

Fundamental Concepts in TCP/IP Networking

Virtual Local Area Network (VLAN)



Learning Objectives

- Explain the purpose of VLAN in a switched network
- Analyze how a switch forwards frames based VLAN configuration in a multi-switched environment
- Configure a switch port to be assigned to a VLAN based on requirements
- Configure a trunk port on a LAN switch
- Troubleshoot VLAN and trunk configurations in a switched network

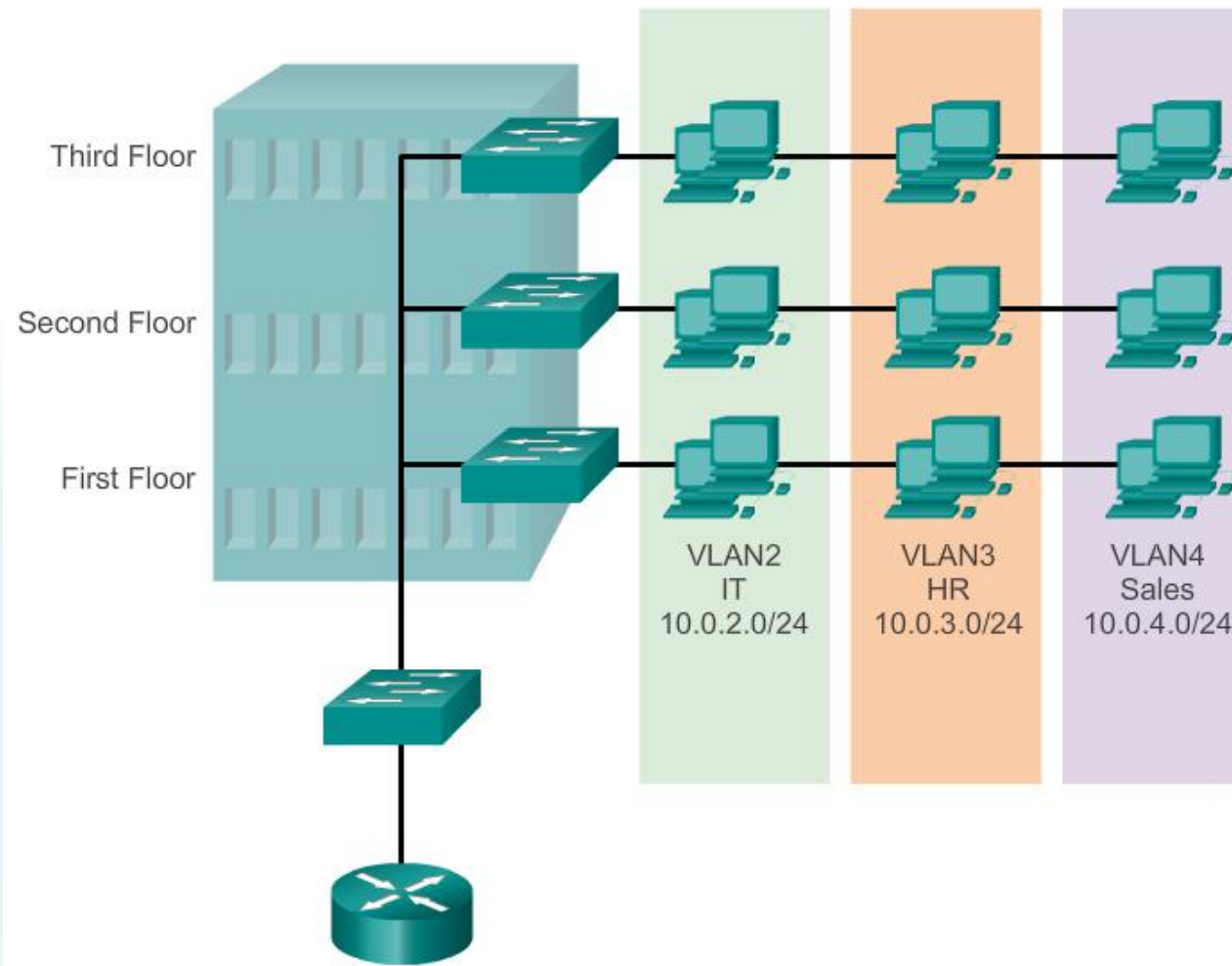


VLAN Definitions

- VLAN (virtual LAN) is a logical partition of a layer 2 network
- Multiple partition can be created, allowing for multiple VLANs to co-exist
- Each VLAN is a broadcast domain, usually with its own IP network
- VLANs are mutually isolated and packets can only pass between them through a router
- The partitioning of the layer 2 network takes inside a layer 2 device, usually a switch.
- The hosts grouped within a VLAN are unaware of the VLAN's existence



VLAN Definitions



Benefits of VLANs

- Security
- Cost reduction
- Better performance
- Shrink broadcast domains
- Improved IT staff efficiency
- Simpler project and application management



Types of VLANs

- Data VLAN
- Default VLAN
- Native VLAN
- Management VLAN



Types of VLANs

7

VLAN 1

```
Switch# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gi0/1, Gi0/2
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

- All ports assigned to VLAN 1 to forward data by default.
- Native VLAN is VLAN 1 by default.
- Management VLAN is VLAN 1 by default.
- VLAN 1 cannot be renamed or deleted.



Voice VLANs

- VoIP traffic is time-sensitive and requires:
 - Assured bandwidth to ensure voice quality
 - Transmission priority over other types of network traffic
 - Ability to be routed around congested areas on the network
 - Delay of less than 150 ms across the network
- The voice VLAN feature enables access ports to carry IP voice traffic from an IP phone
- Because the sound quality of an IP phone call can deteriorate if the data is unevenly sent, the switch supports quality of service (QoS)



VLAN Trunks

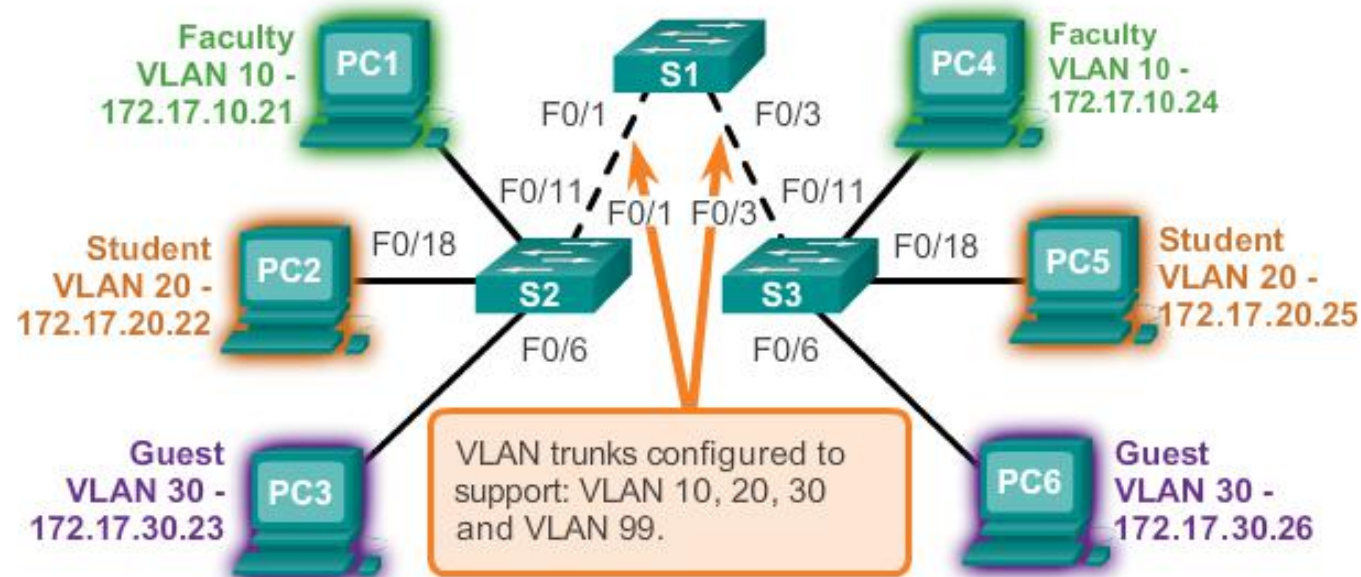
- ▶ A VLAN trunk carries more than one VLAN
- ▶ Usually established between switches so same-VLAN devices can communicate even if physically connected to different switches
- ▶ A VLAN trunk is not associated to any VLANs. Neither is the trunk ports used to establish the trunk link
- ▶ Cisco IOS supports IEEE802.1q, a popular VLAN trunk protocol



VLAN Trunks

VLAN 10 Faculty/Staff - 172.17.10.0/24
VLAN 20 Students - 172.17.20.0/24
VLAN 30 Guest - 172.17.30.0/24
VLAN 99 Management and Native - 172.17.99.0/24

F0/1-5 are 802.1Q trunk interfaces with native VLAN 99.
F0/11-17 are in VLAN 10.
F0/18-24 are in VLAN 20.
F0/6-10 are in VLAN 30.



Controlling Broadcast Domains with VLANs

11

- ▶ VLANs can be used to limit the reach of broadcast frames
- ▶ A VLAN is a broadcast domain of its own
- ▶ Therefore, a broadcast frame sent by a device in a specific VLAN is forwarded within that VLAN only.
- ▶ This help controlling the reach of broadcast frames and their impact in the network
- ▶ Unicast and multicast frames are forwarded within the originating VLAN as well



Tagging Ethernet Frames for VLAN Identification

- ▶ Frame tagging is used to properly transmit multiple VLAN frames through a trunk link
- ▶ Switches will tag frames to identify the VLAN they belong. Different tagging protocols exist, with IEEE 802.1q being a very popular one
- ▶ The protocol defines the structure of the tagging header added to the frame
- ▶ Switches will add VLAN tags to the frames before placing them into trunk links and remove the tags before forwarding frames through non-trunk ports
- ▶ Once properly tagged, the frames can transverse any number of switches via trunk links and still be forward within the correct VLAN at the destination



Native VLANs and 802.1q Tagging

- ▶ A frame that belongs to the native VLAN will not be tagged
- ▶ A frame that is received untagged will remain untagged and placed in the native VLAN when forwarded
- ▶ If there are not ports associated to the native VLAN and no other trunk links, an untagged frame will be dropped
- ▶ In Cisco switches, the native VLAN is VLAN 1 by default



VLAN Assignment-VLAN Ranges On Catalyst Switches

14

- The Catalyst 2960 and 3560 Series switches support over 4,000 VLANs
- These VLANs are split into 2 categories:
- Normal Range VLANs
 - VLAN numbers from 1 through 1005
 - Configurations stored in the vlan.dat (in the flash)
 - VTP can only learn and store normal range VLANs
- Extended Range VLANs
 - VLAN numbers from 1006 through 4096
 - Configurations stored in the running-config (in the NVRAM)
 - VTP does not learn extended range VLANs



Creating a VLAN

Cisco Switch IOS Commands

Enter global configuration mode.	S1# configure terminal
Create a VLAN with a valid id number.	S1(config)# vlan vlan_id
Specify a unique name to identify the VLAN.	S1(config)# name vlan_name
Return to the privileged EXEC mode.	S1(config)# end



Assigning Ports To VLANs

Cisco Switch IOS Commands

Enter global configuration mode.	S1 # configure terminal
Enter interface configuration mode for the SVI.	S1(config) # interface <i>interface_id</i>
Configure the management interface IP address.	S1(config) # ip address 172.17.99.11
Set the port to access mode.	S1(config-if) # switchport mode access
Assign the port to a VLAN.	S1(config-if) # switchport access vlan <i>vlan_id</i>
Return to the privileged EXEC mode.	S1(config-if) # end



Configuring IEEE 802.1q Trunk Links

Cisco Switch IOS Commands

Enter global configuration mode.	S1# configure terminal
Enter interface configuration mode for the SVI.	S1(config)# interface <i>interface_id</i>
Force the link to be a trunk link.	S1(config)# switchport mode trunk
Specify a native VLAN for untagged 802.1Q trunks.	S1(config-if)# switchport trunk native vlan <i>vlan_id</i>
Specify the list of VLANs to be allowed on the trunk link.	S1(config-if)# switchport trunk allowed vlan <i>vlan-list</i>
Return to the privileged EXEC mode.	S1(config-if)# end

```

S1(config)# interface FastEthernet0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# switchport trunk allowed vlan 10,20,30
S1(config-if)# end

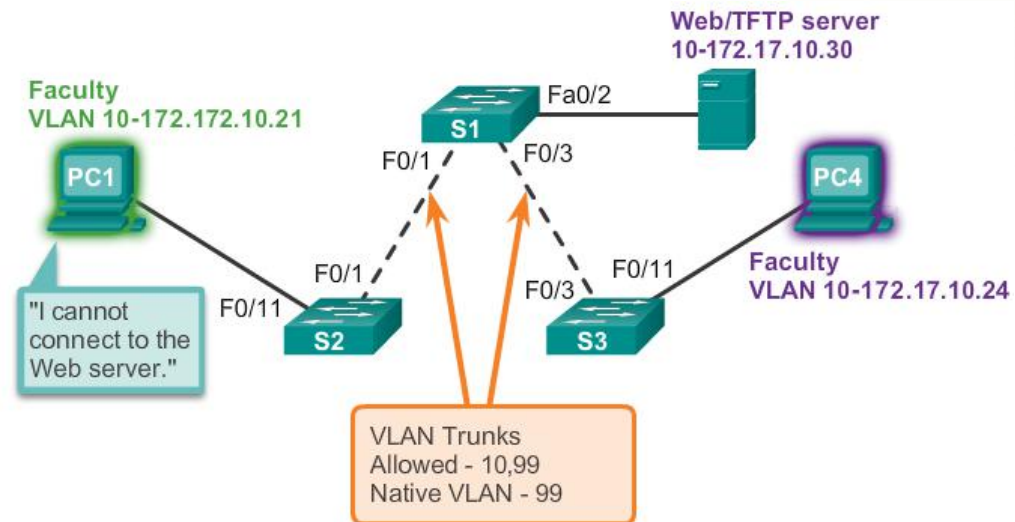
```



Troubleshooting VLANs and Trunks-Addressing Issues with VLAN

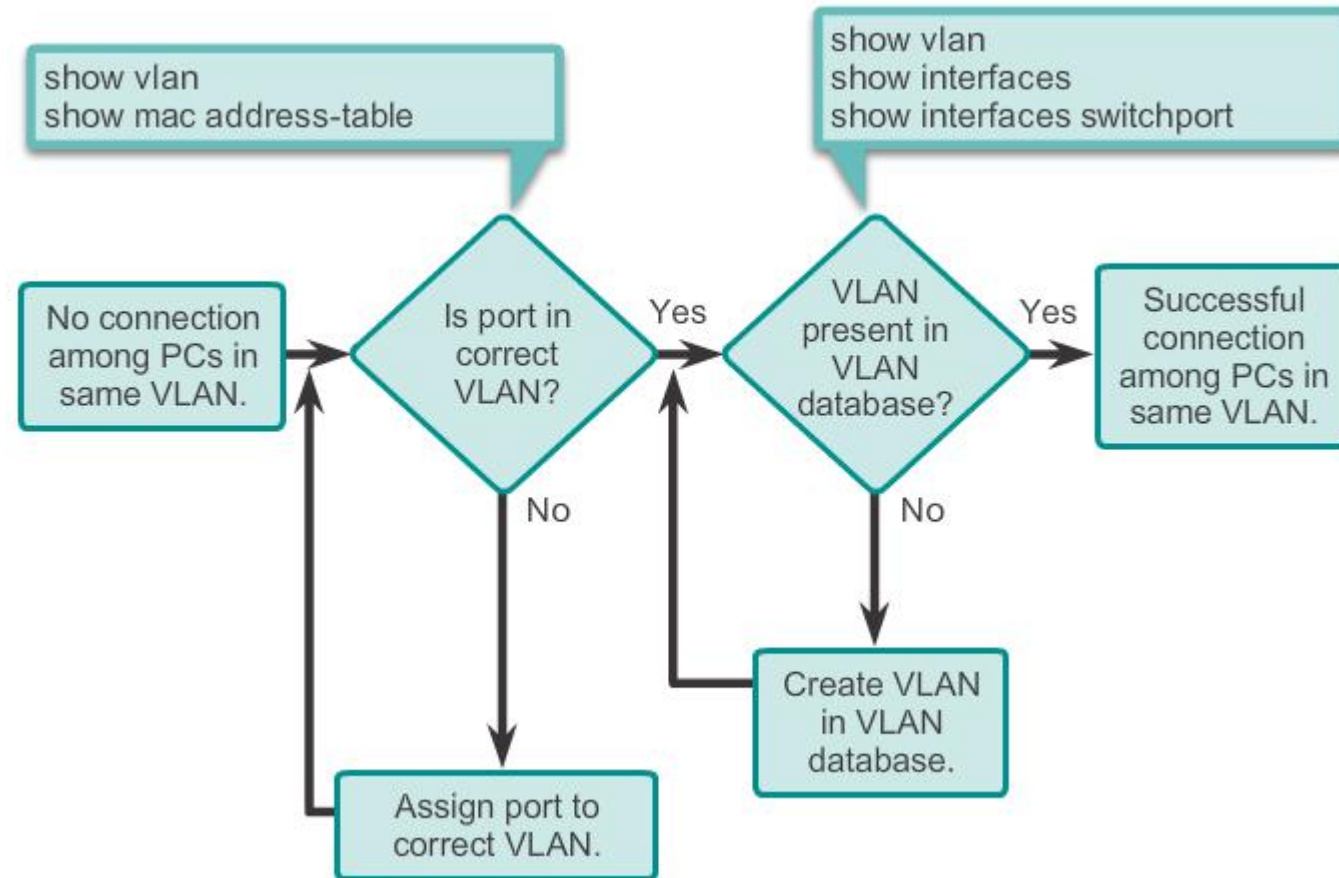
18

- ▶ It is very common practice to associate a VLAN with a IP network
- ▶ Since different IP networks only communicate through a router, all devices within a VLAN must be part of the same IP network in order to communicate
- ▶ In the picture below, PC1 can't communicate to the server because it has a wrong IP address configured



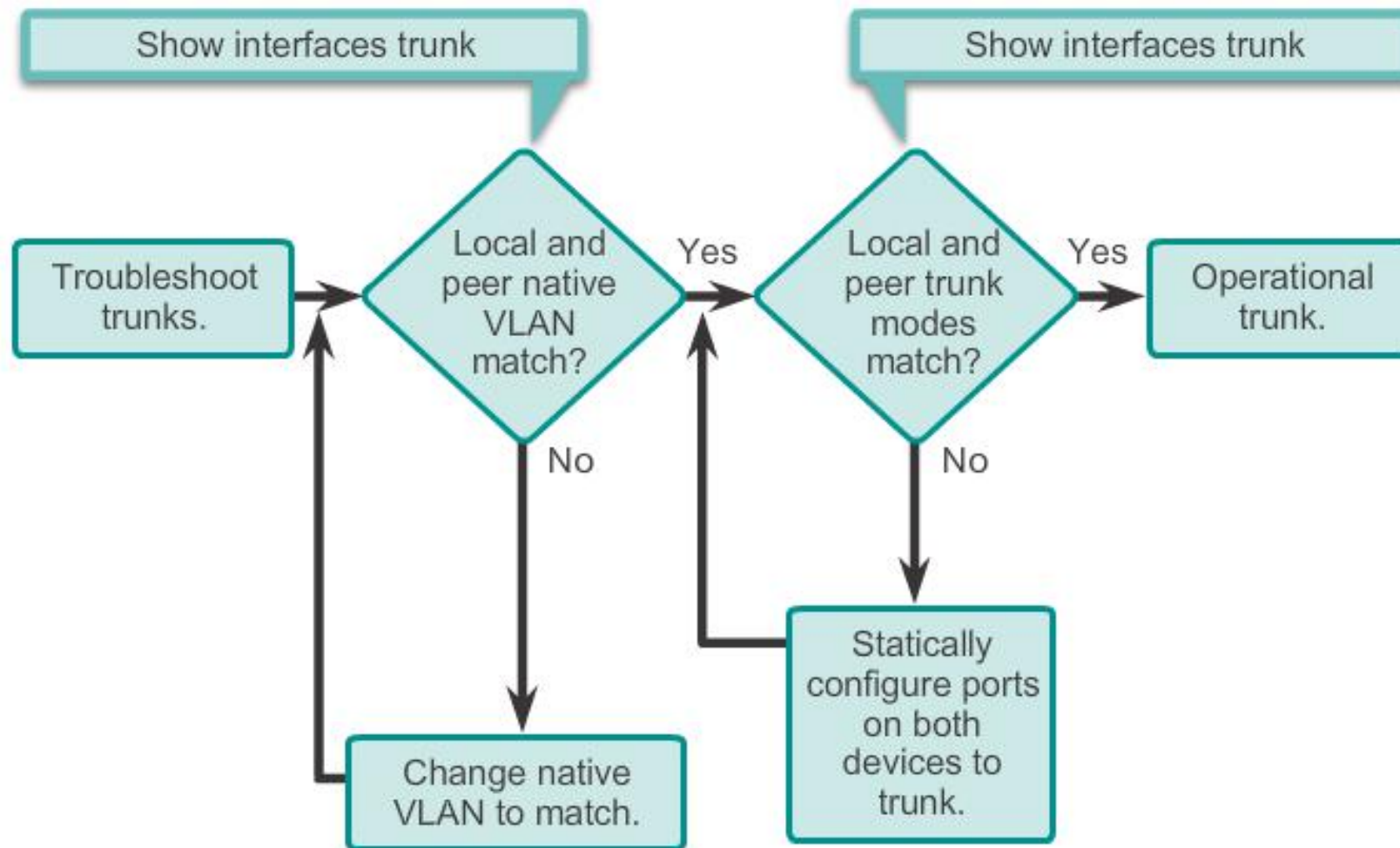
Missing VLANs

- If all IP addresses mismatch have been solved but device still can't connect, check if the VLAN exists in the switch.



Introduction to Troubleshooting Trunks

20



Common Problems With Trunks

- ▶ Trunking issues are usually associated with incorrect configurations.
- ▶ The most common type of trunk configuration errors are:
 1. Native VLAN mismatches
 2. Trunk mode mismatches
 3. Allowed VLANs on trunks
- ▶ If a trunk problem is detected, the best practice guidelines recommend to troubleshoot in the order shown above.



Trunk Mode Mismatches

- ▶ If a port on a trunk link is configured with a trunk mode that is incompatible with the neighboring trunk port, a trunk link fails to form between the two switches
- ▶ Check the status of the trunk ports on the switches using the **show interfaces trunk** command
- ▶ To fix the problem, configure the interfaces with proper trunk modes.

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic auto	Access	Trunk	Trunk	Access
Dynamic desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Limited connectivity
Access	Access	Access	Limited connectivity	Access



Incorrect VLAN List

- ▶ VLANs must be allowed in the trunk before their frames can be transmitted across the link
- ▶ Use the **switchport trunk allowed vlan** command to specify which VLANs are allowed in a trunk link **(in Cisco IOS)**.
- ▶ To ensure the correct VLANs are permitted in a trunk, use the **show interfaces trunk** command **(in Cisco IOS)**.



Attacks on VLANs-Switch spoofing Attack

- There are a number of different types of VLAN attacks in modern switched networks. VLAN hopping is one them.
- The default configuration of the switch port is dynamic auto
- By configuring a host to act as a switch and form a trunk, an attacker could gain access to any VLAN in the network.
- Because the attacker is now able to access other VLANs, this is called a VLAN hopping attack
- To prevent a basic switch spoofing attack, turn off trunking on all ports, except the ones that specifically require trunking



Design Best Practices For VLANs -VLAN Design Guideline

25

- ▶ Move all ports from VLAN1 and assign them to a not-in-use VLAN
- ▶ Shut down all unused switch ports
- ▶ Separate management and user data traffic
- ▶ Change the management VLAN to a VLAN other than VLAN1. The same goes to the native VLAN
- ▶ Make sure that only devices in the management VLAN can connect to the switches
- ▶ The switch should only accept SSH connections
- ▶ Disable autonegotiation on trunk ports
- ▶ Do not use the auto or desirable switch port modes



Routing Concepts

Routing Protocols

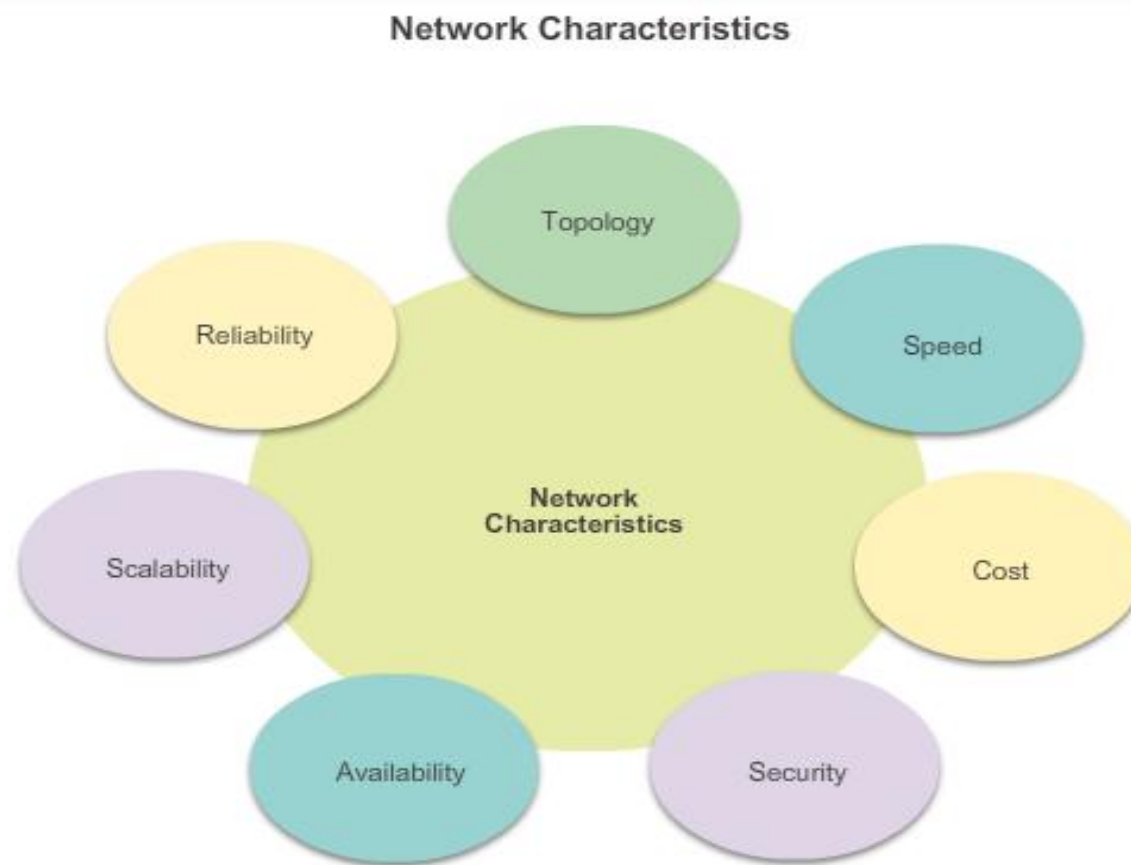


Learning Objectives

- ▶ Configure a router to route between multiple directly connected networks
- ▶ Describe the primary functions and features of a router.
- ▶ Explain how routers use information in data packets to make forwarding decisions in a small to medium-sized business network.
- ▶ Explain the encapsulation and de-encapsulation process used by routers when switching packets between interfaces
- ▶ Compare ways in which a router builds a routing table when operating in a small to medium-sized business network.
- ▶ Explain routing table entries for directly connected networks.
- ▶ Explain how a router builds a routing table of directly connected networks.
- ▶ Explain how a router builds a routing table using static routes.
- ▶ Explain how a router builds a routing table using a dynamic routing protocol.



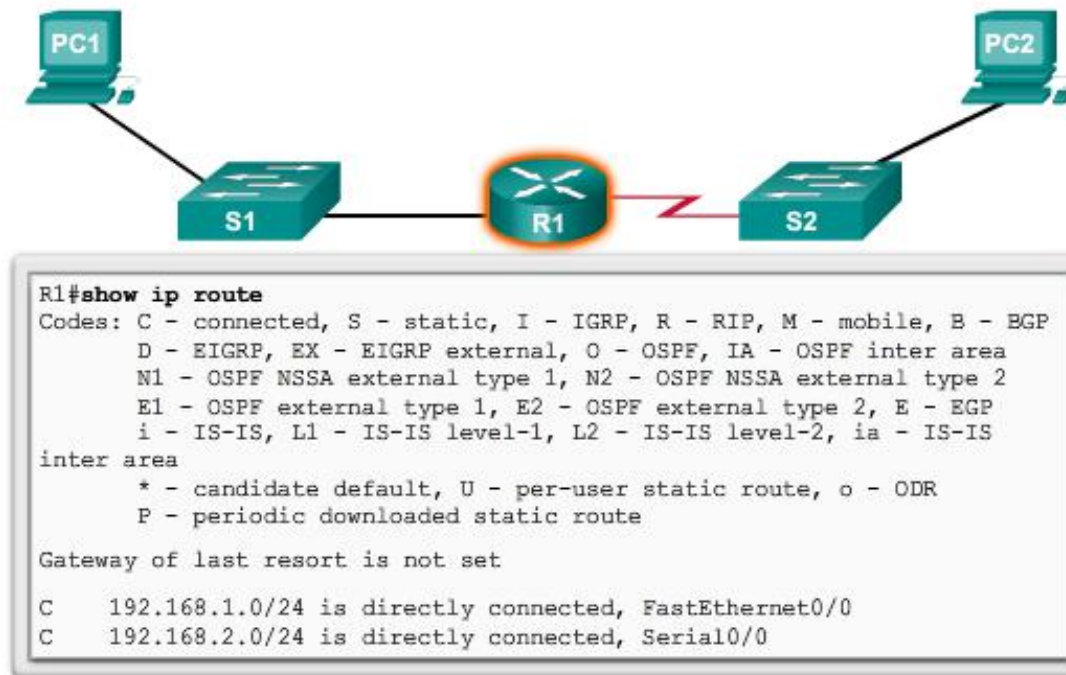
Characteristics of a Network



Why Routing?

- ▶ The router is responsible for the routing of traffic between networks.

Routers Route Packets



Cisco IOS command line interface (CLI) can be used to view the route table.

Routers are Computers

- ▶ Routers are specialized computers containing the following required components to operate:
 - Central processing unit (CPU)
 - Operating system (OS) - Cisco Routers use Cisco IOS, Juniper and Huawei have their own OS.
 - Memory and storage (RAM, ROM, NVRAM, Flash, hard drive)
- ▶ Routers utilize the following memory:

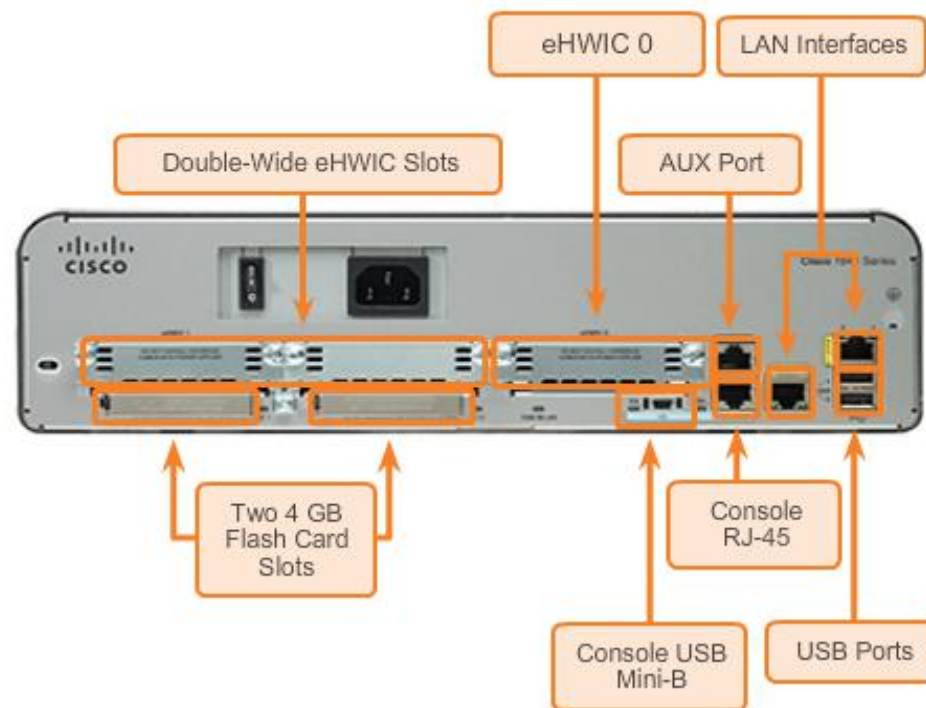
Memory	Volatile / Non-Volatile	Stores
RAM	Volatile	<ul style="list-style-type: none">▪ Running IOS▪ Running configuration file▪ IP routing and ARP tables▪ Packet buffer
ROM	Non-Volatile	<ul style="list-style-type: none">▪ Bootup instructions▪ Basic diagnostic software▪ Limited IOS
NVRAM	Non-Volatile	<ul style="list-style-type: none">▪ Startup configuration file
Flash	Non-Volatile	<ul style="list-style-type: none">▪ IOS▪ Other system files



Routers are Computers

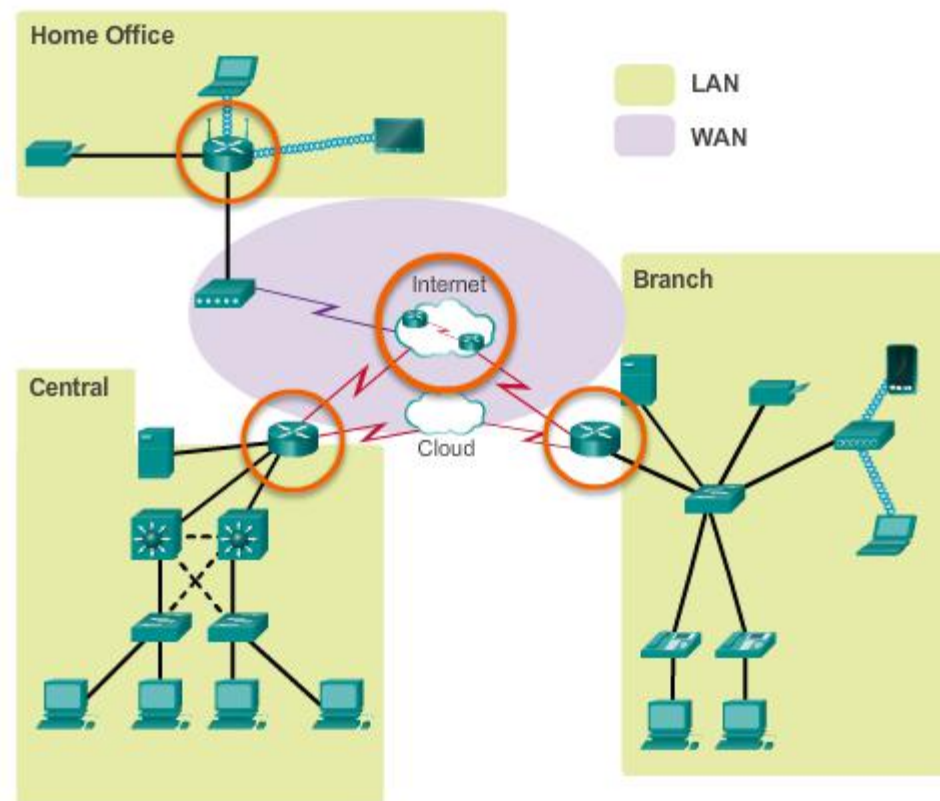
- ▶ Routers use specialized ports and network interface cards to interconnect to other networks

Back Panel of a Router



Routers Interconnect Networks

- ▶ Routers can connect multiple networks.
- ▶ Routers have multiple interfaces, each on a different IP network.



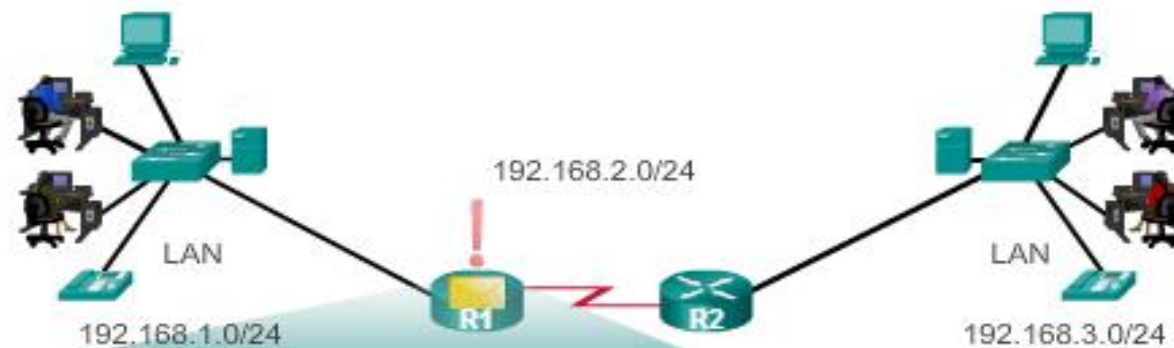
Routers Choose Best Paths

- ▶ Determine the best path to send packets
 - Uses its routing table to determine path
- ▶ Forward packets toward their destination
 - Forwards packet to interface indicated in routing table.
 - Encapsulates the packet and forwards out toward destination.
- ▶ Routers use static routes and dynamic routing protocols to learn about remote networks and build their routing tables.



Routers Choose Best Paths

How the Router Works



R1#show ip route

Codes:

C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
 * - candidate default, U - per-user static route, o - ODR
 P - periodic downloaded static route

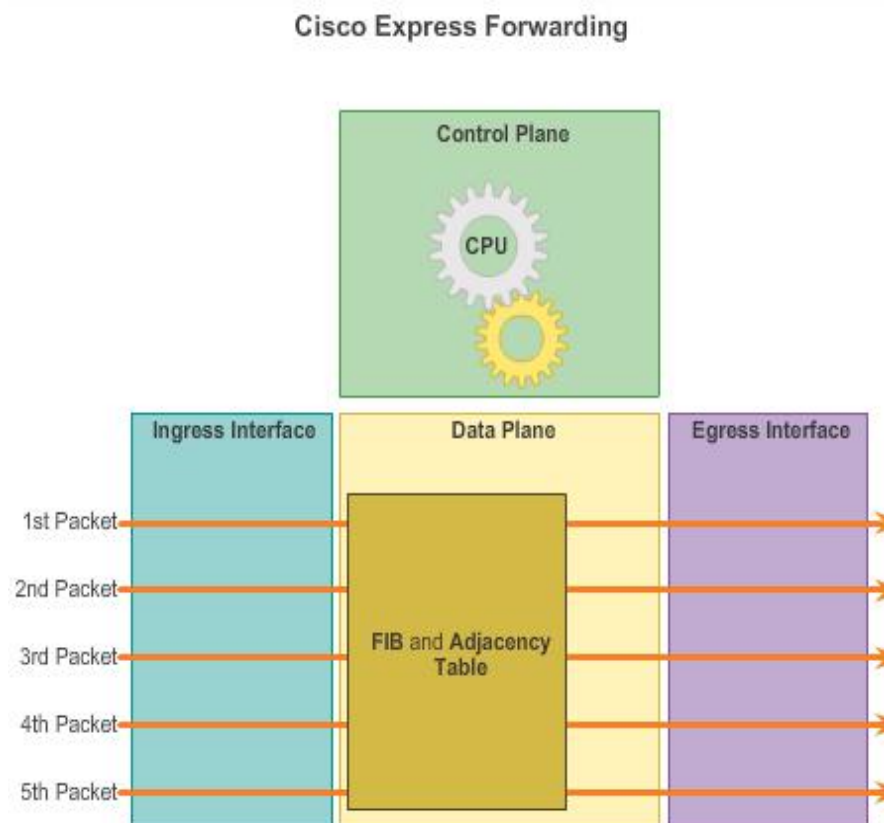
Gateway of last resort is not set

C 192.168.1.0/24 is directly connected, FastEthernet0/0
 C 192.168.2.0/24 is directly connected, Serial0/0/0
 S 192.168.3.0/24 is directly connected, Serial0/0/0

Routers use the routing table like a map to discover the best path for a given network.

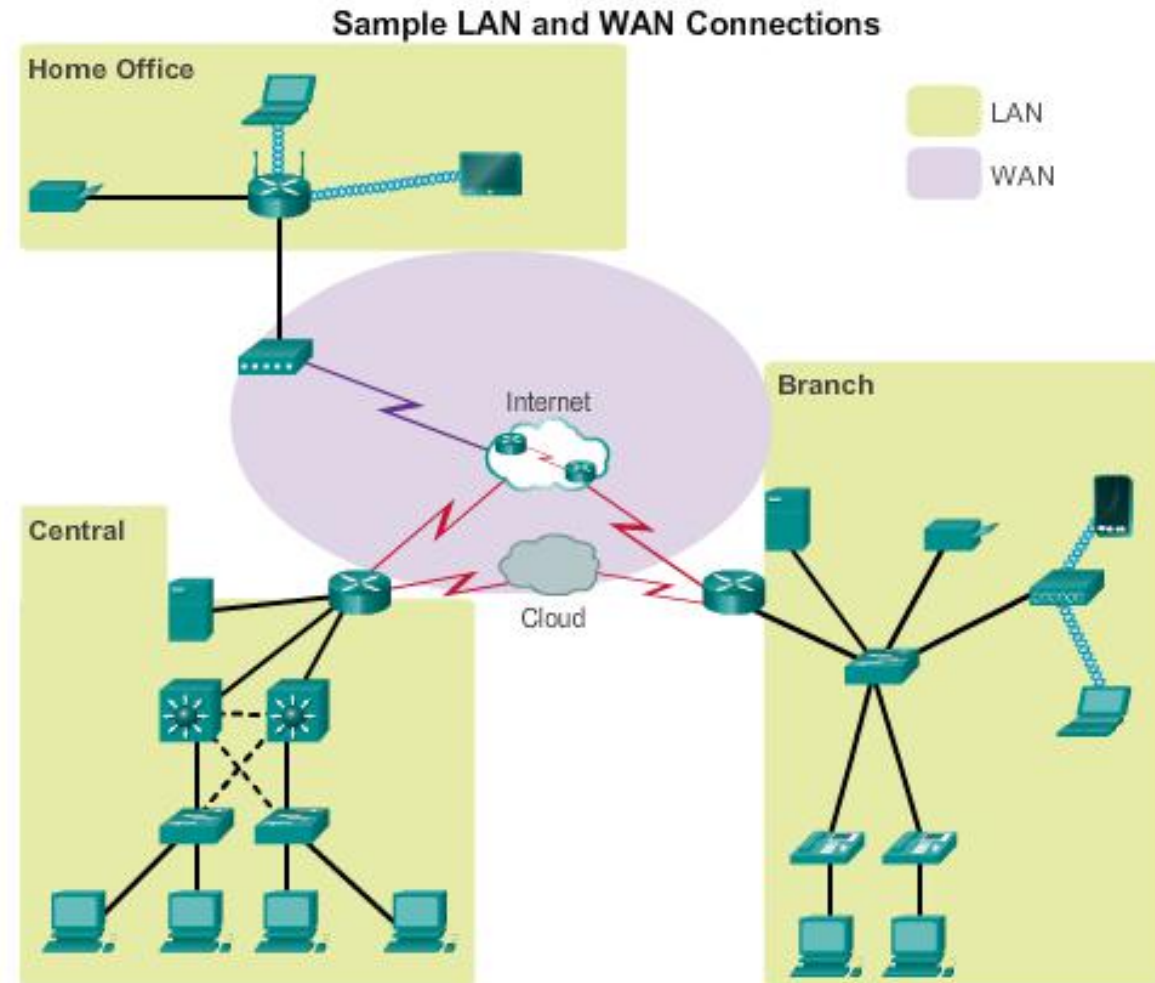
Packet Forwarding Methods

- **Process switching** – An older packet forwarding mechanism still available for Cisco routers.
- **Fast switching** – A common packet forwarding mechanism which uses a fast-switching cache to store next hop information.
- **Cisco Express Forwarding (CEF)** – The most recent, fastest, and preferred Cisco IOS packet-forwarding mechanism. Table entries are not packet-triggered like fast switching but change-triggered.



Connect Devices - Connect to a Network

36

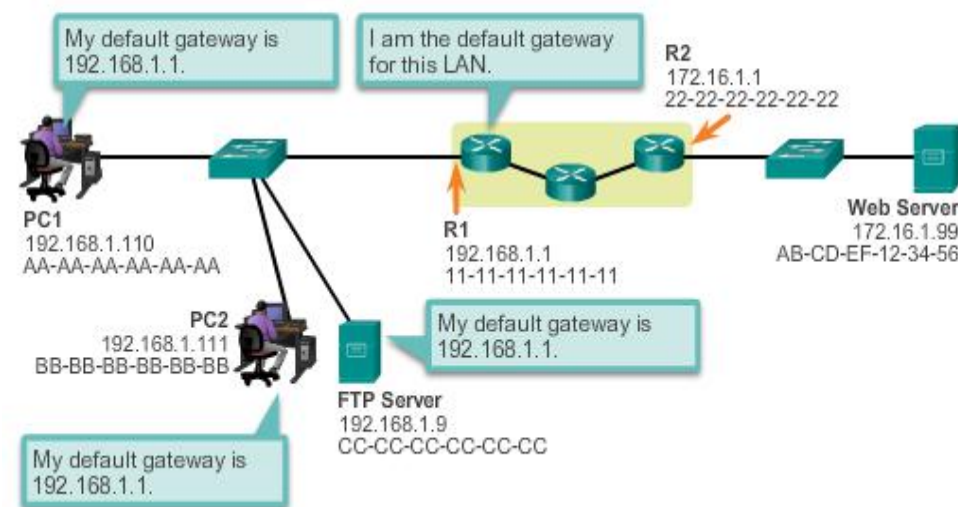


Default Gateways

To enable network access devices must be configured with the following IP address information

- **IP address** - Identifies a unique host on a local network.
- **Subnet mask** - Identifies the host's network subnet.
- **Default gateway** - Identifies the router a packet is sent to when the destination is not on the same local network subnet.

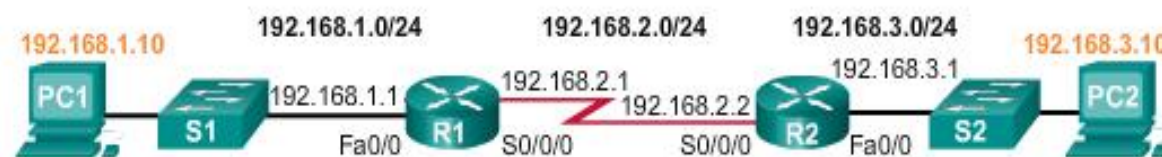
Destination MAC Address	Source MAC Address	Source IP Address	Destination MAC Address	Data
11-11-11-11-11-11	AA-AA-AA-AA-AA-AA	192.168.1.110	172.16.1.99	



Document Network Addressing

Network Documentation should include at least the following in a topology diagram and addressing table:

- Device names
- Interfaces
- IP addresses and
- subnet mask
- Default gateways



Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	192.168.2.1	255.255.255.0	N/A
R2	Fa0/0	192.168.3.1	255.255.255.0	N/A
	S0/0/0	192.168.2.2	255.255.255.0	N/A
PC1	N/A	192.168.1.10	255.255.255.0	192.168.1.1
PC2	N/A	192.168.3.10	255.255.255.0	192.168.3.1







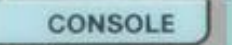



Enable IP on a Host

- **Statically Assigned IP address** – host is manually assigned the IP address, subnet mask and default gateway. DNS server IP address can also be assigned.
 - Used to identify specific network resources such as network servers and printers
 - Can be used in very small networks with few hosts.
- **Dynamically Assigned IP Address** – IP Address information is dynamically assigned by a server using Dynamic Host Configuration Protocol (DHCP)
- Most hosts acquire their IP address information through DHCP
- DHCP services can be provided by routers



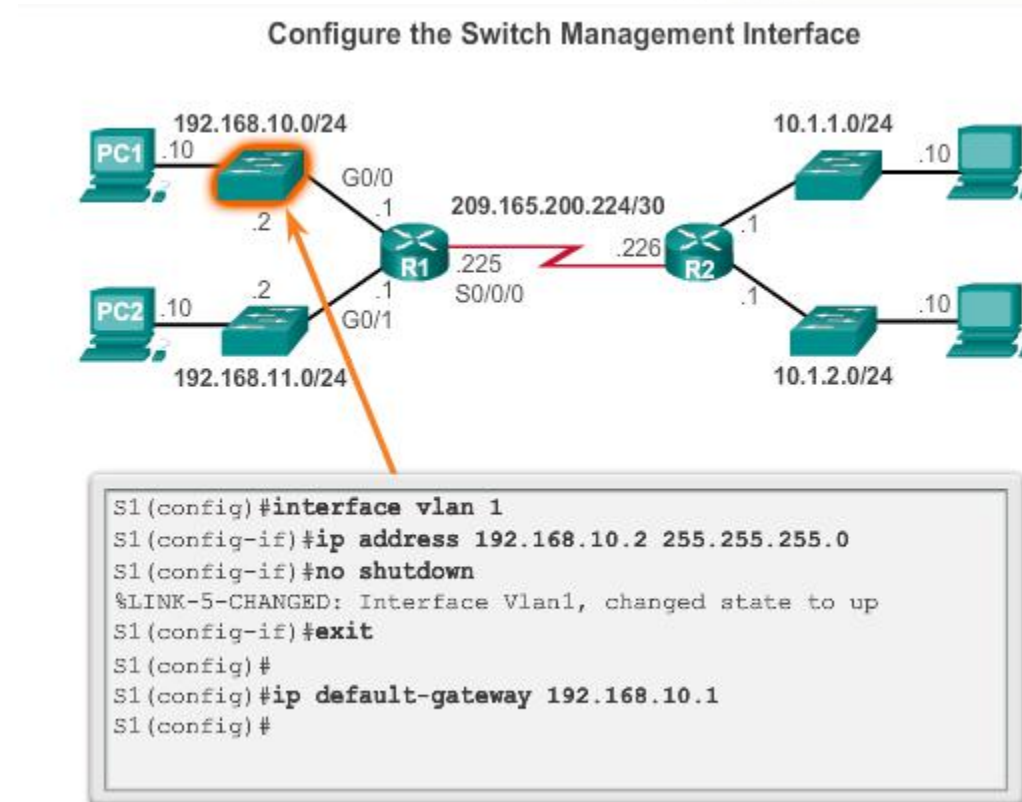
Console Access

- **Console access requires:**
 - **Console cable** – RJ-45-to-DB-9 console cable
 - **Terminal emulation software** – Tera Term, PuTTY, HyperTerminal

Port on Computer	Cable Required	Port on ISR	Terminal Emulation
 Serial Port	 Console Cable	 RJ45 Console Port	 Tera Term
 USB Type-A Port	 USB-to-RS-232 Serial Port Adapter	 RJ45 Console Port	
	 USB Type-A to USB Type-B (Mini-B) Cable	 USB Type-B (Mini-B USB) Console Port	 PuTTY

Enable IP on a Switch

- ▶ Network infrastructure devices require IP addresses to enable remote management.
- ▶ On a switch the management IP address is assigned on a virtual interface



Basic Settings on a Router (Cisco) - Configure Basic Router Settings

- Basics tasks that should be first configured on a Cisco Router and Cisco Switch:
 - **Name the device** – Distinguishes it from other routers
 - **Secure management access** – Secures privileged EXEC, user EXEC, and Telnet access, and encrypts passwords to their highest level

