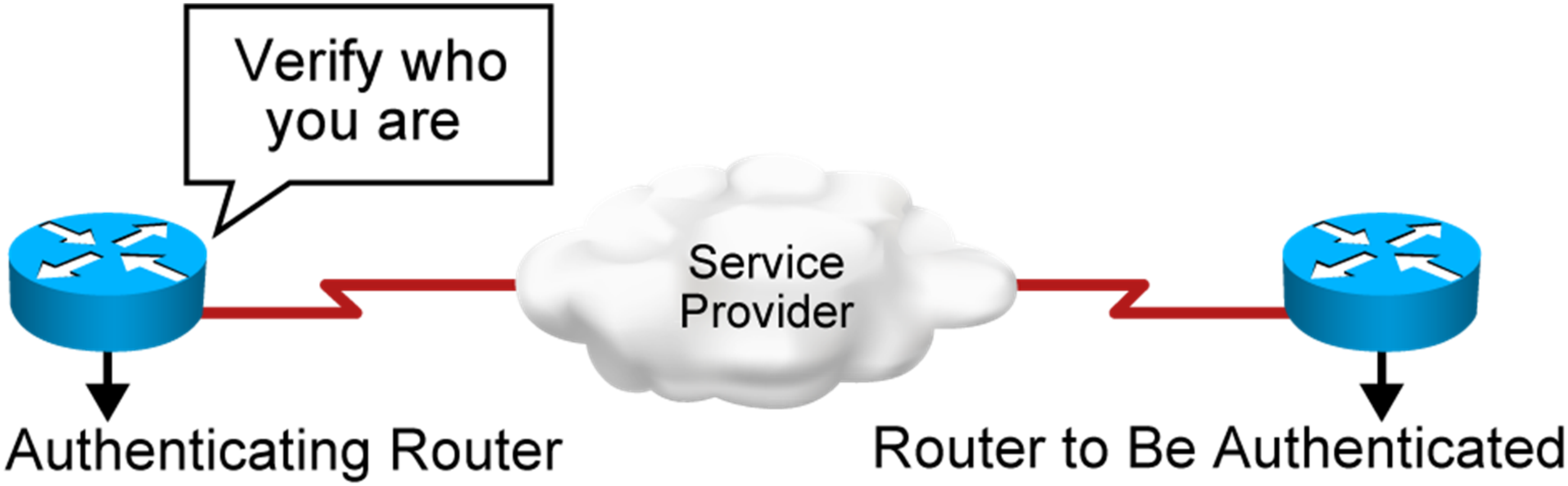
PPP Authentication: CHAP

Challenge Handshake Authentication Protocol:

- Hash values, not actual passwords, are sent across the link.
- The local router or external server is in control of authentication attempts.



Configuring CHAP for PPP Authentication



Authenticating Router

Enabling PPP

- ☑ PPP encapsulation

Enabling PPP Authentication

- ☑ Hostname
- ☑ Username and password
- ☑ PPP authentication

Router to Be Authenticated

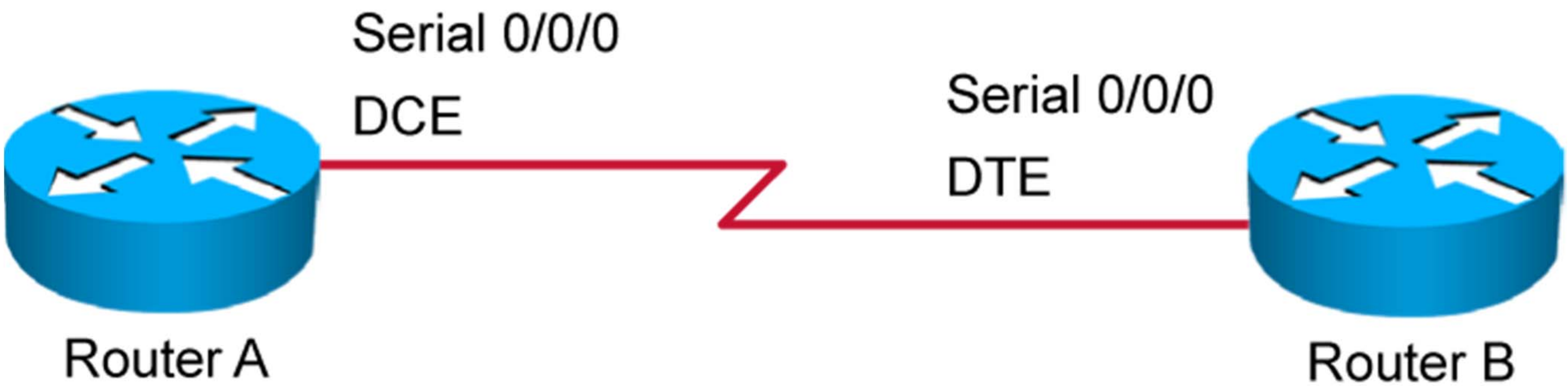
Enabling PPP

- ☑ PPP encapsulation

Enabling PPP Authentication

- ☑ Hostname
- ☑ Username and password
- ☑ PPP authentication

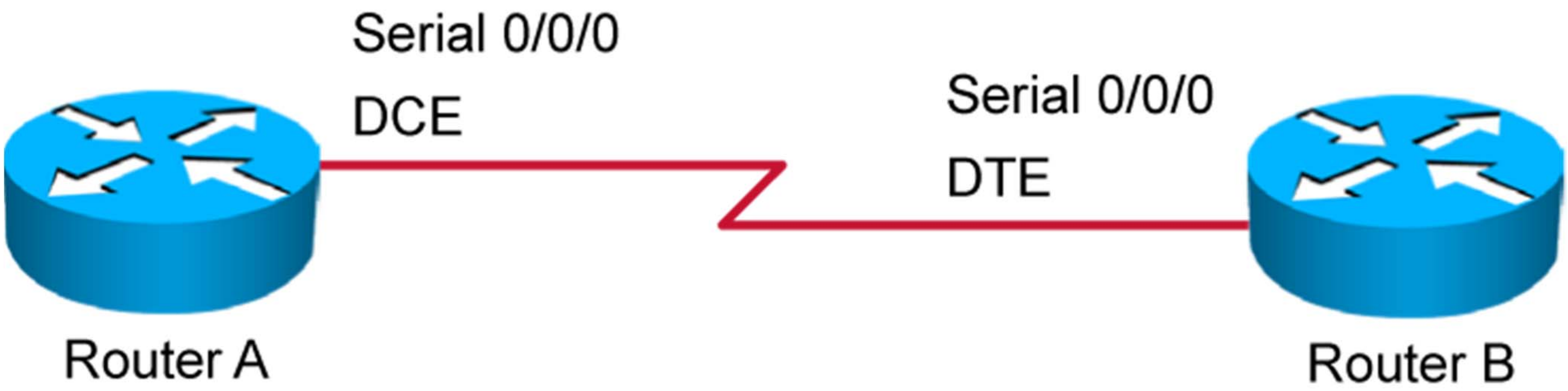
Configuring CHAP for PPP Authentication (Cont.)




```
Router(config)#hostname RouterA
RouterA(config)#username RouterB password C1sco123
RouterA(config)#interface Serial 0/0/0
RouterA(config-if)#ip address 10.0.1.1 255.255.255.0
RouterA(config-if)#encapsulation ppp
RouterA(config-if)#ppp authentication chap
RouterA(config-if)#clockrate 64000
```

Configuring CHAP authentication on Router A

Configuring CHAP for PPP Authentication (Cont.)




```
Router(config)#hostname RouterB
RouterB(config)#username RouterA password C1sco123
RouterB(config)#interface Serial 0/0/0
RouterB(config-if)#ip address 10.0.1.2 255.255.255.0
RouterB(config-if)#encapsulation ppp
RouterB(config-if)#ppp authentication chap
```

Configuring CHAP authentication on Router B

Verifying CHAP Configuration

```
RouterA#show interfaces Serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.0.1.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, CDPCP, loopback not set
  Keepalive set (10 sec)
  CRC checking enabled
  Last input 00:00:21, output 00:00:03, output hang never
  Last clearing of "show interface" counters 00:00:47
  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
<output omitted>
```

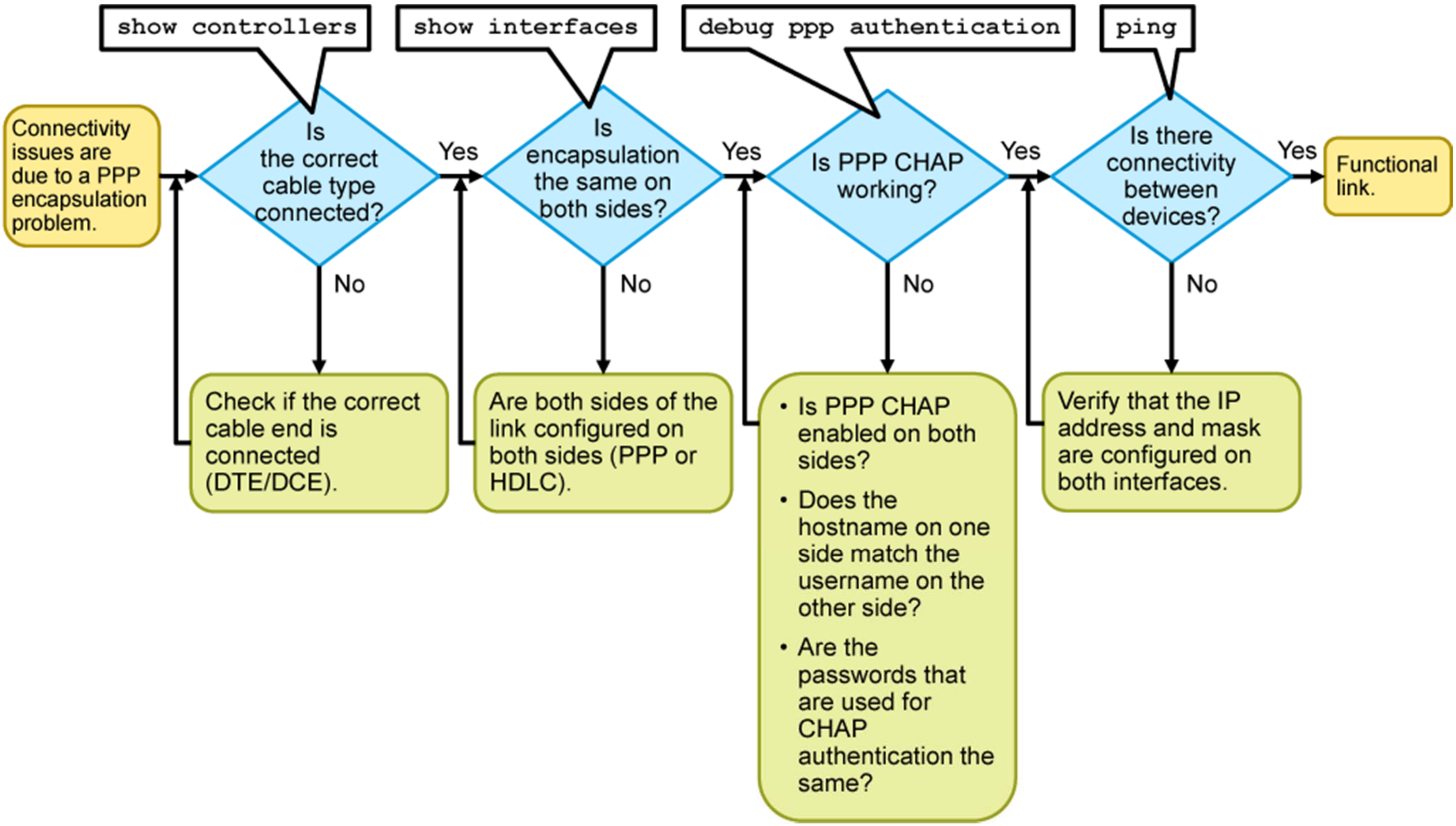
Verifies the PPP encapsulation configuration on the Serial 0/0/0 interface and verifies that the connection is still working after configuring authentication.