```
R1(config)#enable secret class
R1(config)#
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#
R1(config)#service password-encryption
R1(config)#
```

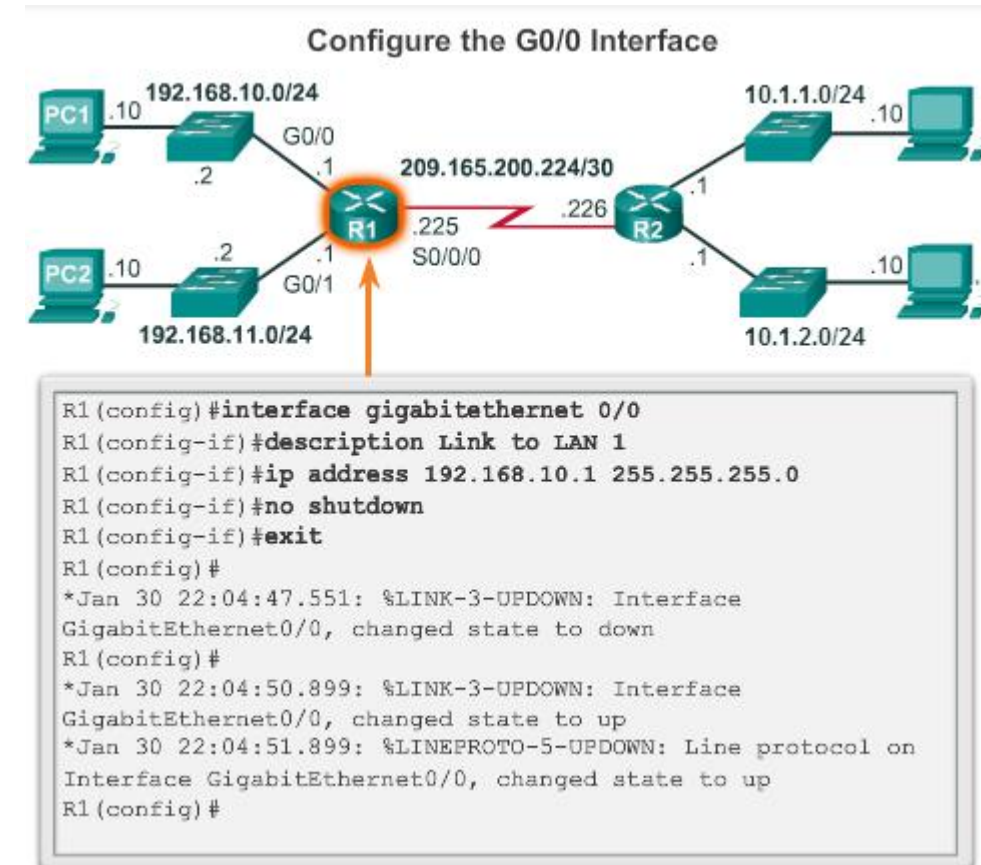
- **Configure a banner** – Provides legal notification of unauthorized access.



Configure Router Interfaces

To be available a router interface must be:

- **Configured with an address and subnet mask .**
- **Activated** – by default LAN and WAN interfaces are not activated. Must be activated using no shutdown command.
- Other parameters - serial cable end labeled DCE must be configured with the **clock rate** command.
- Optional description can be included.



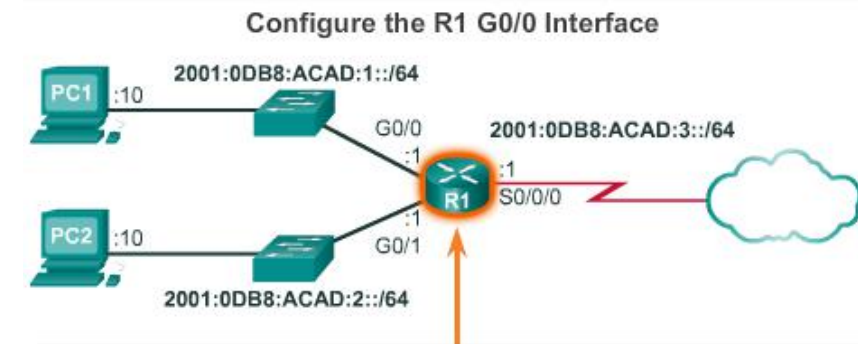
Configure an IPv6 Router Interface

- **Configure interface with IPv6 address and subnet mask.** Use the **ipv6 address** *ipv6-address/ipv6-length* [**link-local** | **eui-64**] interface configuration command.

- **Activate** – using **no shutdown** command.

IPv6 interfaces can support more than one address:

- Configure a specified global unicast - *ipv6-address /ipv6-length*
- Configure a global IPv6 address with an interface identifier (ID) in the low-order 64 bits - *ipv6-address /ipv6-length eui-64*
- Configure a link-local address - *ipv6-address /ipv6-length link-local*

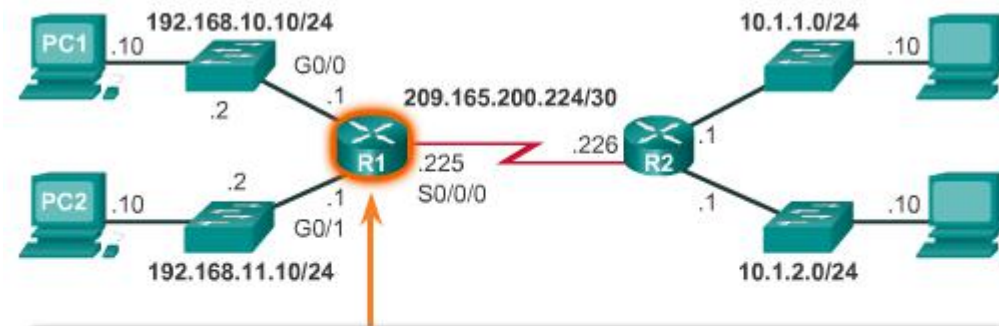


```
R1(config)#interface gigabitethernet 0/0
R1(config-if)#description Link to LAN 1
R1(config-if)#ipv6 address 2001:db8:acad:1::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
*Feb 3 21:38:37.279: %LINK-3-UPDOWN: Interface
GigabitEthernet0/0, changed state to down
*Feb 3 21:38:40.967: %LINK-3-UPDOWN: Interface
GigabitEthernet0/0, changed state to up
*Feb 3 21:38:41.967: %LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet0/0, changed state to up
R1(config)#
```

Configure a Loopback Interface

- ▶ Loopback interface is a logical interface internal to the router.
- ▶ It is not assigned to a physical port, it is considered a software interface that is automatically in an UP state.
- ▶ Useful for testing and important in the OSPF routing process.

Configure the Loopback0 Interface



```
R2 (config)#interface loopback 0
R2 (config-if)#ip address 10.0.0.1 255.255.255.0
R2 (config-if)#exit
R1 (config)#
*Jan 30 22:04:50.899: %LINK-3-UPDOWN: Interface loopback0,
changed state to up
*Jan 30 22:04:51.899: %LINEPROTO-5-UPDOWN: Line protocol on
Interface loopback0, changed state to up
```

Verify Connectivity of Directly Connected Networks

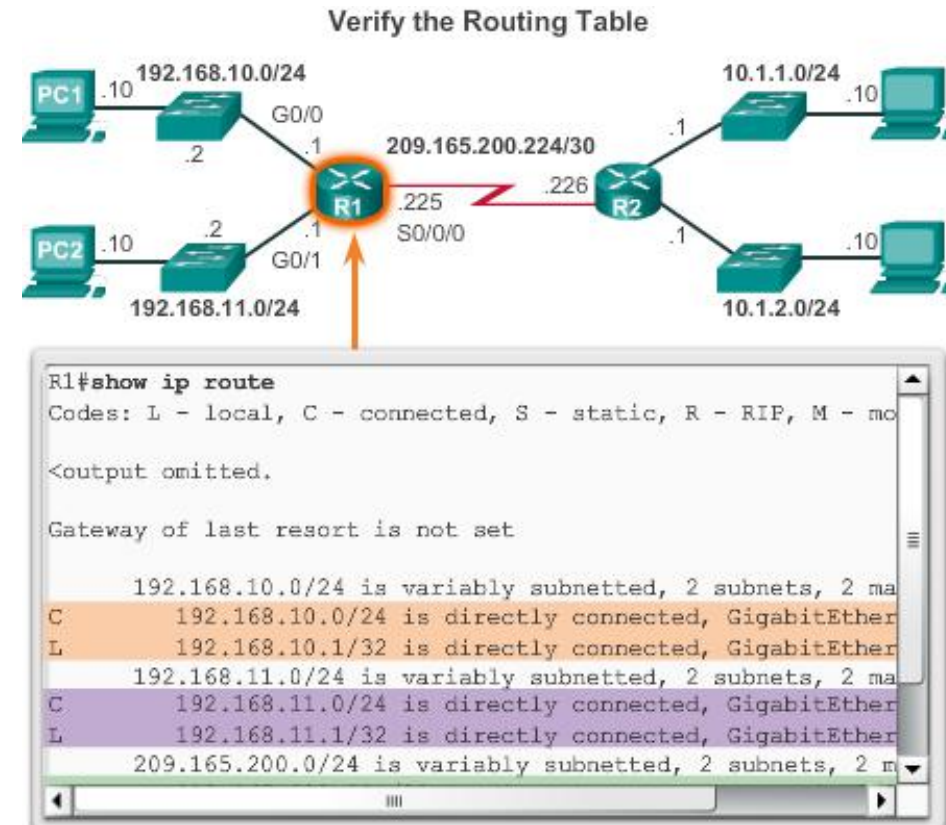
Verify Interface Settings

Show commands to verify operation and configuration of interface.

- **show ip interfaces brief**
- **show ip route**
- **show running-config**

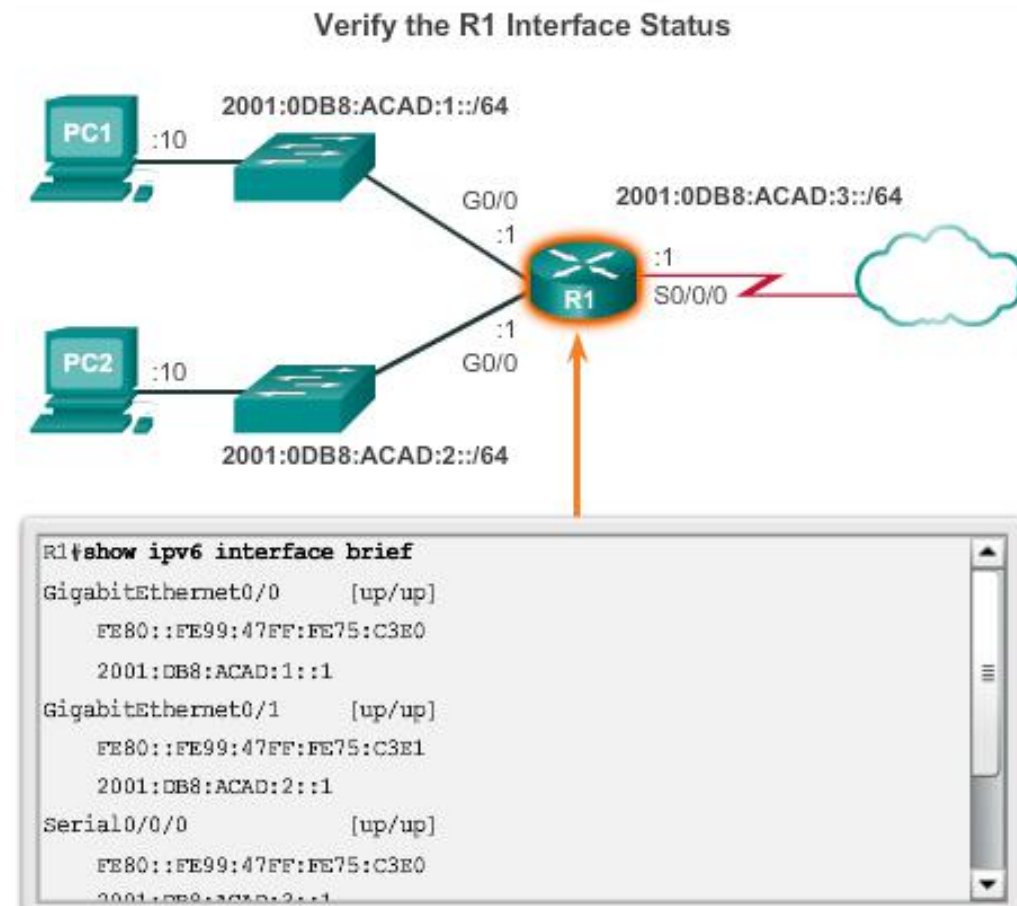
Show commands to gather more detailed interface information.

- **show interfaces**
- **show ip interfaces**



Verify Interface Settings

- ▶ **show ipv6 interface brief** - displays a summary for each of the interfaces.
- ▶ **show ipv6 interface gigabitethernet 0/0** - displays the interface status and all the IPv6 addresses for this interface.
- ▶ **show ipv6 route** - verify that IPv6 networks and specific IPv6 interface addresses have been installed in the IPv6 routing table.
- ▶ **show interface**
- ▶ **show ipv6 routers**



Filter Show Command Output

- ▶ Use the **terminal length** *number* command to specify the number of lines to be displayed. A value of 0 (zero) prevents the router from pausing between screens of output.
- ▶ To filter specific output of commands use the **(|) pipe character** after show command. Parameters that can be used after pipe include:

```
R1#show ip interface brief
Interface                IP-Address      OK? Method Status
Embedded-Service-Engine0/0 unassigned      YES unset  administrat
GigabitEthernet0/0       192.168.10.1    YES manual  up
GigabitEthernet0/1       192.168.11.1    YES manual  up
Serial0/0/0              209.165.200.225 YES manual  up
Serial0/0/1              unassigned      YES unset  administrat

R1#show ip interface brief | exclude unassigned
Interface                IP-Address      OK? Method Status
GigabitEthernet0/0       192.168.10.1    YES manual  up
GigabitEthernet0/1       192.168.11.1    YES manual  up
Serial0/0/0              209.165.200.225 YES manual  up
```

e

```
R1#show ip interface brief
Interface                IP-Address      OK? Method Status
Embedded-Service-Engine0/0 unassigned      YES unset  administrat
GigabitEthernet0/0       192.168.10.1    YES manual  up
GigabitEthernet0/1       192.168.11.1    YES manual  up
Serial0/0/0              209.165.200.225 YES manual  up
Serial0/0/1              unassigned      YES unset  administrat
R1#
R1#show ip interface brief | include up
GigabitEthernet0/0       192.168.10.1    YES manual  up
GigabitEthernet0/1       192.168.11.1    YES manual  up
Serial0/0/0              209.165.200.225 YES manual  up
R1#
```



Command History Feature

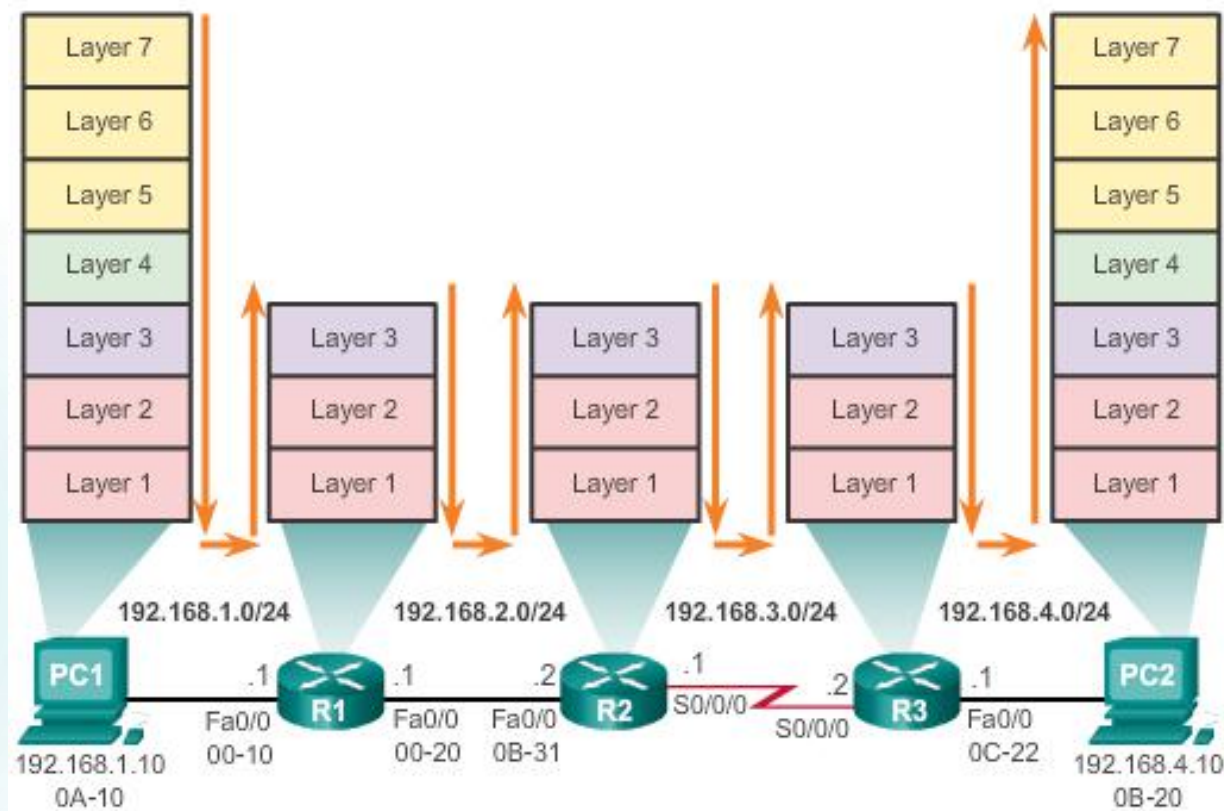
- ▶ Recall commands – **Ctrl+P** or the **UP Arrow**
- ▶ To return to more recent commands – **Ctrl+N** or **Down Arrow**
- ▶ Command history is enabled and captures the last 10 commands in buffer – **show history** displays contents
- ▶ Use **terminal history size** to increase or decrease size of the buffer.



Switching Packets between Networks

Router Switching Functions

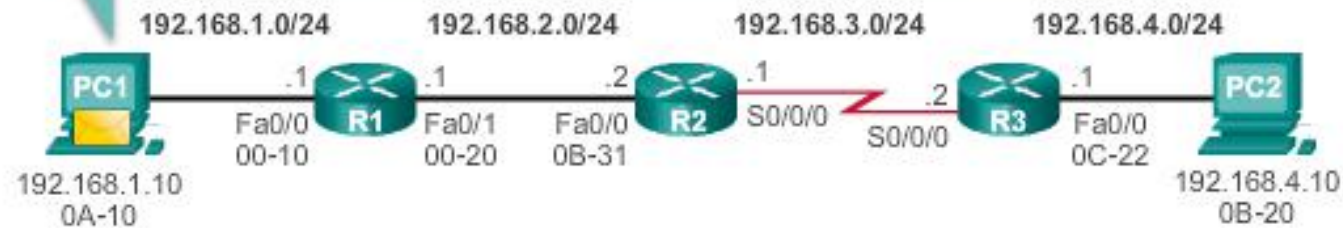
Encapsulating and De-Encapsulating Packets



Send a Packet

PC1 Sends a Packet to PC2

Because PC2 is on different network, I will encapsulate the packet and send it to the router on MY network. Let me find that MAC address....



Layer 2 Data Link Frame

Dest. MAC	Source MAC	Type	Source IP	Dest. IP	IP fields	Data	Trailer
00-10	0A-10	800	192.168.1.10	192.168.4.10			

Packet's Layer 3 data

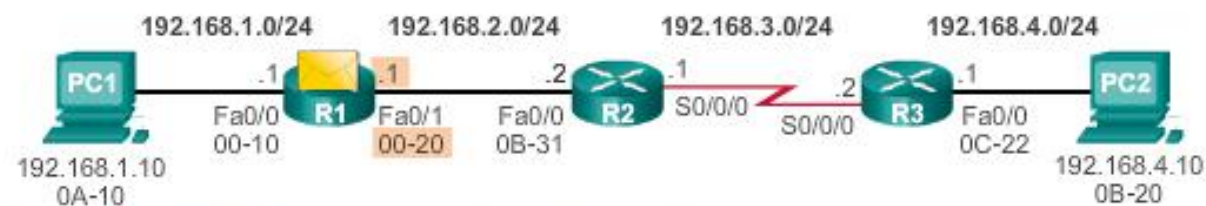
PC1's ARP Cache for R1

IP Address	MAC Address
192.168.1.1	00-10



Forward to the Next Hop

R3 Forwards the Packet to PC2



Layer 2 Data Link Frame

Packet's Layer 3 data

Dest. MAC 0B-31	Source MAC 00-20	Type 800	Source IP 192.168.1.10	Dest. IP 192.168.4.10	IP fields	Data	Trailer
--------------------	---------------------	----------	---------------------------	--------------------------	-----------	------	---------

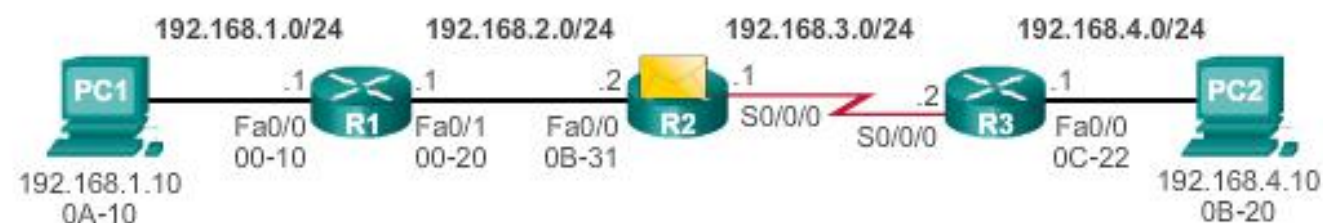
R1's Routing Table

Network	Hops	Next-hop-IP	Exit Interface
192.168.1.0/24	0	Dir. Connect.	Fa0/0
192.168.2.0/24	0	Dir. Connect.	Fa0/1
192.168.3.0/24	1	192.168.2.2	Fa0/1
192.168.4.0/24	2	192.168.2.2	Fa0/1



Packet Routing

R2 Forwards the Packet to R3



Layer 2 Data Link Frame

Packet's Layer 3 data

Address 0x8F	Control 0x00	Type 800	Source IP 192.168.1.10	Dest. IP 192.168.4.10	IP fields	Data	Trailer
-----------------	-----------------	----------	---------------------------	--------------------------	-----------	------	---------

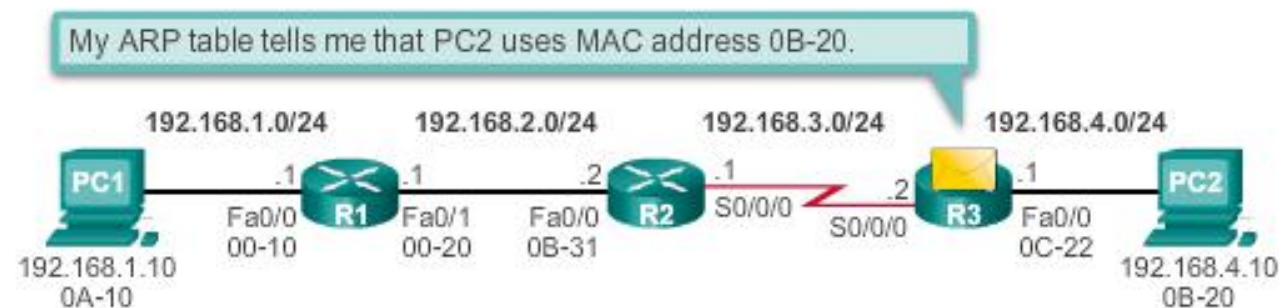
R2's Routing Table

Network	Hops	Next-hop-IP	Exit Interface
192.168.1.0/24	1	192.168.3.1	Fa0/0/0
192.168.2.0/24	0	Dir. Connect.	Fa0/0/0
192.168.3.0/24	0	Dir. Connect.	S0/0/0
192.168.4.0/24	1	192.162.3.2	S0/0/0



Reach the Destination

R3 Forwards the Packet to PC2



Layer 2 Data Link Frame

Dest. MAC	Source MAC	Type	Source IP	Dest. IP	IP fields	Data	Trailer
0B-20	0C-22	800	192.168.1.10	192.168.4.10			

Packet's Layer 3 data

IP Address	MAC Address
192.168.4.10	0B-20

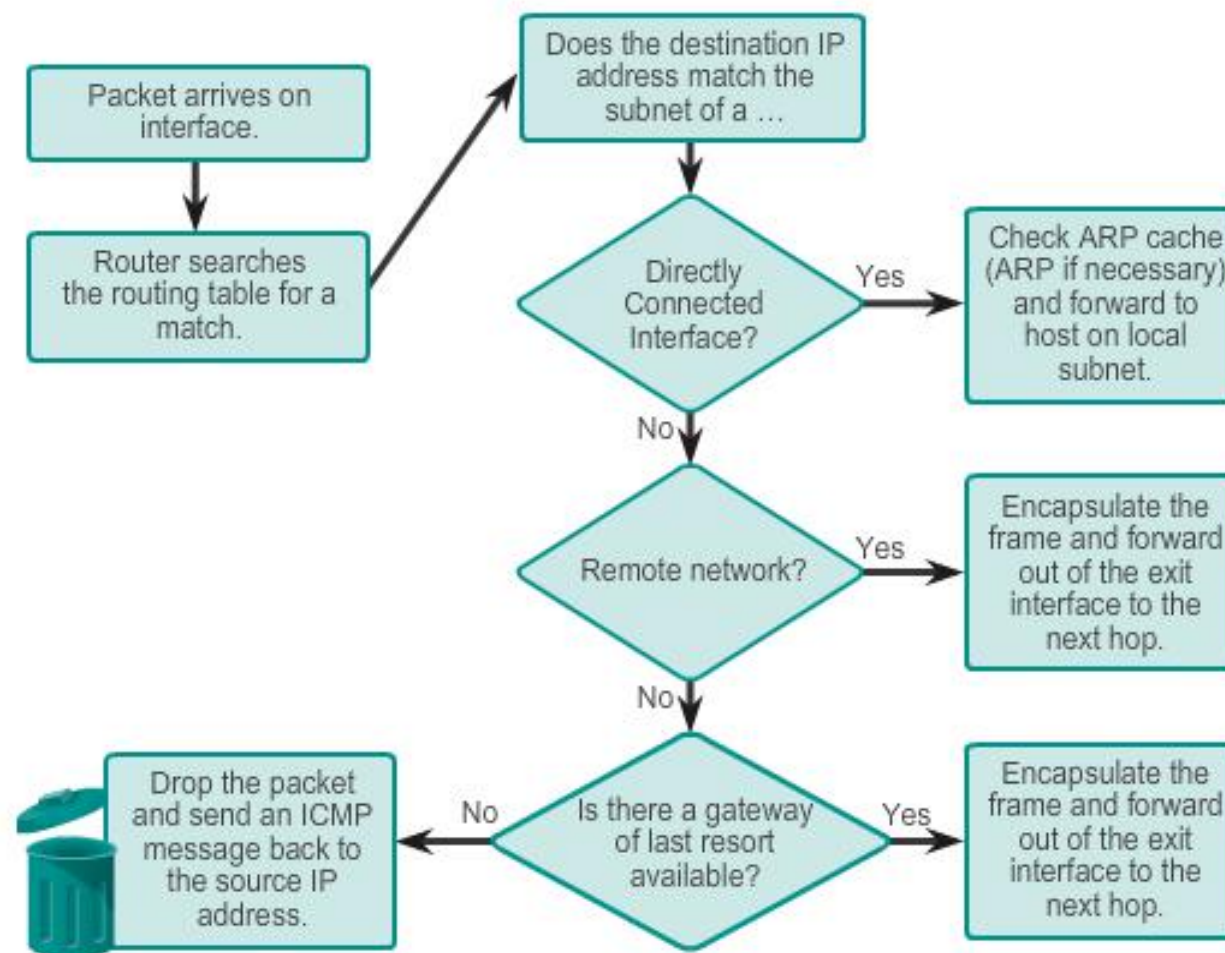
R3's Routing Table

Network	Hops	Next-hop-IP	Exit Interface
192.168.1.0/24	2	192.168.3.1	S0/0/0
192.168.2.0/24	1	192.162.3.1	S0/0/0
192.168.3.0/24	0	Dir. Connect.	S0/0/0
192.168.4.0/24	0	Dir. Connect.	Fa0/0



Path Determination Routing Decisions

Packet Forwarding Decision Process



Best Path

- Best path is selected by a routing protocol based on the value or metric it uses to determine the distance to reach a network.
- A metric is the value used to measure the distance to a given network.
- Best path to a network is the path with the lowest metric.
- Dynamic routing protocols use their own rules and metrics to build and update routing tables for example:
 - **Routing Information Protocol (RIP)** - Hop count
 - **Open Shortest Path First (OSPF)** - Cost based on cumulative bandwidth from source to destination
 - **Enhanced Interior Gateway Routing Protocol (EIGRP)** - Bandwidth, delay, load, reliability



Load Balancing

- When a router has two or more paths to a destination with equal cost metrics, then the router forwards the packets using both paths equally.



Path Determination of the route

Administrative Distance

- If multiple paths to a destination are configured on a router, the path installed in the routing table is the one with the best Administrative Distance (AD).
- Administrative Distance is the “trustworthiness”
- The Lower the AD the more trustworthy the route.

Route Source	Default Administrative Distances
Connected	0
Static	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
External EIGRP	170
Internal BGP	200



Administrative Distance

- If multiple paths to a destination are configured on a router, the path installed in the routing table is the one with the best (lowest) Administrative Distance (AD).
- Administrative Distance is the “trustworthiness” of the route
- The Lower the AD the more trustworthy the route.

Default Administrative Distances

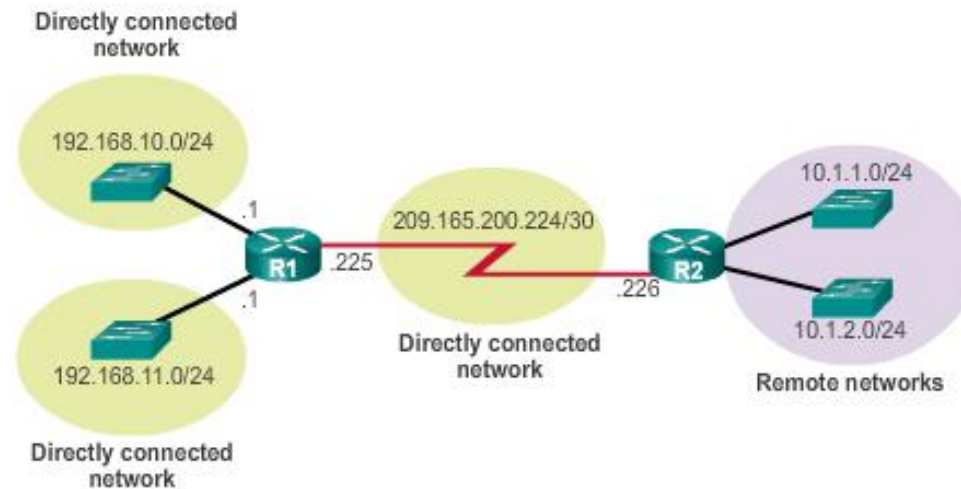
Route Source	Administrative Distance
Connected	0
Static	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
External EIGRP	170
Internal BGP	200



The Routing Table

The Routing Table

- Routing Table is a file stored in RAM that contains information about
 - Directly Connected Routes
 - Remote Routes
 - Network or Next hop Associations

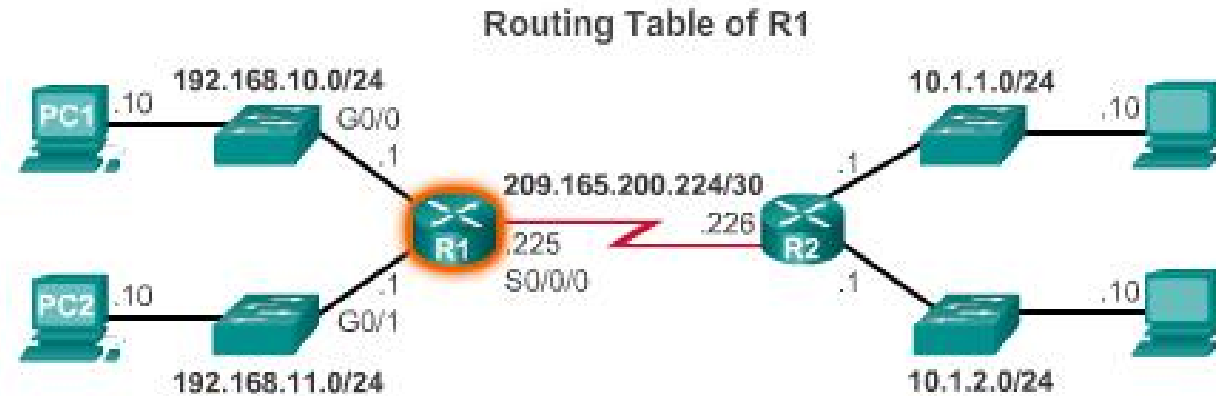


Routing Table Sources

- ▶ Show ip route command is used to display the contents of the routing table
- ▶ **Link local Interfaces** –Added to the routing table when an interface is configured.
- ▶ **Directly connected interfaces** -Added to the routing table when an interface is configured and active.
- ▶ **Static routes** - Added when a route is manually configured and the exit interface is active.
- ▶ **Dynamic routing protocol** - Added when EIGRP or OSPF are implemented and networks are identified.



Routing Table Sources



```
R1#show ip route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
```

```
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
```

```
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
```

```
IS-IS inter area
```

```
* - candidate default, U - per-user static route, o - ODR
```

```
P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

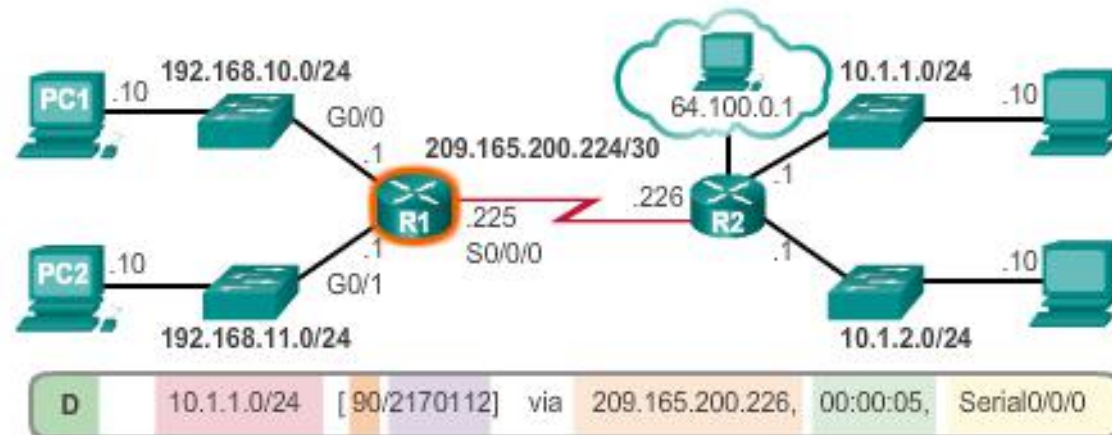
```
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
```

```
D 10.1.1.0/24 [90/2170112] via 209.165.200.226, 00:00:05,
```

Remote Network Routing Entries

- Interpreting the entries in the routing table.

Remote Network Entry Identifiers



Legend

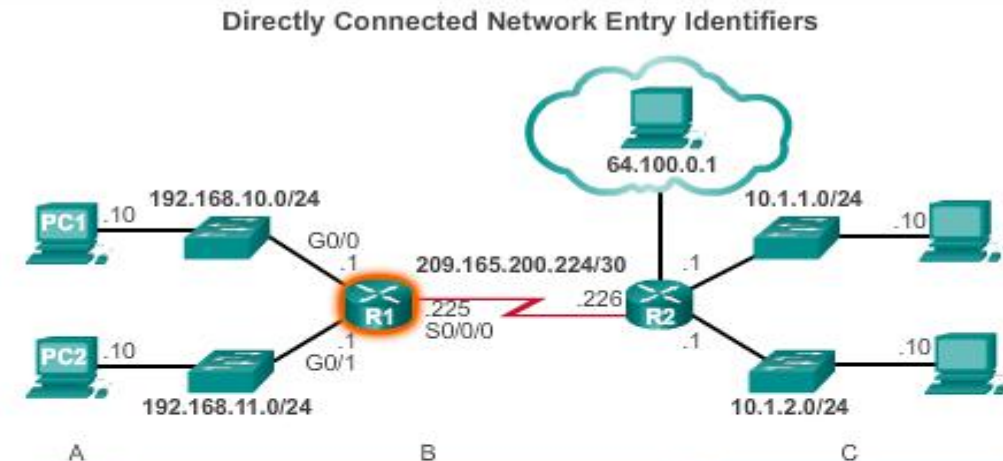
- Identifies how the network was learned by the router.
- Identifies the destination network.
- Identifies the administrative distance (trustworthiness) of the route source.
- Identifies the metric to reach the remote network.
- Identifies the next-hop IP address to reach the remote network.
- Identifies the amount of elapsed time since the network was discovered.
- Identifies the outgoing interface on the router to reach the destination network.



Directly Connected Routes

Directly Connected Interfaces

- ▶ A newly deployed router, without any configured interfaces, has an empty routing table.
- ▶ An active, configured directly connected interface creates two routing table entries Link Local (L) and Directly Connected (C)



A	B	C
C	192.168.10.0/24 is directly connected,	GigabitEthernet0/0
L	192.168.10.1/32 is directly connected,	GigabitEthernet0/0

Legend

- Identifies how the network was learned by the router.
- Identifies the destination network and how it is connected.
- Identifies the interface on the router connected to the destination network.



Statically Learned Routes

Static Routes

- ▶ Manually configured
- ▶ Define an explicit path between two networking devices.
- ▶ Must be manually updated if the topology changes.
- ▶ Benefits include improved security and control of resources.
- ▶ Static route to a specific network.
 - **ip route** *network mask {next-hop-ip | exit-intf}*
- ▶ Default Static Route used when the routing table does not contain a path for a destination network.
 - `ip route 0.0.0.0 0.0.0.0 {exit-intf | next-hop-ip}`



Static Routes Example

Entering and Verifying a Static Default Route



```
R1(config)#ip route 0.0.0.0 0.0.0.0 Serial0/0/0
R1(config)#exit
R1#
*Feb 1 10:19:34.483: %SYS-5-CONFIG_I: Configured from console
by console

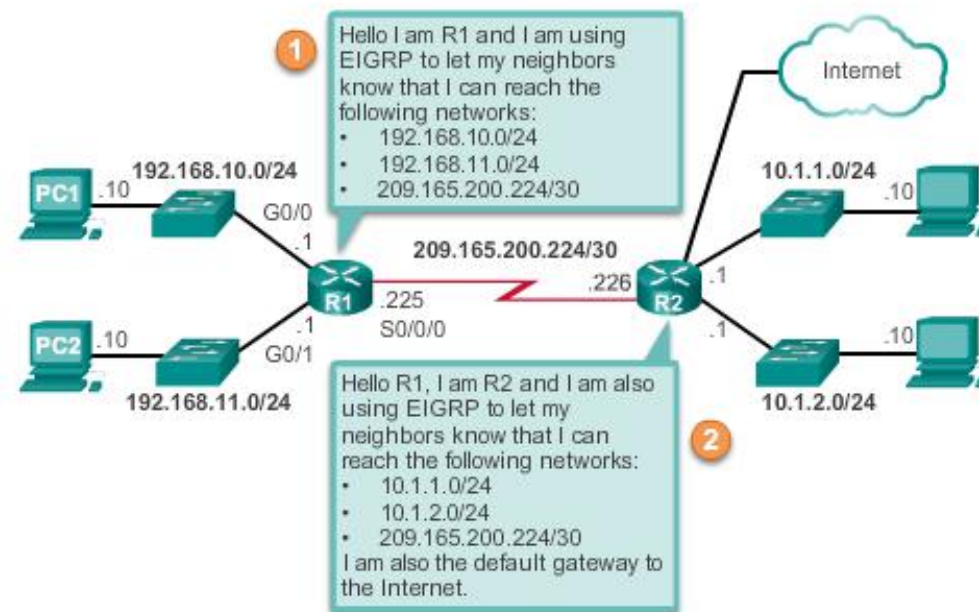
R1#show ip route | begin Gateway
Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S* 0.0.0.0/0 is directly connected, Serial0/0/0
  192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.10.0/24 is directly connected, GigabitEthernet0/0
L   192.168.10.1/32 is directly connected, GigabitEthernet0/0
  192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.11.0/24 is directly connected, GigabitEthernet0/1
L   192.168.11.1/32 is directly connected, GigabitEthernet0/1
```



Dynamic Routing

- ▶ Used by routers to share information about the reachability and status of remote networks.
- ▶ Performs network discovery and maintaining routing tables.