Verifying CHAP Configuration (Cont.)

```
RouterA#debug ppp authentication
Oct 23 11:08:10.642: %LINK-3-UPDOWN: Interface Serial0/0/0, changed state
to up
Oct 23 11:08:10.642: Se0/0/0 PPP: Authorization required
Oct 23 11:08:10.674: Se0/0/0 CHAP: O CHALLENGE id 4 len 28 from "RouterX"
Oct 23 11:08:10.718: Se0/0/0 CHAP: I CHALLENGE id 1 len 28 from "RouterY"
Oct 23 11:08:10.718: Se0/0/0 CHAP: Using hostname from unknown source
Oct 23 11:08:10.718: Se0/0/0 CHAP: Using password from AAA
Oct 23 11:08:10.718: Se0/0/0 CHAP: O RESPONSE id 1 len 28 from "RouterX"
Oct 23 11:08:10.722: Se0/0/0 CHAP: I RESPONSE id 4 len 28 from "RouterY"
Oct 23 11:08:10.722: Se0/0/0 PPP: Sent CHAP LOGIN Request
Oct 23 11:08:10.726: Se0/0/0 PPP: Received LOGIN Response PASS
Oct 23 11:08:10.726: Se0/0/0 PPP: Sent LCP AUTHOR Request
Oct 23 11:08:10.726: Se0/0/0 PPP: Sent IPCP AUTHOR Request
Oct 23 11:08:10.726: Se0/0/0 LCP: Received AAA AUTHOR Response PASS
Oct 23 11:08:10.726: Se0/0/0 IPCP: Received AAA AUTHOR Response PASS
Oct 23 11:08:10.726: Se0/0/0 CHAP: O SUCCESS id 4 len 4
Oct 23 11:08:10.742: Se0/0/0 CHAP: I SUCCESS id 1 len 4
Oct 23 11:08:11.742: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to up
```

The **debug ppp authentication** command shows the successful CHAP output and verifies PPP authentication.

Troubleshooting Serial Connections



Summary

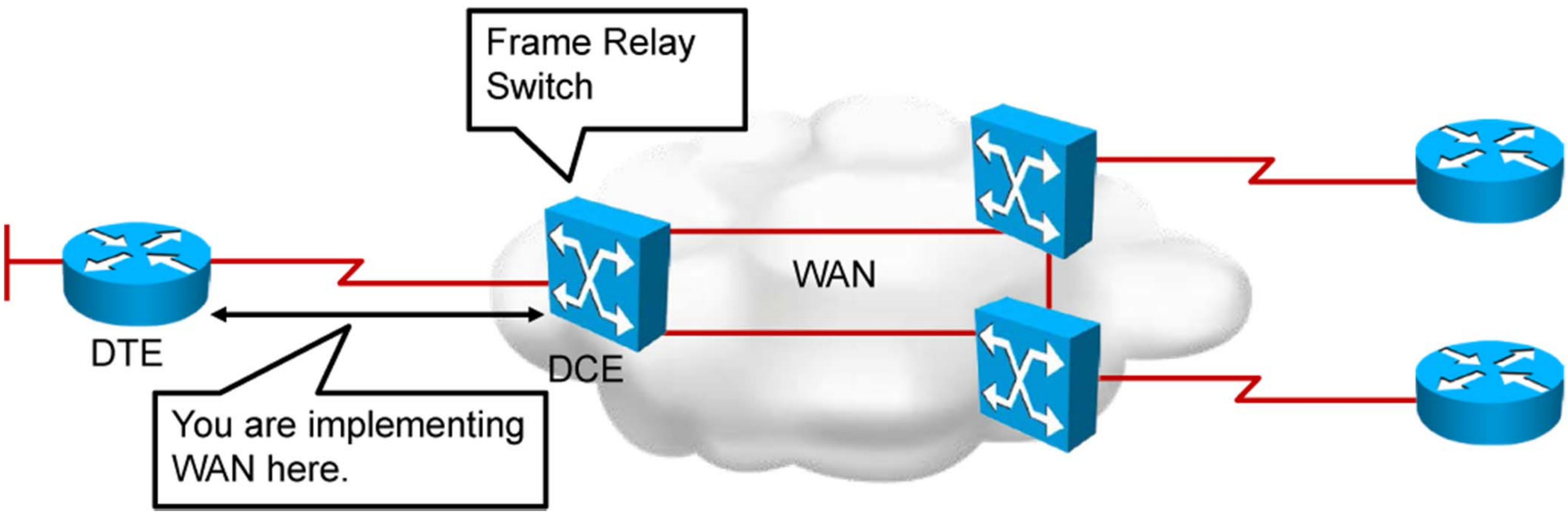
- In addition to the ISO-developed HDLC, there is a Cisco implementation of HDLC, which is the default encapsulation for serial lines on Cisco routers.
- PPP is a common Layer 2 protocol for the WAN. There are two components of PPP: LCP, which negotiates the connection, and NCP, which encapsulates traffic.
- To set PPP as the encapsulation method to be used by a serial interface, use the **encapsulation ppp** interface configuration command.
- You can configure PPP to use PAP or CHAP. PAP sends everything in plaintext. CHAP uses an MD5 hash.
- For CHAP authentication, the remote device must have a corresponding username entry for the local router, with a matching password.

Establishing a WAN Connection Using Frame Relay

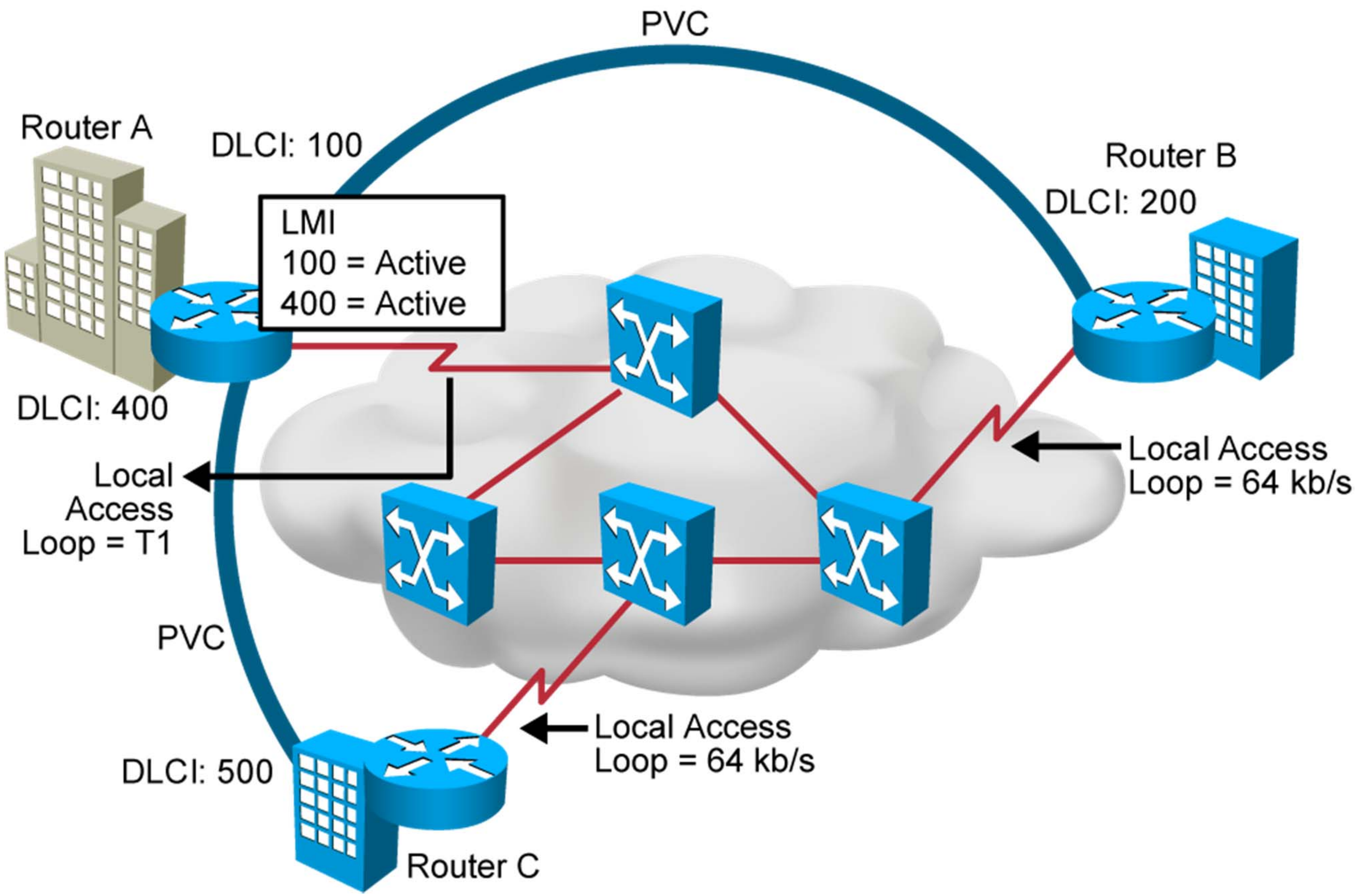
Wide-Area Networks

Understanding Frame Relay

- Used for WAN networks
- Connection-oriented, packet-switching service
- Connections made by virtual circuits

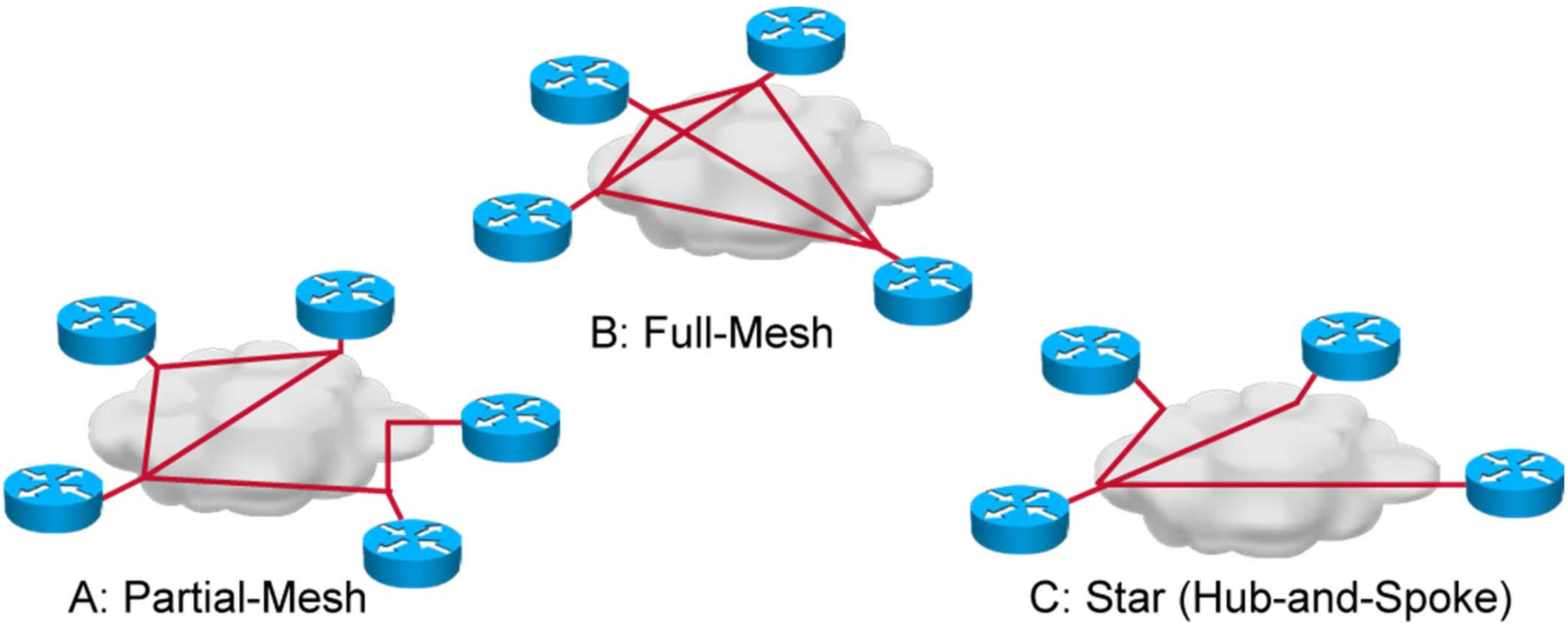


Understanding Frame Relay (Cont.)



Frame Relay Topologies

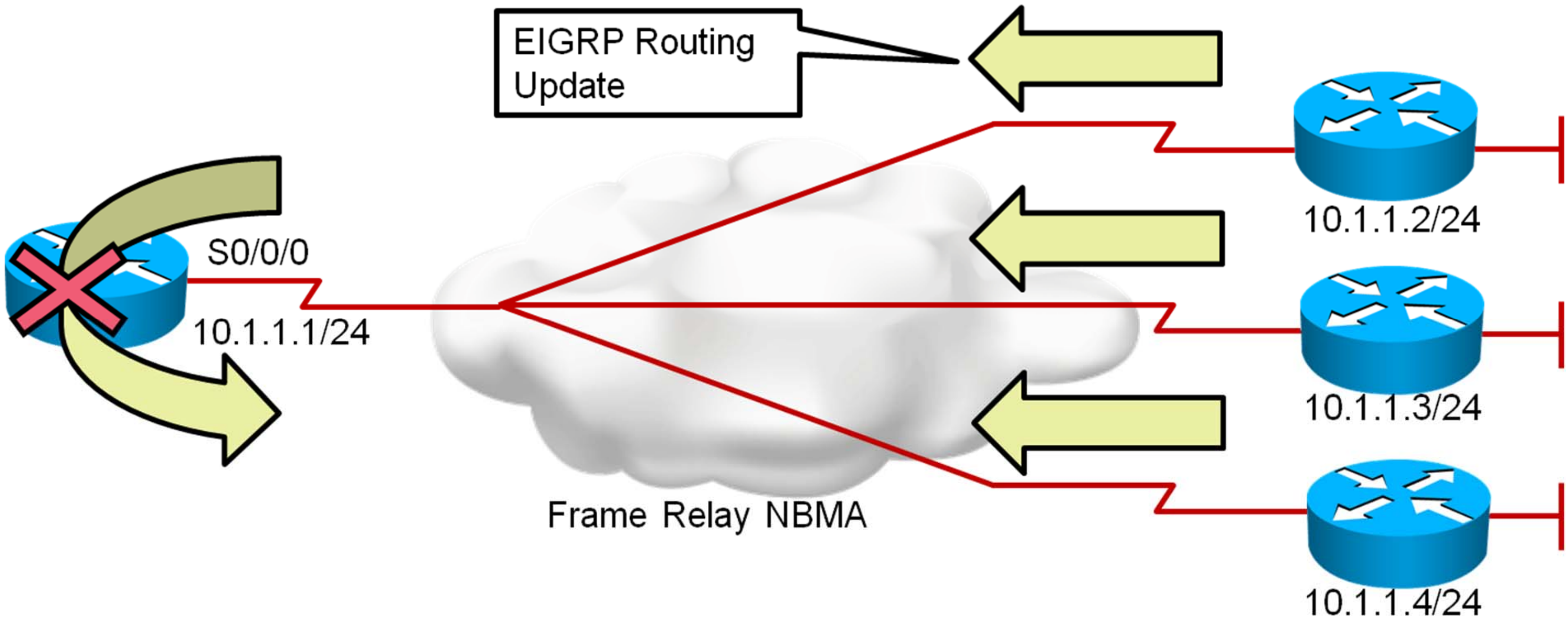
Frame Relay provides NBMA connectivity.



Frame Relay Reachability Issues

Frame Relay NBMA connectivity causes issues with routing protocols:

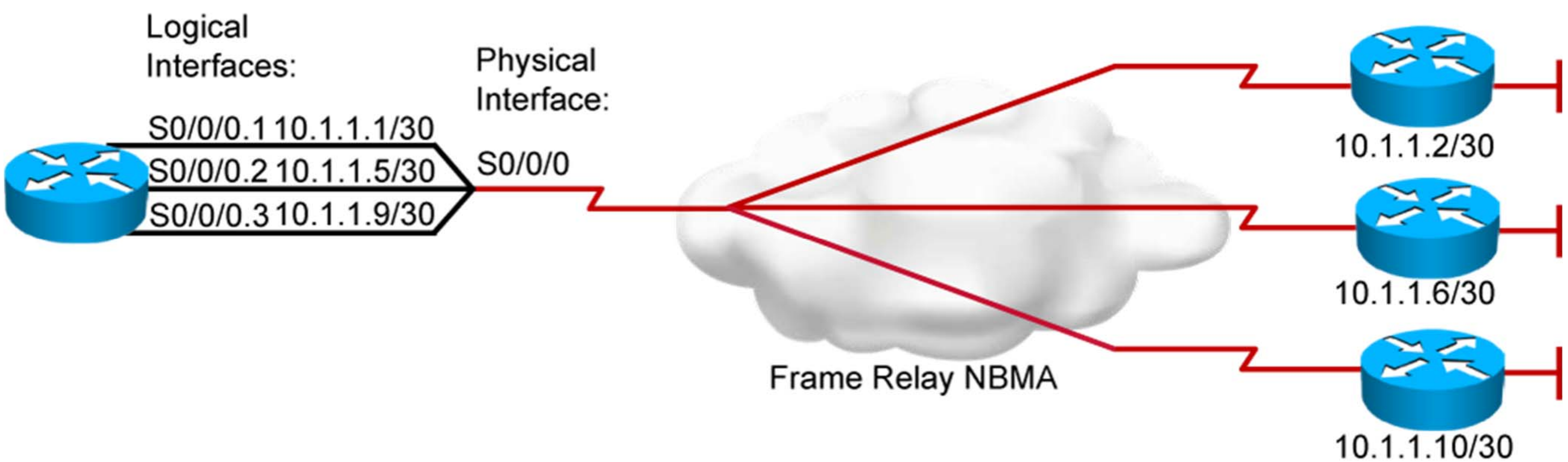
- Split horizon (EIGRP)
- Neighbor discovery and DR and BDR election (OSPF)
- Broadcast replication



Frame Relay Reachability Issues (Cont.)

Subinterfaces are one solution to routing problems in NBMA networks:

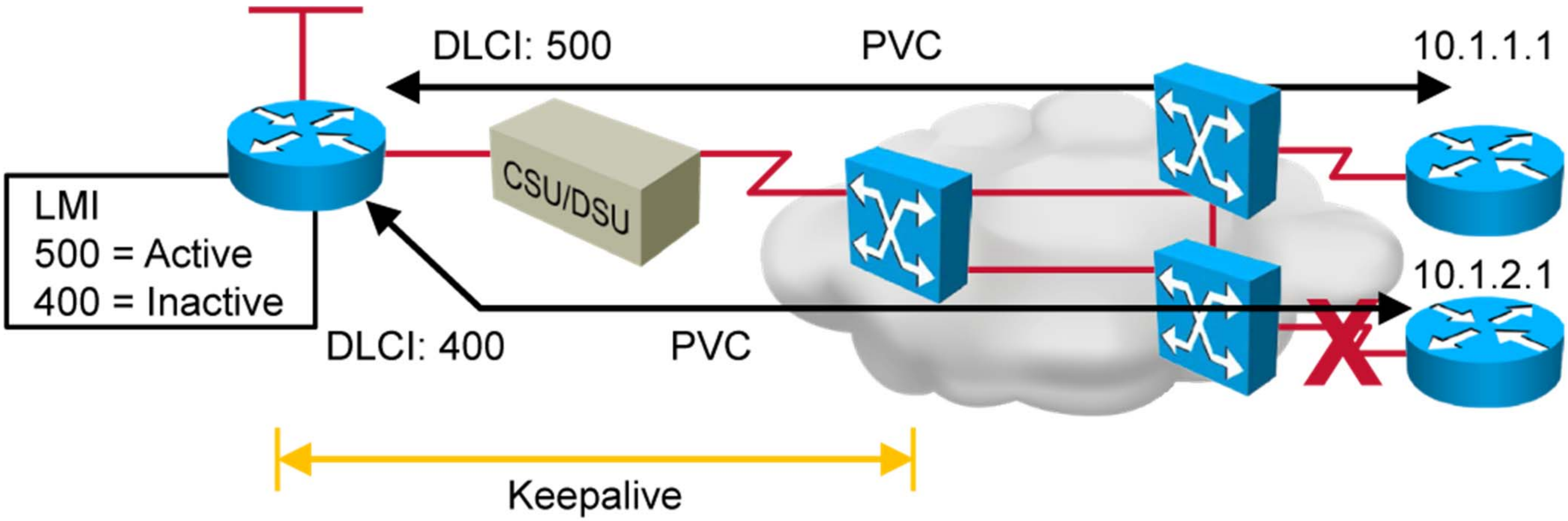
- A physical interface simulates multiple, logical, point-to-point interfaces.
- Each subinterface is on a separate IP network.
- Each subinterface is associated with a Frame Relay PVC.