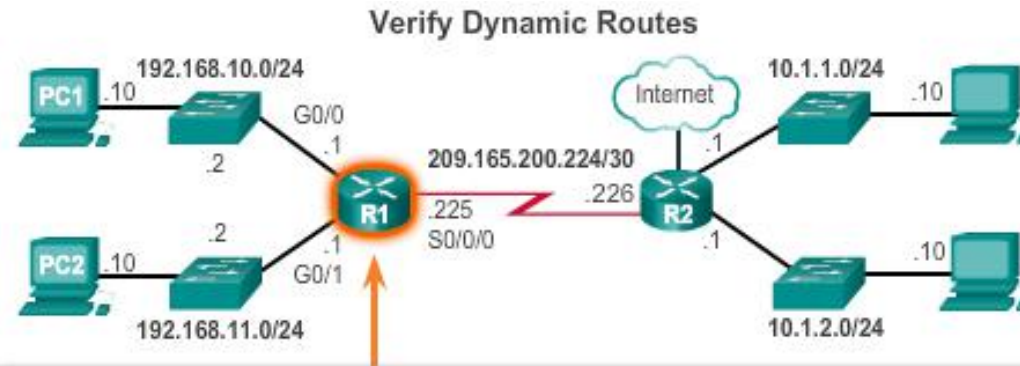


IPv4 Routing Protocols

- Routers can support a variety of dynamic IPv4 routing protocols including:
- **EIGRP** – Enhanced Interior Gateway Routing Protocol
- **OSPF** – Open Shortest Path First
- **IS-IS** – Intermediate System-to-Intermediate System
- **RIP** – Routing Information Protocol



IPv4 Routing Protocols



```
R1#show ip route | begin Gateway
Gateway of last resort is 209.165.200.226 to network 0.0.0.0

D*EX 0.0.0.0/0 [170/2297856] via 209.165.200.226, 00:07:29, Serial0/0/0
    10.0.0.0/24 is subnetted, 2 subnets
D      10.1.1.0 [90/2172416] via 209.165.200.226, 00:07:29, Serial0/0/0
D      10.1.2.0 [90/2172416] via 209.165.200.226, 00:07:29, Serial0/0/0
    192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.10.0/24 is directly connected, GigabitEthernet0/0
L      192.168.10.1/32 is directly connected, GigabitEthernet0/0
    192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.11.0/24 is directly connected, GigabitEthernet0/1
L      192.168.11.1/32 is directly connected, GigabitEthernet0/1
    209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C      209.165.200.224/30 is directly connected, Serial0/0/0
L      209.165.200.225/32 is directly connected, Serial0/0/0
R1#
```



Static Routing



Learning Objectives

- ▶ Explain the advantages and disadvantages of static routing.
- ▶ Explain the purpose of different types of static routes.
- ▶ Configure IPv4 static routes by specifying a next-hop address.
- ▶ Configure an IPv4 default routes.
- ▶ Explain the use of legacy classful addressing in network implementation.
- ▶ Explain the purpose of CIDR in replacing classful addressing.
- ▶ Design and implement a hierarchical addressing scheme.
- ▶ Configure a floating static route to provide a backup connection.
- ▶ Explain how a router processes packets when a static route is configured.
- ▶ Troubleshoot common static and default route configuration issues.



Reach Remote Networks

- ▶ A router can learn about remote networks in one of two ways:
 - Manually - Remote networks are manually entered into the route table using static routes.
 - Dynamically - Remote routes are automatically learned using a dynamic routing protocol.



Why Use Static Routing?

- **Static routing** provides some advantages over dynamic routing, including:
 - ▶ Static routes are not advertised over the network, resulting in better security.
 - ▶ Static routes use less bandwidth than dynamic routing protocols, no CPU cycles are used to calculate and communicate routes.
 - ▶ The path a static route uses to send data is known.



Why Use Static Routing? (continued)

Static routing has the following **disadvantages**:

- ▶ Initial configuration and maintenance is time-consuming.
- ▶ Configuration is error-prone, especially in large networks.
- ▶ Administrator intervention is required to maintain changing route information.
- ▶ Does not scale well with growing networks; maintenance becomes cumbersome.
- ▶ Requires complete knowledge of the whole network for proper implementation.



When to Use Static Routes

Static routing has three primary uses:

- ▶ Providing ease of routing table maintenance in smaller networks that are not expected to grow significantly.
- ▶ Routing to and from stub networks. A **stub network** is a network accessed by a single route, and the router has no other neighbors.
- ▶ Using a single default route to represent a path to any network that does not have a more specific match with another route in the routing table. Default routes are used to send traffic to any destination beyond the next upstream router.



Types of Static Routes - Static Route Applications

76

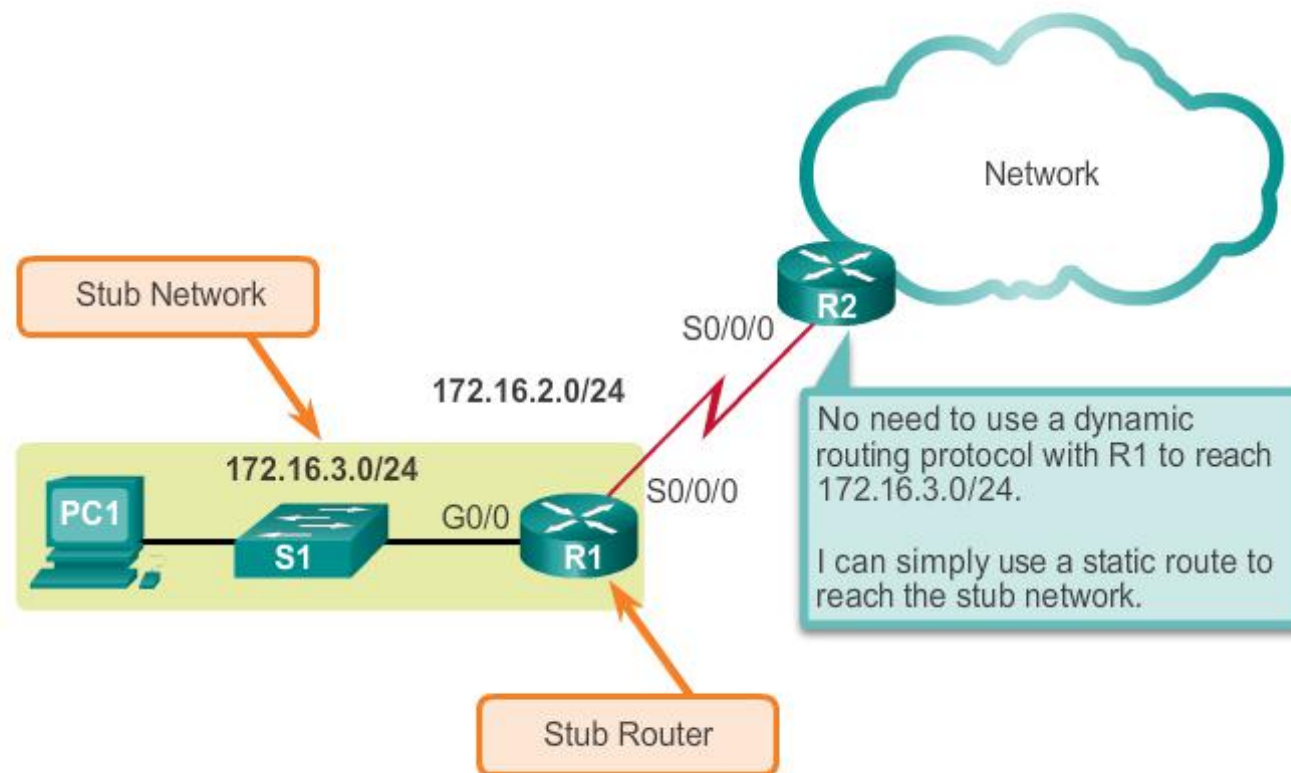
Static Routes are often used to:

- ▶ Connect to a specific network
- ▶ Provide a Gateway of Last Resort for a stub network
- ▶ Reduce the number of routes advertised by summarizing several contiguous networks as one static route
- ▶ Create a backup route in case a primary route link fails



Standard Static Route

Connecting to a Stub Network



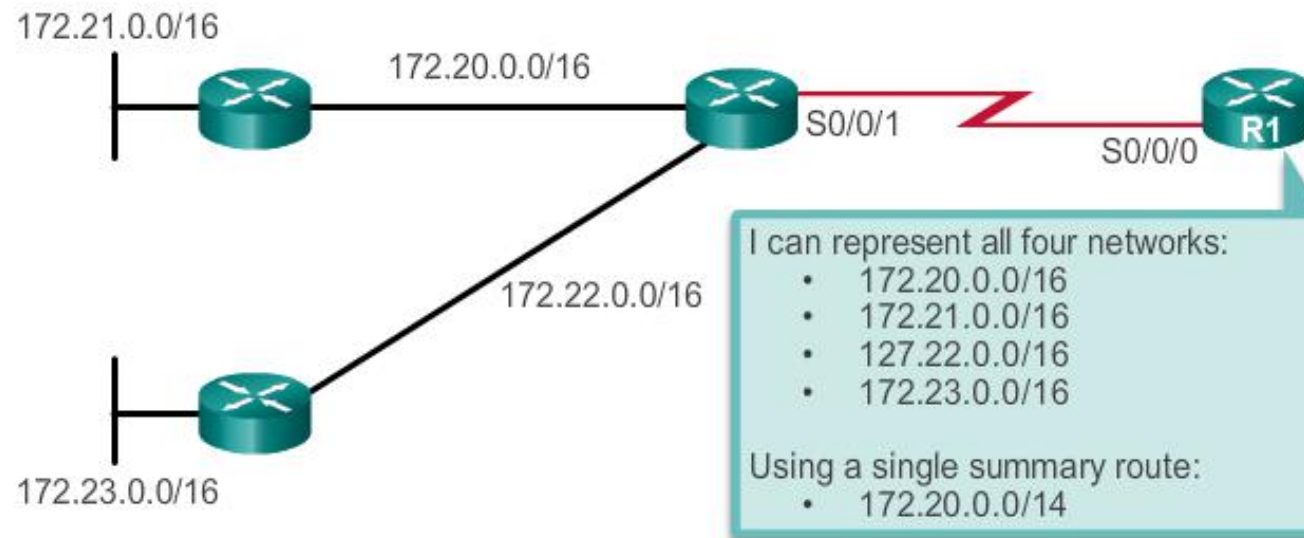
Default Static Route

- ▶ A default static route is a route that matches all packets.
- ▶ A default route identifies the gateway IP address to which the router sends all IP packets that it does not have a learned or static route.
- ▶ A default static route is simply a static route with 0.0.0.0/0 as the destination IPv4 address.



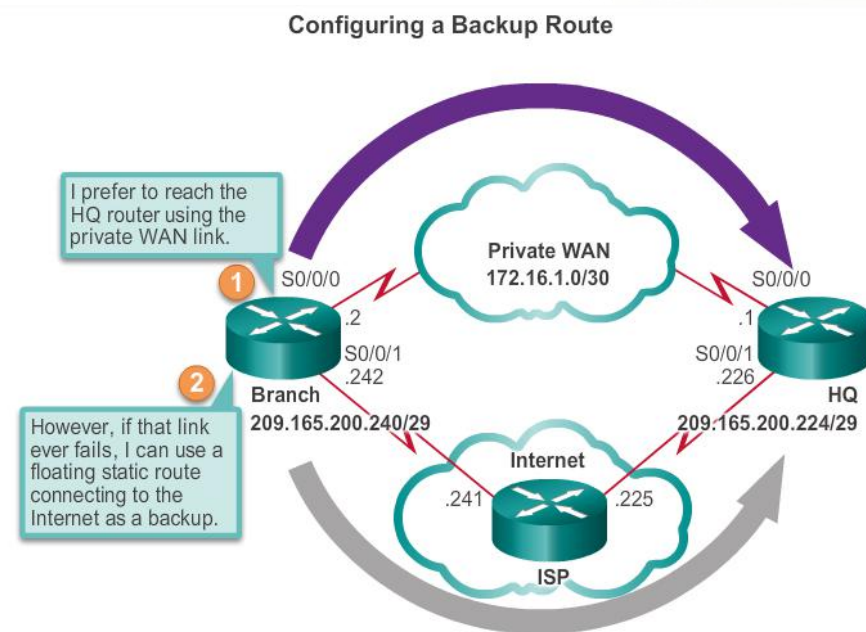
Summary Static Route

Using One Summary Static Route



Floating Static Route

- ▶ Floating static routes are static routes that are used to provide a **backup** path to a primary static or dynamic route, in the event of a link failure.
- ▶ The floating static route is only used when the primary route is not available.
- ▶ In order to accomplish this, the floating static route is configured with a higher administrative distance than the primary route.



Configure IPv4 Static Routes - ip route Command

ip route Command Syntax

```
Router(config)#ip route network-address subnet-mask  
{ip-address | exit-intf}
```

Parameter	Description
network-address	Destination network address of the remote network to be added to the routing table.
subnet-mask	<ul style="list-style-type: none">• Subnet mask of the remote network to be added to the routing table.• The subnet mask can be modified to summarize a group of networks.
ip-address	<ul style="list-style-type: none">• Commonly referred to as the next-hop router's IP address.• Typically used when connecting to a broadcast media (i.e., Ethernet).• Commonly creates a recursive lookup.
exit-intf	<ul style="list-style-type: none">• Use the outgoing interface to forward packets to the destination network.• Also referred to as a directly attached static route.• Typically used when connecting in a point-to-point configuration.



Next-Hop Options

The next hop can be identified by an IP address, exit interface, or both. How the destination is specified creates one of the three following route types:

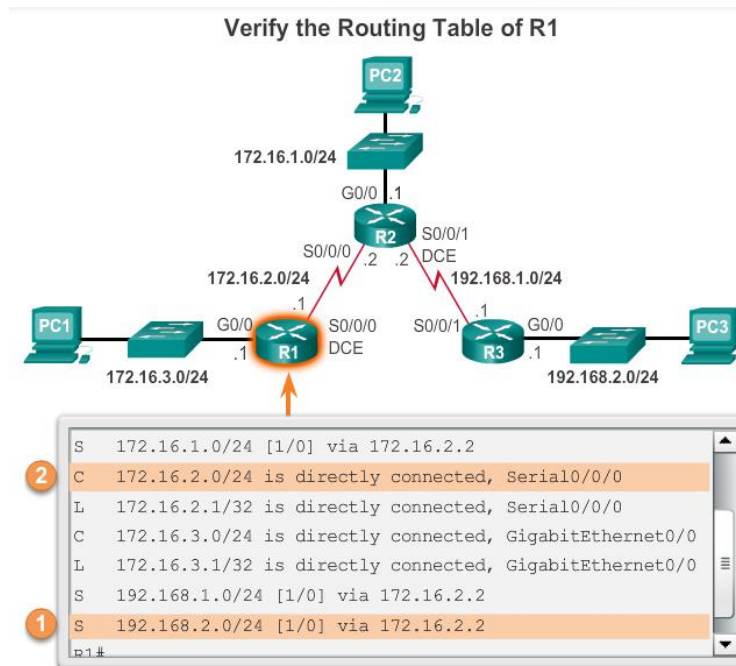
- ▶ Next-hop route - Only the next-hop IP address is specified.
- ▶ Directly connected static route - Only the router exit interface is specified.
- ▶ Fully specified static route - The next-hop IP address and exit interface are specified.



Configure a Next-Hop Static Route

When a packet is destined for the 192.168.2.0/24 network, R1:

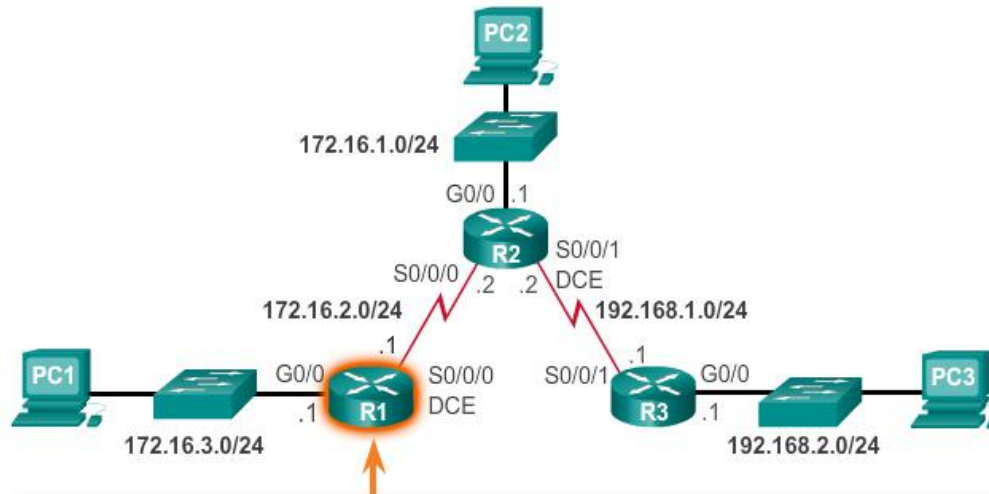
1. Looks for a match in the routing table and finds that it has to forward the packets to the next-hop IPv4 address 172.16.2.2.
2. R1 must now determine how to reach 172.16.2.2; therefore, it searches a second time for a 172.16.2.2 match.



Configure Directly Connected Static Route

84

Configure Directly Attached Static Routes on R1



```
R1 (config) #ip route 172.16.1.0 255.255.255.0 s0/0/0
R1 (config) #ip route 192.168.1.0 255.255.255.0 s0/0/0
R1 (config) #ip route 192.168.2.0 255.255.255.0 s0/0/0
R1 (config) #
```

```
S    172.16.1.0/24 is directly connected, Serial0/0/0
C    172.16.2.0/24 is directly connected, Serial0/0/0
L    172.16.2.1/32 is directly connected, Serial0/0/0
C    172.16.3.0/24 is directly connected, GigabitEthernet0/0
L    172.16.3.1/32 is directly connected, GigabitEthernet0/0
S    192.168.1.0/24 is directly connected, Serial0/0/0
S    192.168.2.0/24 is directly connected, Serial0/0/0
R1#
```



Default Static Route

Default Static Route Syntax

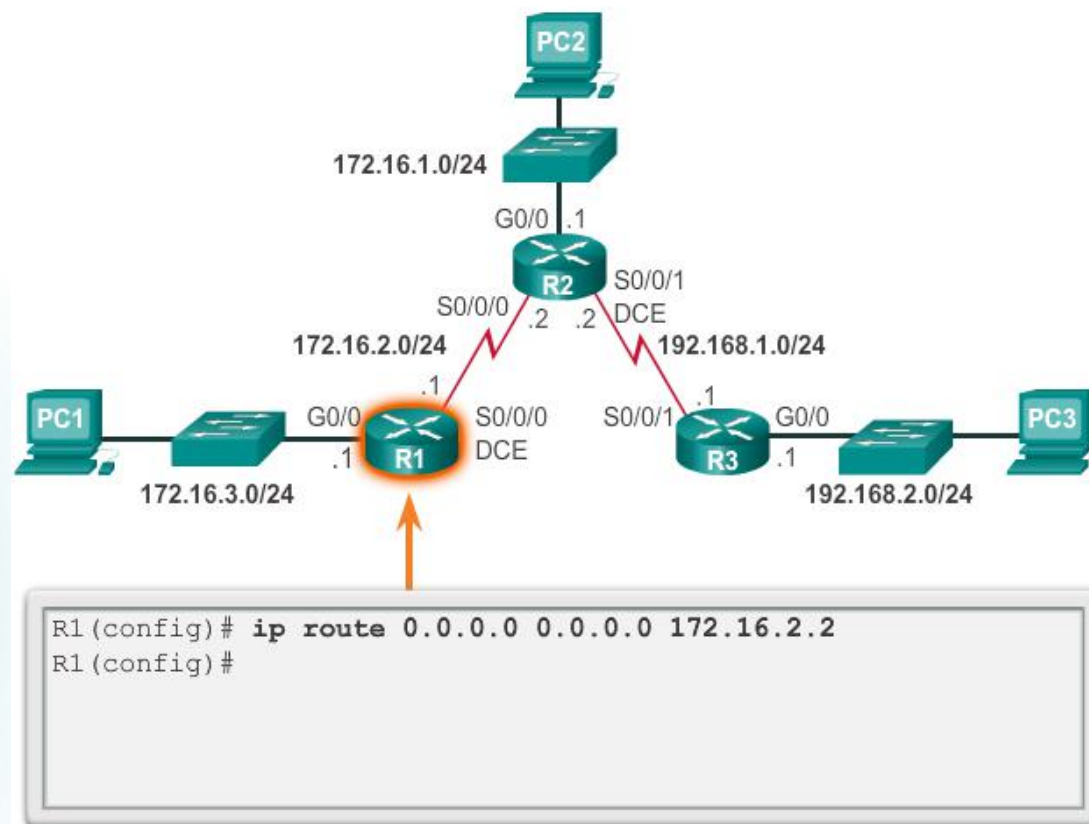
```
Router(config)#ip route 0.0.0.0 0.0.0.0 {ip-address | exit-intf}
```

Parameter	Description
0.0.0.0	Matches any network address.
0.0.0.0	Matches any subnet mask.
ip-address	<ul style="list-style-type: none">• Commonly referred to as the next-hop router's IP address.• Typically used when connecting to a broadcast media (i.e., Ethernet).• Commonly creates a recursive lookup.
exit-intf	<ul style="list-style-type: none">• Use the outgoing interface to forward packets to the destination network.• Also referred to as a directly attached static route.• Typically used when connecting in a point-to-point configuration.



Configure a Default Static Route

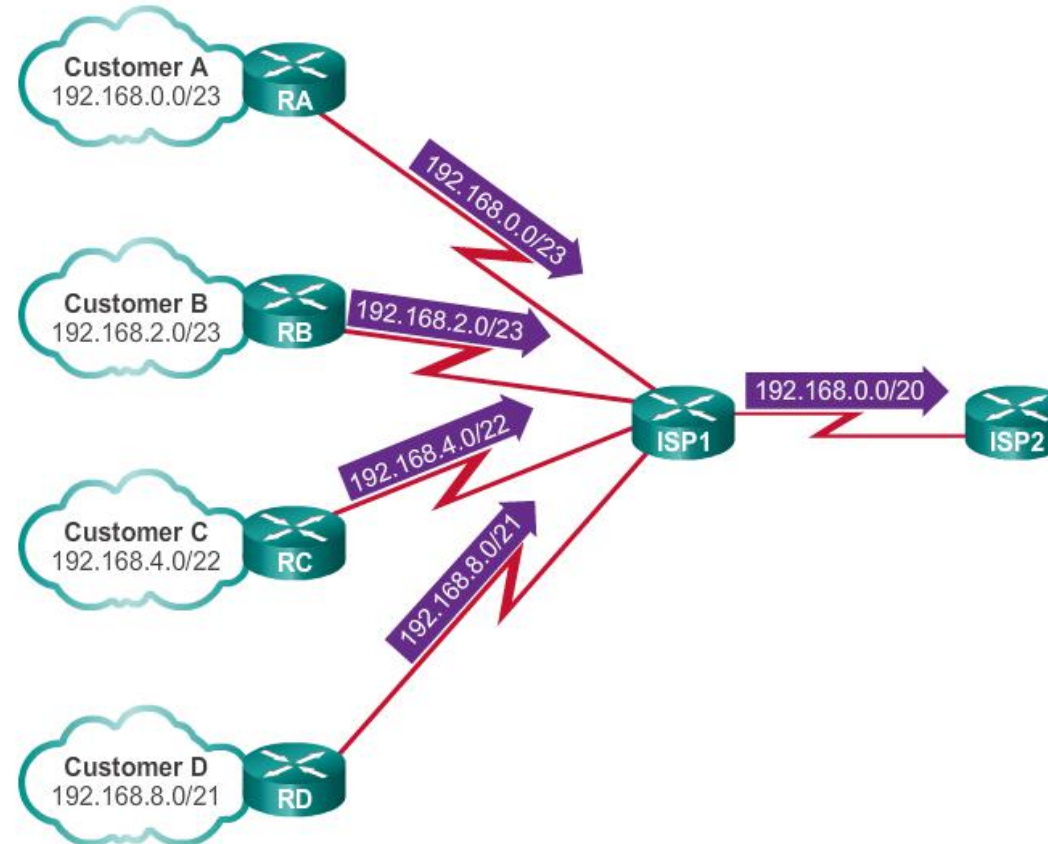
Configuring a Default Static Route



CIDR and Route Summarization

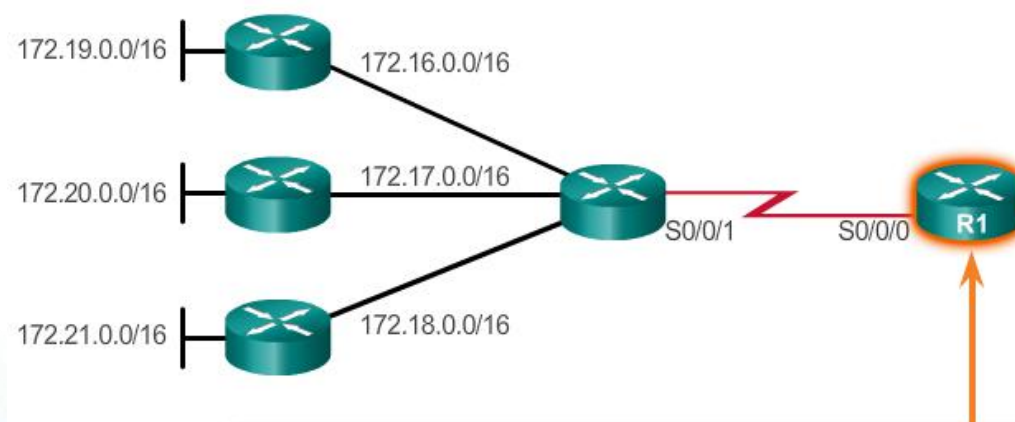
87

Summarizing Supernet Routes



Static Routing CIDR Example

One Summary Static Route



```
R1 (config) #no ip route 172.16.0.0 255.255.0.0 s0/0/0
R1 (config) #no ip route 172.17.0.0 255.255.0.0 s0/0/0
R1 (config) #no ip route 172.18.0.0 255.255.0.0 s0/0/0
R1 (config) #no ip route 172.19.0.0 255.255.0.0 s0/0/0
R1 (config) #no ip route 172.20.0.0 255.255.0.0 s0/0/0
R1 (config) #no ip route 172.21.0.0 255.255.0.0 s0/0/0
R1 (config) #
R1 (config) #ip route 172.16.0.0 255.248.0.0 s0/0/0
R1 (config) #
```



Calculate a Summary Route

Calculating a Route Summary

Step 1: List networks in binary format.

172.20.0.0	10101100 . 00010100 . 00000000 . 00000000
172.21.0.0	10101100 . 00010101 . 00000000 . 00000000
172.22.0.0	10101100 . 00010110 . 00000000 . 00000000
172.23.0.0	10101100 . 00010111 . 00000000 . 00000000

Step 2: Count the number of far-left matching bits to determine the mask.

Answer: 14 matching bits = /14 or 255.252.0.0

Step 3: Copy the matching bits and add zero bits to determine the network address.

10101100 . 00010100 . 00000000 . 00000000
<div style="display: inline-block; width: 100px; border-top: 1px solid black; margin-top: 5px;"></div> Copy <div style="display: inline-block; width: 100px; border-top: 1px solid black; margin-top: 5px;"></div> Add zero bits <div style="display: inline-block; width: 100px; border-top: 1px solid black; margin-top: 5px;"></div>

Answer: 172.20.0.0



Routing Dynamically



Learning Objectives

- ▶ Explain the basic operation of dynamic routing protocols.
- ▶ Compare and contrast dynamic and static routing.
- ▶ Determine which networks are available during an initial network discovery phase.
- ▶ Define the different categories of routing protocols.
- ▶ Describe the process by which distance vector routing protocols learn about other networks.
- ▶ Identify the types of distance-vector routing protocols.
- ▶ Explain the process by which link-state routing protocols learn about other networks.
- ▶ Describe the information sent in a link-state update.
- ▶ Describe advantages and disadvantages of using link-state routing protocols.



The Evolution of Dynamic Routing Protocols

- ▶ Dynamic routing protocols used in networks since the late 1980s
- ▶ Newer versions support the communication based on IPv6

Routing Protocols Classification

	Interior Gateway Protocols				Exterior Gateway Protocols
	Distance Vector		Link-State		Path Vector
IPv4	RIPv2	EIGRP	OSPFv2	IS-IS	BGP-4
IPv6	RIPng	EIGRP for IPv6	OSPFv3	IS-IS for IPv6	BGP-MP



Purpose of Dynamic Routing Protocols

➤ **Routing Protocols**

- ❑ Used to facilitate the exchange of routing information between routers

➤ **Purpose of dynamic routing protocols includes:**

- ❑ Discovery of remote networks
- ❑ Maintaining up-to-date routing information
- ❑ Choosing the best path to destination networks
- ❑ Ability to find a new best path if the current path is no longer available



Purpose of Dynamic Routing Protocols

Main components of dynamic routing protocols include:

- ▶ **Data structures** - Routing protocols typically use tables or databases for its operations. This information is kept in RAM.
- ▶ **Routing protocol messages** - Routing protocols use various types of messages to discover neighboring routers, exchange routing information, and other tasks to learn and maintain accurate information about the network.
- ▶ **Algorithm** - Routing protocols use algorithms for facilitating routing information for best path determination.



The Role of Dynamic Routing Protocols

➤ Advantages of dynamic routing

- Automatically share information about remote networks
- Determine the best path to each network and add this information to their routing tables
- Compared to static routing, dynamic routing protocols require less administrative overhead
- Help the network administrator manage the time-consuming process of configuring and maintaining static routes

➤ Disadvantages of dynamic routing

- Dedicate part of a routers resources for protocol operation, including CPU time and network link bandwidth
- **Times when static routing is more appropriate**



Dynamic verses Static Routing -Using Static Routing

- Networks typically use a combination of both static and dynamic routing
- Static routing has several primary uses
 - ✓ Providing ease of routing table maintenance in smaller networks that are not expected to grow significantly
 - ✓ Routing to and from a stub network
 - ❑ a network with only one default route out and no knowledge of any remote networks
 - ✓ Accessing a single default router
 - ❑ used to represent a path to any network that does not have a match in the routing table



Static Routing Scorecard

Static Routing Advantages and Disadvantages

Advantages	Disadvantages
Easy to implement in a small network.	Suitable only for simple topologies or for special purposes such as a default static route. Configuration complexity increases dramatically as network grows.
Very secure. No advertisements are sent as compared to dynamic routing protocols.	
Route to destination is always the same.	Manual intervention required to re-route traffic.
No routing algorithm or update mechanism required; therefore, extra resources (CPU or RAM) are not required.	



Dynamic Routing Scorecard

Dynamic Routing Advantages and Disadvantages

Advantages	Disadvantages
Suitable in all topologies where multiple routers are required.	Can be more complex to implement.
Generally independent of the network size.	Less secure. Additional configuration settings are required to secure.
Automatically adapts topology to reroute traffic if possible.	Route depends on the current topology.
	Requires additional CPU, RAM, and link bandwidth.



Dynamic Routing Protocol Operation

- ▶ In general, the operations of a dynamic routing protocol can be described as follows:
 - ❑ The router sends and receives routing messages on its interfaces.
 - ❑ The router shares routing messages and routing information with other routers that are using the same routing protocol.
 - ❑ Routers exchange routing information to learn about remote networks.
 - ❑ When a router detects a topology change the routing protocol can advertise this change to other routers.



Achieving Convergence

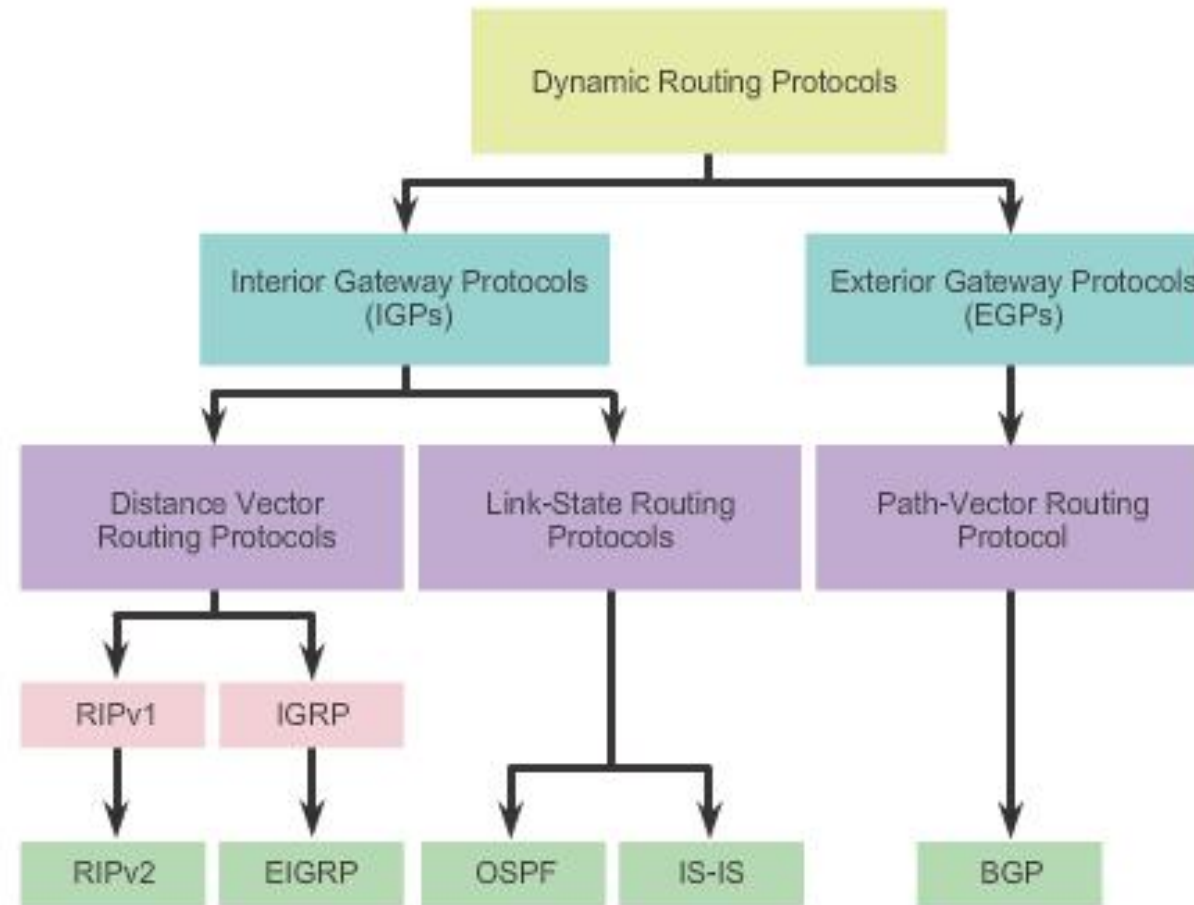
- Network converged when all routers have complete and accurate information about the entire network.
- Convergence time is the time it takes routers to share information, calculate best paths, and update their routing tables.
- A network is not completely operable until the network has converged.
- Convergence properties include the speed of propagation of routing information and the calculation of optimal paths. The speed of propagation refers to the amount of time it takes for routers within the network to forward routing information.
- Generally, older protocols, such as RIP, are slow to converge, whereas modern protocols, such as EIGRP and OSPF, converge more quickly.



Classifying Routing Protocols

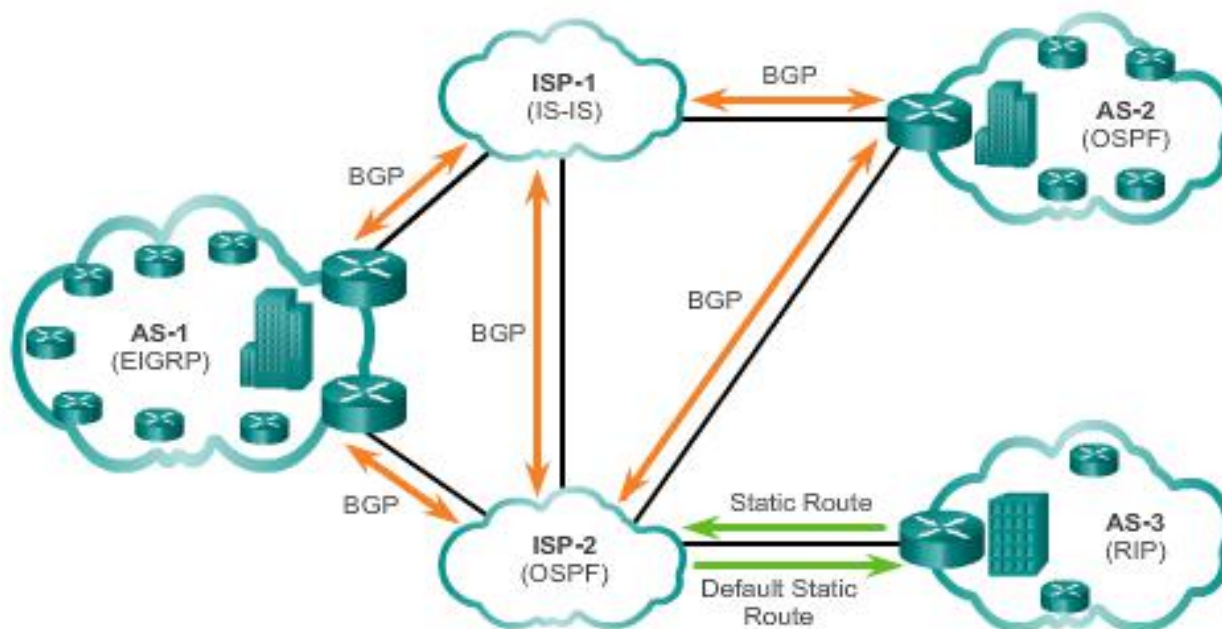
101

Routing Protocols Classification



IGP and EGP Routing Protocols

IGP versus EGP Routing Protocols



Interior Gateway Protocols (IGP) -

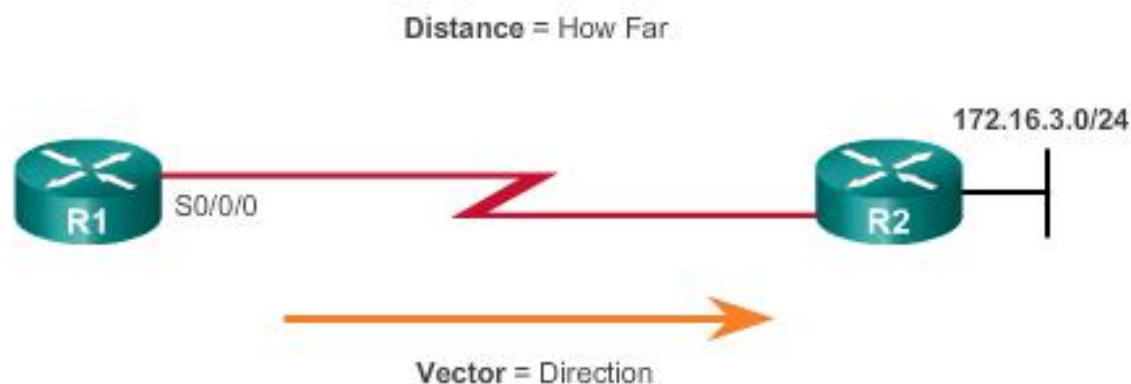
- Used for routing within an Autonomous System
- Include RIP, EIGRP, OSPF, and IS-IS

Exterior Gateway Protocols (EGP) -

- Used for routing between Autonomous System
- Official routing protocol used by the Internet

Distance Vector Routing Protocols

The Meaning of Distance Vector



For R1, 172.16.3.0/24 is one hop away (distance) it can be reached through R2 (vector)

Distance vector IPv4 IGPs:

- **RIPv1** - First generation legacy protocol
- **RIPv2** - Simple distance vector routing protocol
- **IGRP** - First generation Cisco proprietary protocol (obsolete)
- **EIGRP** - Advanced version of distance vector routing



Distance Vector or Link-State Routing Protocols

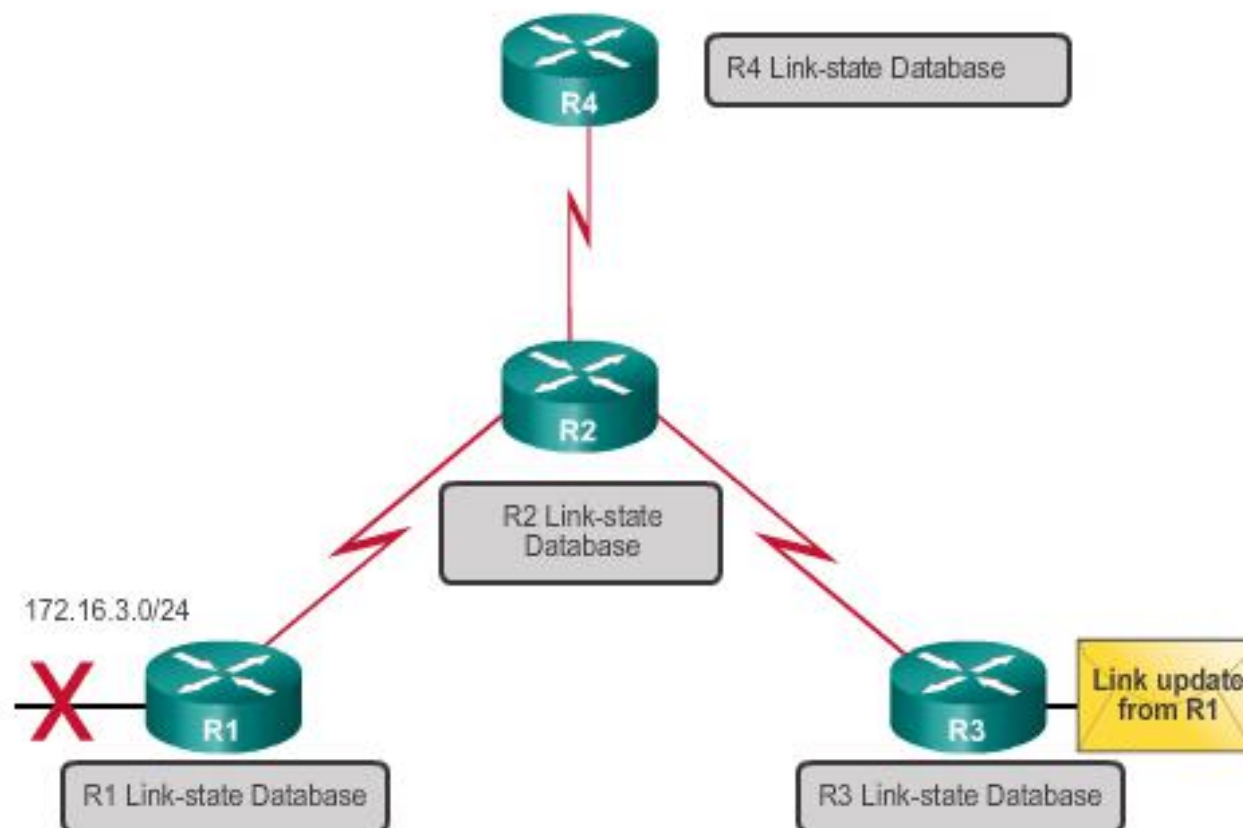
Distance vector protocols use routers as sign posts along the path to the final destination.

A link-state routing protocol is like having a complete map of the network topology. The sign posts along the way from source to destination are not necessary, because all link-state routers are using an identical map of the network. A link-state router uses the link-state information to create a topology map and to select the best path to all destination networks in the topology.



Link-State Routing Protocols

Link-State Protocol Operation



Link-state protocols forward updates when the state of a link changes.

Link-state IPv4 IGPs:

- **OSPF** - Popular standards based routing protocol
- **IS-IS** - Popular in provider networks.