Frame Relay Signaling

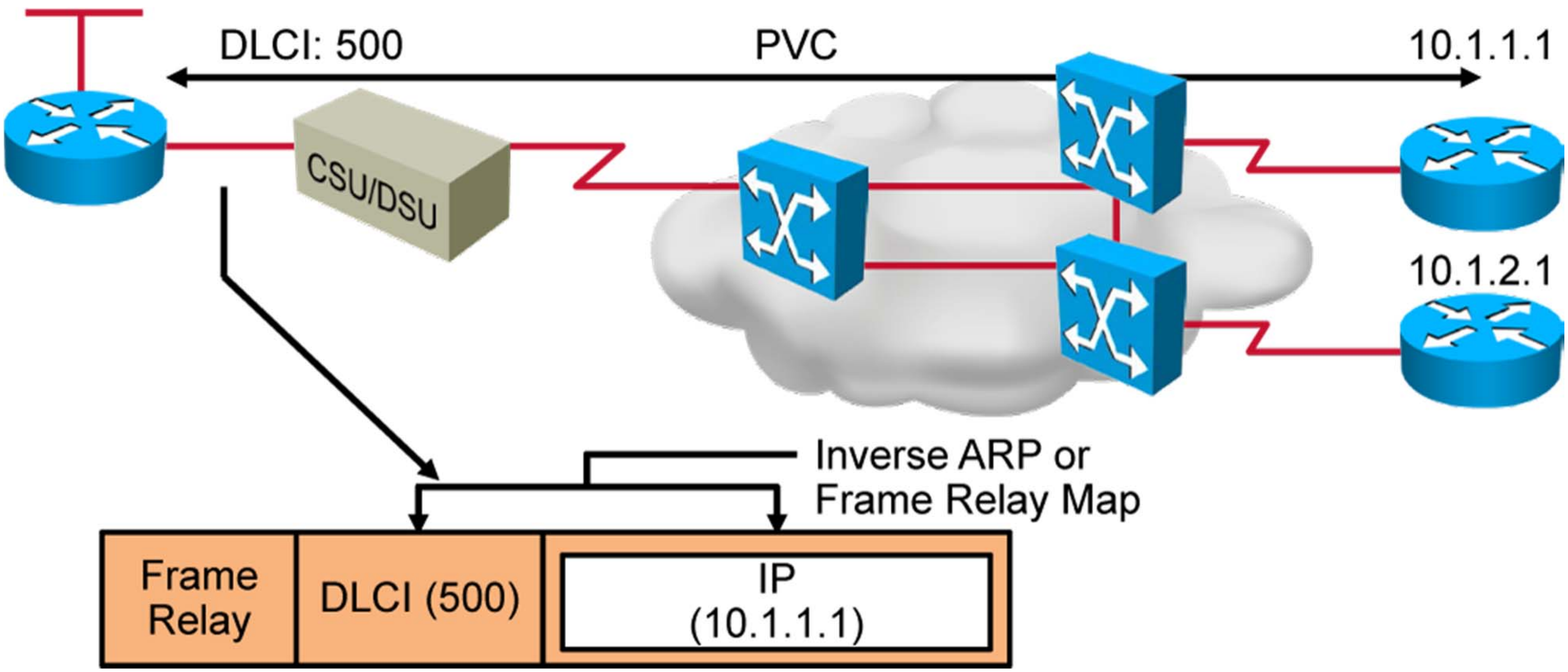
Cisco supports three LMI standards:

- Cisco
- ANSI T1.617 Annex D
- Q.933 ITU-T Annex A

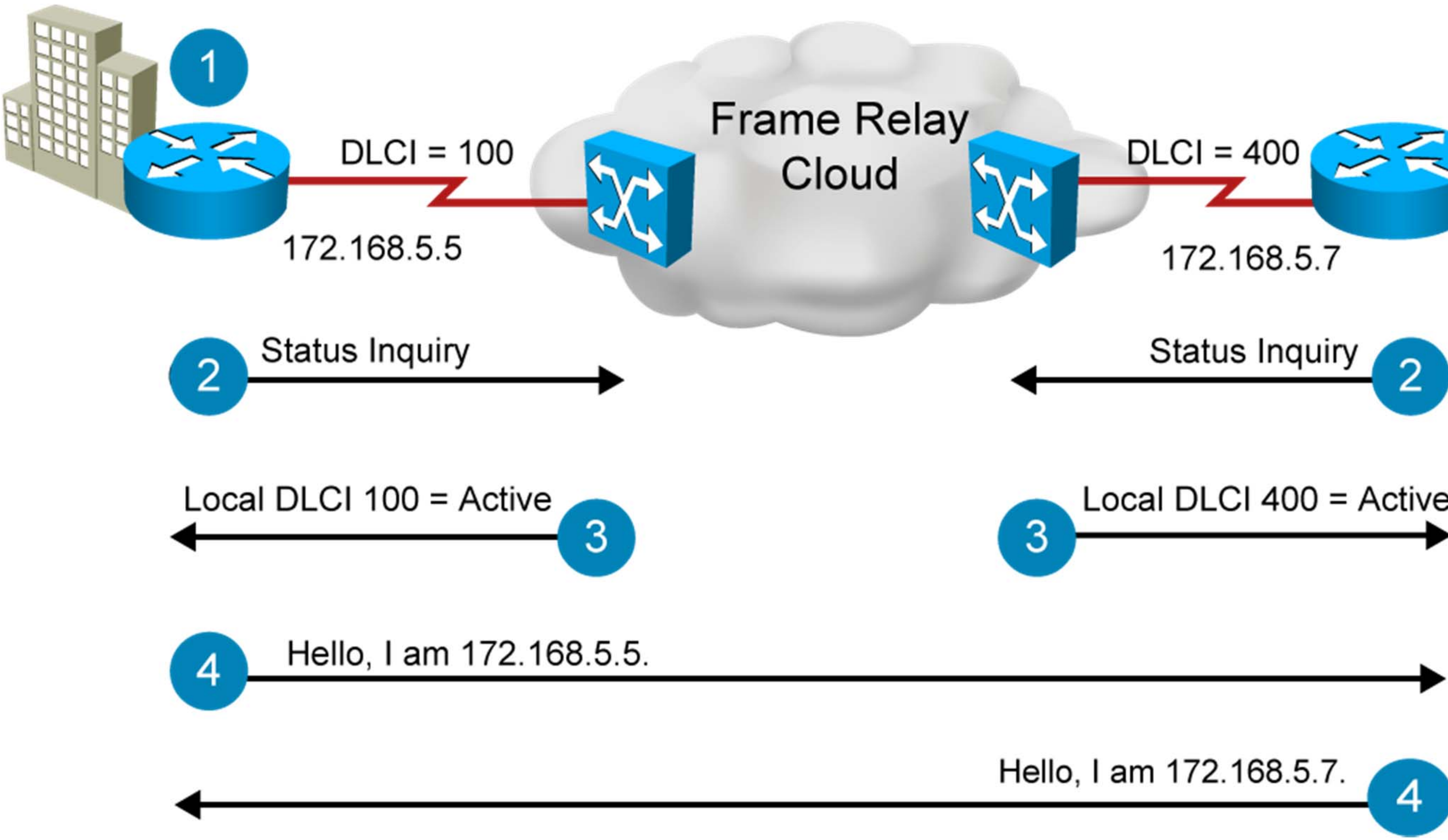


Frame Relay Address Mapping

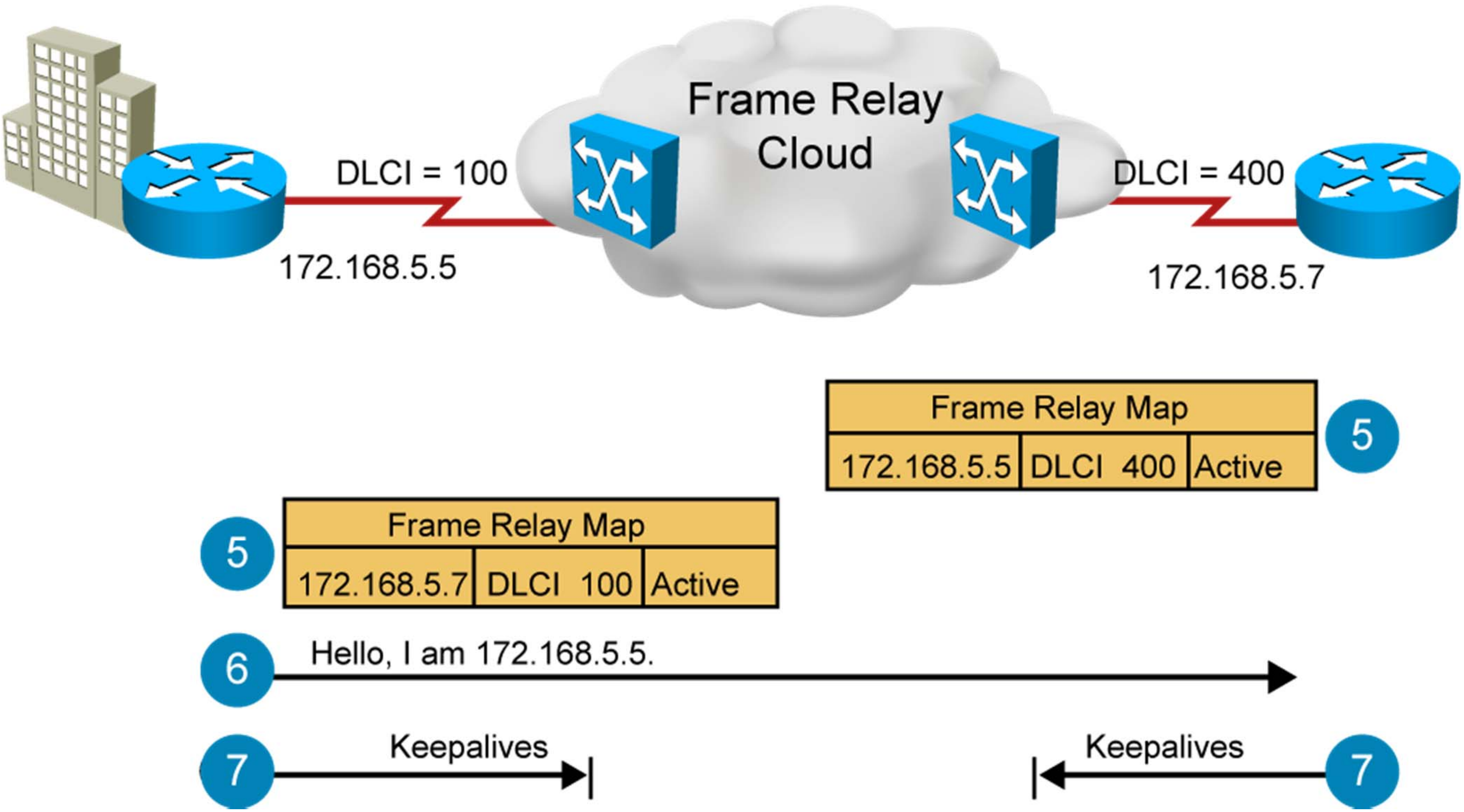
- Automatic discovery of DLCI is from the Frame Relay switch using LMI.
- Local DLCI must be mapped to a destination network layer address:
  - Automatic mapping with Inverse ARP
  - Manual configuration using a static Frame Relay map



Frame Relay Address Mapping (Cont.)



Frame Relay Address Mapping (Cont.)

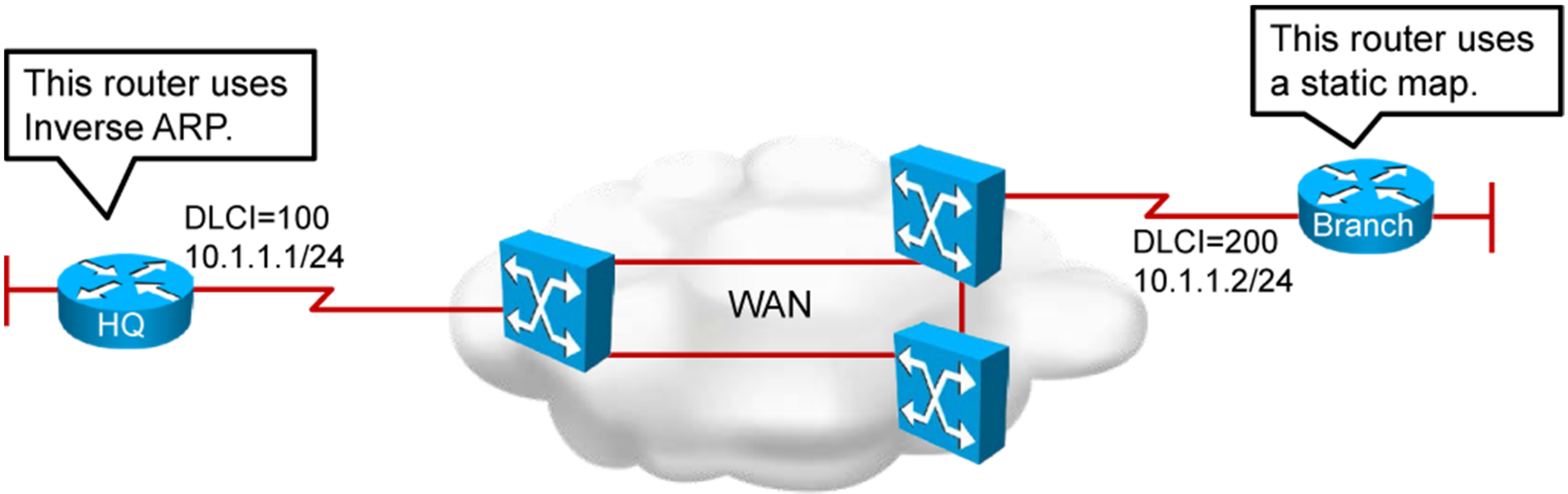


Frame Relay Address Mapping (Cont.)

Configure a static Frame Relay map in these situations:

- A Frame Relay peer does not support Inverse ARP.
- You want to control broadcast traffic across a PVC.
- You want to have different Frame Relay encapsulations across PVCs.

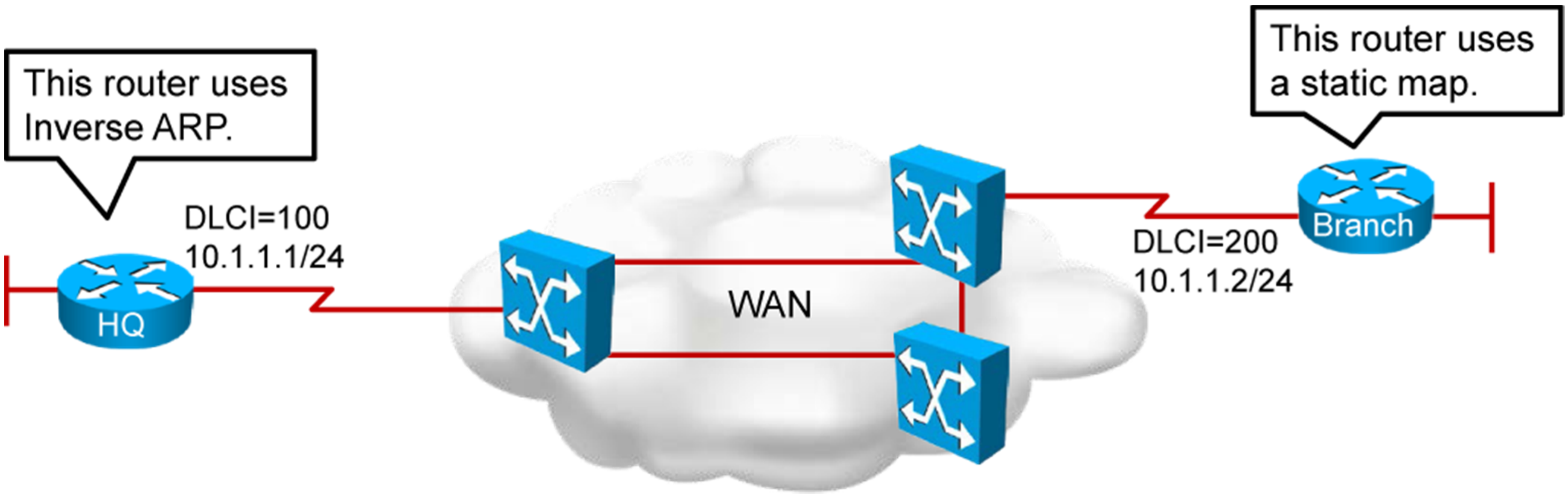
Configuring Frame Relay




```
HQ(router)#interface Serial0/0/0
HQ(router-if)#ip address 10.1.1.1 255.255.255.0
HQ(router-if)#encapsulation frame-relay
HQ(router-if)#bandwidth 64
```

Configuration on the HQ router

Configuring Frame Relay (Cont.)




```
Branch(router)#interface Serial0/0/0
Branch(router-if)#ip address 10.1.1.2 255.255.255.0
Branch(router-if)#encapsulation frame-relay
Branch(router-if)#bandwidth 64
```

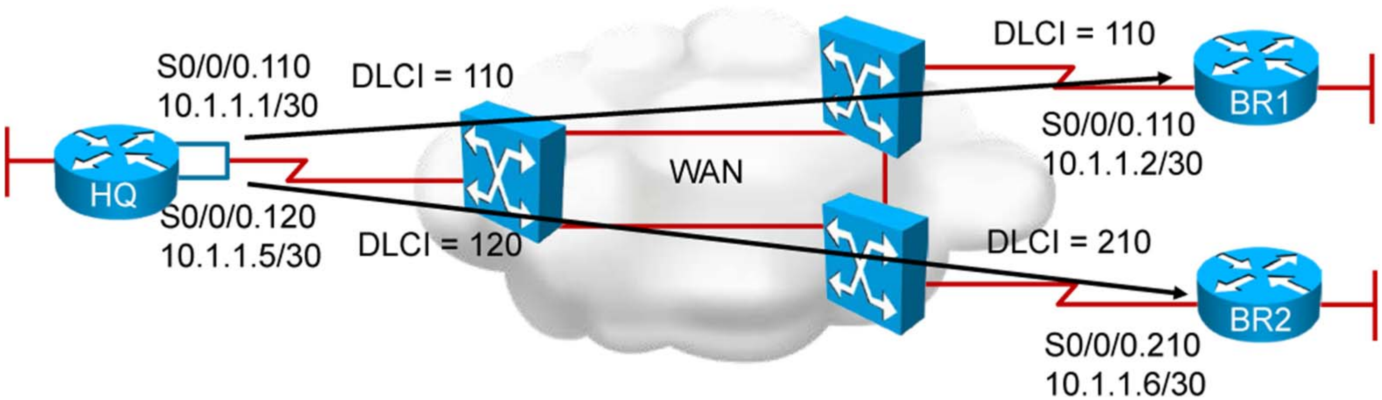
Configuration on the Branch router

Point-to-Point vs. Multipoint

Two types of subinterfaces:

- Point-to-point:
  - Subinterfaces act like leased lines.
  - Each point-to-point subinterface requires its own subnet.
  - Point-to-point is applicable to hub-and-spoke topologies.
- Multipoint:
  - Subinterfaces act like NBMA networks, so they do not resolve split-horizon issues.
  - Multipoint can save address space because it uses a single subnet.
  - Multipoint is applicable to partial-mesh and full-mesh topologies.

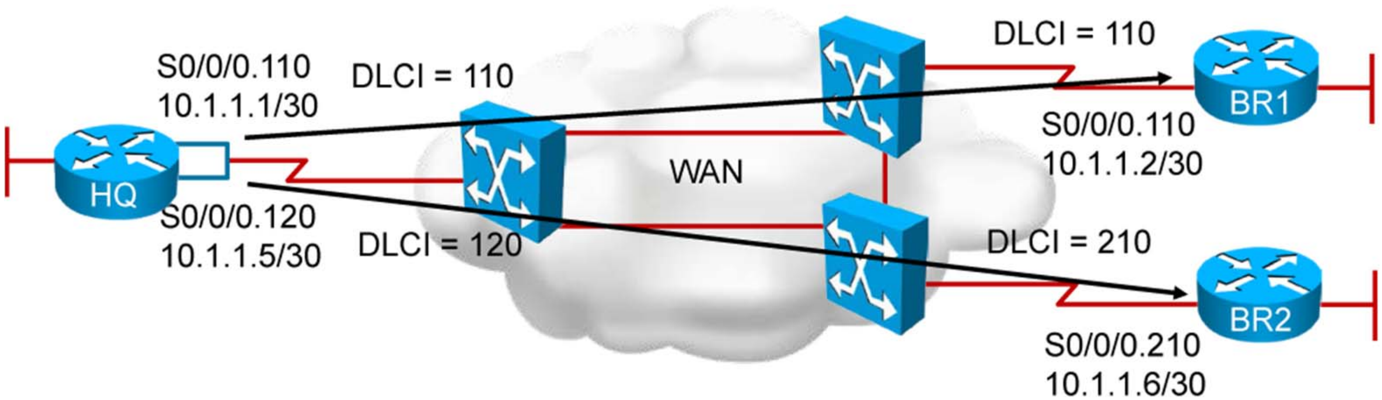
Configuring Point-to-Point Frame Relay




```
HQ(router)#interface Serial0/0/0
HQ(router-if)#no ip address
HQ(router-if)#encapsulation frame-relay
HQ(router-if)#interface Serial0/0/0.110 point-to-point
HQ(router-subif)#ip address 10.1.1.1 255.255.255.252
HQ(router-subif)#bandwidth 64
HQ(router-subif)#frame-relay interface-dlci 110
HQ(router-subif)#interface Serial0/0/0.120 point-to-point
HQ(router-subif)#ip address 10.1.1.5 255.255.255.252
HQ(router-subif)#bandwidth 64
HQ(router-subif)#frame-relay interface-dlci 120
```

Configuration of point-to-point subinterfaces on the HQ router

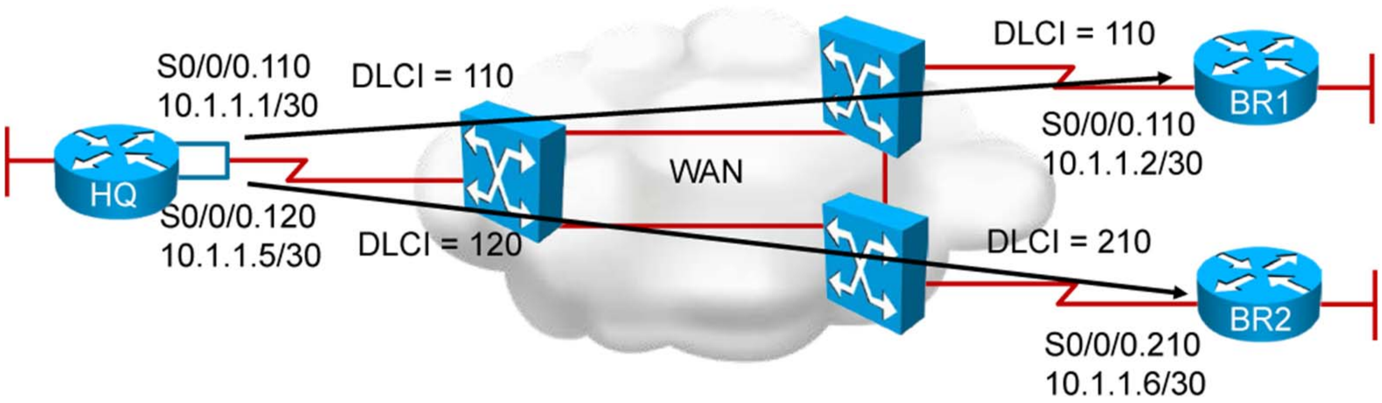
Configuring Point-to-Point Frame Relay (Cont.)




```
BR1(router)#interface Serial0/0/0
BR1(router-if)#no ip address
BR1(router-if)#encapsulation frame-relay
BR1(router-if)#interface Serial0/0/0.110 point-to-point
BR1(router-subif)#ip address 10.1.1.2 255.255.255.0
BR1(router-subif)#bandwidth 64
BR1(router-subif)#frame-relay interface-dlci 110
```

Configuration of Branch 1 for point-to-point Frame Relay

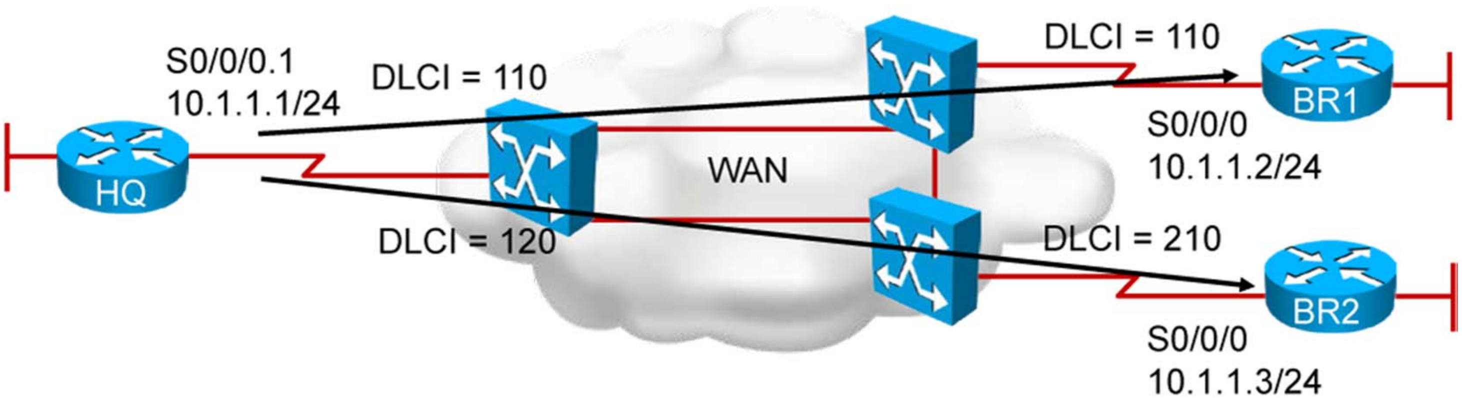
Configuring Point-to-Point Frame Relay (Cont.)




```
BR2(router)#interface Serial0/0/0
BR2(router-if)#no ip address
BR2(router-if)#encapsulation frame-relay
BR2(router-if)#interface Serial0/0/0.210 point-to-point
BR2(router-subif)#ip address 10.1.1.6 255.255.255.0
BR2(router-subif)#bandwidth 64
BR2(router-subif)#frame-relay interface-dlci 210
```

Configuration of Branch 2 for point-to-point Frame Relay

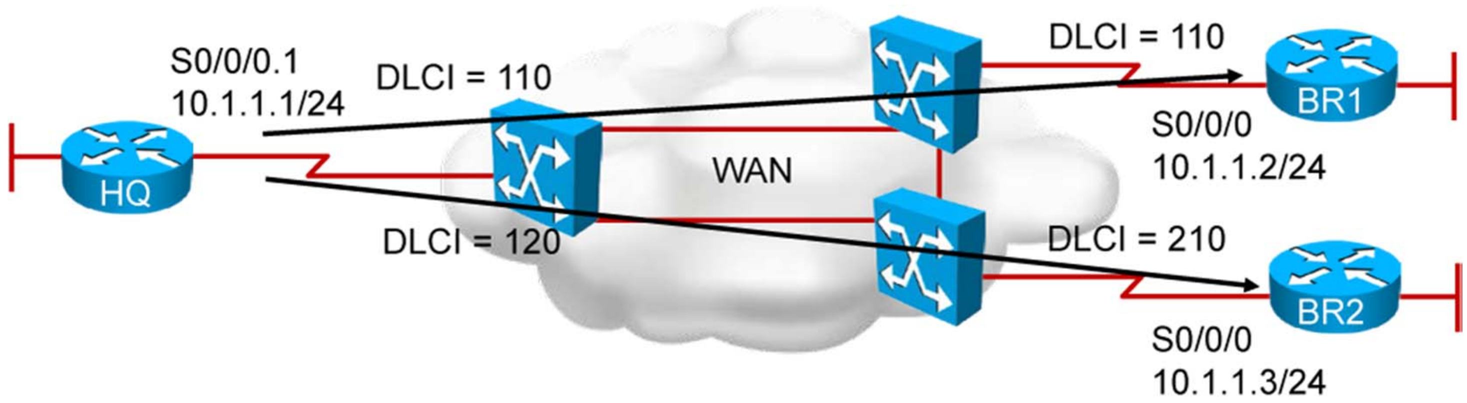
Configuring Multipoint Frame Relay




```
HQ(router)#interface Serial0/0/0
HQ(router-if)#no ip address
HQ(router-if)#encapsulation frame-relay
HQ(router-if)#interface Serial0/0/0.1 multipoint
HQ(router-subif)#ip address 10.1.1.1 255.255.255.0
HQ(router-subif)#bandwidth 64
HQ(router-subif)#frame-relay map ip 10.1.1.2 110 broadcast
HQ(router-subif)#frame-relay map ip 10.1.1.3 120 broadcast
```