Classful Routing Protocols

- Classful routing protocols do not send subnet mask information in their routing updates
 - Only RIPv1 and IGRP are classful
 - Created when network addresses were allocated based on classes (class A, B, or C)
 - Cannot provide variable length subnet masks (VLSMs) and classless interdomain routing (CIDR)
 - Create problems in discontinuous networks



Routing Protocol Characteristics

	Distance Vector				Link State	
	RIPv1	RIPv2	IGRP	EIGRP	OSPF	IS-IS
Speed Convergence	Slow	Slow	Slow	Fast	Fast	Fast
Scalability - Size of Network	Small	Small	Small	Large	Large	Large
Use of VLSM	No	Yes	No	Yes	Yes	Yes
Resource Usage	Low	Low	Low	Medium	High	High
Implementation and Maintenance	Simple	Simple	Simple	Complex	Complex	Complex



Routing Protocol Metrics

- A metric is a measurable value that is assigned by the routing protocol to different routes based on the usefulness of that route
 - Used to determine the overall “cost” of a path from source to destination
 - Routing protocols determine the best path based on the route with the lowest cost



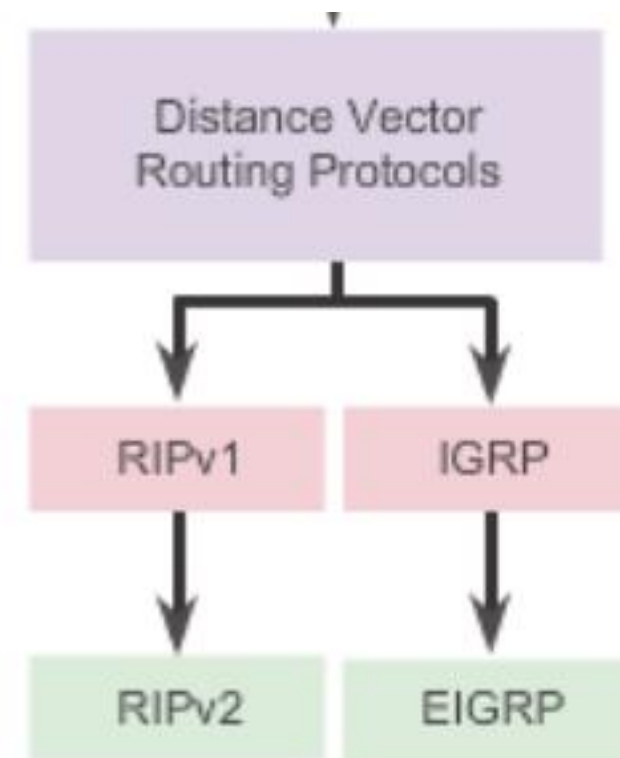
Distance Vector Dynamic Routing



Distance Vector Technologies

Distance vector routing protocols

- Share updates between neighbors
- Not aware of the network topology
- Some send periodic updates to broadcast IP 255.255.255.255 even if topology has not changed
- Updates consume bandwidth and network device CPU resources
- RIPv2 and EIGRP use multicast addresses
- EIGRP will only send an update when topology has changed



Distance Vector Algorithm

Purpose of Routing Algorithms

- Sending and receiving updates
- Calculate best path and install route
- Detect and react to topology changes



- RIP uses the Bellman-Ford algorithm as its routing algorithm
- IGRP and EIGRP use the Diffusing Update Algorithm (DUAL) routing algorithm developed by Cisco

Routing Information Protocol

112

RIPv1 versus RIPv2

Routing updates
broadcasted every 30
seconds

Characteristics and Features	RIPv1	RIPv2
Metric	Both use hop count as a simple metric. The maximum number of hops is 15.	
Updates Forwarded to Address	255.255.255.255	224.0.0.9
Supports VLSM	✗	✓
Supports CIDR	✗	✓
Supports Summarization	✗	✓
Supports Authentication	✗	✓

Updates use
UDP port 520

RIPng is based on RIPv2 with a 15 hop limitation and the administrative distance of 120



Enhanced Interior-Gateway Routing Protocol

IGRP versus EIGRP

Characteristics and Features	IGRP	EIGRP
Metric	Both use a composite metric consisting of bandwidth and delay. Reliability and load can also be included in the metric calculation.	
Updates Forwarded to Address	255.255.255.255	224.0.0.10
Supports VLSM	✗	✓
Supports CIDR	✗	✓
Supports Summarization	✗	✓
Supports Authentication	✗	✓

EIGRP

- Bounded triggered updates
- Hello keepalives mechanism
- Maintains a topology table
- Rapid convergence
- Multiple network layer protocol support

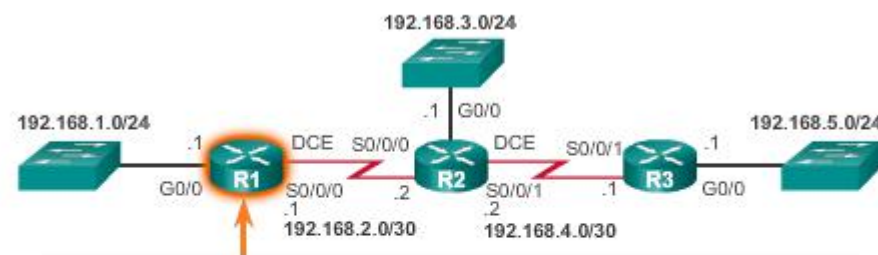


Configuring the RIP Protocol

Router RIP Configuration Mode - Advertising Networks

```
R1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# router rip
R1(config-router)#
```

Advertising the R1 Networks



```
R1(config)#router rip
R1(config-router)#network 192.168.1.0
R1(config-router)#network 192.168.2.0
R1(config-router)#
```

Examining Default RIP Settings

Verifying RIP Settings on R1

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "rip"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Sending updates every 30 seconds, next due in 16 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Redistributing: rip

  Default version control: send version 1, receive any version
  Interface                Send Recv Triggered RIP Key-chain
  GigabitEthernet0/0       1      1 2
  Serial0/0/0              1      1 2

Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  192.168.1.0
  192.168.2.0

Routing Information Sources:
  Gateway         Distance      Last Update
  192.168.2.2      120          00:00:15
Distance: (default is 120)

R1#
```

Verifying RIP Routes on R1

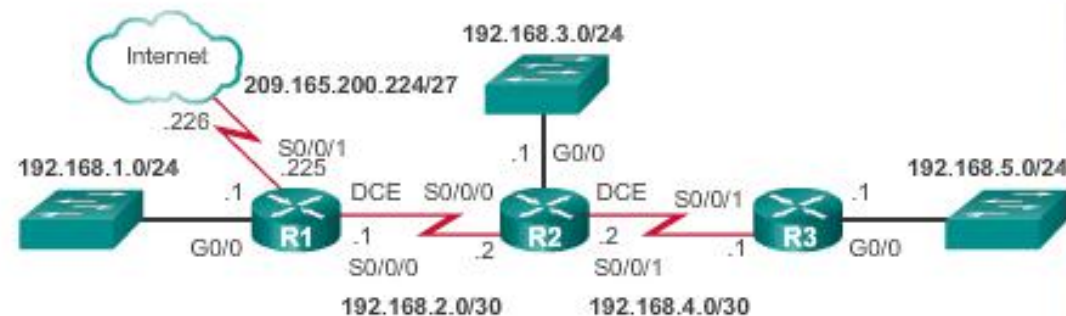
```
R1# show ip route | begin Gateway
Gateway of last resort is not set

    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
    192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, Serial0/0/0
L       192.168.2.1/32 is directly connected, Serial0/0/0
R       192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:24, Serial0/0/0
R       192.168.4.0/24 [120/1] via 192.168.2.2, 00:00:24, Serial0/0/0
R       192.168.5.0/24 [120/2] via 192.168.2.2, 00:00:24, Serial0/0/0
R1#
```



Propagating a Default Route

Propagating a Default Route on R1



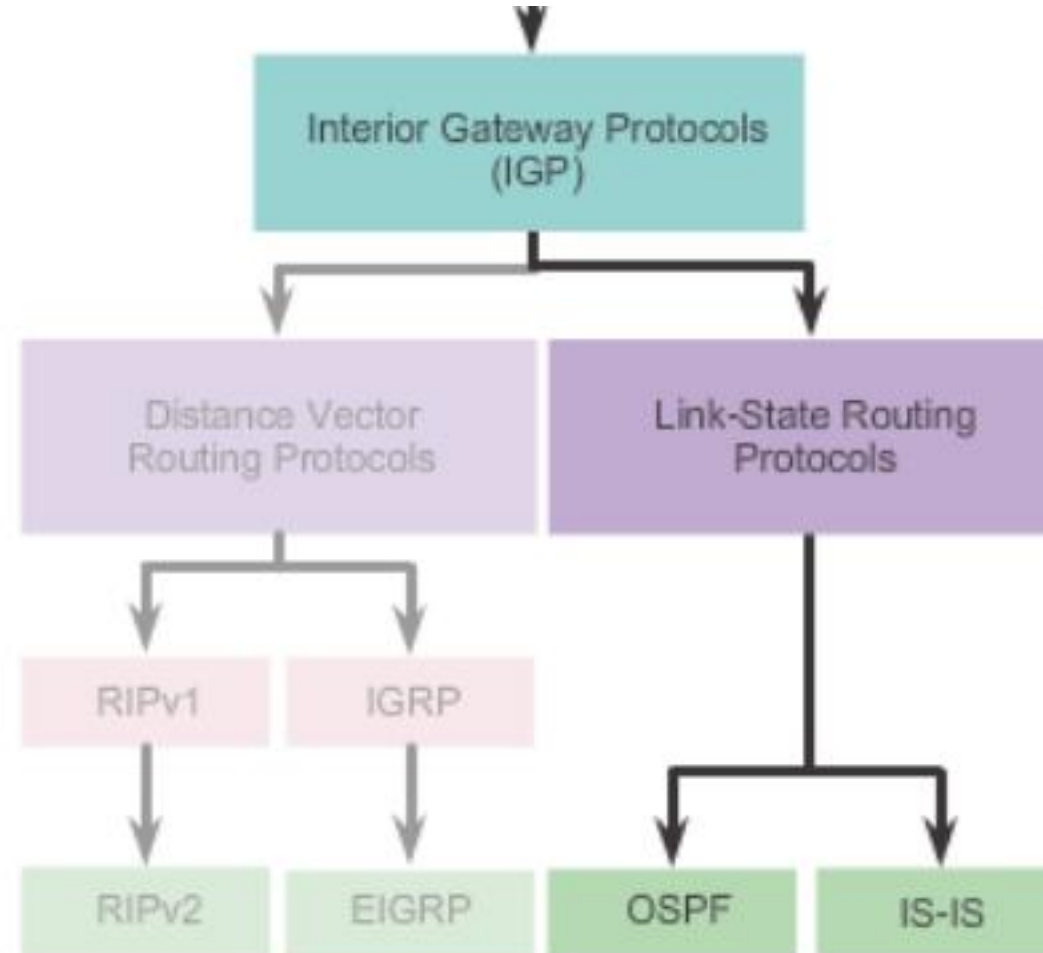
```
R1(config)# ip route 0.0.0.0 0.0.0.0 S0/0/1 209.165.200.226
R1(config)# router rip
R1(config-router)# default-information originate
R1(config-router)# ^Z
R1#
*Mar 10 23:33:51.801: %SYS-5-CONFIG_I: Configured from console by console
R1# show ip route | begin Gateway
Gateway of last resort is 209.165.200.226 to network 0.0.0.0