Configuration of multipoint subinterfaces on the HQ router

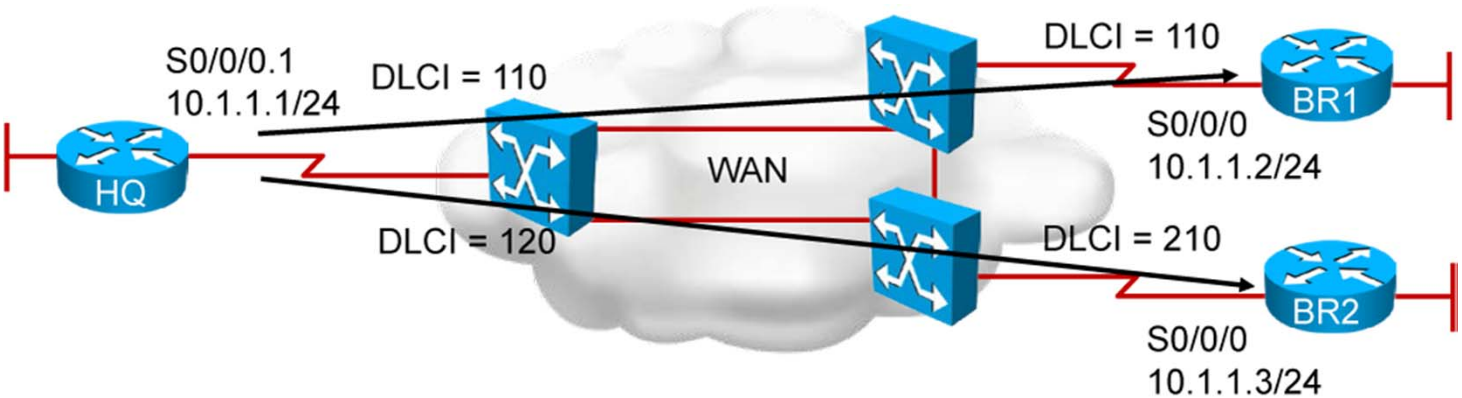
Configuring Multipoint Frame Relay (Cont.)




```
BR1(router)#interface Serial0/0/0
BR1(router-if)#encapsulation frame-relay
BR1(router-if)#ip address 10.1.1.2 255.255.255.252
BR1(router-if)#bandwidth 64
BR1(router-if)#frame-relay map ip 10.1.1.1 110
```

Configuration of multipoint subinterfaces on the Branch 1 router

Configuring Multipoint Frame Relay (Cont.)




```
BR2(router)#interface Serial0/0/0
BR2(router-if)#encapsulation frame-relay
BR2(router-if)#ip address 10.1.1.6 255.255.255.252
BR2(router-if)#bandwidth 64
BR2(router-if)#frame-relay map ip 10.1.1.1 210
```

Configuration of multipoint subinterfaces on the Branch 2 router

Verifying Frame Relay Configuration

```
Branch#show interfaces Serial0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY, loopback not set
  Keepalive set (10 sec)
  LMI enq sent  630, LMI stat recvd 616, LMI upd recvd 0, DTE LMI up
  LMI enq recvd 15, LMI stat sent  0, LMI upd sent  0
  LMI DLCI 1023  LMI type is CISCO  frame relay DTE
  Broadcast queue 0/64, broadcasts sent/dropped 9/0, interface broadcasts 0
  Last input 00:00:04, output 00:00:04, output hang never
  Last clearing of "show interface" counters 01:45:04
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair

<output omitted>
```

Displays interface status, information, and counters

Verifying Frame Relay Configuration (Cont.)

```
Branch#show frame-relay lmi

LMI Statistics for interface Serial0/0/0 (Frame Relay DTE) LMI TYPE = CISCO
  Invalid Unnumbered info 0              Invalid Prot Disc 0
  Invalid dummy Call Ref 0               Invalid Msg Type 0
  Invalid Status Message 0               Invalid Lock Shift 0
  Invalid Information ID 0               Invalid Report IE Len 0
  Invalid Report Request 0               Invalid Keep IE Len 0
  Num Status Enq. Sent 834               Num Status msgs Rcvd 820
  Num Update Status Rcvd 0               Num Status Timeouts 14
  Last Full Status Req 00:00:21          Last Full Status Rcvd 00:00:21
```

Displays LMI statistics

Verifying Frame Relay Configuration (Cont.)

```
Branch#show frame-relay pvc

PVC Statistics for interface Serial0/0/0 (Frame Relay DTE)

              Active     Inactive      Deleted       Static
  Local          1            0            0            0
  Switched       0            0            0            0
  Unused         0            0            0            0

DLCI = 120, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE =
Serial0/0/0

  input pkts 18            output pkts 18           in bytes 962
  out bytes 962            dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 13        out bcast bytes 442
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 02:32:29, last time pvc status changed 02:32:29
```

Displays PVC statistics

Verifying Frame Relay Configuration (Cont.)

```
Branch#show frame-relay map
Serial0/0/0 (up): ip 192.168.1.2 dlci 120(0x78,0x1C80), dynamic,
              broadcast,
              CISCO, status defined, active
```

Displays Frame Relay map entries

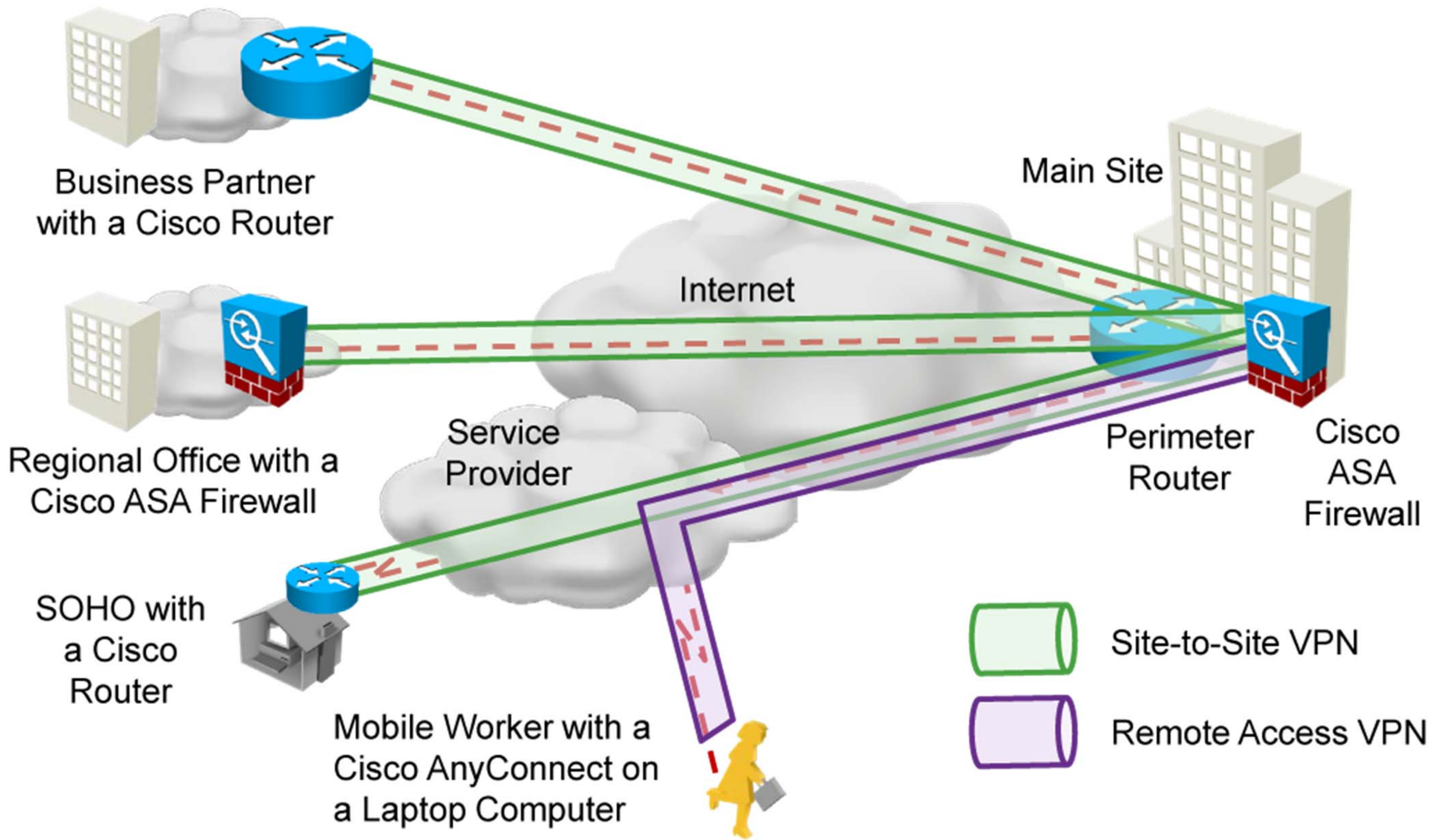
Summary

- Frame Relay is a packet-switched, connection-oriented, data-link technology.
- LMI is a signaling standard between the router and the Frame Relay switch. LMI is responsible for managing the connection and maintaining the status between the devices.
- In Frame Relay, a local DLCI must be mapped to a remote destination IP address, either manually or using Inverse ARP.
- To configure basic Frame Relay, set the encapsulation type to Frame Relay on an interface.
- It is recommended that you use Frame Relay point-to-point subinterfaces to solve routing protocol issues.

Introducing VPN Solutions

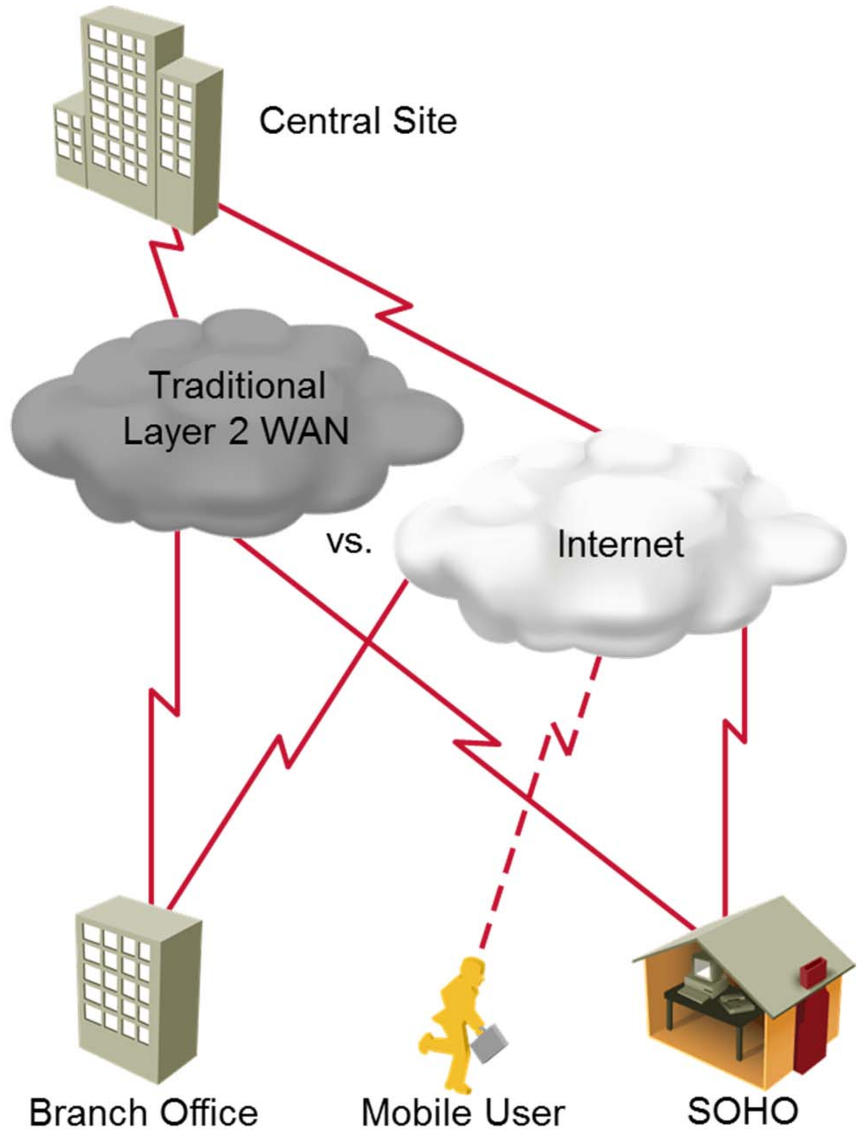
Wide-Area Networks

VPNs and Their Benefits



VPNs and Their Benefits (Cont.)

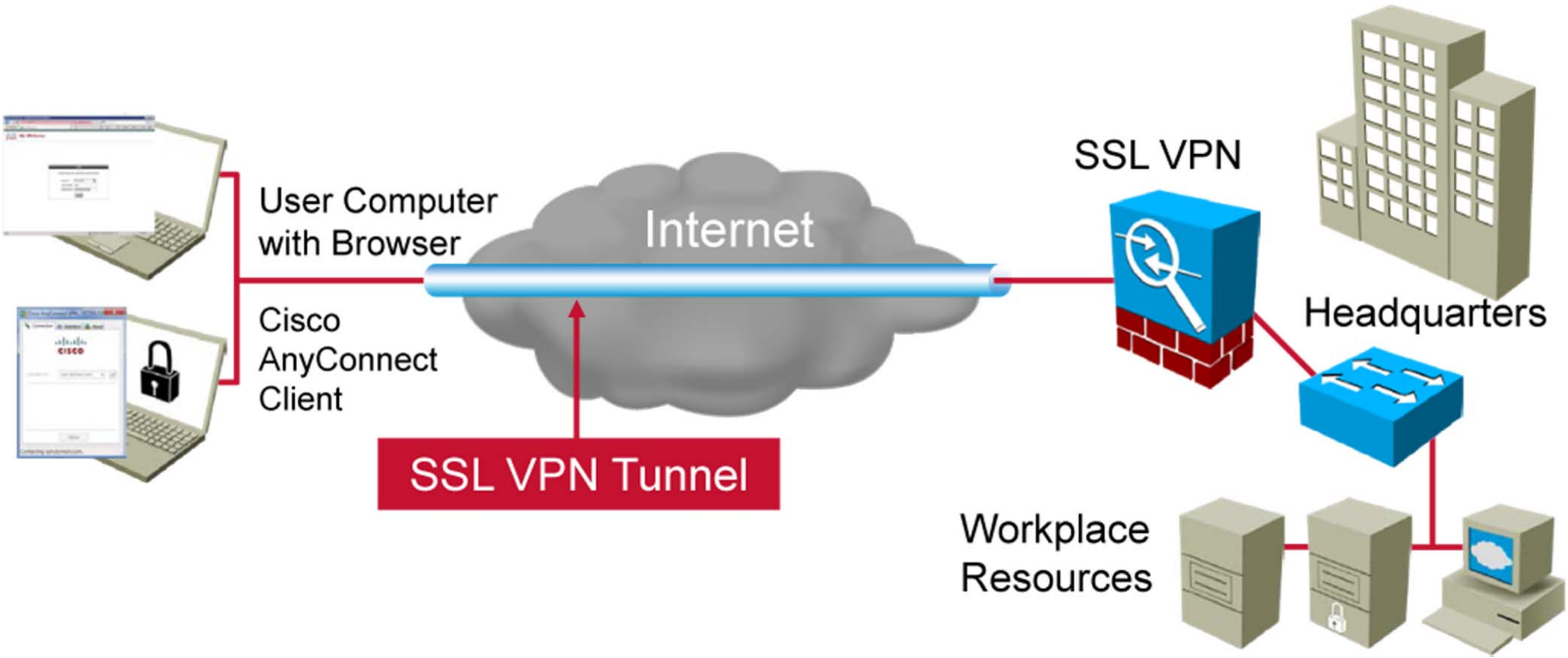
- VPN requirements:
  - Connecting HQ and Branch
- VPN characteristics:
  - Virtual: Information within a private network is transported over a public network.
  - Private: Traffic is separated by a tunnel so that it can be encrypted to keep the data confidential.
- VPN benefits:
  - Cost savings
  - Scalability
  - Compatibility
  - Security



Cisco SSL VPN Solutions

Here are two Cisco SSL VPN solutions:

- Cisco AnyConnect SSL VPN
- Clientless Cisco SSL VPN



IPsec Characteristics

- IPsec acts at the network layer, protecting and authenticating IP packets.
- IPsec is a framework of open standards that is algorithm-independent.
- IPsec services provide four critical functions:
  - Confidentiality
  - Data integrity
  - Authentication
  - Anti-replay protection

Summary

- Organizations implement VPNs because they are less expensive, easier to scale than traditional WANs, and can provide security.
- A site-to-site VPN is an extension of a classic WAN network.
- Remote-access VPNs can support the needs of telecommuters, mobile users, and extranet, consumer-to-business traffic.
- IPsec protects and authenticates IP packets and is a framework of open standards that is algorithm-independent.

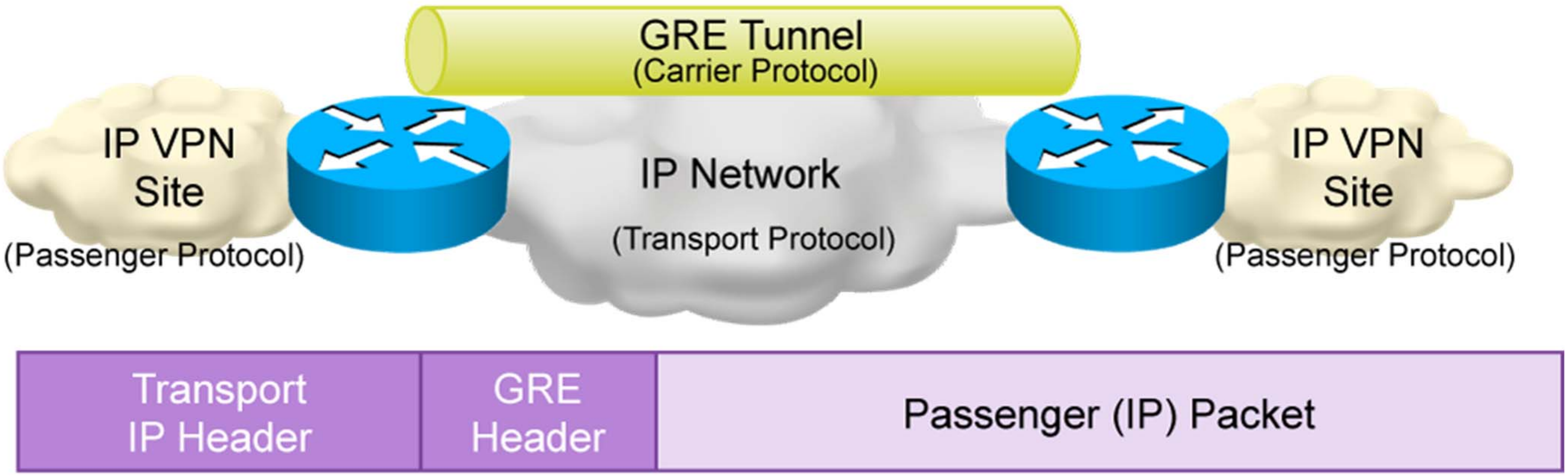
Configuring GRE Tunnels

Wide-Area Networks

GRE Tunnel Overview

GRE = Generic Routing Encapsulation:

- One of many tunneling protocols
- IP protocol 47 defines GRE packets
- Allows routing information to be passed between connected networks
- No encryption



GRE Tunnel Configuration

GRE implementation plan:

- Learn the IP addresses.
- Create a tunnel interface.
- Specify GRE tunnel mode as the tunnel interface mode (optional).
- Specify the tunnel source and tunnel destination IP addresses.
- Configure an IP address for the tunnel interface.

GRE Tunnel Configuration (Cont.)


```
Branch(config)#interface Tunnel0
Branch(config-if)#tunnel mode gre ip
Branch(config-if)#ip address 192.168.2.1 255.255.255.0
Branch(config-if)#tunnel source 209.165.201.1
Branch(config-if)#tunnel destination 209.165.202.130
```

Configuration of GRE tunnel on the Branch router

GRE Tunnel Configuration (Cont.)


```
HQ(config)#interface Tunnel0
HQ(config-if)#tunnel mode gre ip
HQ(config-if)#ip address 192.168.2.2 255.255.255.0
HQ(config-if)#tunnel source 209.165.202.130
HQ(config-if)#tunnel destination 209.165.201.1
```

Configuration of GRE tunnel on the HQ router

GRE Tunnel Verification

```
Branch#show ip interface brief | include Tunnel

Tunnel0                    192.168.2.1     YES manual up                   up
```

Verifies that the tunnel interface is up.

```
Branch#show interface Tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 192.168.2.1/24
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 209.165.201.1, destination 209.165.202.130
  Tunnel protocol/transport GRE/IP

<output omitted>
```

Verifies that the tunnel interface is up and shows tunnel IPs, source and destination IPs, and tunnel protocol.

GRE Tunnel Verification (Cont.)

```
Branch#show ip route
<output omitted>
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, Tunnel0
L        192.168.2.1/32 is directly connected, Tunnel0
      209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.201.0/27 is directly connected, GigabitEthernet0/1
L        209.165.201.1/32 is directly connected, GigabitEthernet0/1
```

Verifies the tunnel route between the Branch and HQ routers

Summary

- GRE is a tunneling protocol that can encapsulate a wide variety of protocol packet types inside IP tunnels.
- You must configure a tunnel source and tunnel destination to establish a GRE tunnel as the IP address of the tunnel itself.
- You should verify that the tunnel interface is up after configuring it.

Module Summary

- A WAN can be interconnected over a private infrastructure or over a public infrastructure such as the Internet.
- PPP is a common Layer 2 protocol for the WAN. There are two components of PPP: LCP, which negotiates the connection, and NCP, which encapsulates traffic.
- Frame Relay is a packet-switched, connection-oriented, data-link technology.
- Organizations implement VPNs because they are less expensive and easier to scale than traditional WANs, while still offering mechanisms for secure communication.
- GRE is a tunneling protocol that can encapsulate a wide variety of protocol packet types inside of IP tunnels, but it does not provide encryption.