S* 0.0.0.0/0 [1/0] via 209.165.200.226, Serial0/0/1
    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.1.0/24 is directly connected, GigabitEthernet0/0
L    192.168.1.1/32 is directly connected, GigabitEthernet0/0
    192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.2.0/24 is directly connected, Serial0/0/0
L    192.168.2.1/32 is directly connected, Serial0/0/0
R    192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:08,
```

Link-State Dynamic Routing



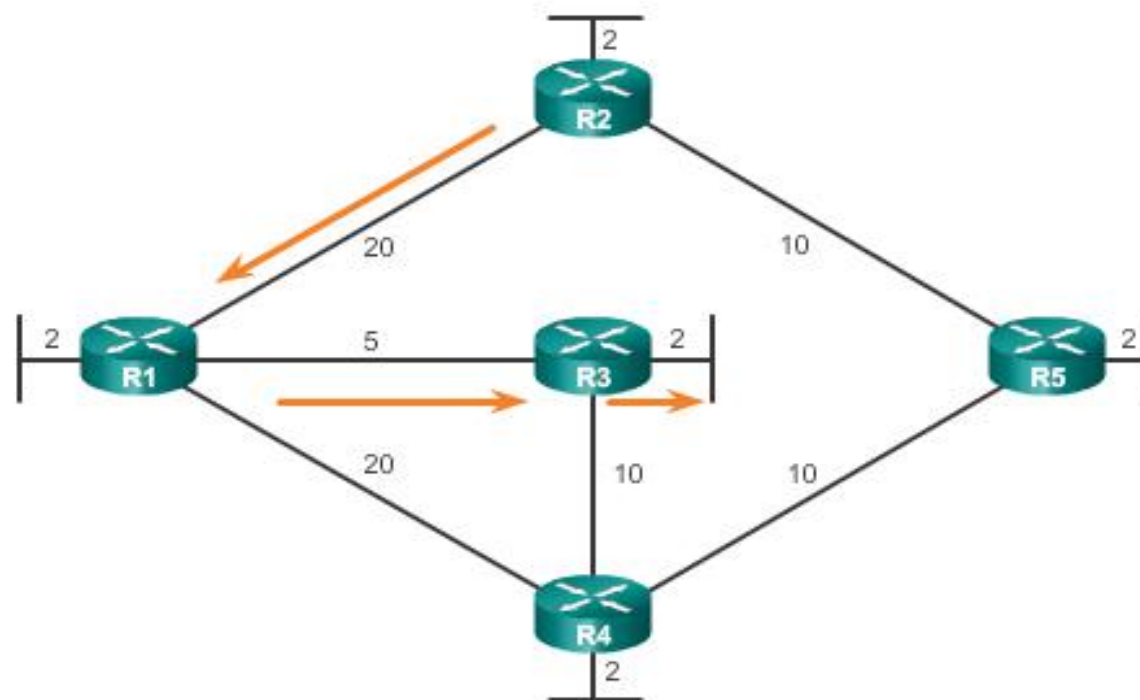
Shortest Path First Protocols



Dijkstra's Algorithm

Dijkstra's Shortest Path First Algorithm

Shortest Path for host on R2 LAN to reach host on R3 LAN:
 $R2 \text{ to } R1 (20) + R1 \text{ to } R3 (5) + R3 \text{ to LAN } (2) = 27$



Link-State Routing Process

Link-State Routing Process

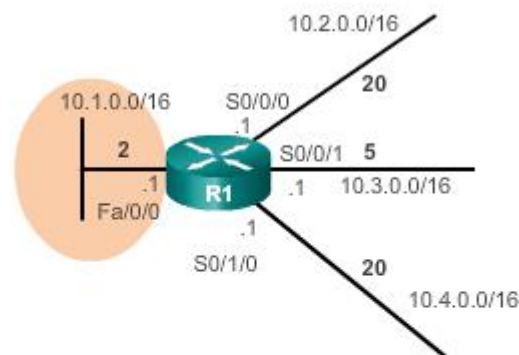
- Each router learns about each of its own directly connected networks.
- Each router is responsible for "saying hello" to its neighbors on directly connected networks.
- Each router builds a Link State Packet (LSP) containing the state of each directly connected link.
- Each router floods the LSP to all neighbors who then store all LSP's received in a database.
- Each router uses the database to construct a complete map of the topology and computers the best path to each destination networks.



Link and Link-State

The first step in the link-state routing process is that each router learns about its own links, its own directly connected networks.

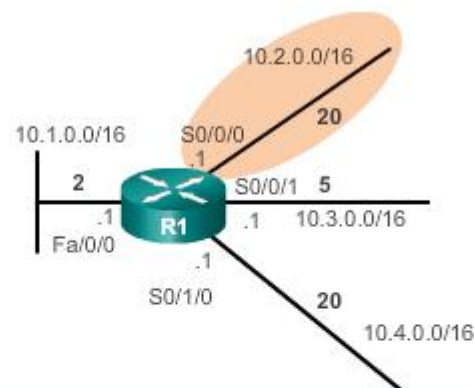
Link-State of Interface Fa0/0



Link 1

- Network: **10.1.0.0/16**
- IP address: **10.1.0.1**
- Type of network: **Ethernet**
- Cost of that link: **2**
- Neighbors: **None**

Link-State of Interface S0/0/0

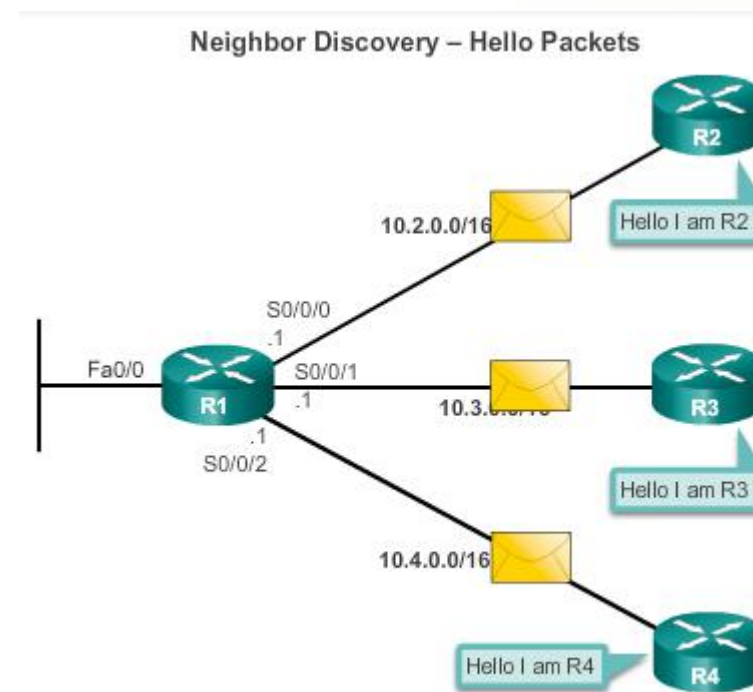
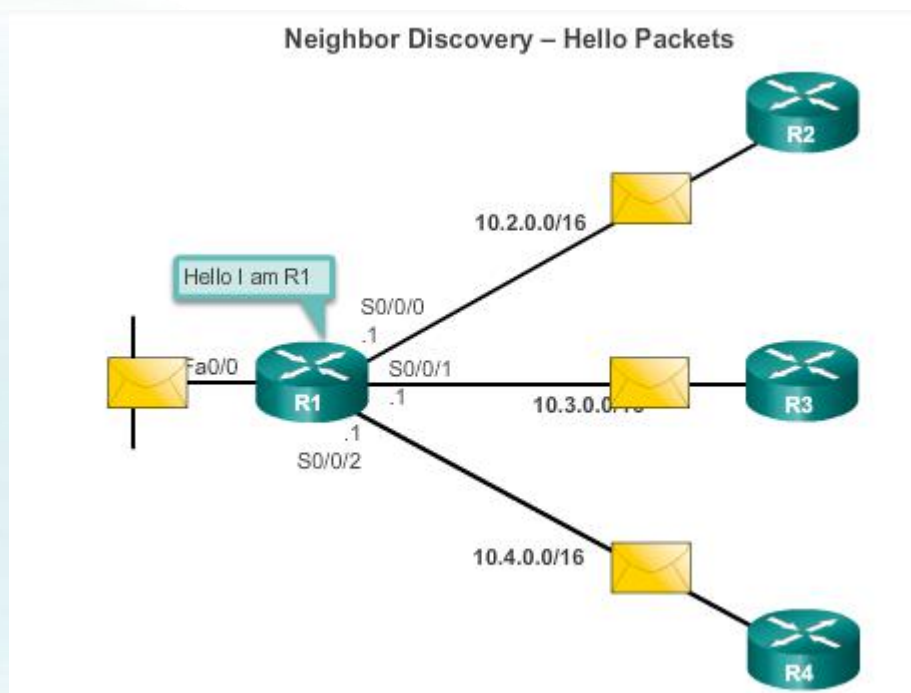


Link 2

- Network: **10.2.0.0/16**
- IP address: **10.2.0.1**
- Type of network: **Serial**
- Cost of that link: **20**
- Neighbors: **R2**

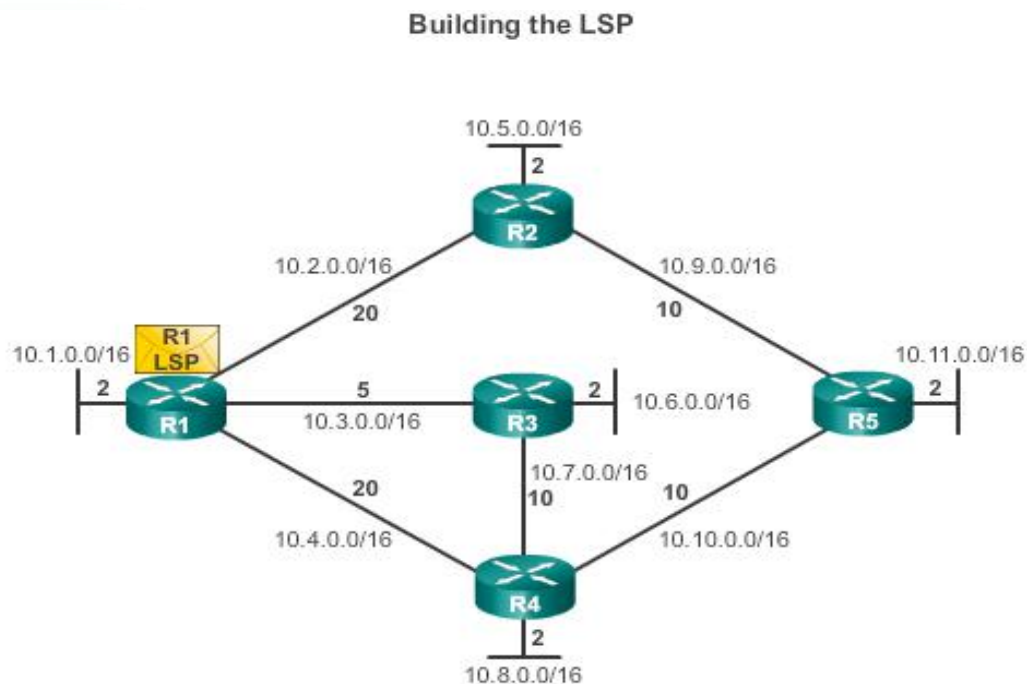
Link-State Updates - Say Hello

The second step in the link-state routing process is that each router is responsible for meeting its neighbors on directly connected networks.



Say Hello

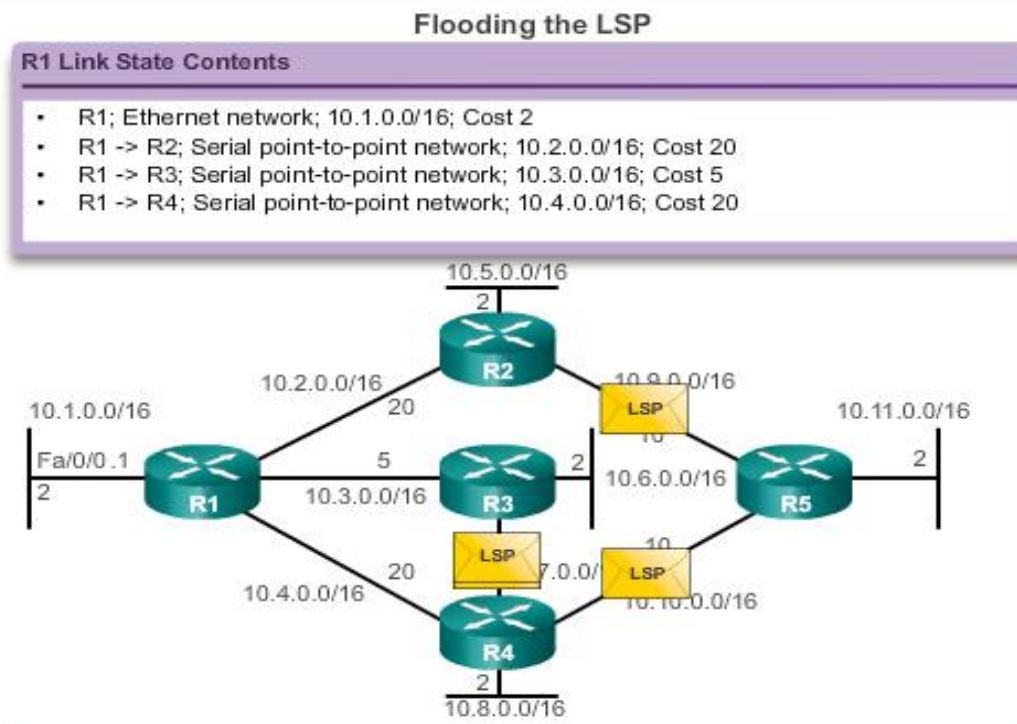
The third step in the link-state routing process is that each router builds a link-state packet (LSP) containing the state of each directly connected link.



1. R1; Ethernet network
10.1.0.0/16; Cost 2
2. R1 -> R2; Serial point-to-point
network; 10.2.0.0/16; Cost 20
3. R1 -> R3; Serial point-to-point
network; 10.3.0.0/16; Cost 5
4. R1 -> R4; Serial point-to-point
network; 10.4.0.0/16; Cost 20

Flooding the LSP

The fourth step in the link-state routing process is that each router floods the LSP to all neighbors, who then store all LSPs received in a database.



Link-State Updates - Building the Link-State Database

The final step in the link-state routing process is that each router uses the database to construct a complete map of the topology and computes the best path to each destination network.

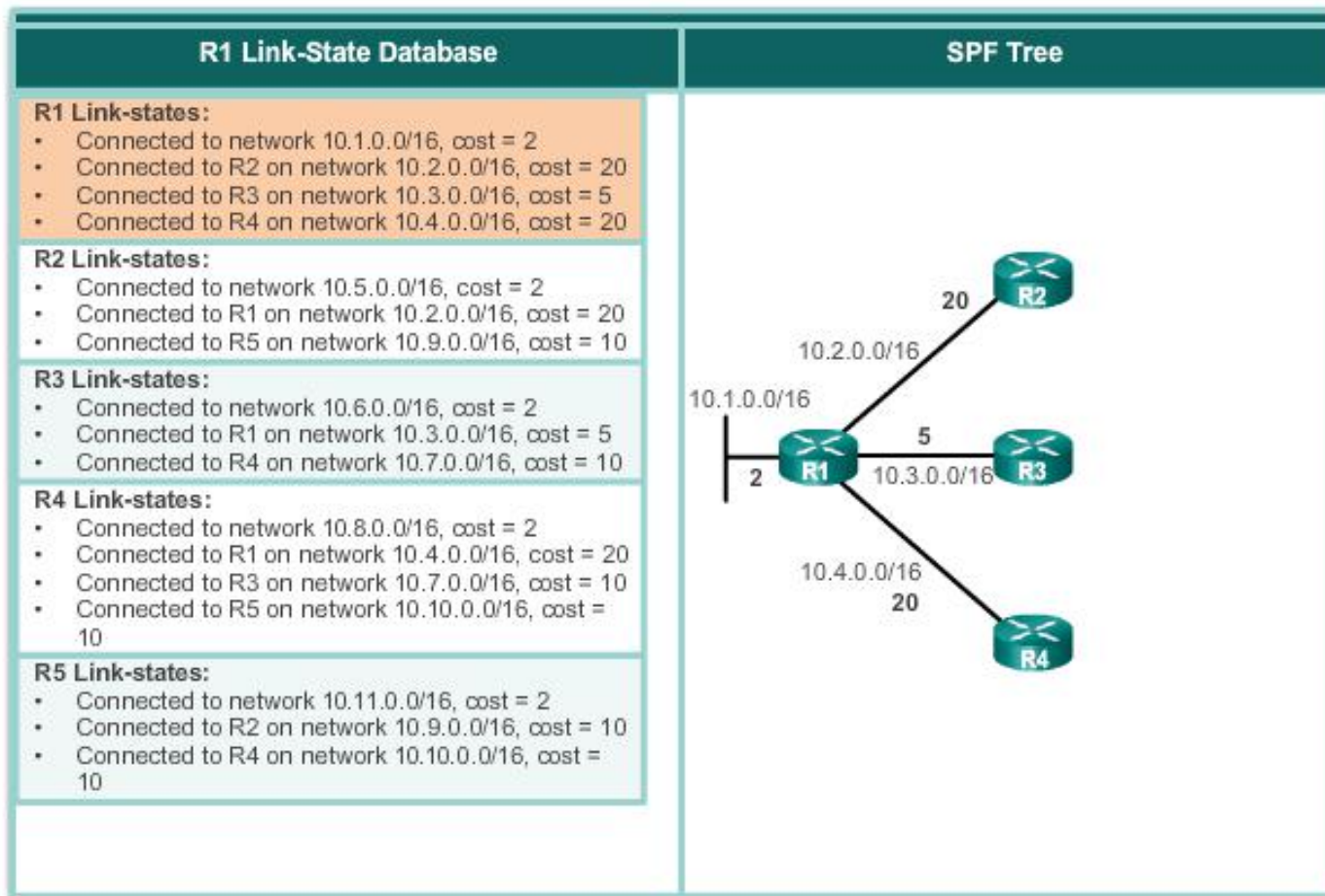
Contents of the Link-State Database

R1 Link-State Database
R1 Link-states: <ul style="list-style-type: none"> • Connected to network 10.1.0.0/16, cost = 2 • Connected to R2 on network 10.2.0.0/16, cost = 20 • Connected to R3 on network 10.3.0.0/16, cost = 5 • Connected to R4 on network 10.4.0.0/16, cost = 20
R2 Link-states: <ul style="list-style-type: none"> • Connected to network 10.5.0.0/16, cost = 2 • Connected to R1 on network 10.2.0.0/16, cost = 20 • Connected to R5 on network 10.9.0.0/16, cost = 10
R3 Link-states: <ul style="list-style-type: none"> • Connected to network 10.6.0.0/16, cost = 2 • Connected to R1 on network 10.3.0.0/16, cost = 5 • Connected to R4 on network 10.7.0.0/16, cost = 10
R4 Link-states: <ul style="list-style-type: none"> • Connected to network 10.8.0.0/16, cost = 2 • Connected to R1 on network 10.4.0.0/16, cost = 20 • Connected to R3 on network 10.7.0.0/16, cost = 10 • Connected to R5 on network 10.10.0.0/16, cost = 10
R5 Link-states: <ul style="list-style-type: none"> • Connected to network 10.11.0.0/16, cost = 2 • Connected to R2 on network 10.9.0.0/16, cost = 10 • Connected to R4 on network 10.10.0.0/16, cost = 10



Building the SPF Tree

Identify the Directly Connected Networks

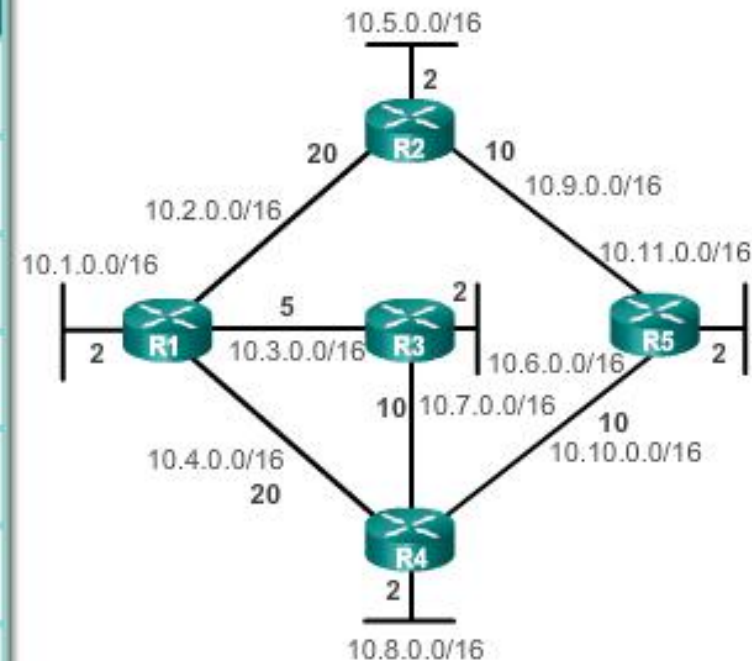


Building the SPF Tree

127

Resulting SPF Tree of R1

Destination	Shortest Path	Cost
10.5.0.0/16	R1 → R2	22
10.6.0.0/16	R1 → R3	7
10.7.0.0/16	R1 → R3	15
10.8.0.0/16	R1 → R3 → R4	17
10.9.0.0/16	R1 → R2	30
10.10.0.0/16	R1 → R3 → R4	25
10.11.0.0/16	R1 → R3 → R4 → R5	27



Adding OSPF Routes to the Routing Table

128

Populate the Routing Table

Destination	Shortest Path	Cost
10.5.0.0/16	R1 → R2	22
10.6.0.0/16	R1 → R3	7
10.7.0.0/16	R1 → R3	15
10.8.0.0/16	R1 → R3 → R4	17
10.9.0.0/16	R1 → R2	30
10.10.0.0/16	R1 → R3 → R4	25
10.11.0.0/16	R1 → R3 → R4 → R5	27

R1 Routing Table

Directly Connected Networks

- 10.1.0.0/16 Directly Connected Network
- 10.2.0.0/16 Directly Connected Network
- 10.3.0.0/16 Directly Connected Network
- 10.4.0.0/16 Directly Connected Network

Remote Networks

- 10.5.0.0/16 via R2 serial 0/0/0, cost=22
- 10.6.0.0/16 via R3 serial 0/0/1, cost=7
- 10.7.0.0/16 via R3 serial 0/0/1, cost=15
- 10.8.0.0/16 via R3 serial 0/0/1, cost=17
- 10.9.0.0/16 via R2 serial 0/0/0, cost=30
- 10.10.0.0/16 via R3 serial 0/0/1, cost=25
- 10.11.0.0/16 via R3 serial 0/0/1, cost=27



Why Use Link-State Protocols?

Advantages of Link-State Routing Protocols

- Each router builds its own topological map of the network to determine the shortest path.
- Immediate flooding of LSPs achieves faster convergence.
- LSPs are sent only when there is a change in the topology and contain only the information regarding that change.
- Hierarchical design used when implementing multiple areas.

Disadvantages compared to distance vector routing protocols:

- Memory Requirements
- Processing Requirements
- Bandwidth Requirements



Protocols that Use Link-State

Only two link-state routing protocols:

- Open Shortest Path First (OSPF) most popular
 - began in 1987
 - two current versions
 - OSPFv2 - OSPF for IPv4 networks
 - OSPFv3 - OSPF for IPv6 networks
- IS-IS was designed by International Organization for Standardization (ISO)



- ▶ The details of each routing protocol is not covered in this course.



Chapter Three

WAN Technologies



Connecting to the WAN



Wollo University-Kombolcha Institute of Technology
College of Informatics
Systems and Network Administration ©2017

Learning Objectives

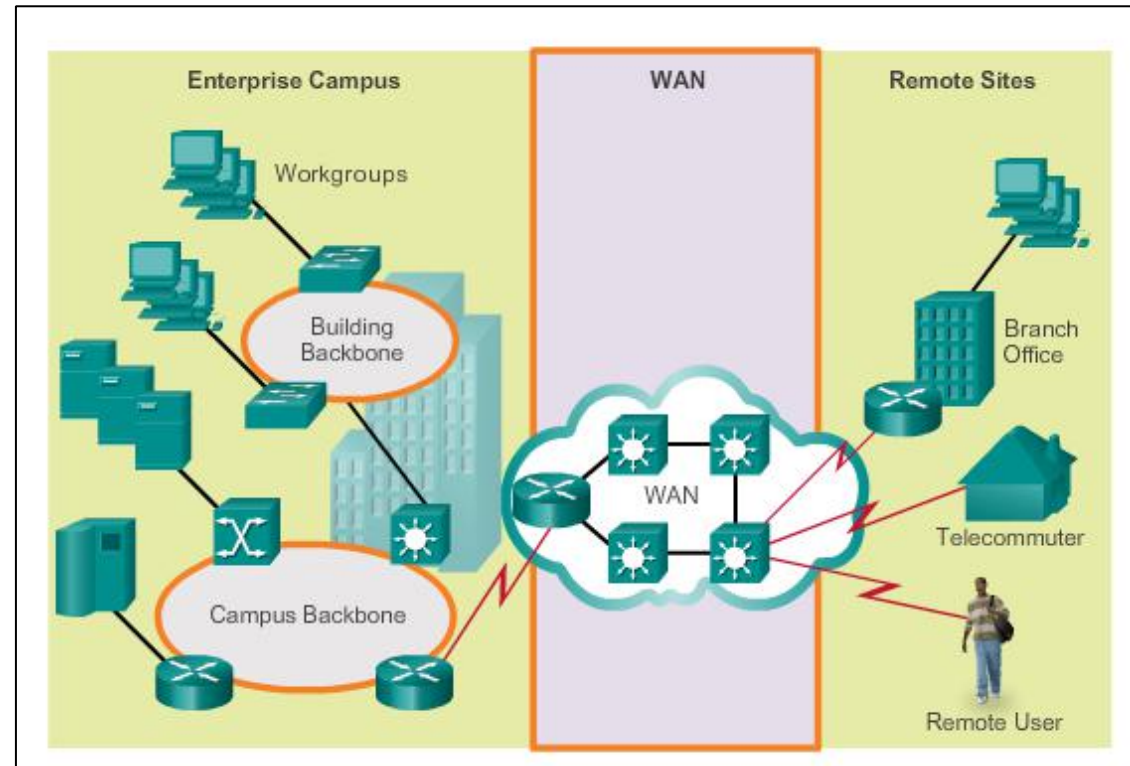
- ▶ Describe the purpose of a WAN.
- ▶ Describe WAN operations.
- ▶ Describe WAN services available.
- ▶ Compare various private WAN technologies.
- ▶ Compare various public WAN technologies.
- ▶ Select the appropriate WAN protocol and service for a specific network requirement.



Purpose of WANs

Why Choose a WAN?

- ▶ Operates beyond the geographic scope of a LAN
- ▶ Used to interconnect the enterprise LAN to remote LANs in branch sites and telecommuter sites
- ▶ Owned by a service provider
- ▶ Organization must pay a fee to use the provider's services to connect sites



Are WANs Necessary?

Businesses require communication among geographically separated sites. Examples include:

- ▶ Regional or branch offices must be able to communicate and share data.
- ▶ Organizations must share information with other customer organizations.
- ▶ Mobile workers must access information that resides on corporate networks.

Home computer users must send and receive data across increasingly larger distances. Examples include:

- ▶ Consumers communicate over the Internet with banks, stores, and a variety of providers of goods and services.
- ▶ Students do research by accessing library indexes and publications located in other parts of the country and in other parts of the world.



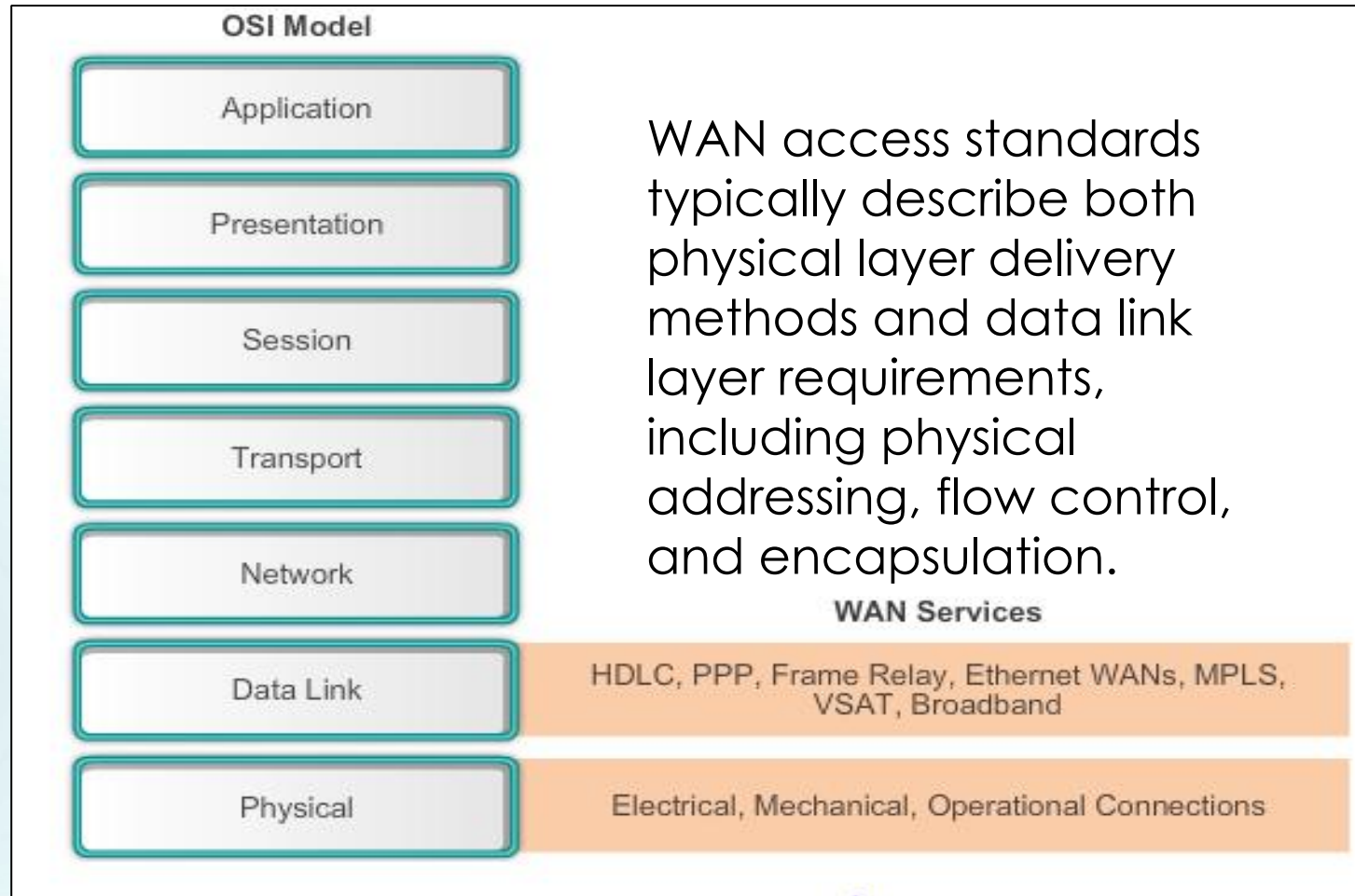
Evolving Networks

- Companies expect their networks to perform optimally and to be able to deliver an ever increasing array of services and applications to support productivity and profitability.

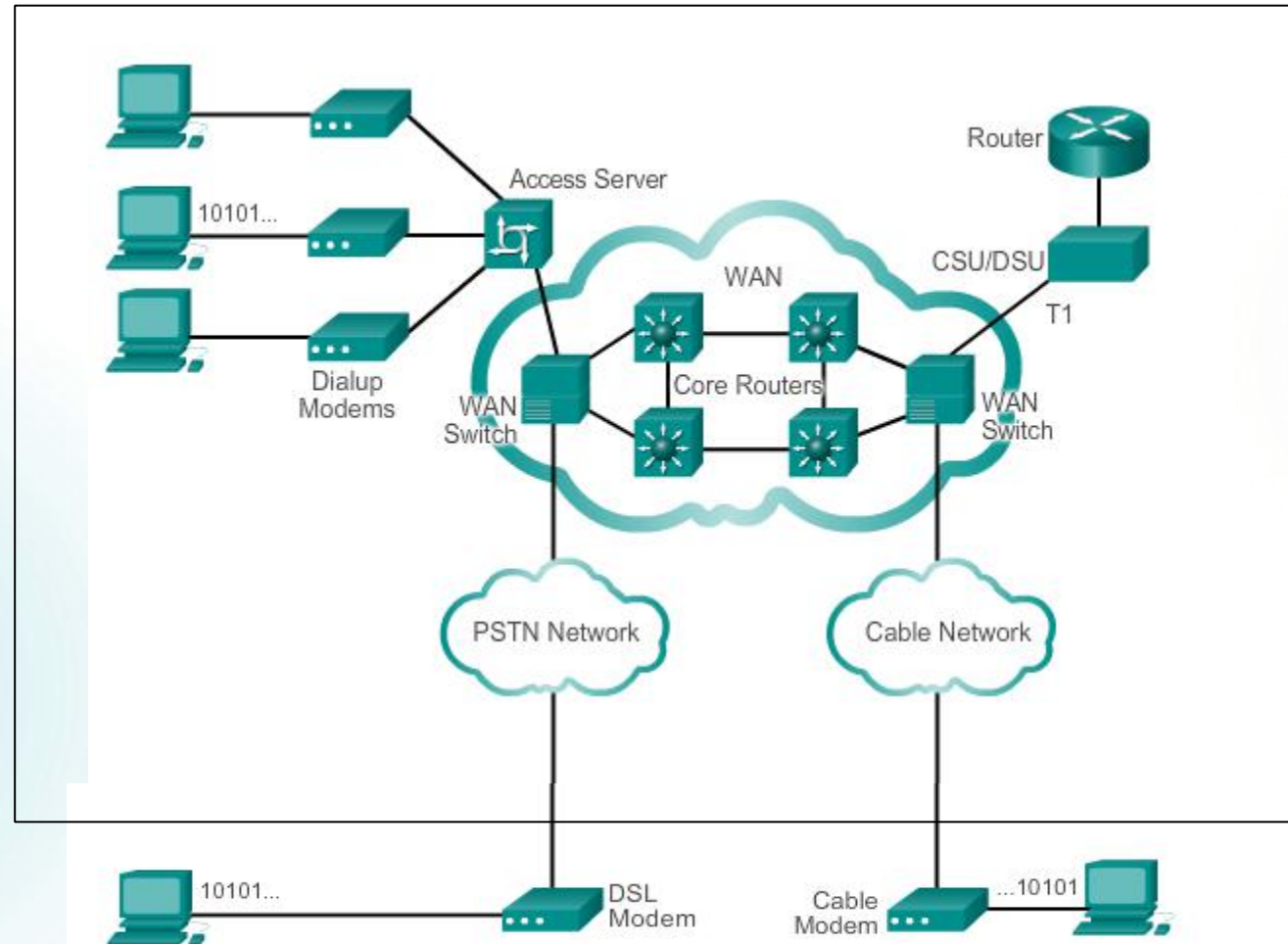


WAN Operations

WANs in the OSI Model

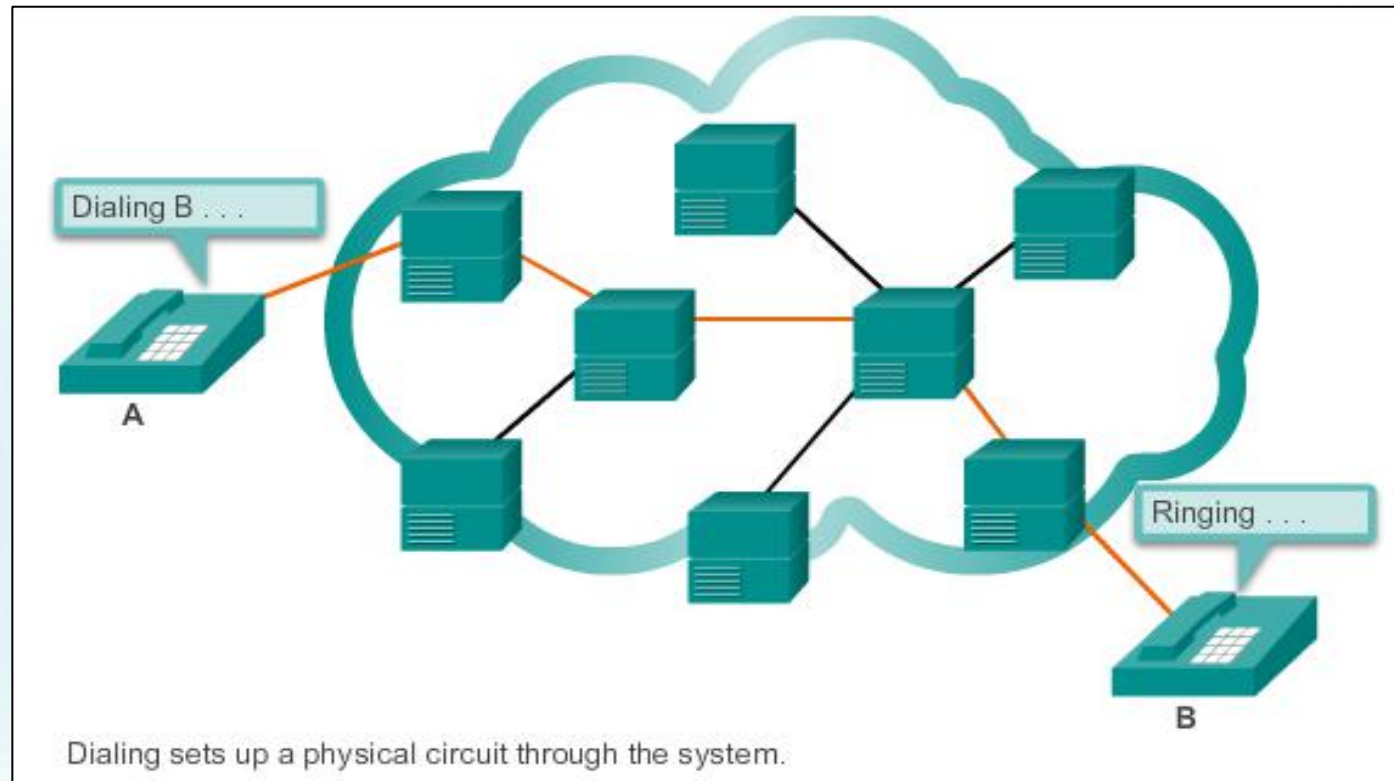


WAN Devices



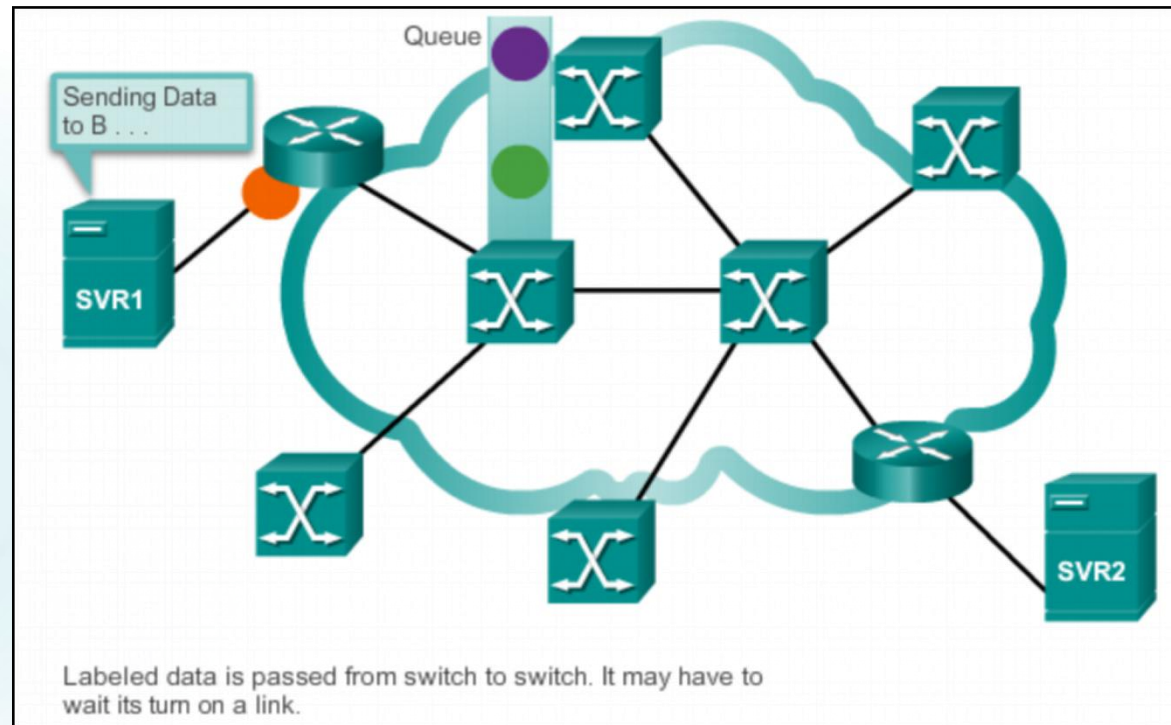
Circuit Switching

The two most common types of circuit-switched WAN technologies are the public switched telephone network (PSTN) and the Integrated Services Digital Network (ISDN).



Packet Switching

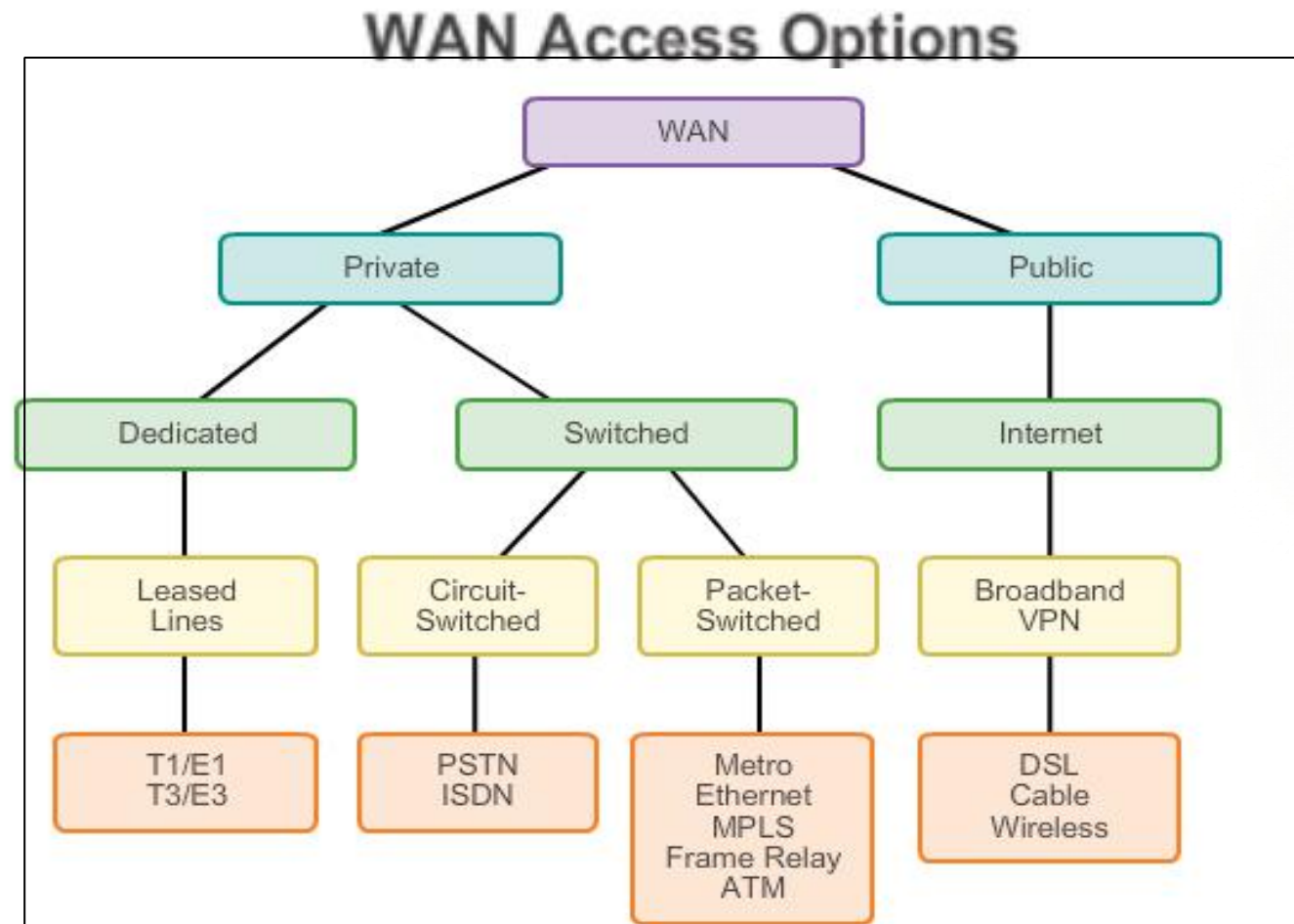
Splits traffic data into packets that are routed over a shared network. Packet-switching allow many pairs of nodes to communicate over the same channel.



Selecting a WAN Technology

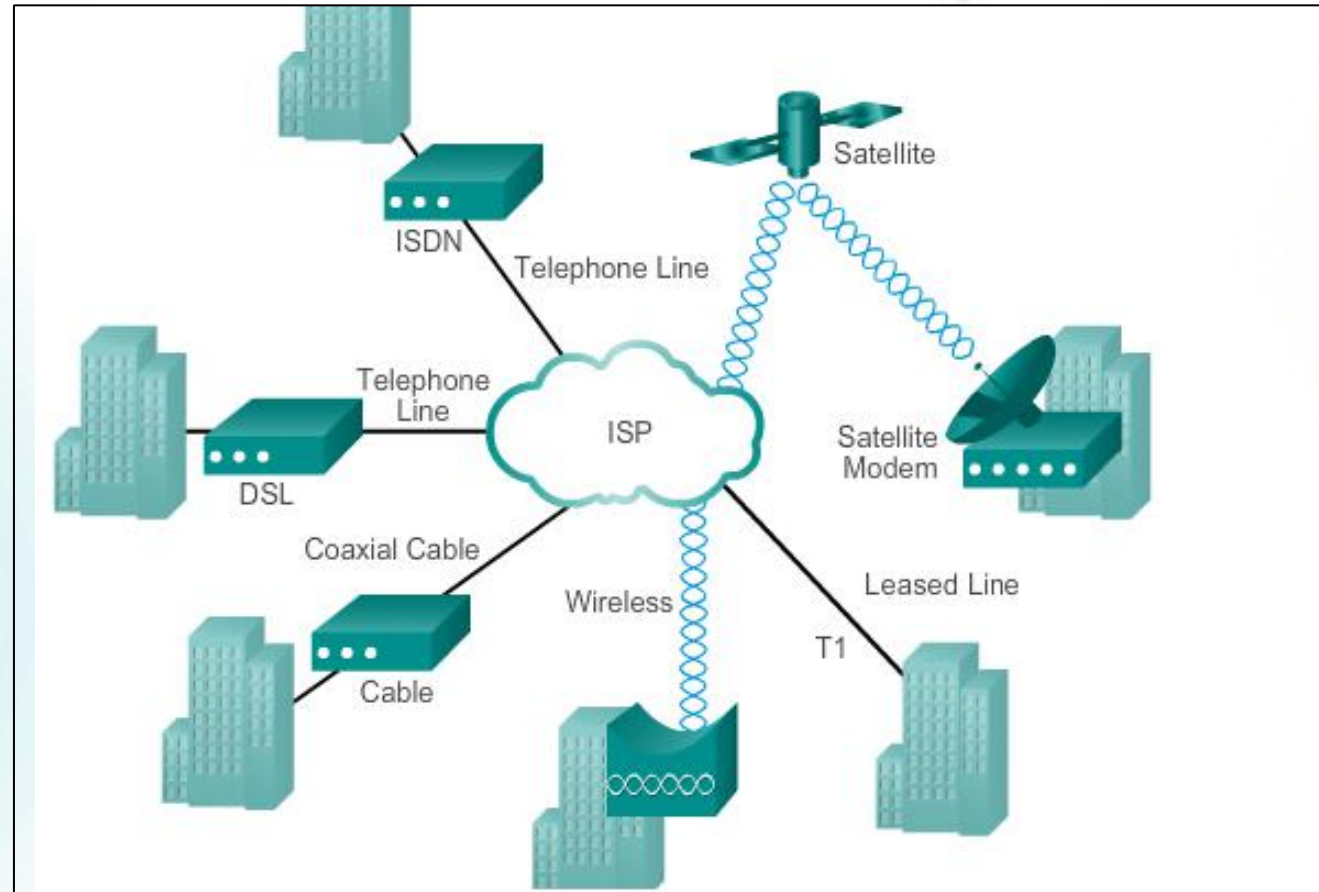


WAN Link Connection Options



Service-Provided Network Infrastructure

WAN Access Technologies



Private WAN Infrastructures

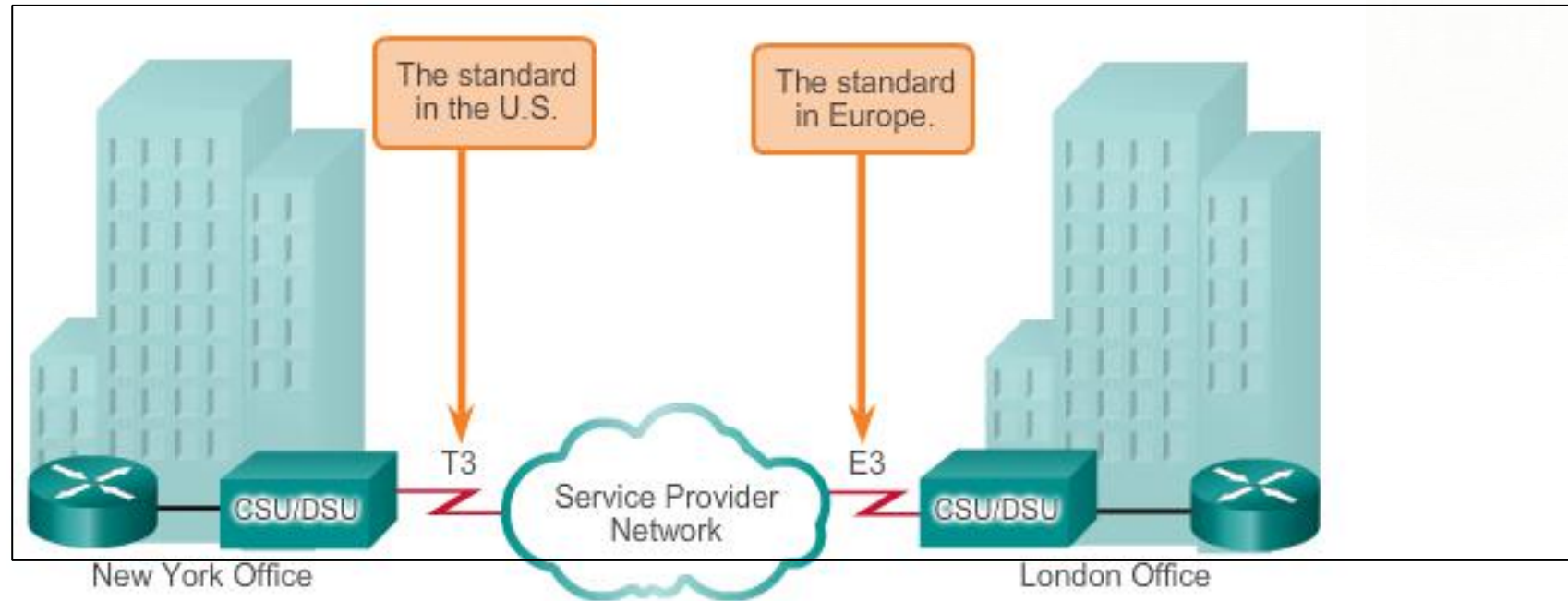
Leased Lines

Advantages:

- Simplicity
- Quality
- Availability

Disadvantages:

- Cost
- Limited flexibility



Private WAN Infrastructures

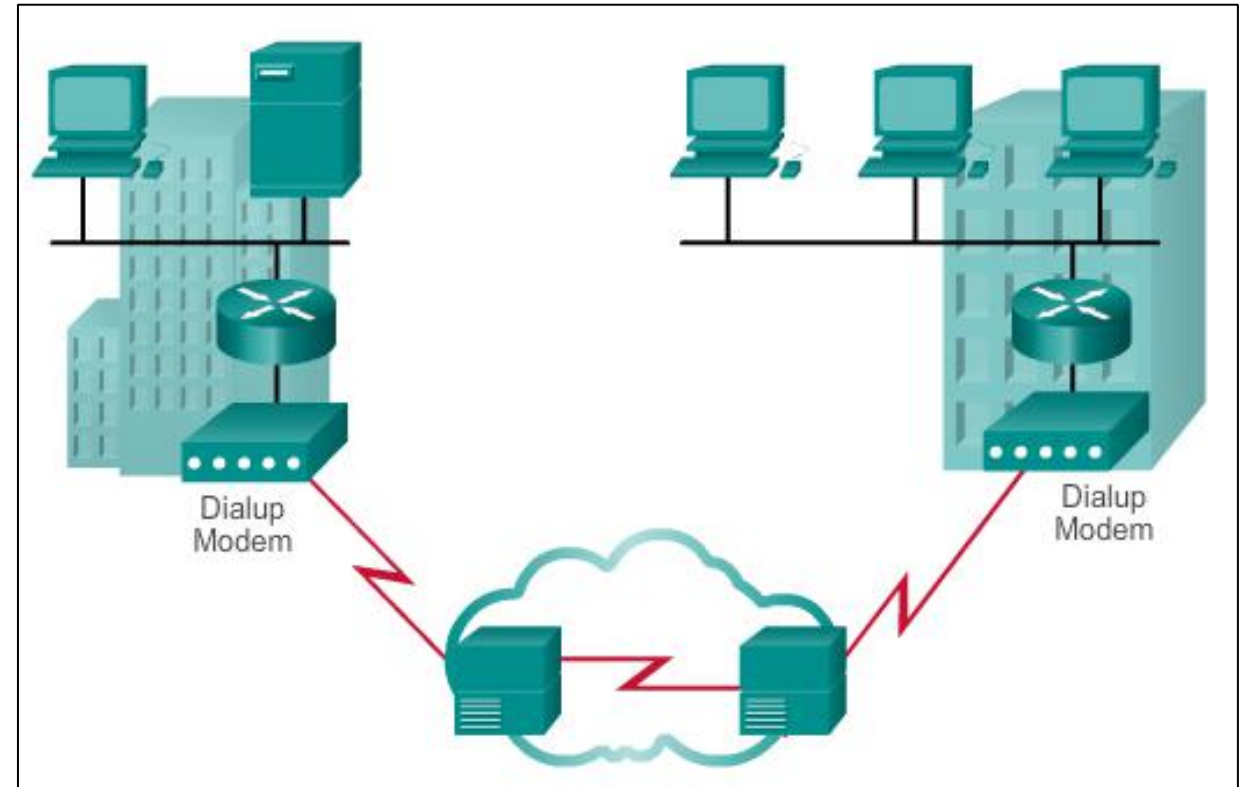
Dialup

Advantages:

- Simplicity
- Availability
- Low implementation cost

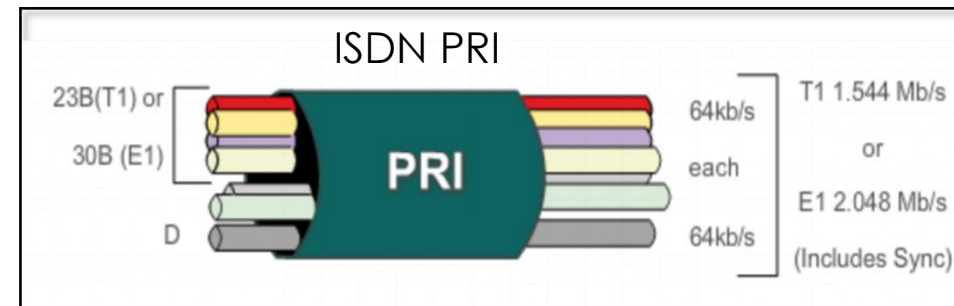
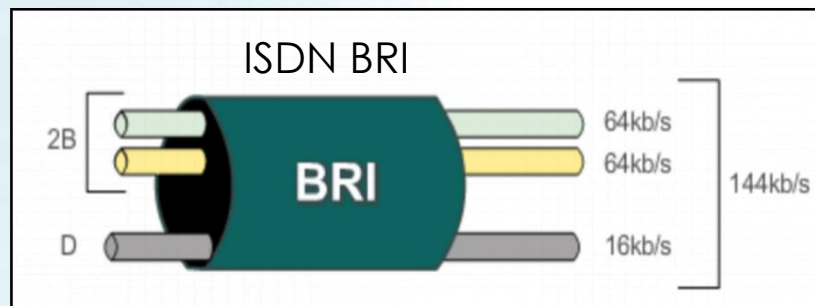
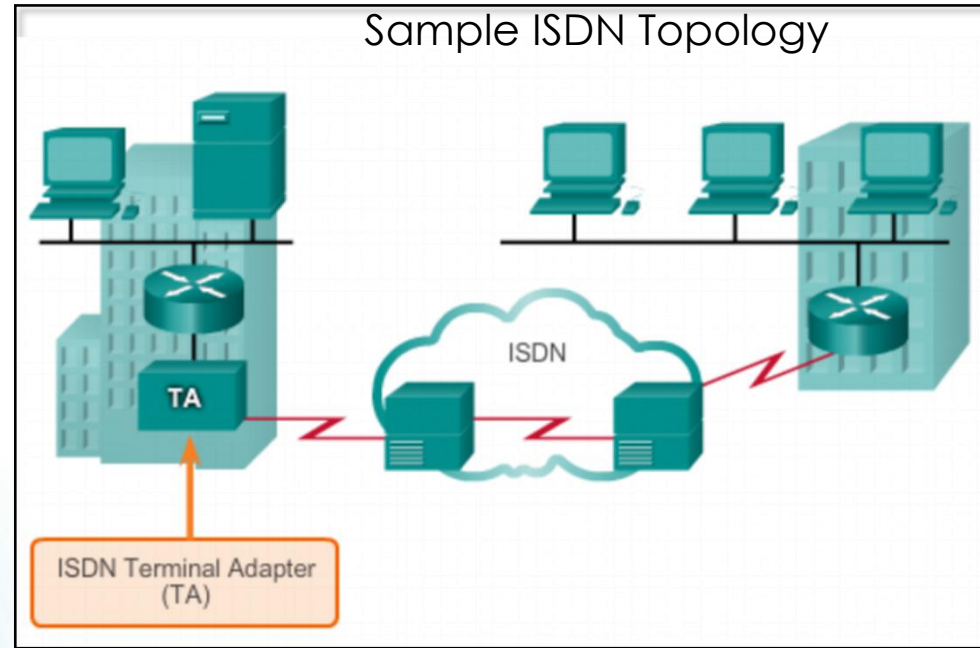
Disadvantages:

- Low data rates
- Relatively long connection time



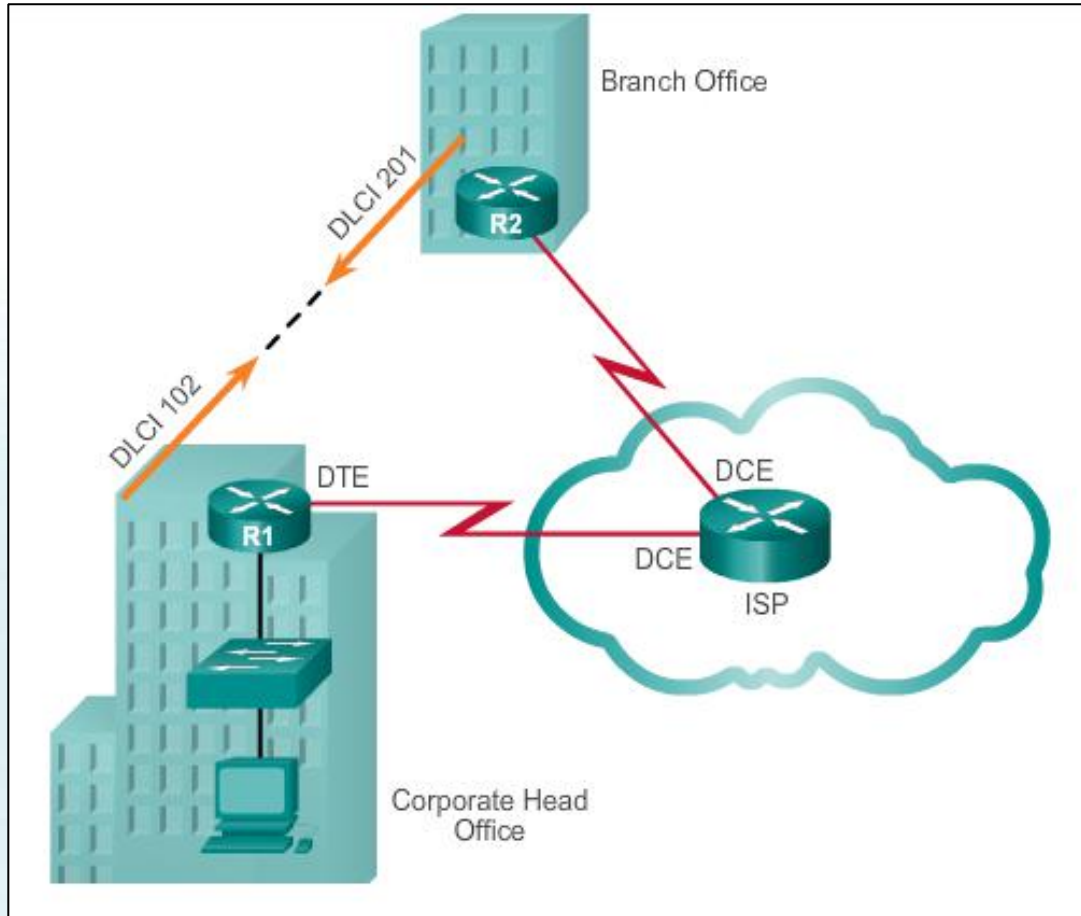
Private WAN Infrastructures

ISDN



Private WAN Infrastructures

Frame Relay

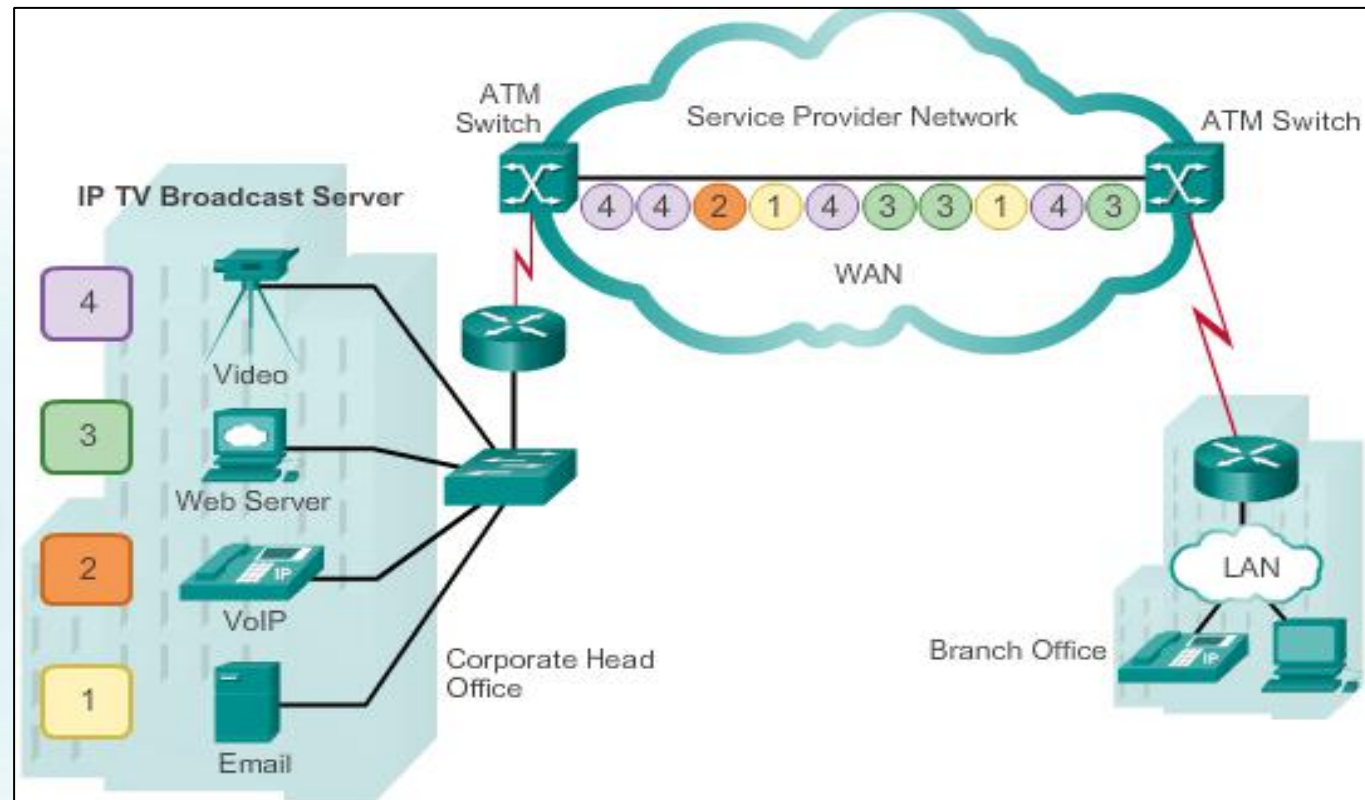


- PVCs carry both voice and data traffic.
- PVCs are uniquely identified by a data-link connection identifier (DLCI).
- PVCs and DLCIs ensure bidirectional communication from one DTE device to another.
- R1 uses DLCI 102 to reach R2 while R2 uses DLCI 201 to reach R1.

Private WAN Infrastructures

ATM

Built on a cell-based architecture, rather than on a frame-based architecture. ATM cells are always a fixed length of 53 bytes.

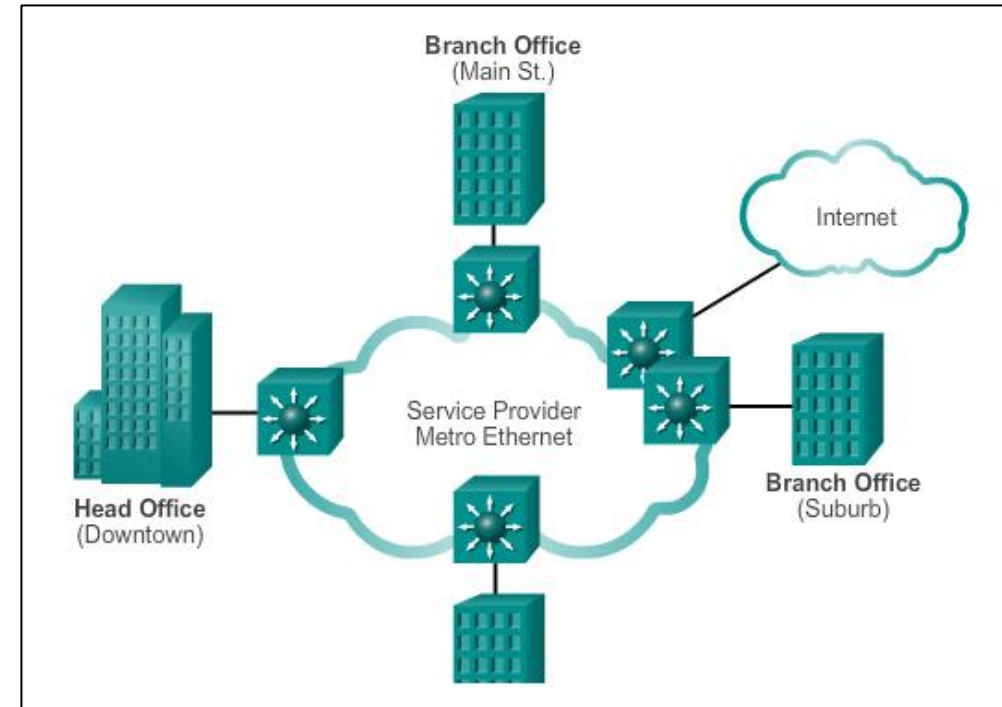


Private WAN Infrastructures

Ethernet WAN

Features and Benefits of Ethernet WAN include:

- Reduced expenses and administration
- Easy integration with existing networks
- Enhanced business productivity
- Service providers now offer Ethernet WAN service using fiber-optic cabling.
- Known as Metropolitan Ethernet (MetroE), Ethernet over MPLS (EoMPLS), and Virtual Private LAN Service (VPLS).



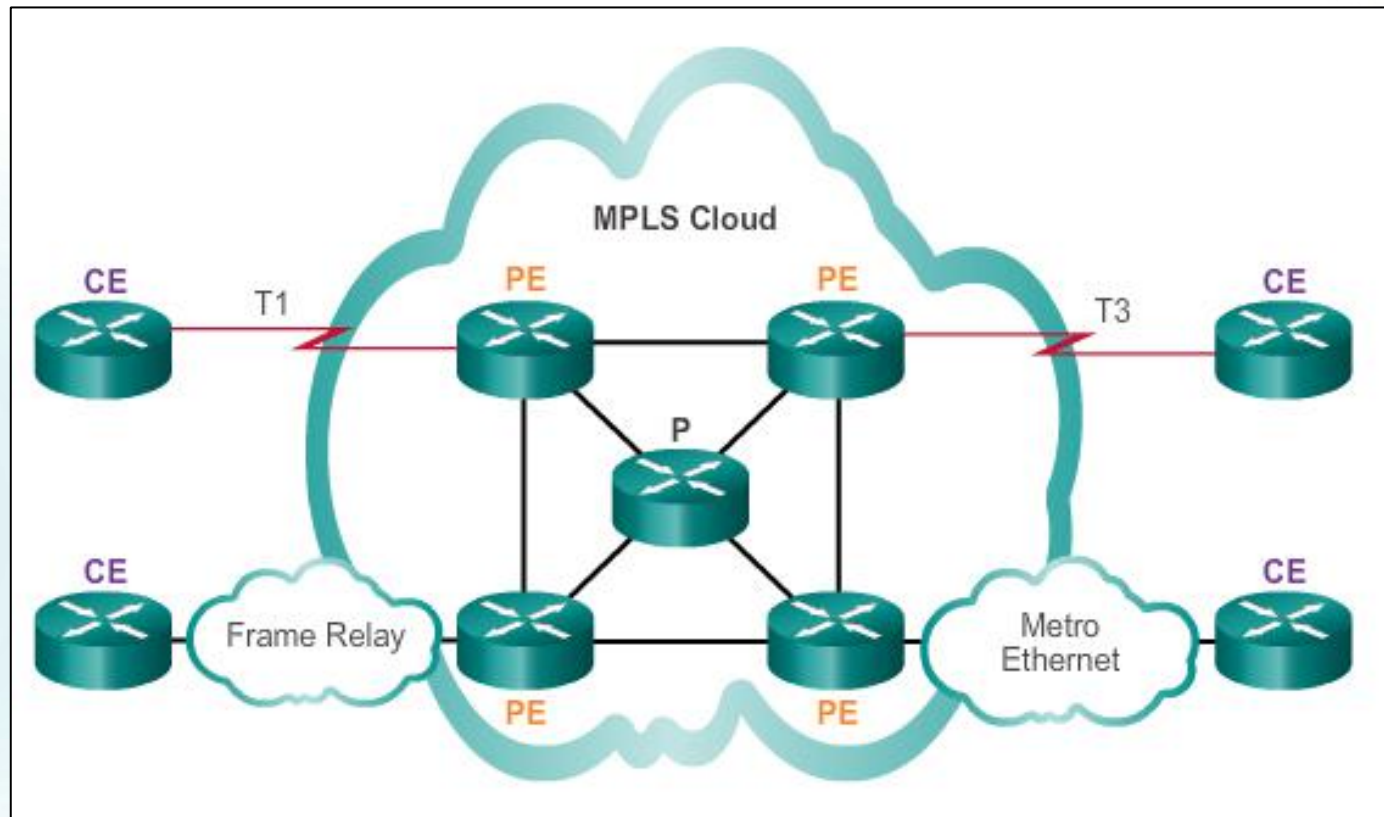
Note: Commonly used to replace the traditional Frame Relay and ATM WAN links.



Private WAN Infrastructures

MPLS

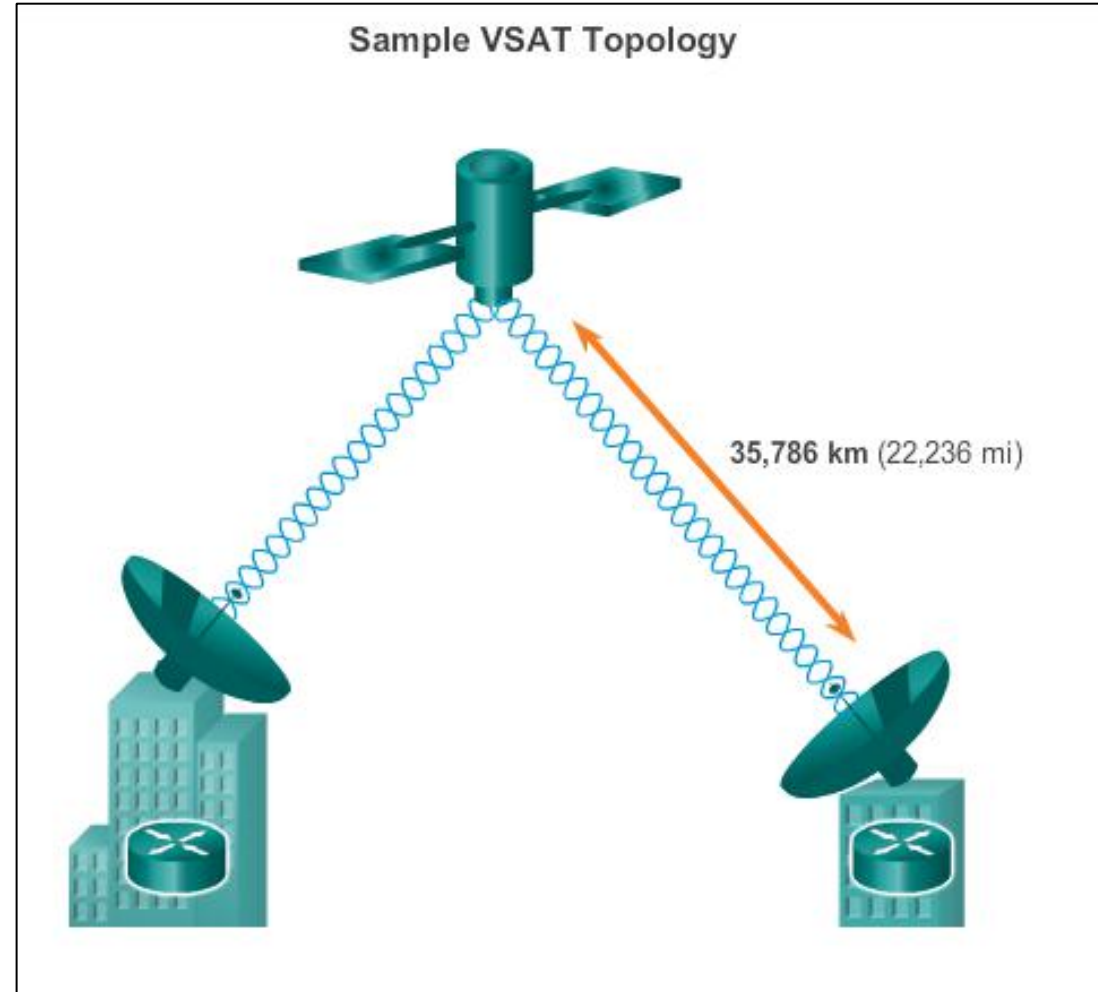
Multiprotocol Label Switching (MPLS) is a multiprotocol high-performance WAN technology that directs data from one router to the next, based on short path labels rather than IP network addresses.



Private WAN Infrastructures

VSAT

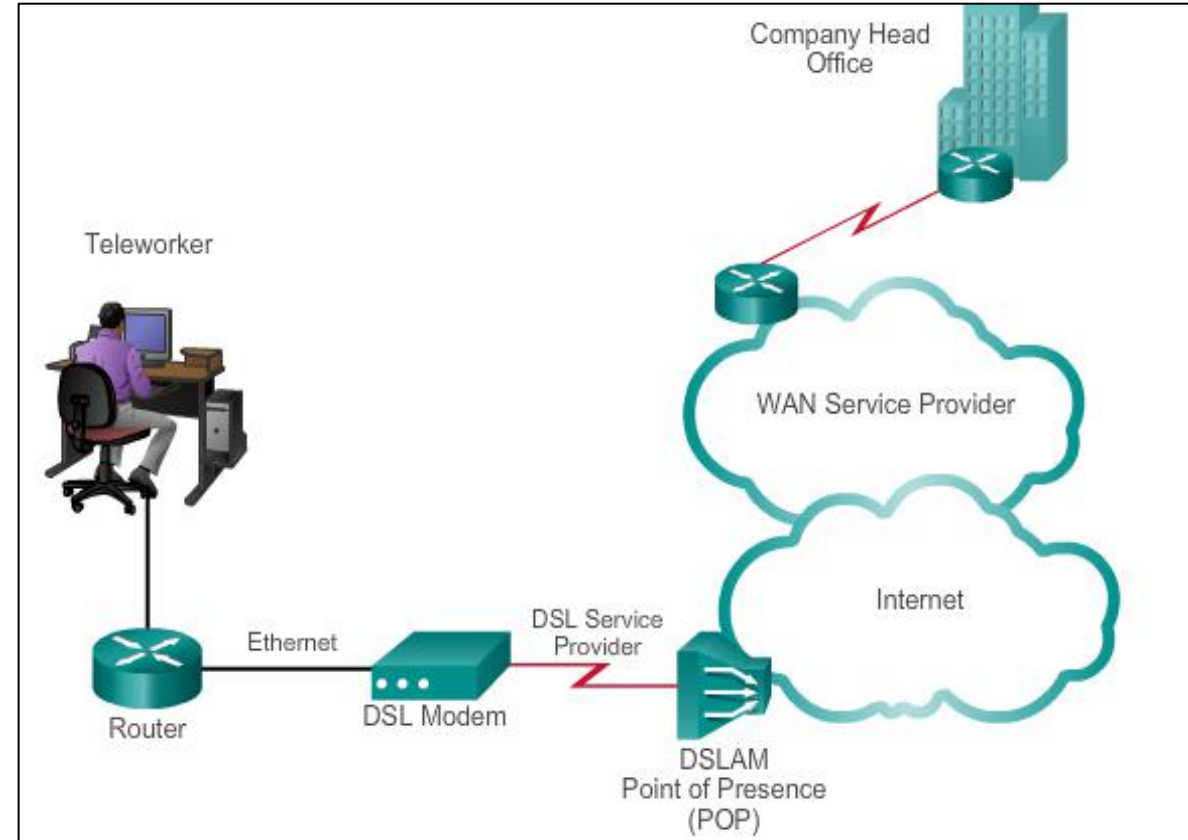
Very small aperture terminal (VSAT) - a solution that creates a private WAN using satellite communications.



Private WAN Infrastructures

DSL

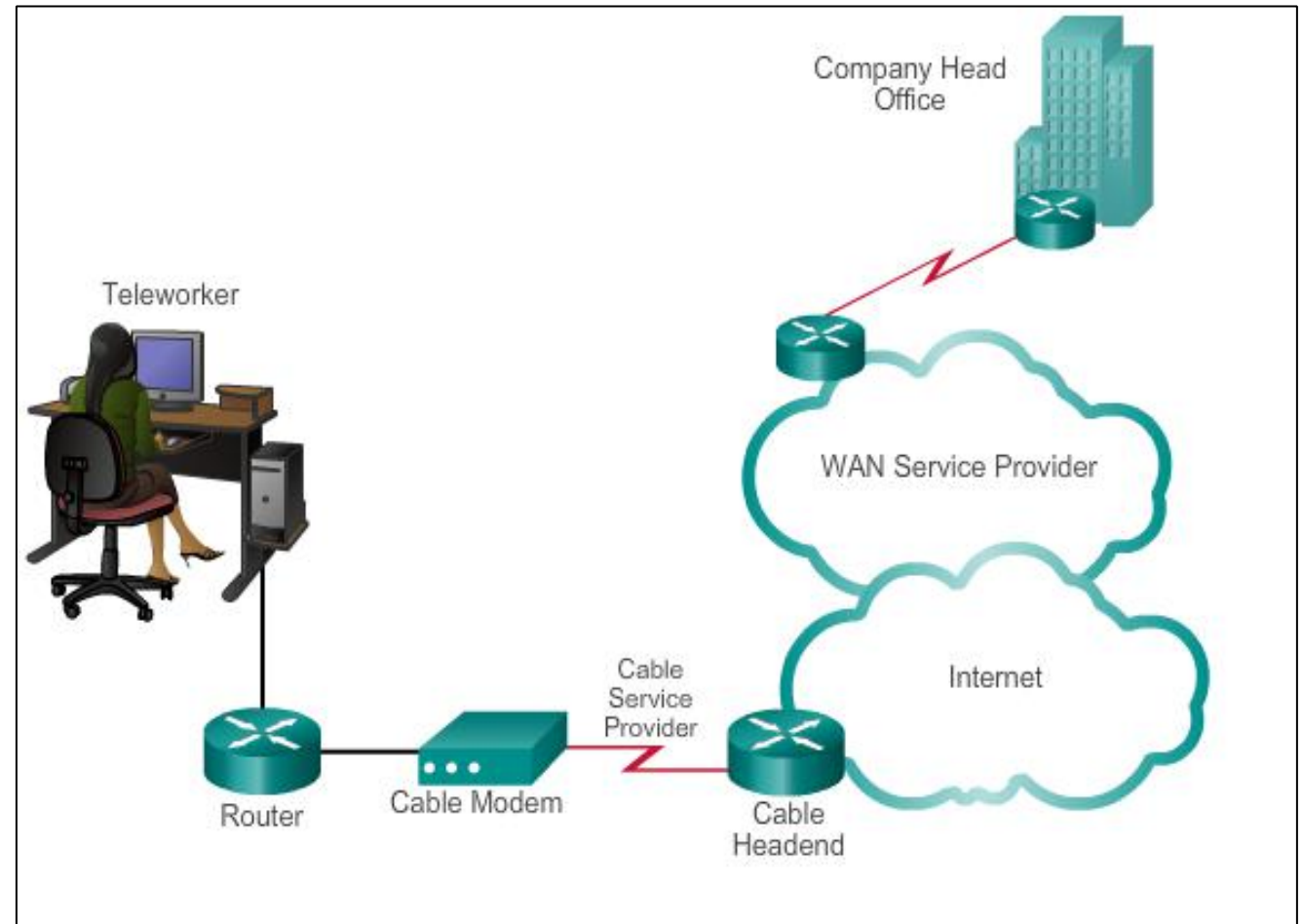
- Always-on connection technology that uses existing twisted-pair telephone lines to transport high-bandwidth data, and provides IP services to subscribers.
- A DSL modem converts an Ethernet signal from the user device to a DSL signal, which is transmitted to the central office.



Private WAN Infrastructures

Cable

- Network access is available from some cable television networks.
- Cable modems provide an always-on connection and a simple installation.

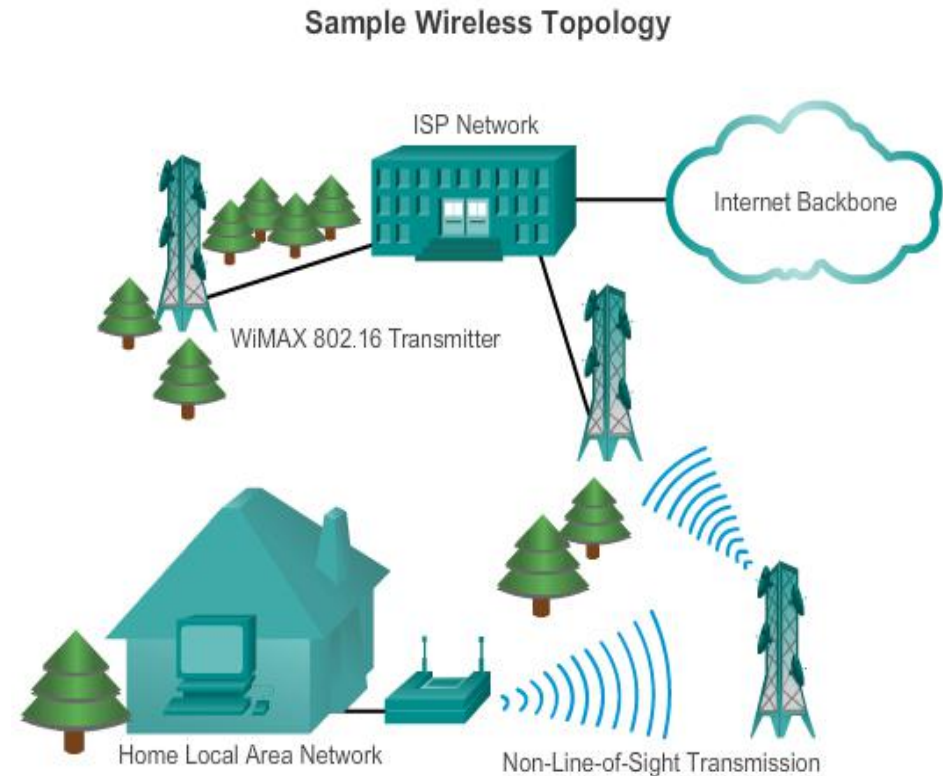


Private WAN Infrastructures

Wireless

New developments in broadband wireless technology:

- **Municipal Wi-Fi** – Many cities have begun setting up municipal wireless
- **WiMAX** – Worldwide Interoperability for Microwave Access (WiMAX) is a new technology that is just beginning to come into use.
- **Satellite Internet**

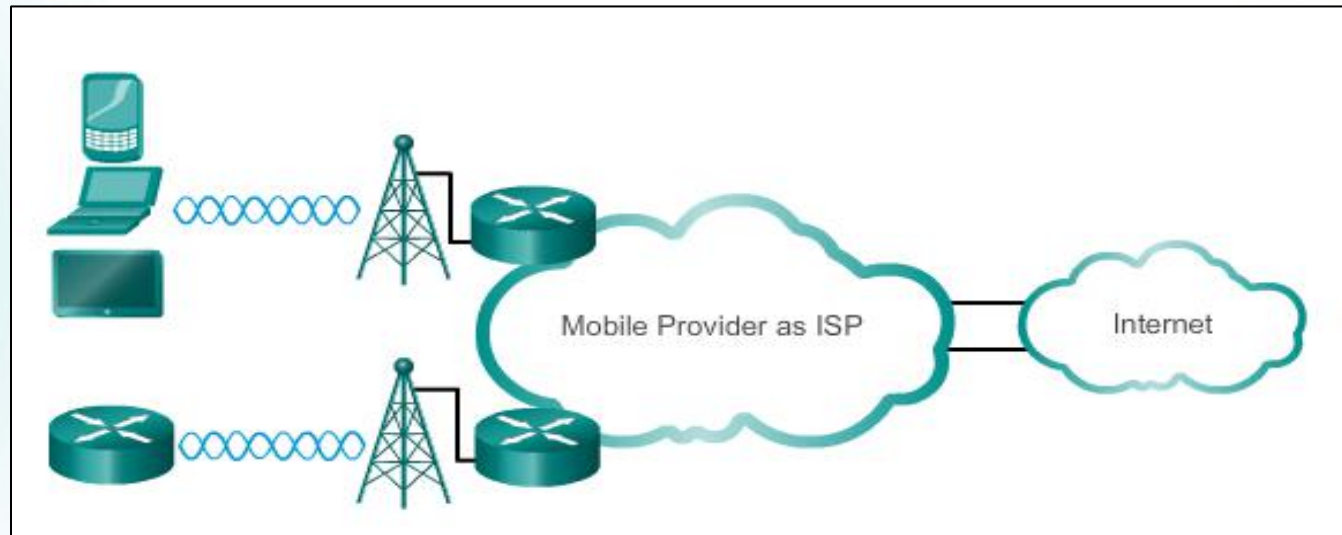


Private WAN Infrastructures

3G/4G Cellular

Common cellular industry terms include:

- **3G/4G Wireless** – Abbreviation for 3rd generation and 4th generation cellular access. These technologies support wireless Internet access.
- **Long-Term Evolution (LTE)** – A newer and faster technology, considered to be part of the 4th generation (4G) technology.



Private WAN Infrastructures

VPN Technology

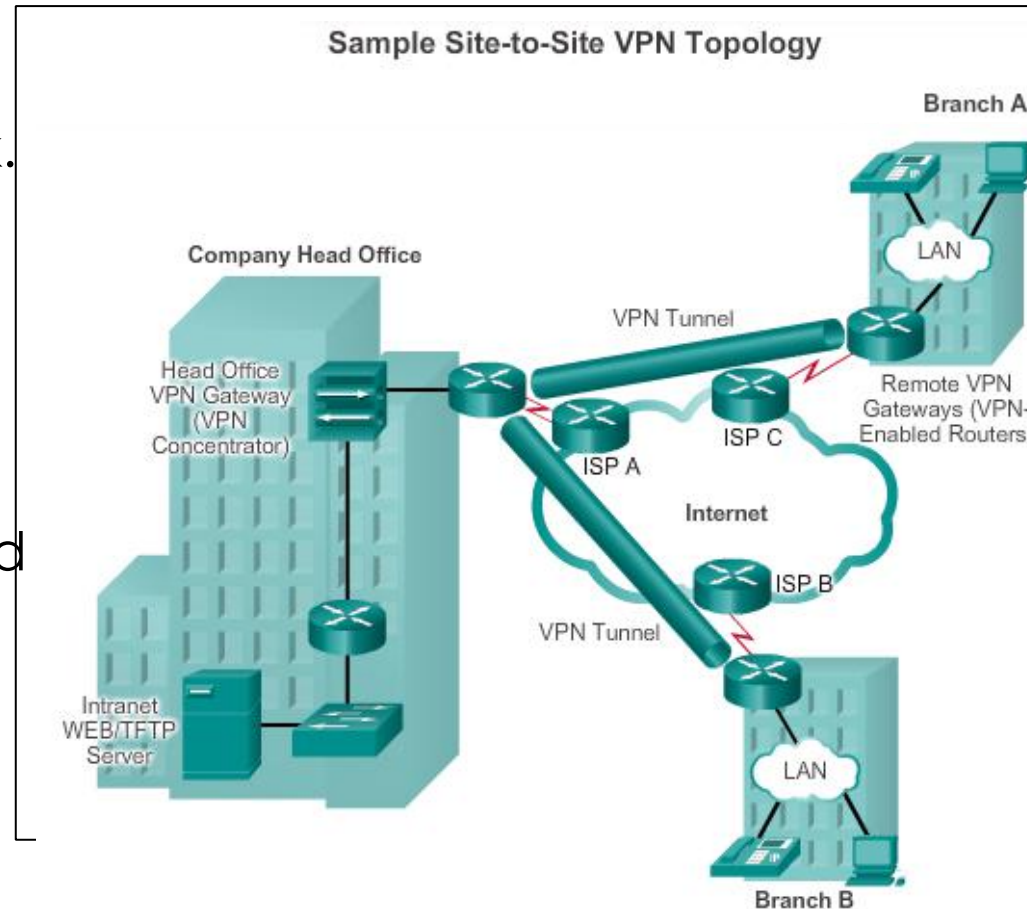
VPN is an encrypted connection between private networks over a public network.

Benefits:

- Cost savings
- Security
- Scalability
- Compatibility with broadband technology

Two types of VPN:

- Site-to-site VPNs
- Remote-access VPNs



Choosing a WAN Link Connection

Answer the following questions when choosing a WAN Connection:

- What is the purpose of the WAN?
- What is the geographic scope?
- What are the traffic requirements?



Choosing a WAN Link Connection



- Should the WAN use a private or public infrastructure?
- For a private WAN, should it be dedicated or switched?
- For a public WAN, what type of VPN access is required?
- Which connection options are available locally?
- What is the cost of the available connection options?



Summary

- ▶ A business can use private lines or the public network infrastructure for WAN connections.
- ▶ WAN access standards operate at layers 1 and 2 of the OSI model, and are defined and managed by the TIA/EIA, ISO, and IEEE.
- ▶ A WAN may be circuit-switched or packet-switched.
- ▶ There is common terminology used to identify the physical components of WAN connections and who, the service provider or the customer, is responsible for which components.
- ▶ Service provider networks are complex and the service provider's backbone networks consist primarily of high-bandwidth fiber optic media.



Summary (cont.)

- ▶ Permanent, dedicated point-to-point connections are provided by using leased lines.
- ▶ Public infrastructure connections include DSL, cable, wireless, and 3G/4G cellular.
- ▶ Security over public infrastructure connections can be provided by using remote-access or site-to-site VPNs.



Point-to-Point Connections



Learning Objectives

In this chapter, you will be able to:

- ▶ Explain the fundamentals of point-to-point serial communication across a WAN.
- ▶ Describe the benefits of using PPP over HDLC in a WAN.
- ▶ Describe the PPP layered architecture and the functions of LCP and NCP.
- ▶ Configure PPP encapsulation on a point-to-point serial link.
- ▶ Configure PPP authentication protocols.



Serial Point-to-Point Overview

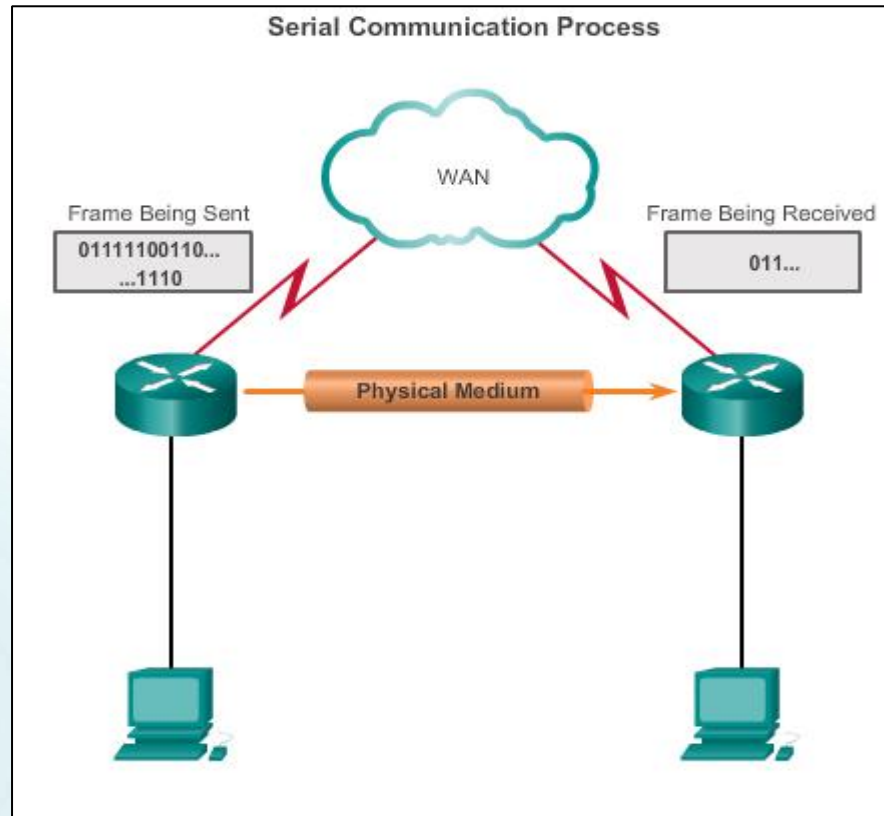


Serial and Parallel Ports

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



Serial Communication



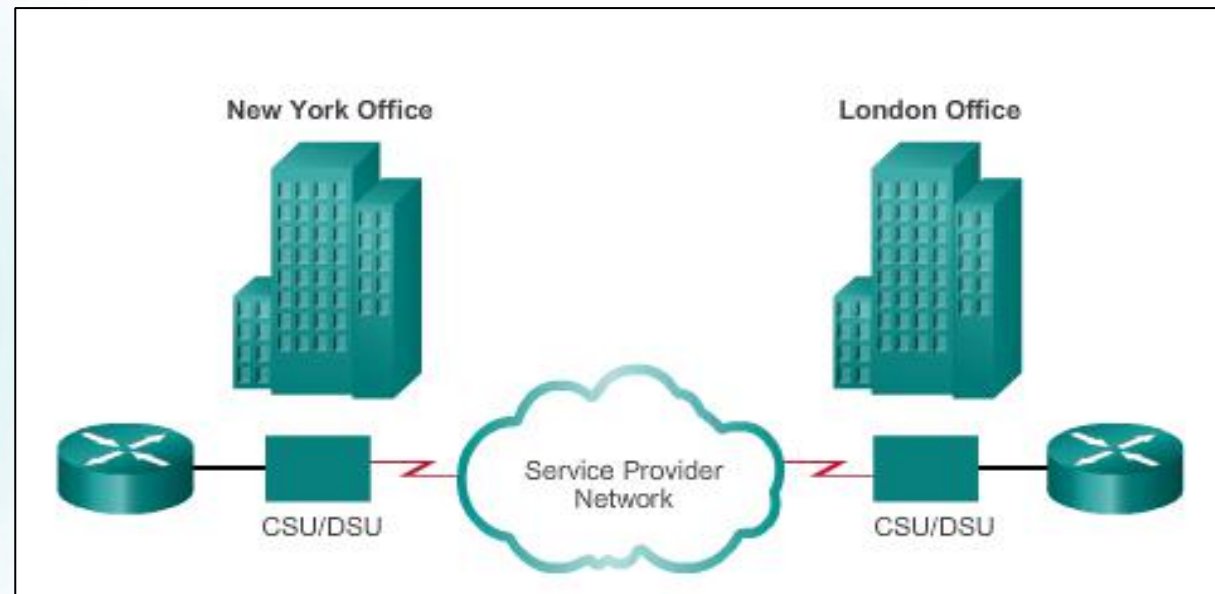
- On the WAN link, data is encapsulated by the protocol used by the sending router.
- Encapsulated frame is sent on a physical medium to the WAN.
- Receiving router uses the same communications protocol to de-encapsulate the frame when it arrives.

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



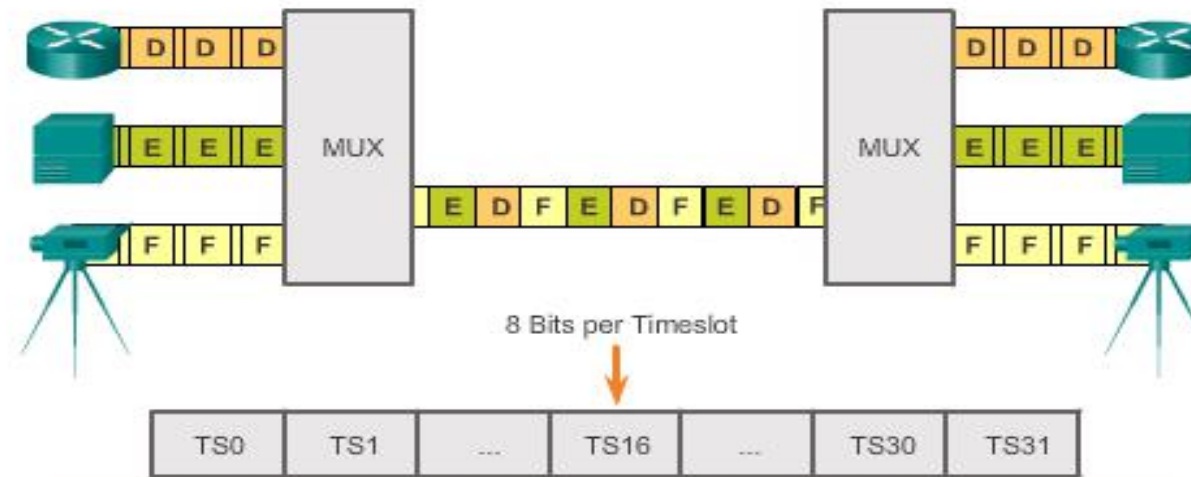
Point-to-Point Communication Links

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



Time-Division Multiplexing

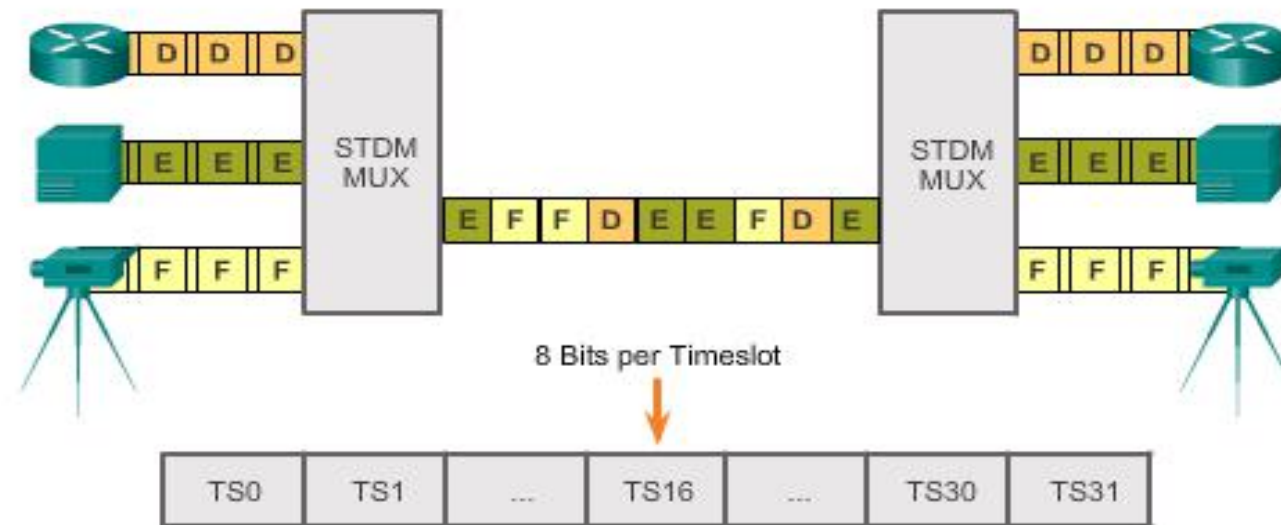
Multiplexing – A scheme that allows multiple logical signals to share a single physical channel.



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

Statistical Time-Division Multiplexing

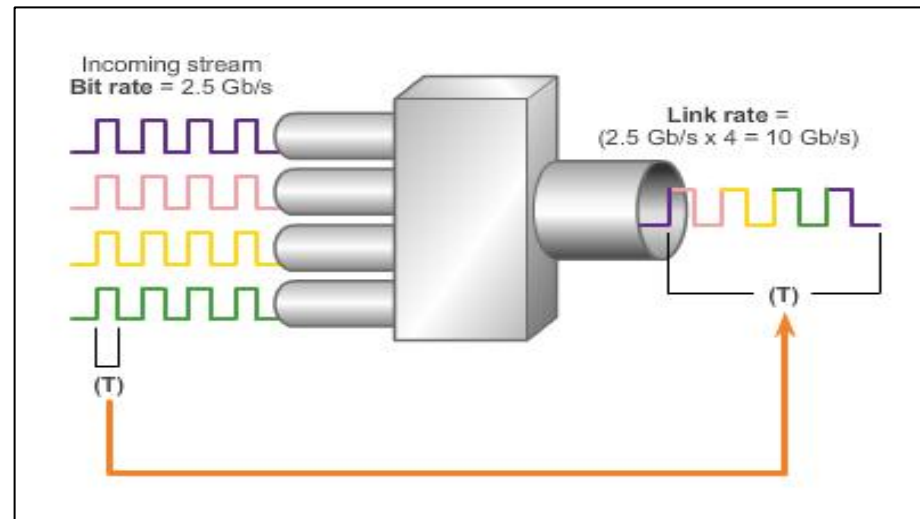
- ▶ STDM uses a variable time-slot length, allowing channels to compete for any free slot space.
- ▶ STDM does not waste high-speed line time with inactive channels using this scheme.



TDM Examples

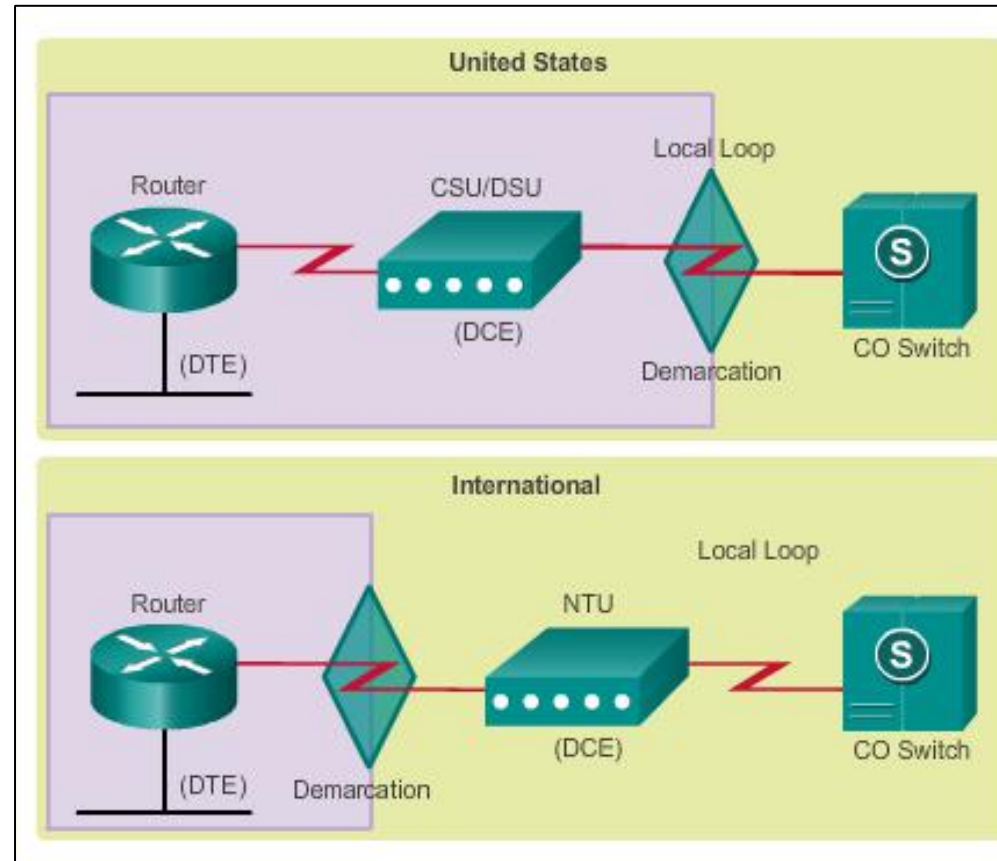
- ▶ The industry uses the Synchronous Optical Networking (SONET) or Synchronous Digital Hierarchy (SDH) standard for optical transport of TDM data.
- ▶ Traffic arriving at the SONET multiplexer from four places at 2.5 Gb/s goes out as a single stream at 4×2.5 Gb/s or 10 Gb/s.

Example:
TDM SONET



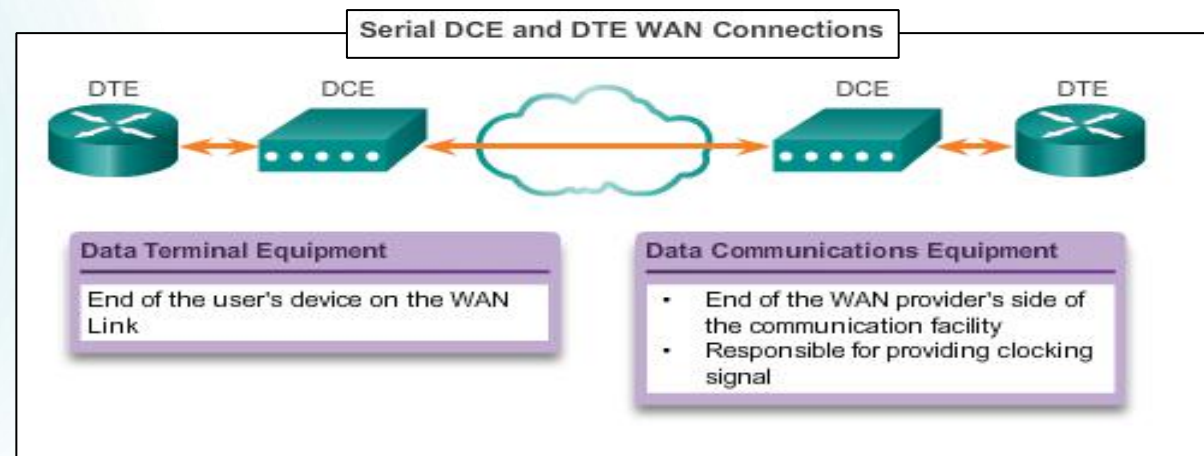
Demarcation Point

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

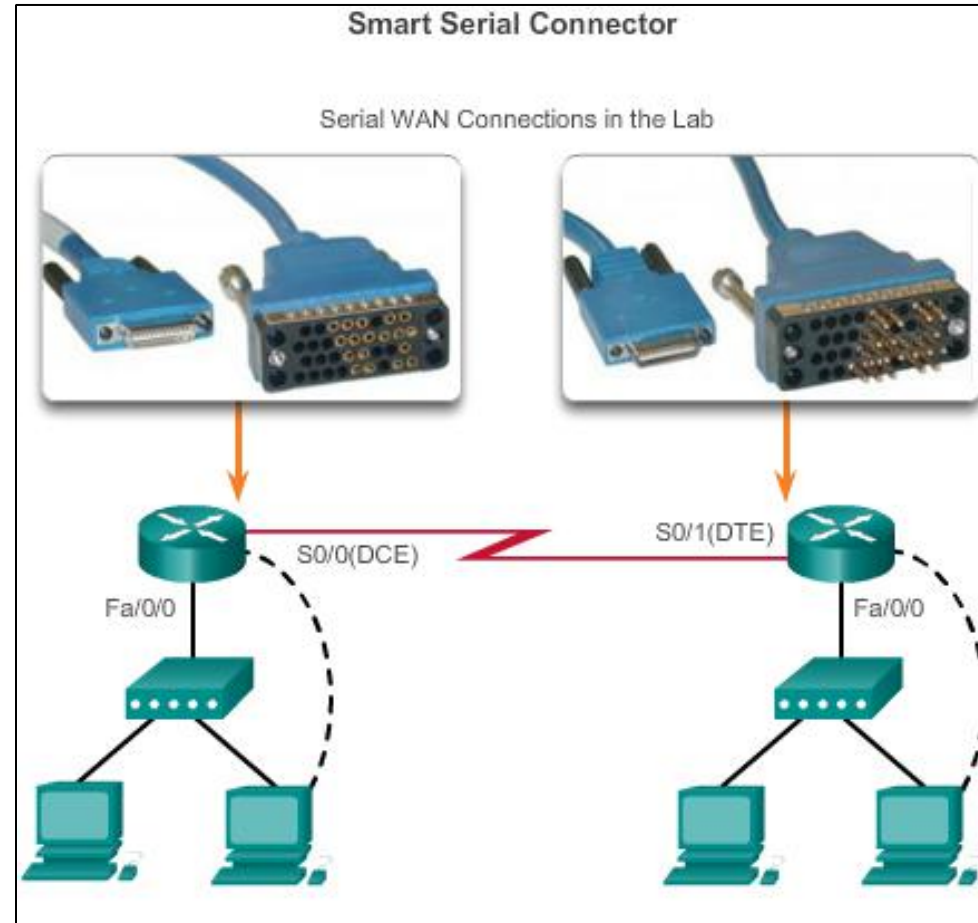


DTE-DCE

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



Serial Cables



Serial Bandwidth

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

Carrier Transmission Rates

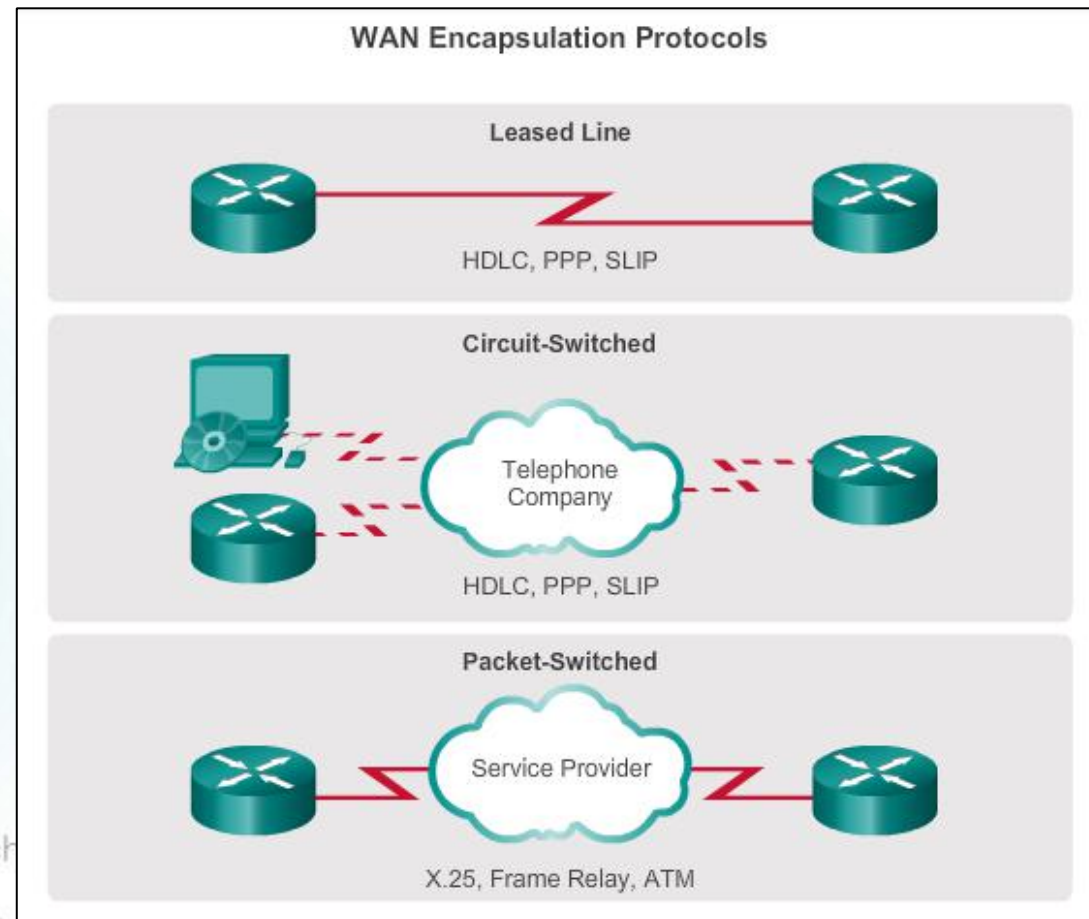
Line Type	Bit Rate Capacity
56	56 kb/s
64	64 kb/s
T1	1.544 Mb/s
E1	2.048 Mb/s
J1	2.048 Mb/s
E3	34.064 Mb/s
T3	44.736 Mb/s
OC-1	51.84 Mb/s
OC-3	155.54 Mb/s
OC-9	466.56 Mb/s
OC-12	622.08 Mb/s
OC-18	933.12 Mb/s
OC-24	1.244 Gb/s
OC-36	1.866 Gb/s
OC-48	2.488 Gb/s
OC-96	4.976 Gb/s
OC-192	9.954 Gb/s
OC-768	39.813 Gb/s



HDLC Encapsulation

WAN Encapsulation Protocols

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



HDLC Encapsulation

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



PPP Operation



Introducing PPP

PPP contains three main components:

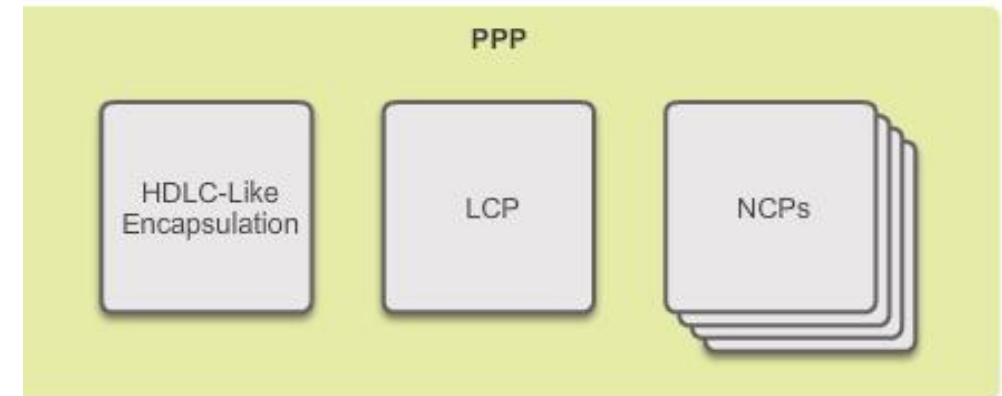
- HDLC protocol for encapsulating datagrams over point-to-point links
- Extensible Link Control Protocol (LCP) to establish, configure, and test the data link connection
- Family of Network Control Protocols (NCPs) to establish and configure different network layer protocols (IPv4, IPv6, AppleTalk, Novell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



HDLC is the default encapsulation method on a serial link.



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

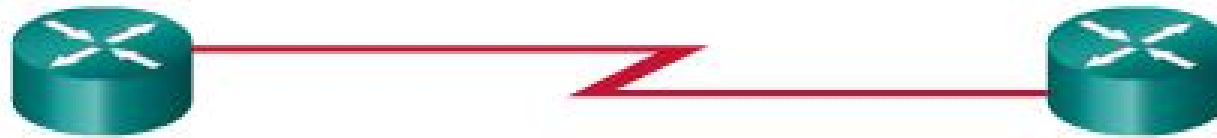


Advantages of PPP

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



Establishing a PPP Session (cont.)



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

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

LCP Operation

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



LCP Operation (cont.)

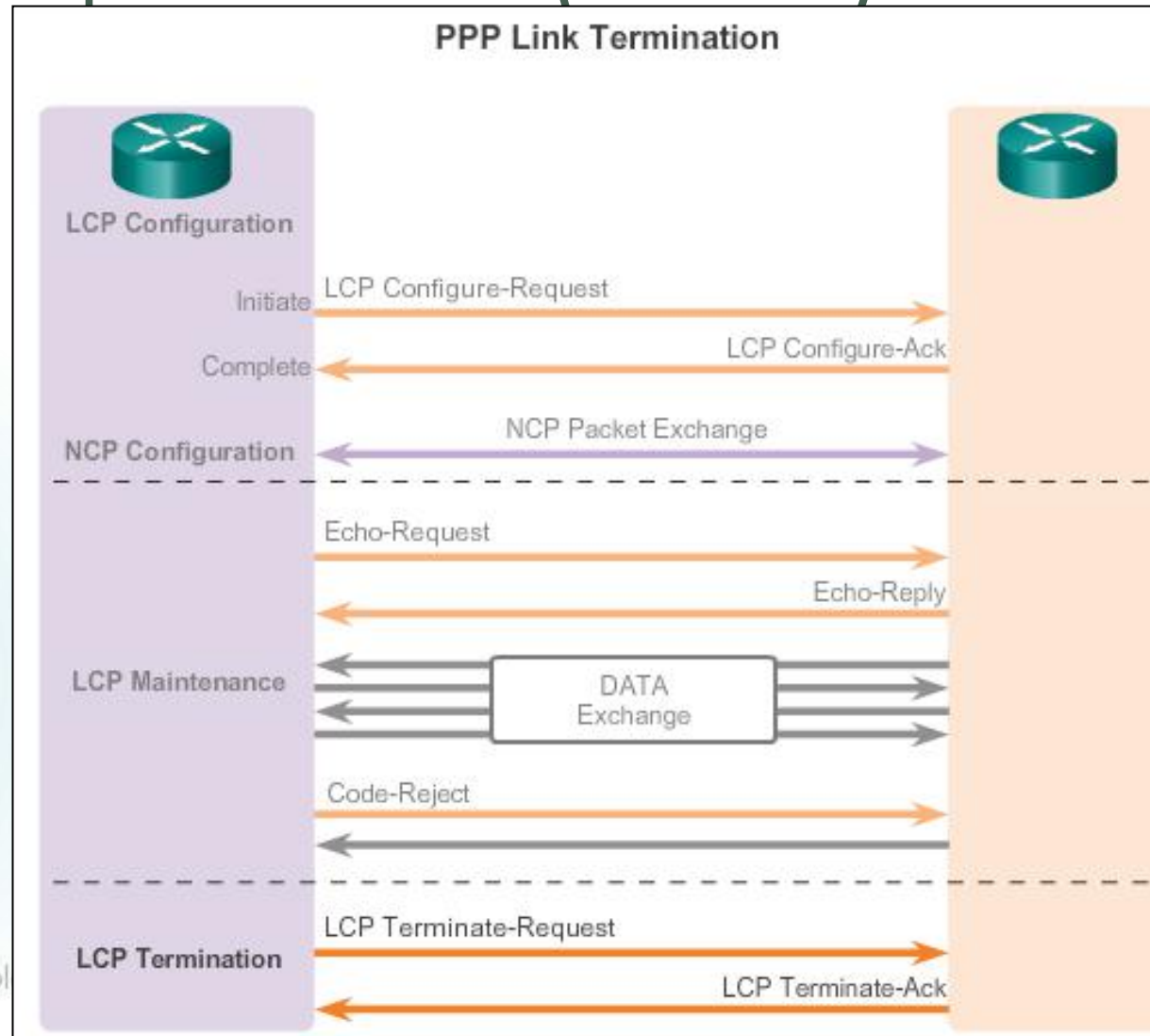
During link maintenance, LCP can use messages to provide feedback and test the link.

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



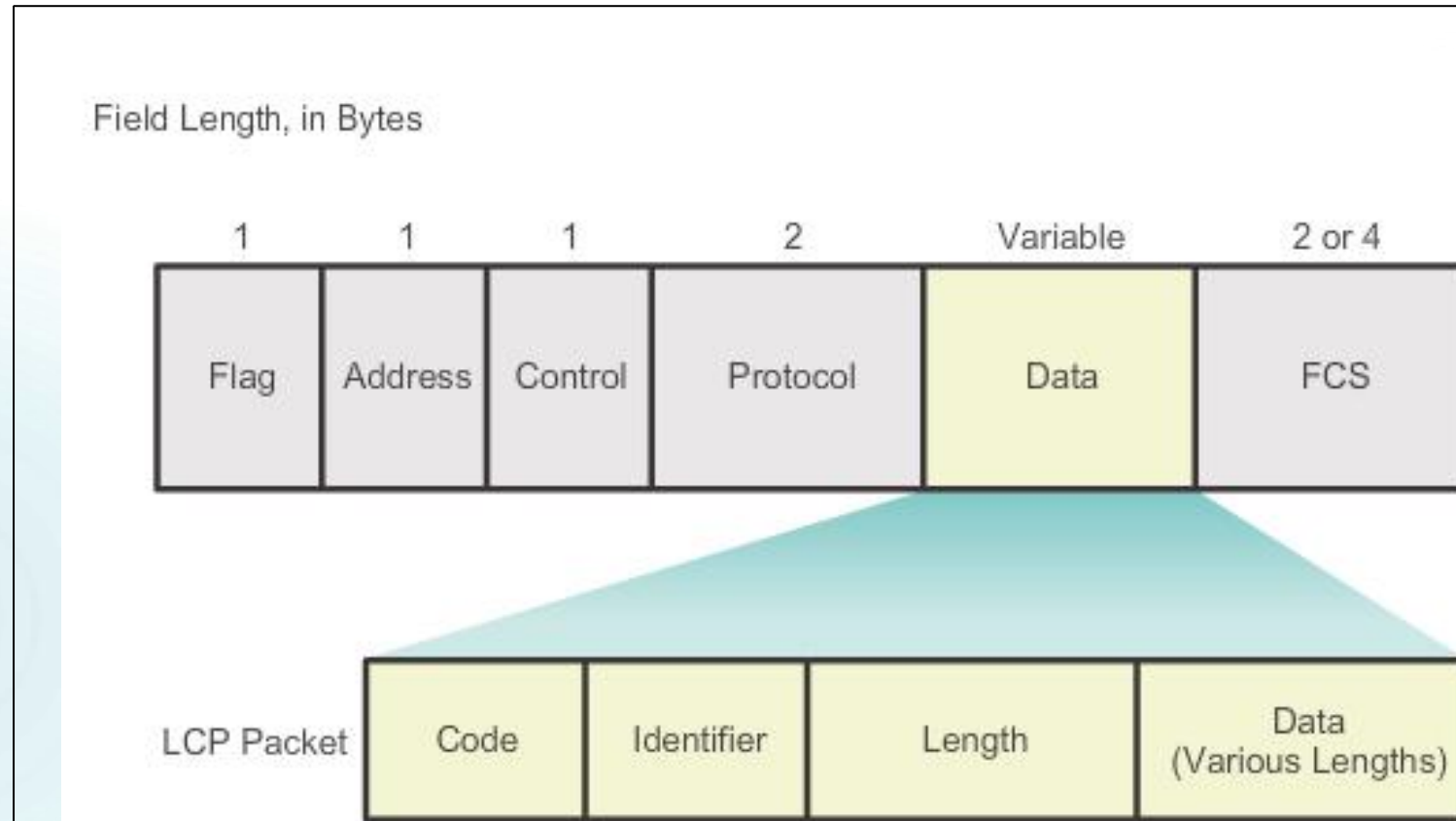
PPP Sessions

LCP Operation (cont.)



PPP Sessions

LCP Packet



LCP Packet

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



LCP Packet (cont.)

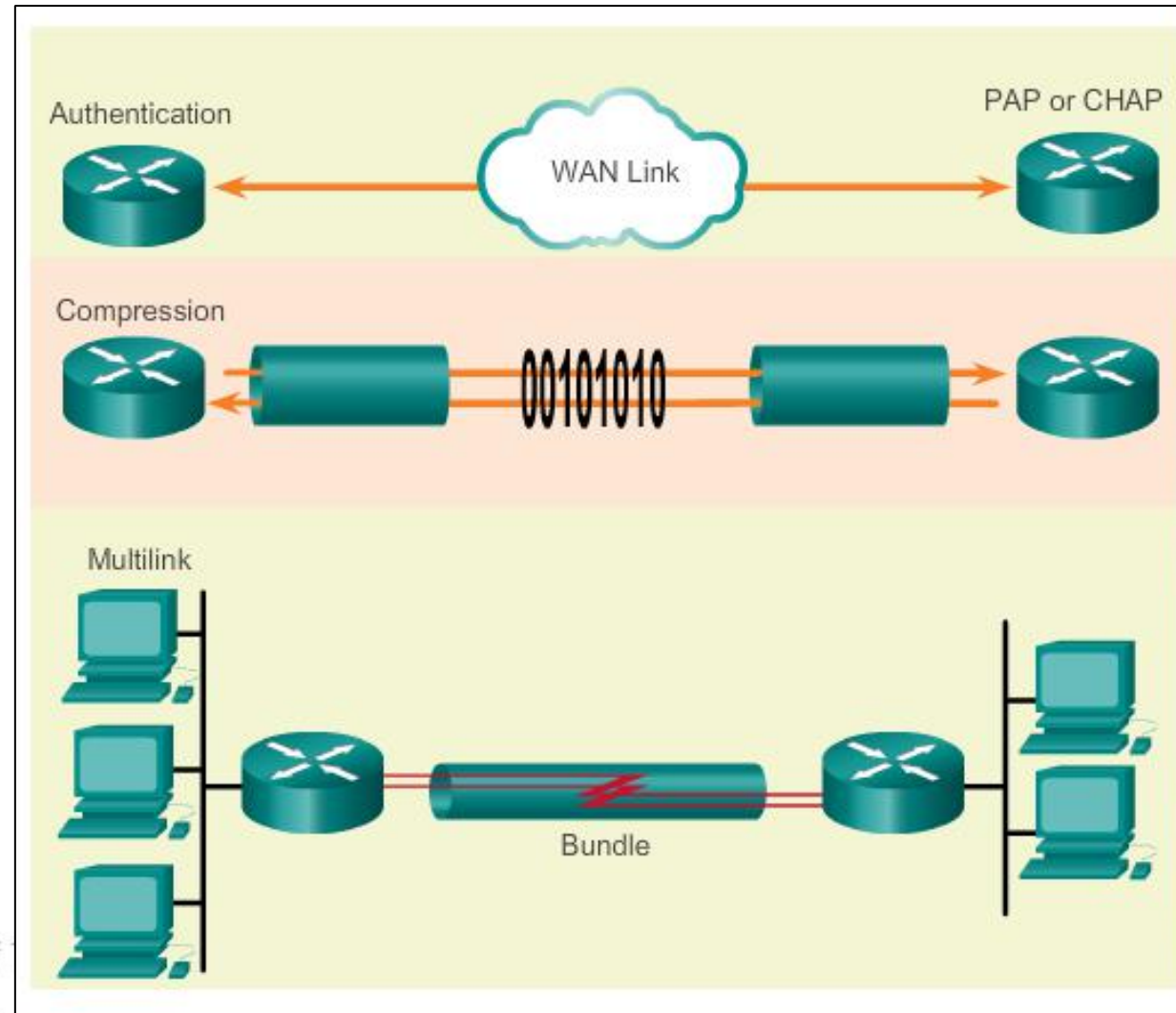
LCP Code	LCP Packet Type	Description
7	Code-Reject	Sent when the LCP code is unknown. The Code-Reject message includes the rejected LCP packet.
8	Protocol-Reject	Sent when the PPP frame contains an unknown Protocol ID. The Protocol-Reject message includes the rejected LCP packet. Protocol-Reject is typically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



PPP Configuration Options

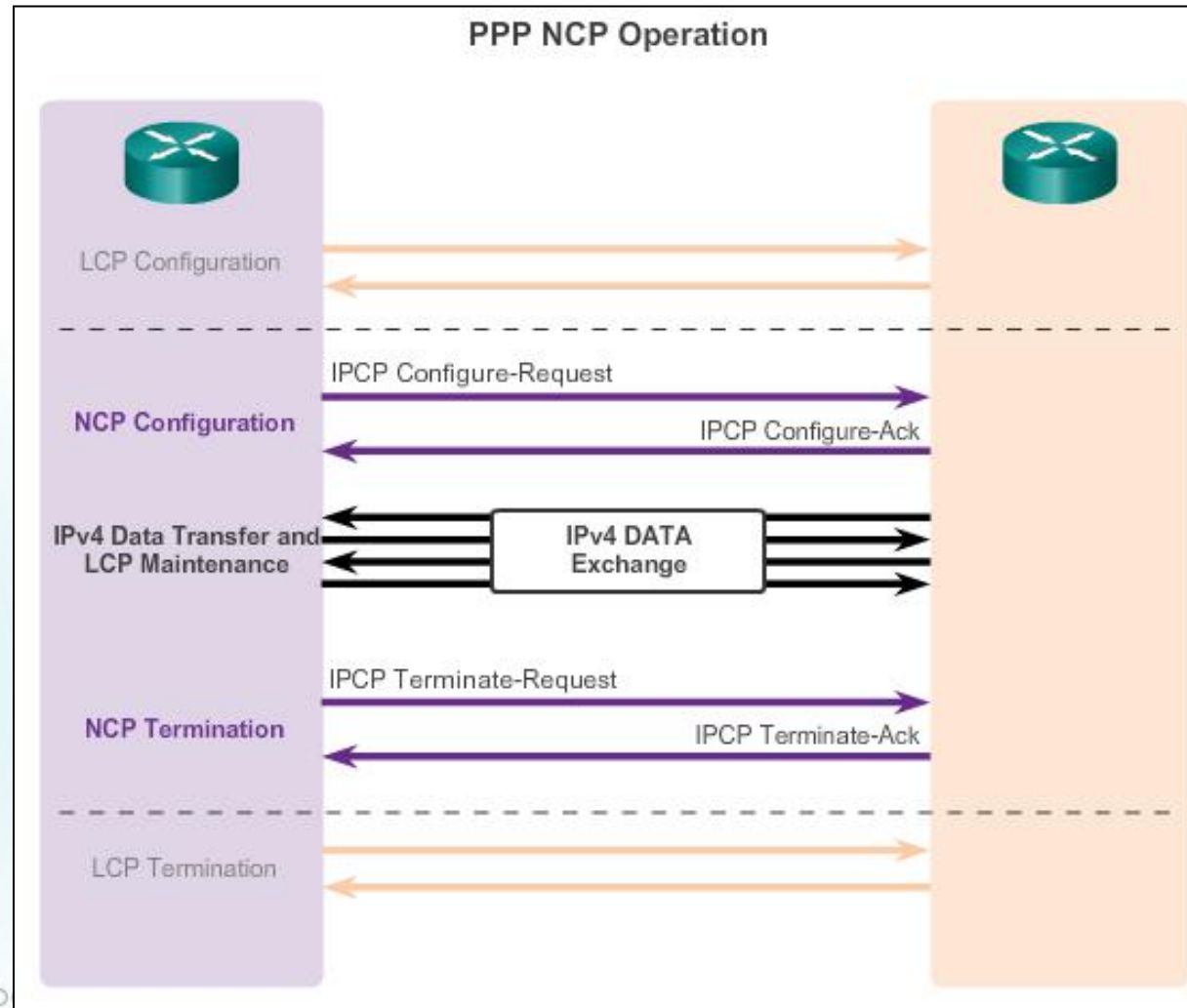
Optional functions include:

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



PPP Sessions

NCP Explained



3.3 Configuring PPP



PPP Configuration Options

- **Authentication** – Two authentication choices are Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP).
- **Compression** – Increases the effective throughput on PPP connections by reducing the amount of data in the frame that must travel across the link. The protocol decompresses the frame at its destination. Two compression protocols available in Cisco routers are Stacker and Predictor.
- **Error detection** – Identifies fault conditions. The Quality and Magic Number options help ensure a reliable, loop-free data link. The Magic Number field helps in detecting links that are in a looped-back condition. Magic numbers are generated randomly at each end of the connection.



PPP Configuration Options

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



Configure PPP

PPP Basic Configuration Command



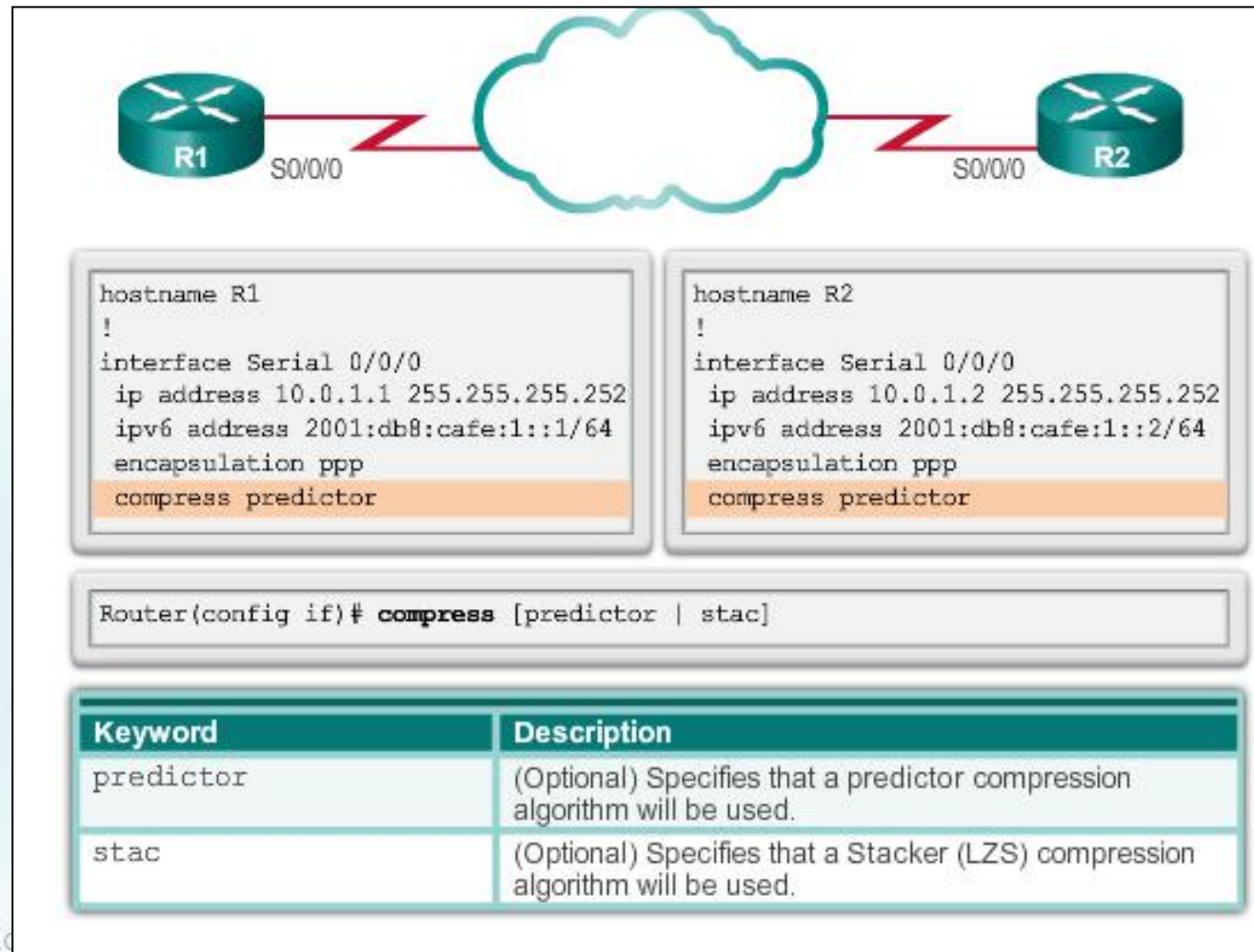
```
hostname R1
!  
interface Serial 0/0/0  
  ip address 10.0.1.1 255.255.255.252  
  ipv6 address 2001:db8:cafe:1::1/64  
  encapsulation ppp
```

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



Configure PPP

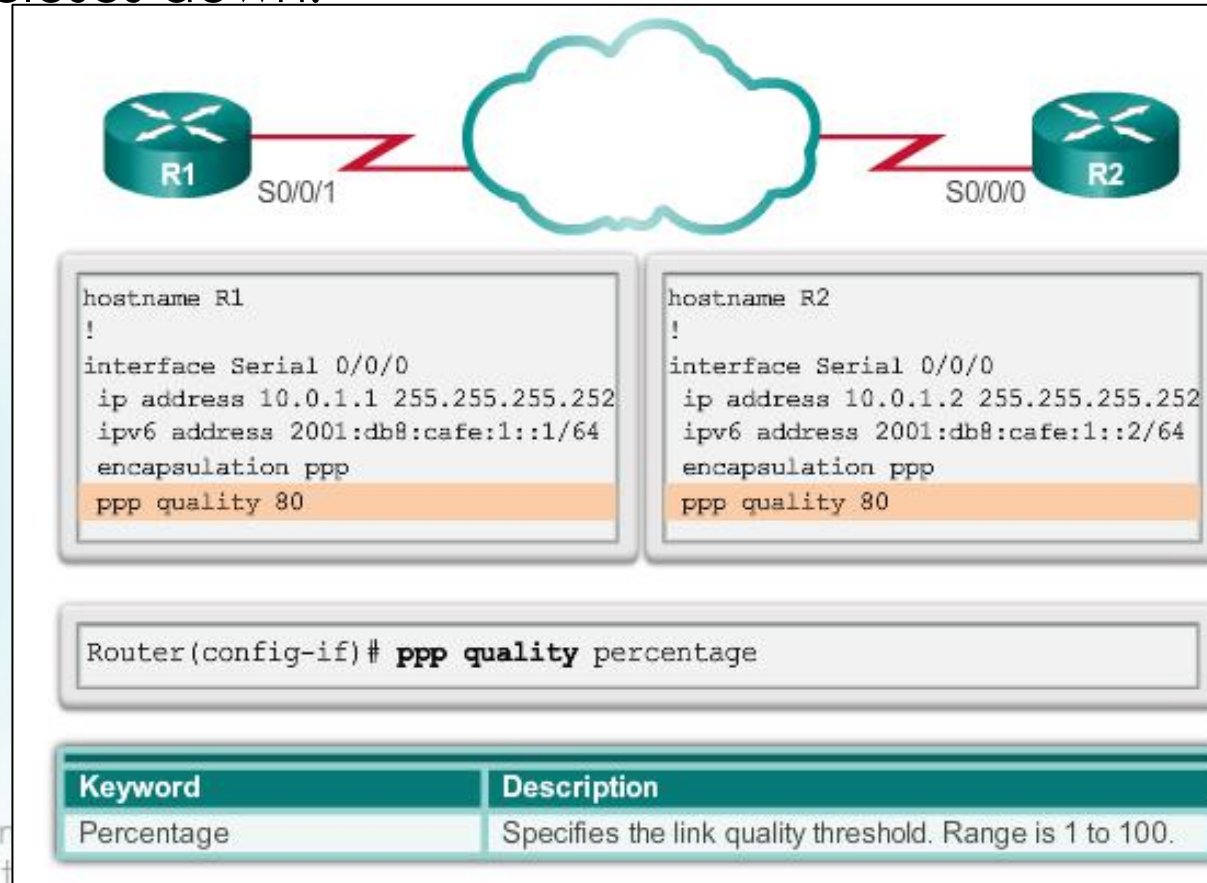
PPP Compression Commands



Configure PPP

PPP Link Quality Monitoring

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



Configure PPP

PPP Multilink Commands



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

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



Configure PPP

Verifying PPP Configuration

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

```
R2# show interfaces serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.0.1.2/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, IPV6CP, CCP, CDPCP, loopback not set
  Keepalive set (10 sec)
  CRC checking enabled
  Last input 00:00:02, output 00:00:02, output hang never
  Last clearing of "show interface" counters 01:29:06
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output
  drops: 0
  Queueing strategy: weighted fair
```



Configure PPP

Verifying PPP Configuration

(cont.)

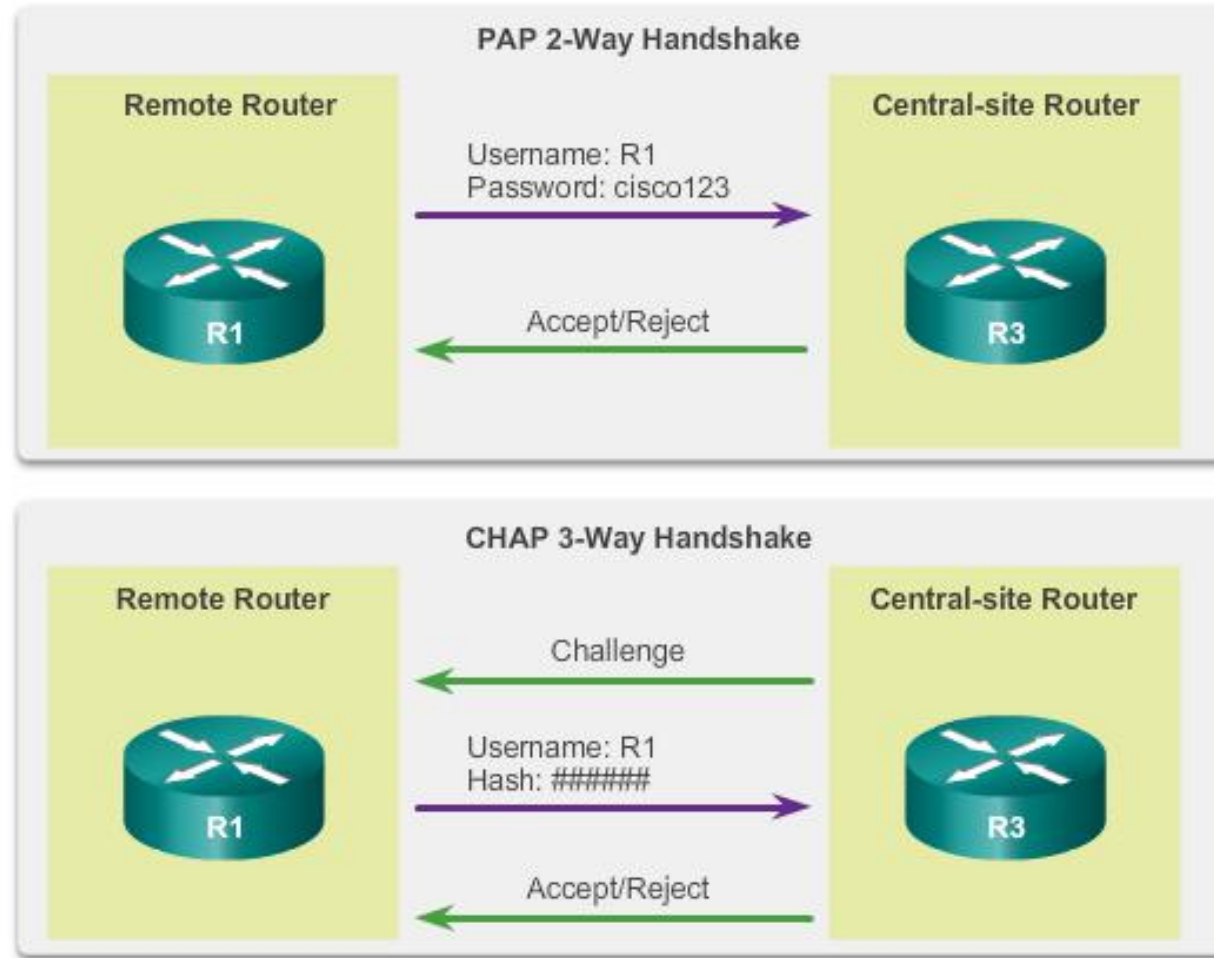
The output indicates the interface Multilink 1, the hostnames of both the local and remote endpoints, and the serial interfaces assigned to the multilink bundle.

```
R3# show ppp multilink

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



PPP Authentication Protocols



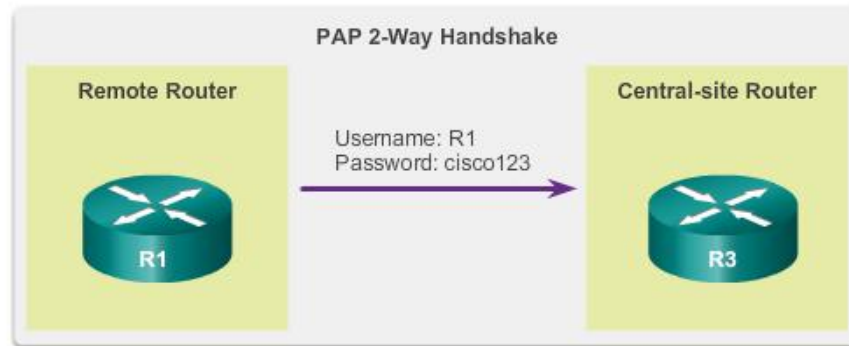
PPP Authentication

Password Authentication

Initiating PAP

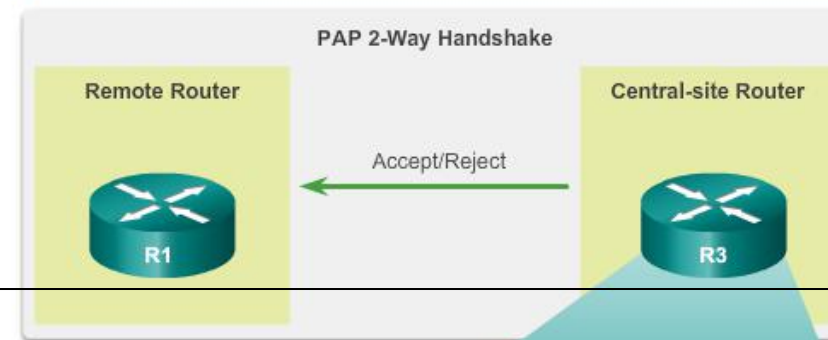
Protocol (PAP)

R1 sends its PAP username and password to R3.



Completing PAP

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



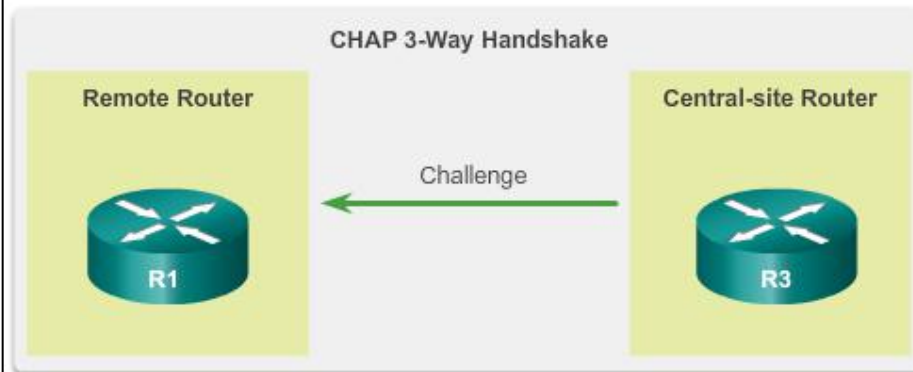
```
username R1 password cisco123
```



PPP Authentication Challenge Handshake Authentication Protocol

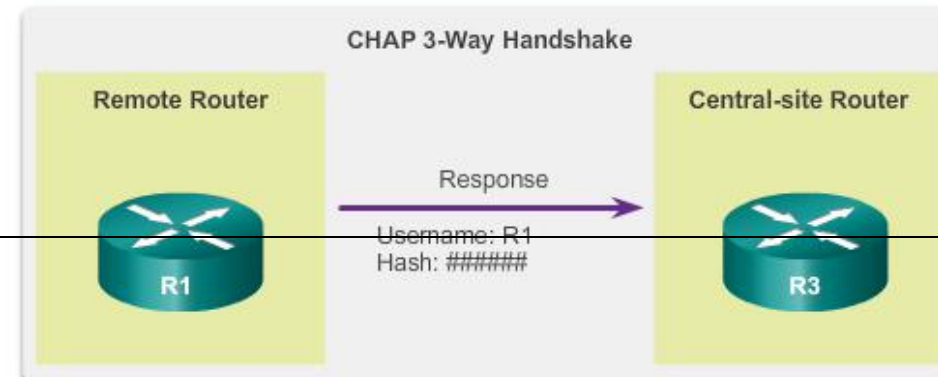
Initiating CHAP

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



Responding CHAP

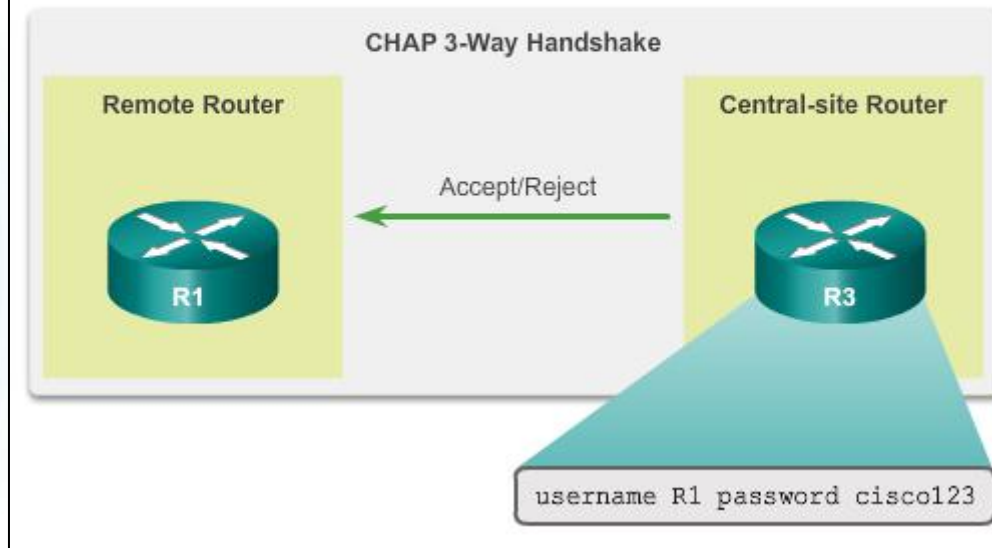
R1 responds to R3's CHAP challenge by sending its CHAP username and a hash value that is based on the CHAP password.



CHAP (cont.)

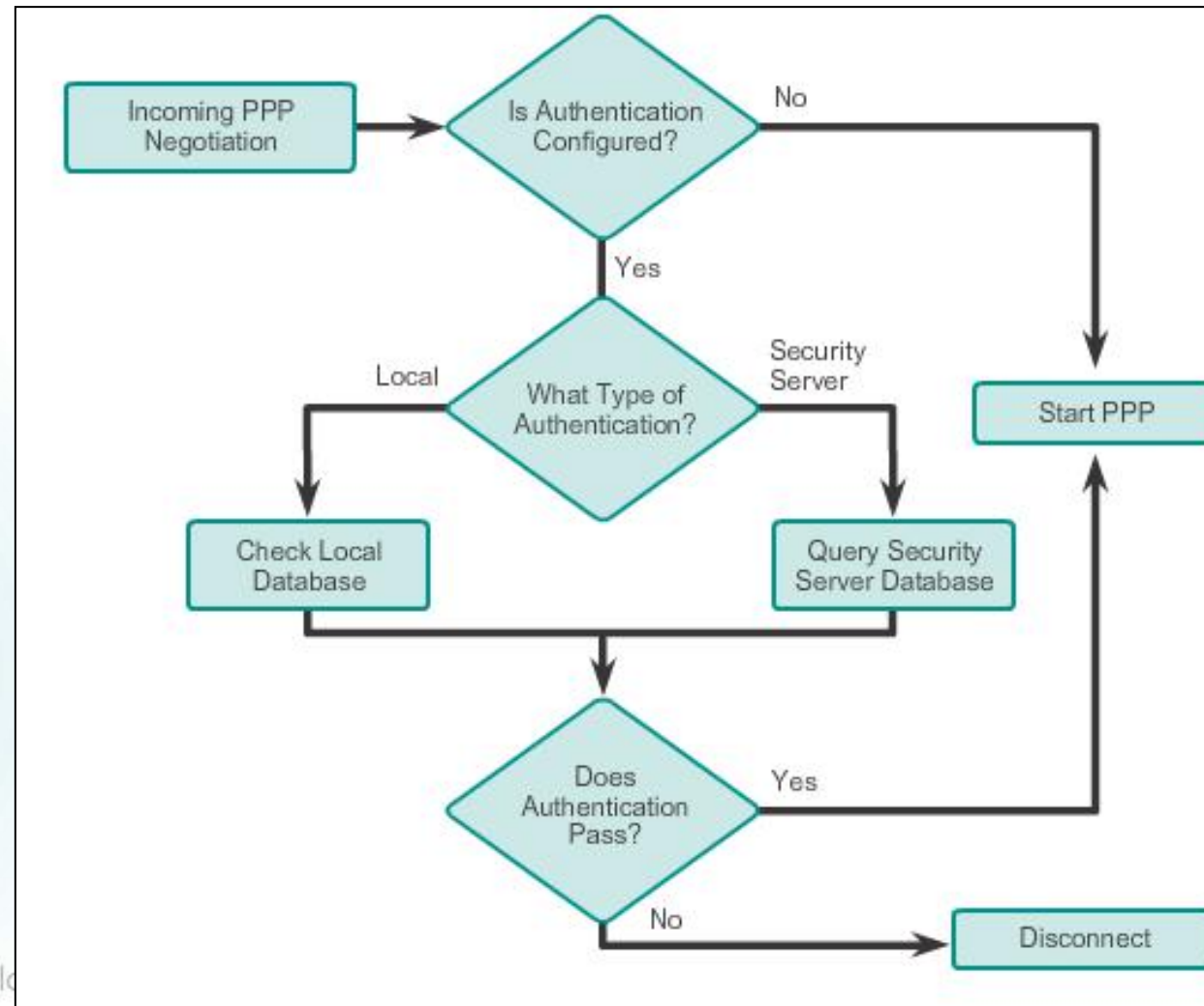
Completing CHAP

Using the username and password for R1 in its local database, R3 compares its calculated hash value with the one sent from R1.



PPP Authentication

PPP Encapsulation and Authentication Process



Configuring PPP

Auth

The ppp authentication Command

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

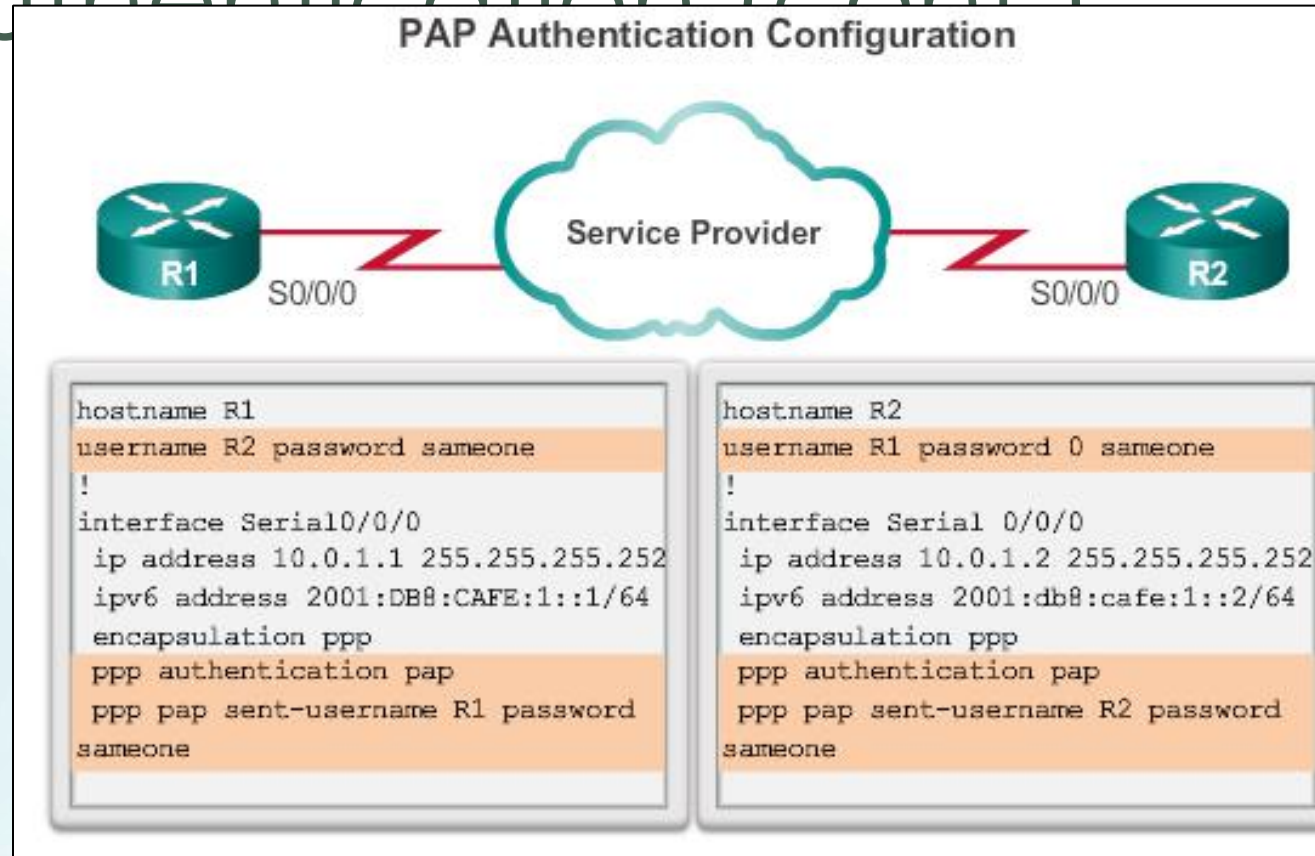
The ppp authentication Command

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



PPP Authentication

Configuring PPP Authentication (cont.)



PPP Authentication

Configuring PPP Authentication (cont.)

CHAP Authentication Configuration



```
hostname R1
username R2 password someone
!
interface Serial0/0/0
 ip address 10.0.1.1 255.255.255.252
 ipv6 address 2001:DB8:CAFE:1::1/64
 encapsulation ppp
 ppp authentication chap
```

```
hostname R2
username R1 password 0 someone
!
interface Serial 0/0/0
 ip address 10.0.1.2 255.255.255.252
 ipv6 address 2001:db8:cafe:1::2/64
 encapsulation ppp
 ppp authentication chap
```



3.4 Troubleshooting WAN Connectivity



Troubleshooting PPP Serial Encapsulation

debug ppp Command Parameters

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

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



Troubleshoot PPP

Troubleshooting a PPP Configuration with Authentication

```
R2# debug ppp authentication
```

```
Serial0: Unable to authenticate. No name received from peer
```

```
Serial0: Unable to validate CHAP response. USERNAME pioneer not found.
```

```
Serial0: Unable to validate CHAP response. No password defined for USERNAME pioneer
```

```
Serial0: Failed CHAP authentication with remote.
```

```
Remote message is Unknown name
```

```
Serial0: remote passed CHAP authentication.
```

```
Serial0: Passed CHAP authentication with remote.
```

```
Serial0: CHAP input code = 4 id = 3 len = 48
```



Chapter 3: Summary

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



Cisco | Networking Academy®

Mind Wide Open™



Wollo University-Kombolcha Institute of Technology
College of Informatics
Systems and Network Administration ©2017

Frame Relay



Learning Objectives

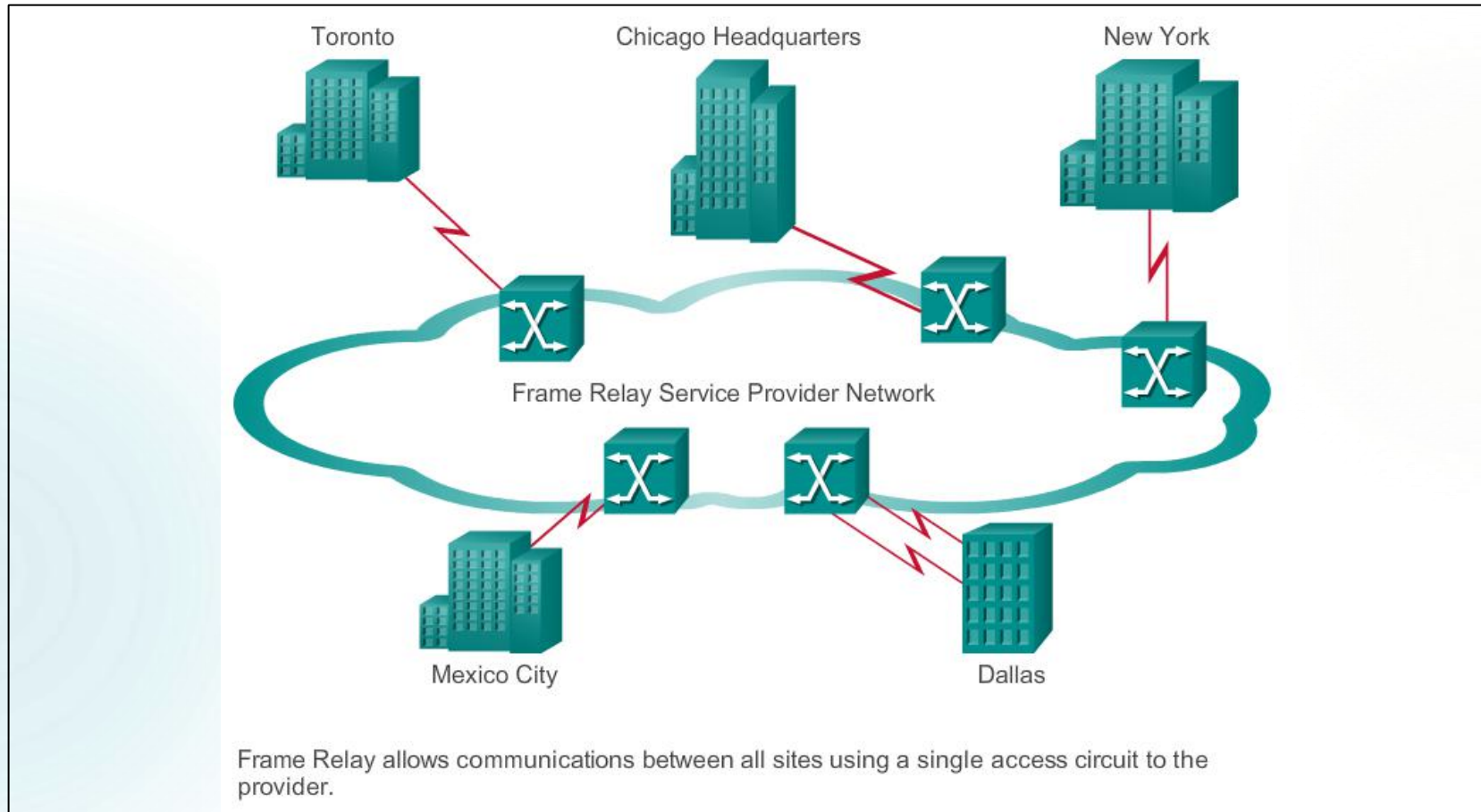
- ▶ Describe the fundamental concepts of Frame Relay technology, including operation, implementation requirements, maps, and Local Management Interface (LMI) operation.
- ▶ Configure a basic Frame Relay permanent virtual circuit (PVC), including configuring and troubleshooting Frame Relay on a router serial interface and configuring a static Frame Relay map.
- ▶ Describe advanced concepts of Frame Relay technology, including subinterfaces, bandwidth, and flow control.
- ▶ Configure an advanced Frame Relay PVC, including solving reachability issues, configuring subinterfaces, and verifying and troubleshooting a Frame Relay configuration.



Introduction to Frame Relay

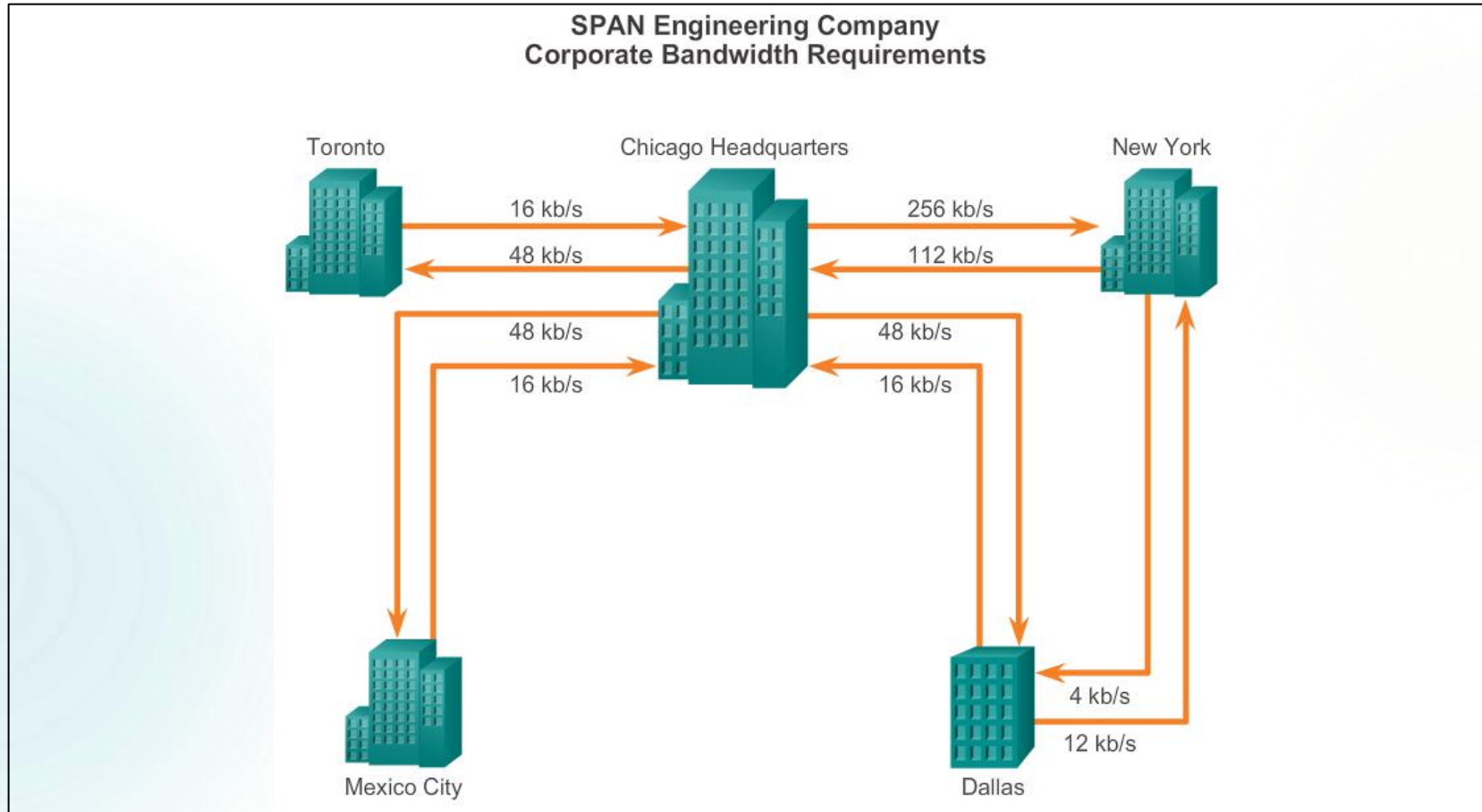


Introducing Frame Relay



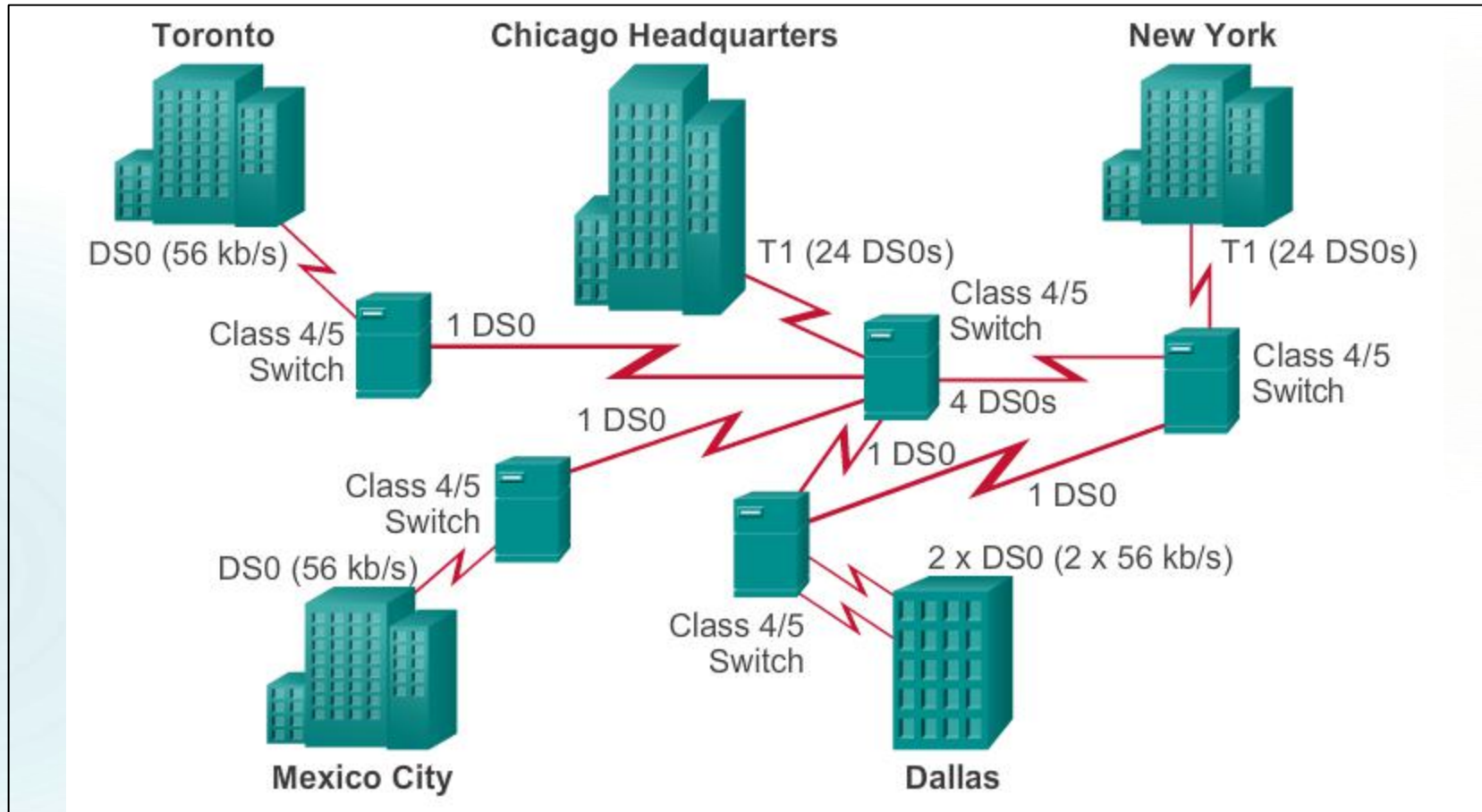
Benefits of Frame Relay

Benefits of Frame Relay WAN Technology



Benefits of Frame Relay

Dedicated Line Requirements



Frame Relay Cost Effectiveness and Flexibility

- ▶ With dedicated lines, customers pay for an end-to-end connection, which includes the local loop and the network link. With Frame Relay, customers only pay for the local loop, and for the bandwidth, they purchase from the network provider.
- ▶ Frame Relay shares bandwidth across a larger base of customers. Typically, a network provider can service 40 or more 56 kb/s customers over one T1 circuit. Using dedicated lines would require more CSU/DSUs (one for each line) and more complicated routing and switching.

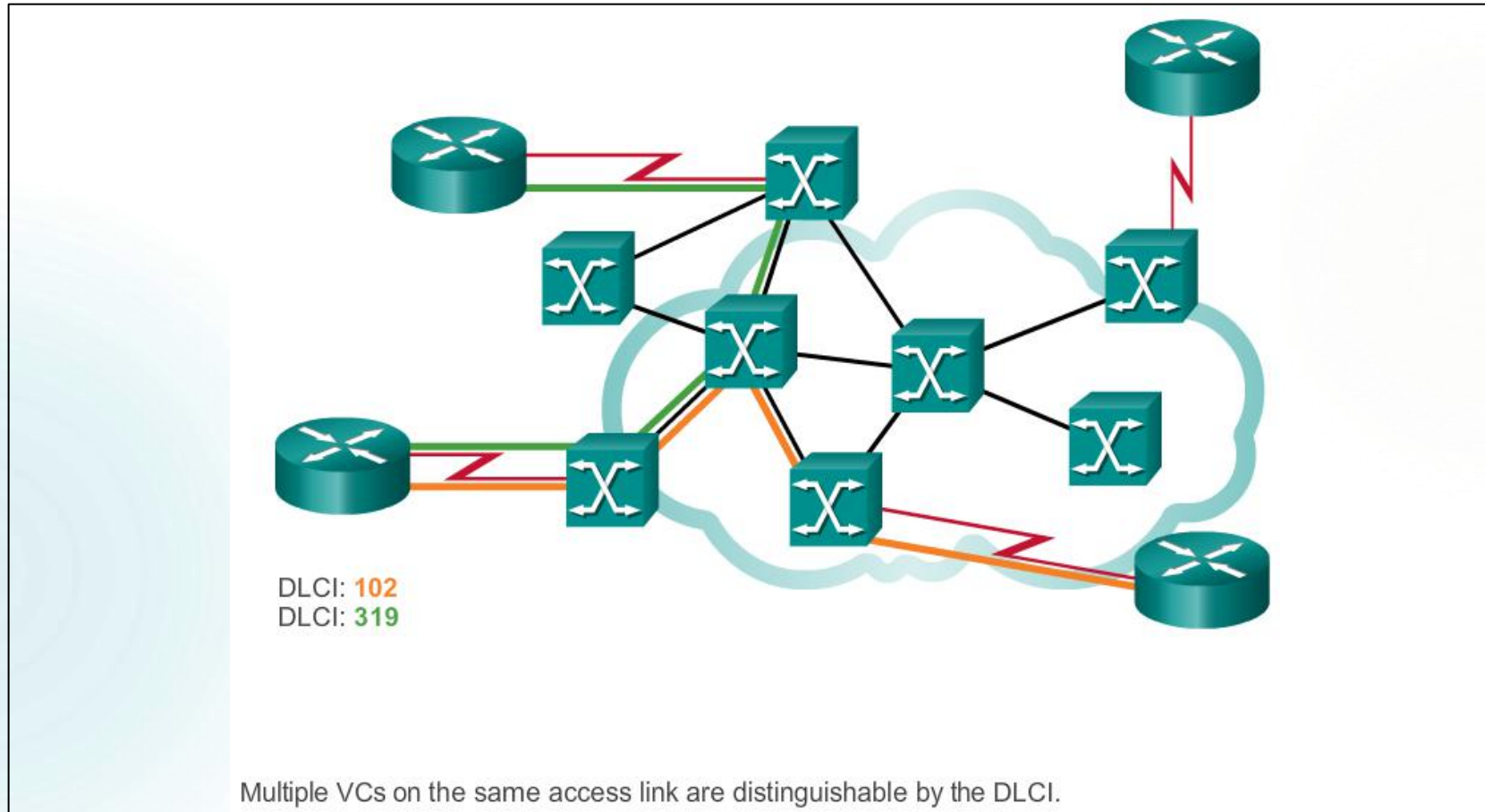


Virtual Circuits

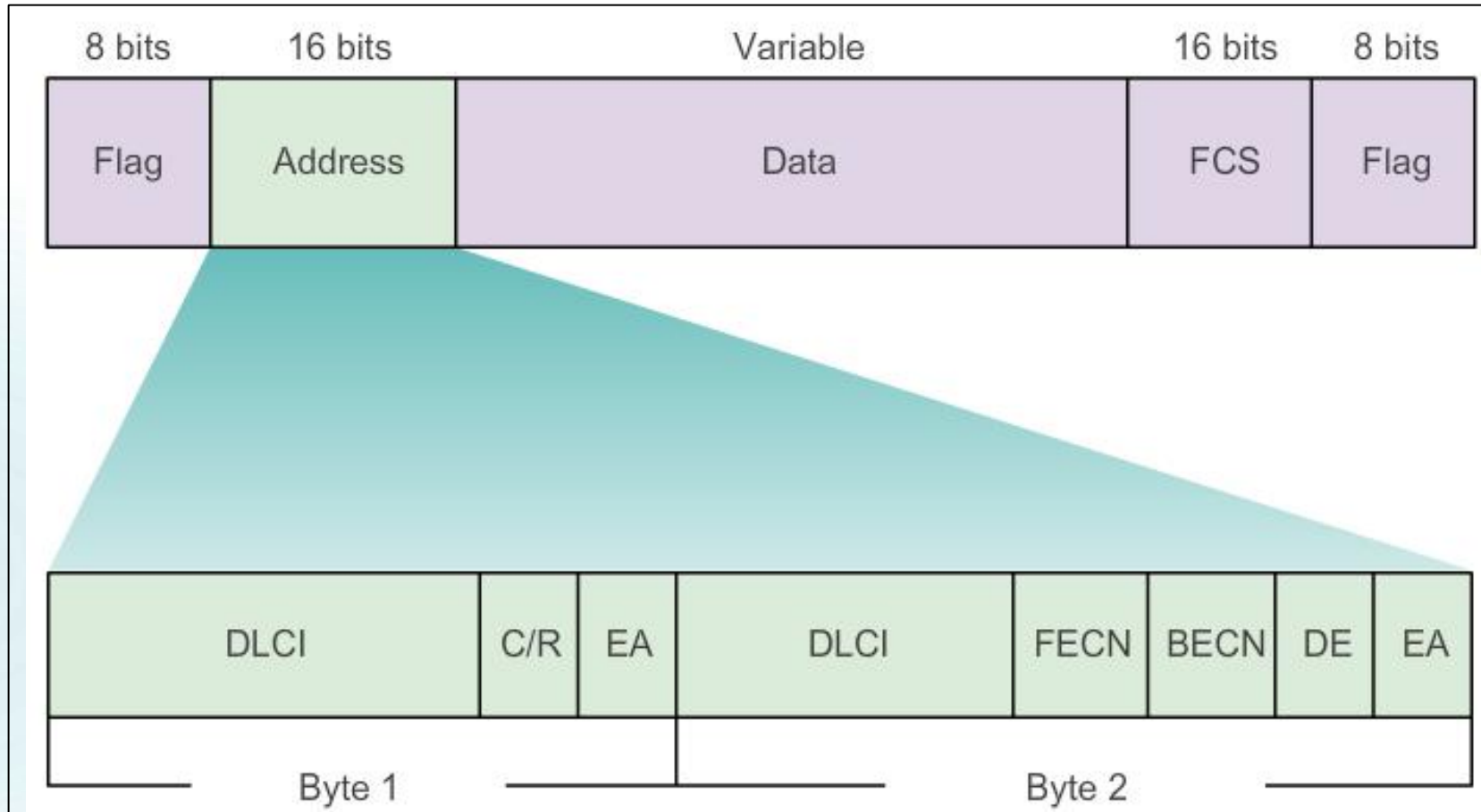
- ▶ **Switched virtual circuits (SVC)** – Established dynamically by sending signaling messages to the network.
- ▶ **Permanent virtual circuits (PVCs)** – Preconfigured by the carrier, and after they are set up, only operate in DATA TRANSFER and IDLE modes.
- ▶ VCs are identified by DLCIs. Frame Relay DLCIs have local significance, which means that the values are not unique in the Frame Relay WAN. A DLCI identifies a VC to the equipment at an endpoint.
- ▶ A DLCI has no significance beyond the single link.



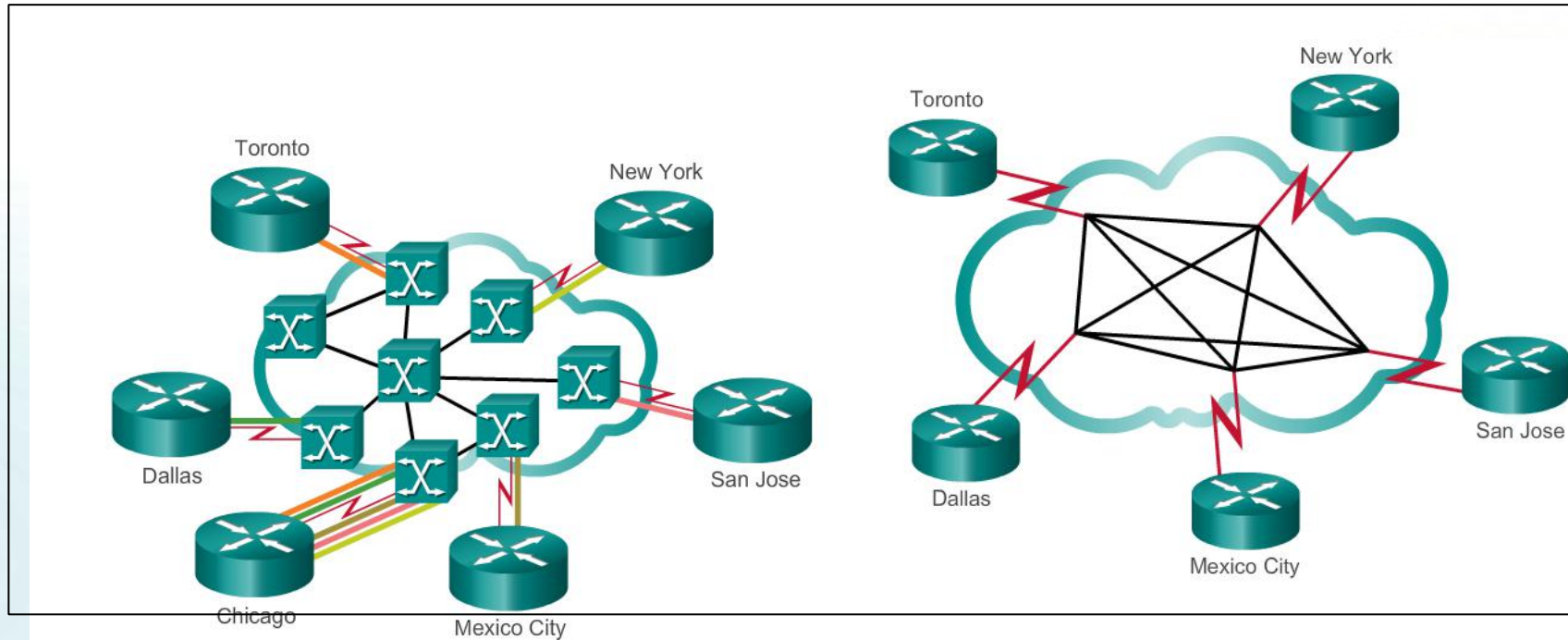
Multiple Virtual Circuits



Frame Relay Encapsulation



Frame Relay Topologies



Frame Relay Star - hub with one physical link carrying 5 VCs

Mesh Topology - Each DTE has one physical link carrying 4 VCs

Frame Relay Address Mapping

```
R1(config)# interface serial 0/0/1
R1(config-if)# ip address 10.1.1.1 255.255.255.0
R1(config-if)# encapsulation frame-relay
R1(config-if)# no frame-relay inverse-arp
R1(config-if)# frame-relay map ip 10.1.1.2 102 broadcast
cisco
R1(config-if)# no shutdown
R1(config-if)#
*Mar 31 18:57:38.994: %LINK-3-UPDOWN: Interface Serial0/0/1,
changed state to up
R1(config-if)#
```

```
R1# show frame-relay map
Serial0/0/1 (up): ip 10.1.1.2 dlci 102(0x66,0x1860), static,
                    broadcast,
                    CISCO, status defined, active
R1#
```



Local Management Interface (LMI)

```
R1# show frame-relay lmi
```

```
LMI Statistics for interface Serial0/0/1 (Frame Relay DTE)
```

```
LMI TYPE = CISCO
```

```
Invalid Unnumbered info 0Invalid Prot Disc 0
```

```
Invalid dummy Call Ref 0Invalid Msg Type 0
```

```
Invalid Status Message 0Invalid Lock Shift 0
```

```
Invalid Information ID 0Invalid Report IE Len 0
```

```
Invalid Report Request 0Invalid Keep IE Len 0
```

```
Num Status Enq. Sent 368Num Status msgs Rcvd 369
```

```
Num Update Status Rcvd 0Num Status Timeouts 0
```

```
Last Full Status Req 00:00:29Last Full Status Rcvd 00:00:29
```

```
R1#
```



LMI Extensions

- ▶ VC status messages
- ▶ Multicasting
- ▶ Global addressing
- ▶ Simple flow control

VC Identifiers	VC Types
0	LMI (ANSI, ITU)
1..15	Reserved for future use
992..1007	CLLM
1008..1022	Reserved for future use (ANSI, ITU)
1019..1020	Multicasting (Cisco)
1023	LMI (Cisco)



Frame Relay Operation

Using LMI and Inverse ARP to Map Addresses

1. The Inverse ARP request includes the source hardware, source Layer 3 protocol address, and the known target hardware address.
2. The Inverse ARP request fills the target Layer 3 protocol address field with all zeroes. It encapsulates the packet for the specific network and sends it directly to the destination device using the VC.
3. Upon receiving an Inverse ARP request, the destination device uses the source device's address to create its own DLCI-to-Layer 3 map.
4. It then sends an Inverse ARP response that includes its Layer 3 address information.
5. When the source device receives the Inverse ARP response, it completes the DLCI-to-Layer 3 map using the provided information.

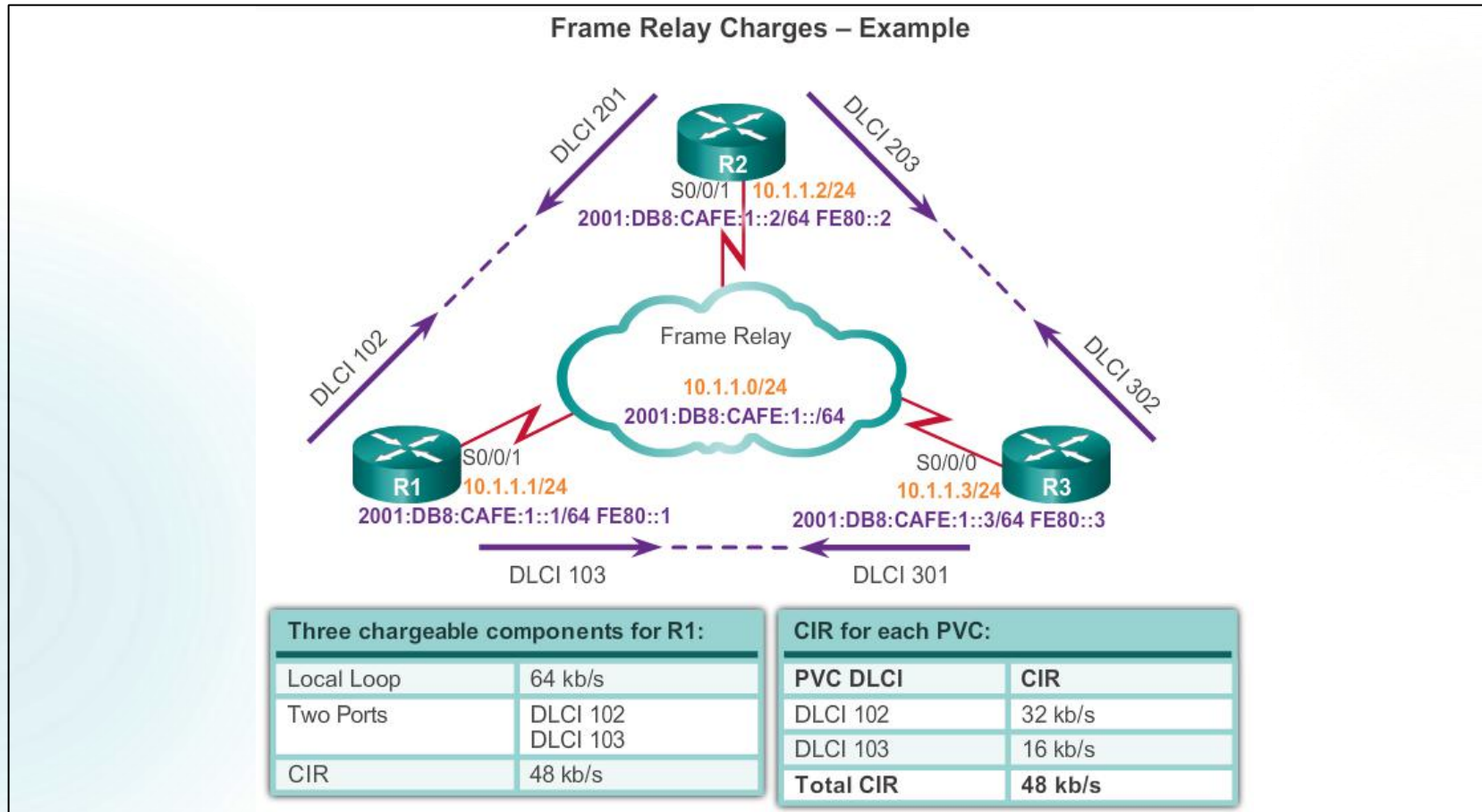


Access Rate and Committed Information Rate

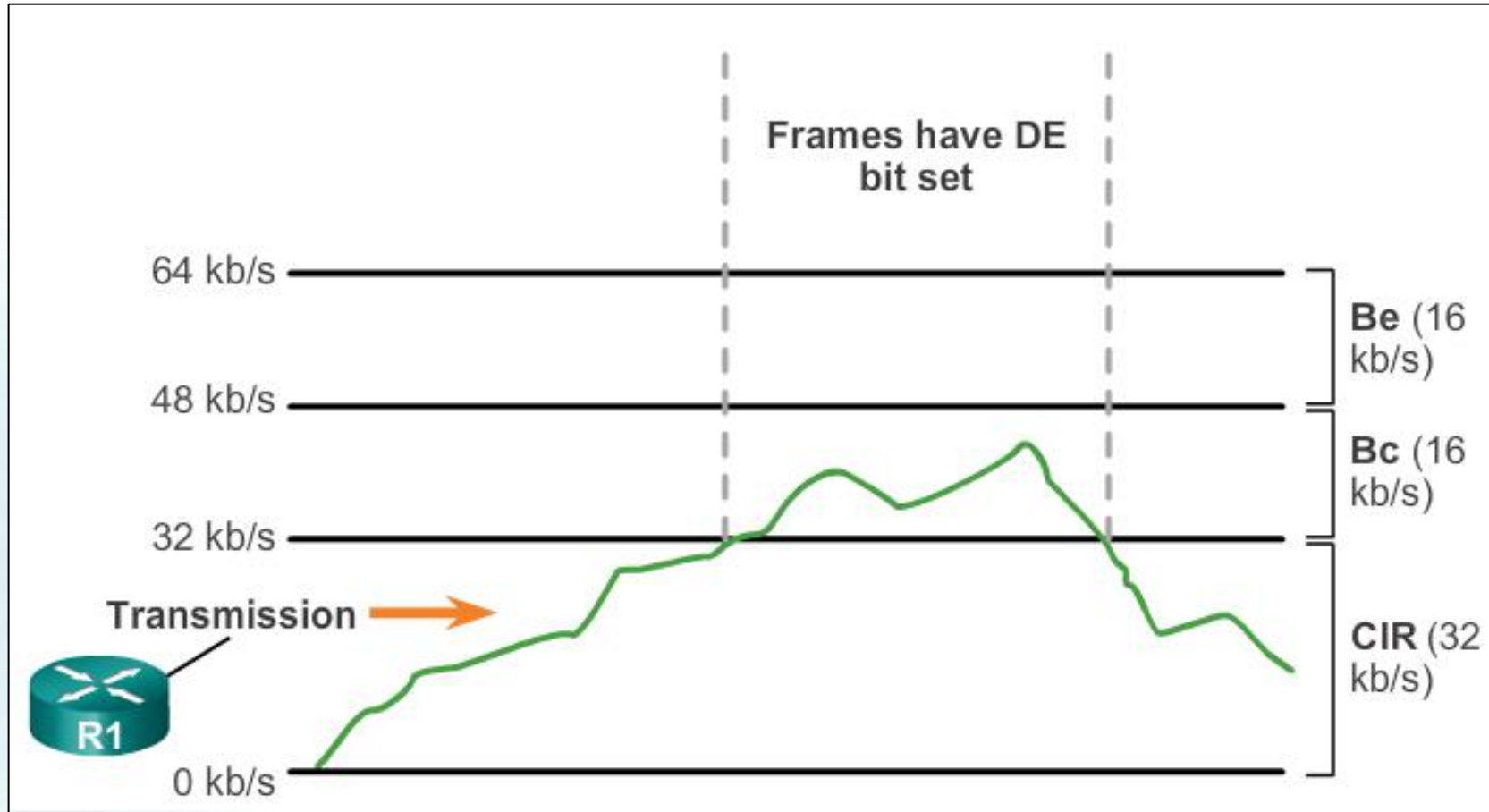
Term	Access
Access Rate	The capacity of the local loop.
Committed Information Rate (CIR)	The capacity through the local loop guaranteed by the provider.



Frame Relay Example



Bursting



Frame Relay Flow Control

- ▶ When the DCE sets the BECN bit to 1, it notifies devices in the direction of the source (upstream) that there is congestion on the network.
- ▶ When the DCE sets the FECN bit to 1, it notifies devices in the direction of the destination (downstream) that there is congestion on the network.
- ▶ DTE devices can set the value of the DE bit to 1 to indicate that the frame has lower importance than other frames. When the network becomes congested, DCE devices discard the frames with the DE bit set to 1 before discarding those that do not.

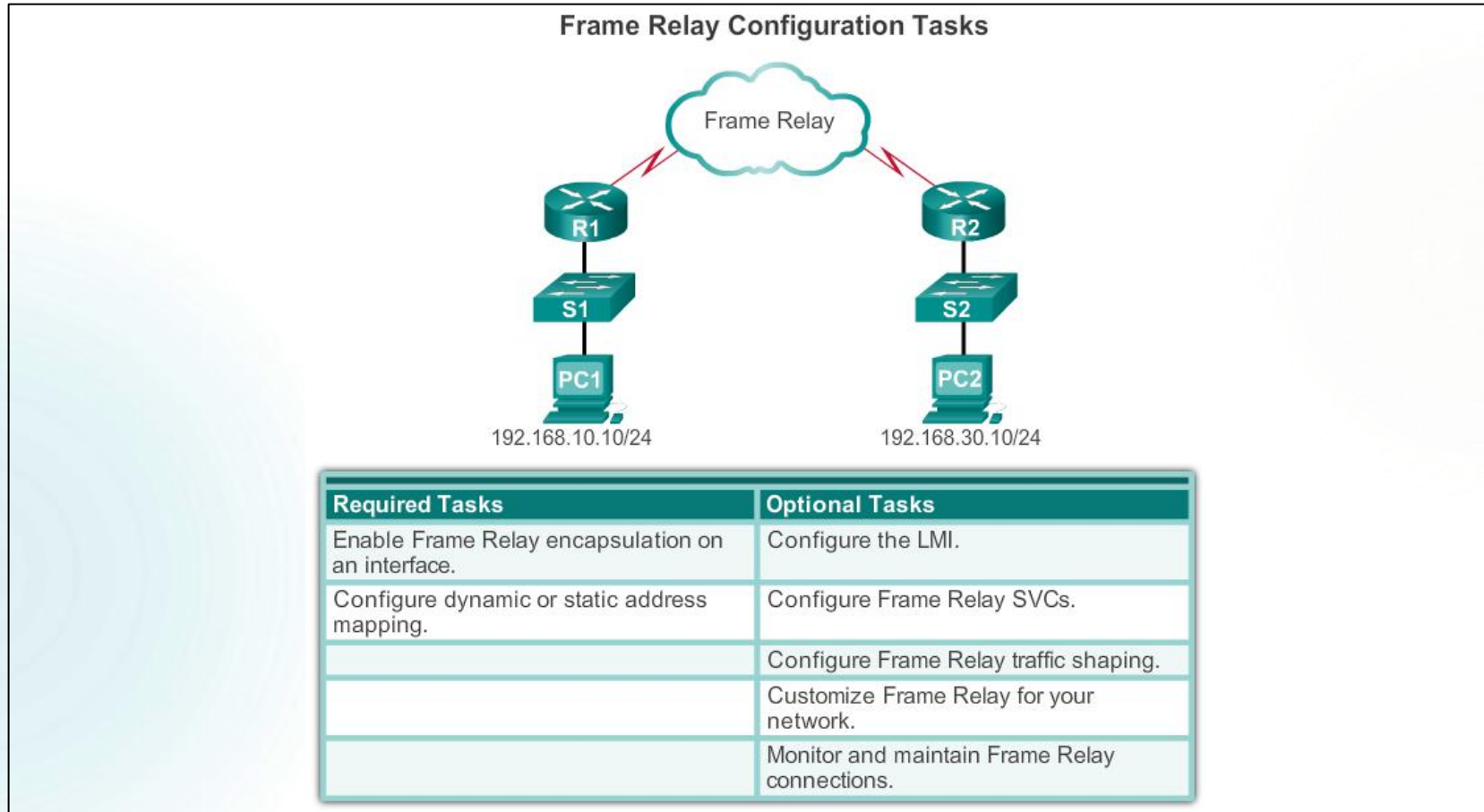


4.2 Configuring Frame Relay



Configure Basic Frame Relay

Basic Frame Relay Configuration Steps



Configuring a Static Frame Relay Map

```
frame-relay map protocol protocol-address dlci [broadcast]
```

Command Parameters	Description
<i>protocol</i>	Defines the supported protocol, bridging, or logical link control: ip (IPv4), ipv6, appletalk, decnet, dlsw, ipx, llc2, rsrb, vines and xns.
<i>protocol-address</i>	Defines the network layer address of the destination router interface.
<i>dlci</i>	Defines the local DLCI used to connect to the remote protocol address.
broadcast	(Optional) Allows broadcasts and multicasts over the virtual circuit. This permits the use of dynamic routing protocols over the VC.



Verifying a Static Frame Relay Map

```
R1# show frame-relay map
```

```
Serial0/0/1 (up): ipv6 2001:DB8:CAFE:1::2 dlci 102(0x66,0x1860),  
                  static, CISCO, status defined, active  
Serial0/0/1 (up): ipv6 FE80::2 dlci 102(0x66,0x1860), static,  
                  broadcast, CISCO, status defined, active  
Serial0/0/1 (up): ip 10.1.1.2 dlci 102(0x66,0x1860), static,  
                  broadcast, CISCO, status defined, active
```

```
R1#
```

```
R2# show frame-relay map
```

```
Serial0/0/1 (up): ipv6 2001:DB8:CAFE:1::1 dlci 201(0xC9,0x3090),  
                  static, CISCO, status defined, active  
Serial0/0/1 (up): ipv6 FE80::1 dlci 201(0xC9,0x3090), static,  
                  broadcast, CISCO, status defined, active  
Serial0/0/1 (up): ip 10.1.1.1 dlci 201(0xC9,0x3090), static,  
                  broadcast, CISCO, status defined, active
```

```
R2#
```



Reachability Issues

Frame Relay networks provide NBMA connectivity, using a hub-and-spoke topology, between remote sites. In an NBMA Frame Relay topology, when a single multipoint interface must be used to interconnect multiple sites, routing update reachability issues may result.

Reachability Issues:

- ▶ Split horizon
- ▶ Broadcast/multicast replication
- ▶ Neighbor Discovery: DR and BDR



Solving Reachability Issues

- ▶ **Disable split horizon** – One method for solving the reachability issues that are produced by split horizon may be to turn off split horizon; however, disabling split horizon increases the chances of routing loops in your network.
- ▶ **Full-meshed topology** – Another method is to use a full-meshed topology; however, this topology increases costs.
- ▶ **Subinterfaces** – In a hub-and-spoke Frame Relay topology, the hub router can be configured with logically assigned interfaces called subinterfaces.



Configure Subinterfaces

Configuring Point-to-Point Subinterfaces

Configuring Point-to-Point Subinterfaces

```
router(config-if)# interface serial number.subinterface-number  
[multipoint | point-to-point]
```

Assigning a DLCI

```
router(config-subif)# frame-relay interface-dlci dlci-number
```



Configure Subinterfaces

Example: Configuring Point-to-Point Subinterfaces

```
R1(config)# interface serial 0/0/1
R1(config-if)# encapsulation frame-relay
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface serial 0/0/1.102 point-to-point
R1(config-subif)# ip address 10.1.1.1 255.255.255.252
R1(config-subif)# bandwidth 64
R1(config-subif)# frame-relay interface-dlci 102
R1(config-fr-dlci)# exit
R1(config-subif)# exit
R1(config)# interface serial 0/0/1.103 point-to-point
R1(config-subif)# ip address 10.1.1.5 255.255.255.252
R1(config-subif)# bandwidth 64
R1(config-subif)# frame-relay interface-dlci 103
R1(config-fr-dlci)#
```



4.3 Troubleshooting Connectivity



Troubleshoot Frame Relay

Verifying Frame Relay Operation: Frame Relay Interface

```
R1# show interfaces serial 0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is GT96K Serial
  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)
  CRC checking enabled
  LMI enq sent 443, LMI stat rcvd 444, LMI up rcvd 0,
  DTE LMI up
  LMI enq rcvd 0, LMI stat sent 0, LMI up sent 0
  LMI DLCI 1023 LMI type is CISCO frame relay DTE
  FR SVC disabled, LAPF state down
  Broadcast queue 0/64, broadcasts sent/dropped 1723/0,
  interface broadcasts 1582
  Last input 00:00:01, output 00:00:01, output hang never
<output omitted>
```



Troubleshoot Frame Relay

Verifying Frame Relay Operation: LMI Operations

```
R1# show frame-relay lmi
```

```
LMI Statistics for interface  
Serial0/0/1
```

```
(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 578
```

```
Num Status msgs Rcvd 579
```

```
Num Update Status Rcvd 0
```

```
Num Status Timeouts 0
```

```
Last Full Status Req 00:00:28
```

```
Last Full Status Rcvd 00:00:28
```

```
R1#
```



Verifying Frame Relay Operation: PVC Status

```
R1# show frame-relay pvc 102
```

```
PVC Statistics for interface Serial0/0/1 (Frame Relay DTE)
```

```
DLCI = 102, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE,  
INTERFACE = Serial0/0/1.102
```

input pkts 1230	output pkts 1243	in bytes 103826
out bytes 105929	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 1228	out bcast bytes 104952	
5 minute input rate 0 bits/sec, 0 packets/sec		
5 minute output rate 0 bits/sec, 0 packets/sec		
pvc create time 01:38:29, last time pvc status changed 01:26:19		

```
R1#
```



Troubleshoot Frame Relay

Verifying Frame Relay Operation: Inverse ARP

```
R1# clear frame-relay inarp
R1# show frame-relay map
Serial0/0/1.102 (up): point-to-point dlci, dlci 102(0x66,0x1860),
broadcast status defined, active
Serial0/0/1.103 (up): point-to-point dlci, dlci 103(0x67,0x1870),
broadcast status defined, active
R1#
```

```
R2# clear frame-relay inarp
R2# show frame-relay map
Serial0/0/1.201 (up): point-to-point dlci, dlci 201(0xC9,0x3090),
broadcast status defined, active
Serial0/0/1.203 (up): point-to-point dlci, dlci 203(0xCB,0x30B0),
broadcast status defined, active
R2#
```

```
R3# show frame-relay map
Serial0/0/0 (up): ip 10.1.1.9 dlci 302(0x12E,0x48E0), dynamic,
broadcast, CISCO, status defined, active
R3#
```



Troubleshooting Frame Relay Operation

```
R1# debug frame lmi
Frame Relay LMI debugging is on
Displaying all Frame Relay LMI data
R1#
*Apr 1 14:57:43.559: Serial0/0/1(in): Status, myseq 22, pak size 29
*Apr 1 14:57:43.559: RT IE 1, length 1, type 0
*Apr 1 14:57:43.559: KA IE 3, length 2, yourseq 22, myseq 22
*Apr 1 14:57:43.559: PVC IE 0x7 , length 0x6 , dlci 102, status 0x2 , bw 0
*Apr 1 14:57:43.559: PVC IE 0x7 , length 0x6 , dlci 103, status 0x2 , bw 0
R1#
*Apr 1 14:57:53.555: Serial0/0/1(out): StEnq, myseq 23, yourseen 22, DTE up
*Apr 1 14:57:53.555: datagramstart = 0xED802AF4, datagramsize = 13
*Apr 1 14:57:53.555: FR encap = 0xFCF10309
*Apr 1 14:57:53.555: 00 75 01 01 03 02 17 16
*Apr 1 14:57:53.555:
*Apr 1 14:57:53.559: Serial0/0/1(in): Status, myseq 23, pak size 13
*Apr 1 14:57:53.559: RT IE 1, length 1, type 1
*Apr 1 14:57:53.559: KA IE 3, length 2, yourseq 23, myseq 23
R1# un all
All possible debugging has been turned off
```



Chapter 4: Summary

This chapter described:

- ▶ The fundamental concepts of Frame Relay technology, including operation, implementation requirements, maps, and Local Management Interface (LMI) operation.
- ▶ How to configure a basic Frame Relay permanent virtual circuit (PVC), including configuring and troubleshooting Frame Relay on a router serial interface and configuring a static Frame Relay map.
- ▶ Advanced concepts of Frame Relay technology including subinterfaces, bandwidth and flow control.
- ▶ Advanced Frame Relay PVCs, including solving reachability issues, configuring subinterfaces, and verifying and troubleshooting a Frame Relay configuration.



Cisco | Networking Academy®

Mind Wide Open™



Wollo University-Kombolcha Institute of Technology
College of Informatics
Systems and Network Administration ©2017

Securing Site-to-Site Connectivity



Learning Objectives

After completing this chapter, students will be able to:

- Describe benefits of VPN technology.
- Describe site-to-site and remote access VPNs.
- Describe the purpose and benefits of GRE tunnels.
- Configure a site-to-site GRE tunnel.
- Describe the characteristics of IPsec.
- Explain how IPsec is implemented using the IPsec protocol framework.



Introduction

- ▶ Security is a concern when using the public Internet to conduct business.
- ▶ Virtual Private Networks (VPNs) are used to ensure the security of data across the Internet.
- ▶ A VPN is used to create a private tunnel over a public network.
- ▶ Data can be secured by using encryption in this tunnel through the Internet and by using authentication to protect data from unauthorized access.

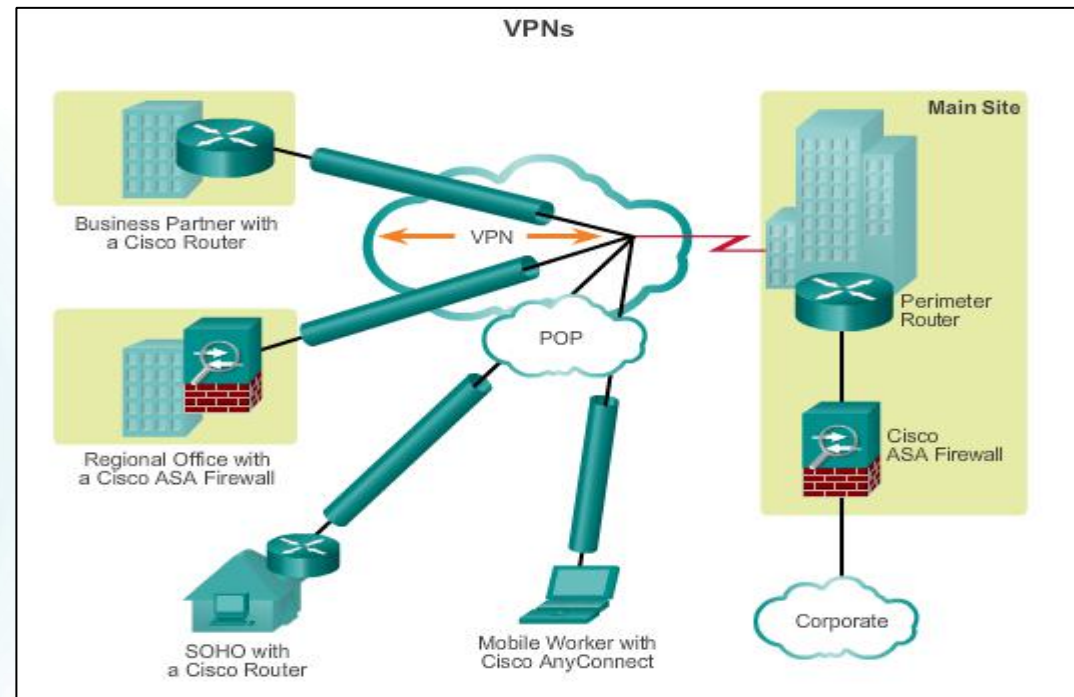


VPNs



Introducing VPNs

- ▶ VPNs are used to create an end-to-end private network connection over third-party networks, such as the Internet or extranets.
- ▶ To implement VPNs, a VPN gateway is necessary: Could be a router, a firewall, or Adaptive Security Appliance (ASA).



Benefits of VPNs

► Cost savings

- Enable organizations to use cost-effective, third-party Internet transport to connect remote offices and remote users to the main site.

► Scalability

- Enable organizations to use the Internet infrastructure within ISPs and devices, which makes it easy to add new users.



Benefits of VPNs (cont.)

► **Compatibility with broadband technology**

- Allow mobile workers and telecommuters to take advantage of high-speed, broadband connectivity, such as DSL and cable, to gain access to the networks of their organization, providing workers flexibility and efficiency.
- Provide a cost-effective solution for connecting remote offices.

► **Security**

- Can include security mechanisms that provide the highest level of security by using advanced encryption and authentication protocols that protect data from unauthorized access.



Types of VPNs

Site-to-Site VPNs

- ▶ Connect entire networks to each other, in the past, a leased line or Frame Relay connection was required to connect sites, but because most corporations now have Internet access, these connections can be replaced with site-to-site VPNs.
- ▶ Internal hosts have no knowledge that a VPN exists.
- ▶ Created when devices on both sides of the VPN connection are aware of the VPN configuration in advance.

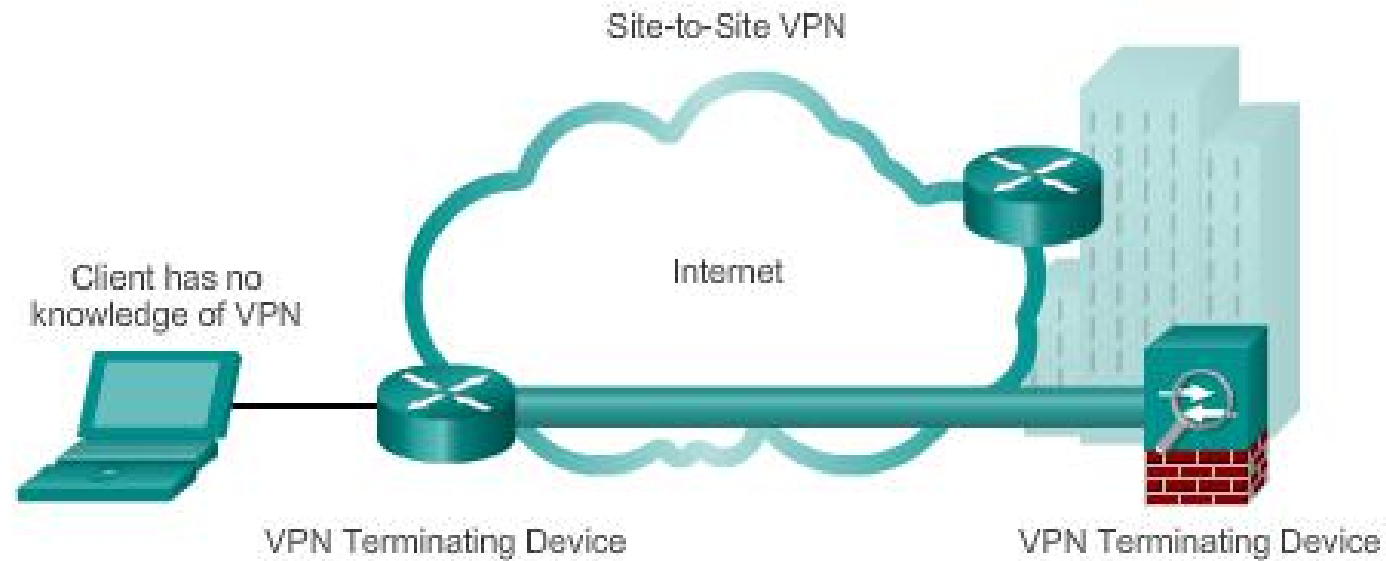


Site-to-Site VPNs (cont.)

- ▶ End hosts send and receive normal TCP/IP traffic through a VPN gateway.
- ▶ The VPN gateway is responsible for encapsulating and encrypting outbound traffic for all traffic from a particular site
- ▶ The VPN gateway then sends it through a VPN tunnel over the Internet to a peer VPN gateway at the target site.
- ▶ Upon receipt, the peer VPN gateway strips the headers, decrypts the content, and relays the packet toward the target host inside its private network.



Site-to-Site VPNs (cont.)

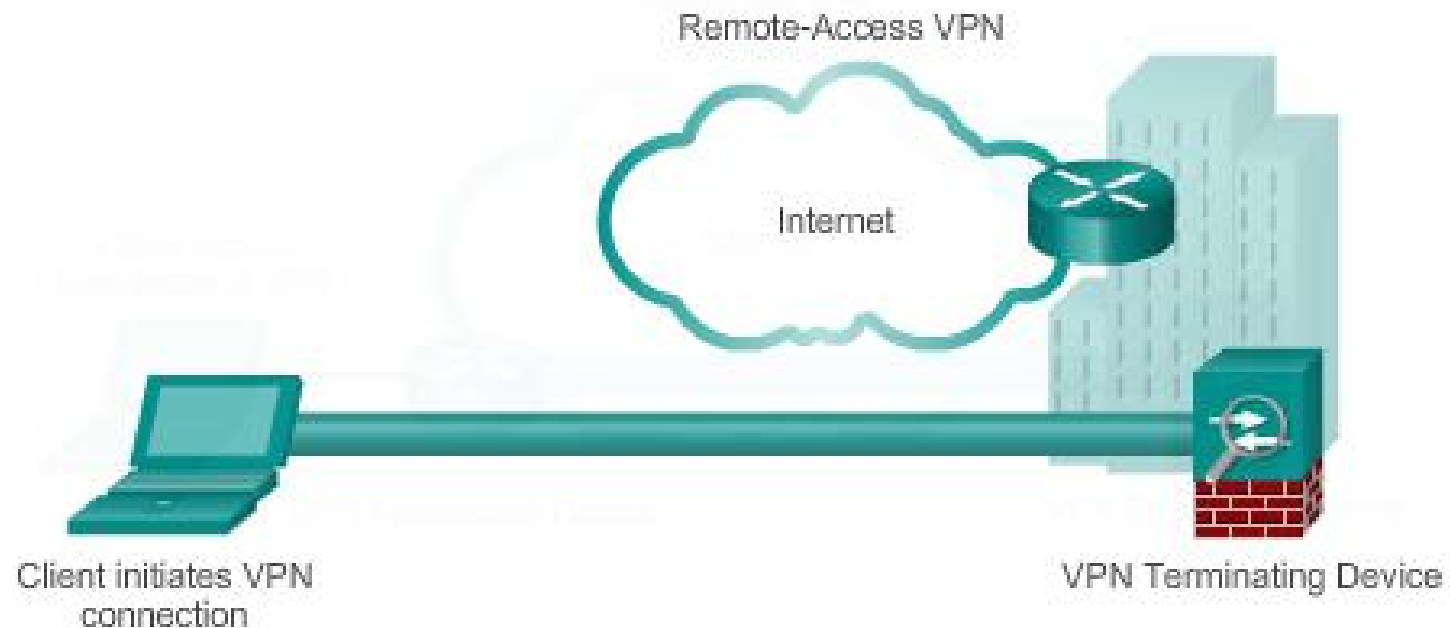


Remote Access VPNs

- Support the needs of telecommuters, mobile users, and extranet, consumer-to-business traffic.
- Support a client/server architecture, where the VPN client (remote host) gains secure access to the enterprise network via a VPN server device at the network edge.
- Used to connect individual hosts that must access their company network securely over the Internet.
- VPN client software may need to be installed on the mobile user's end device (Cisco AnyConnect Secure Mobility Client).
- When the host tries to send any traffic, the VPN Client software encapsulates and encrypts this traffic and sends over the Internet to the VPN gateway at the edge of the target network.



Remote Access VPNs (cont.)

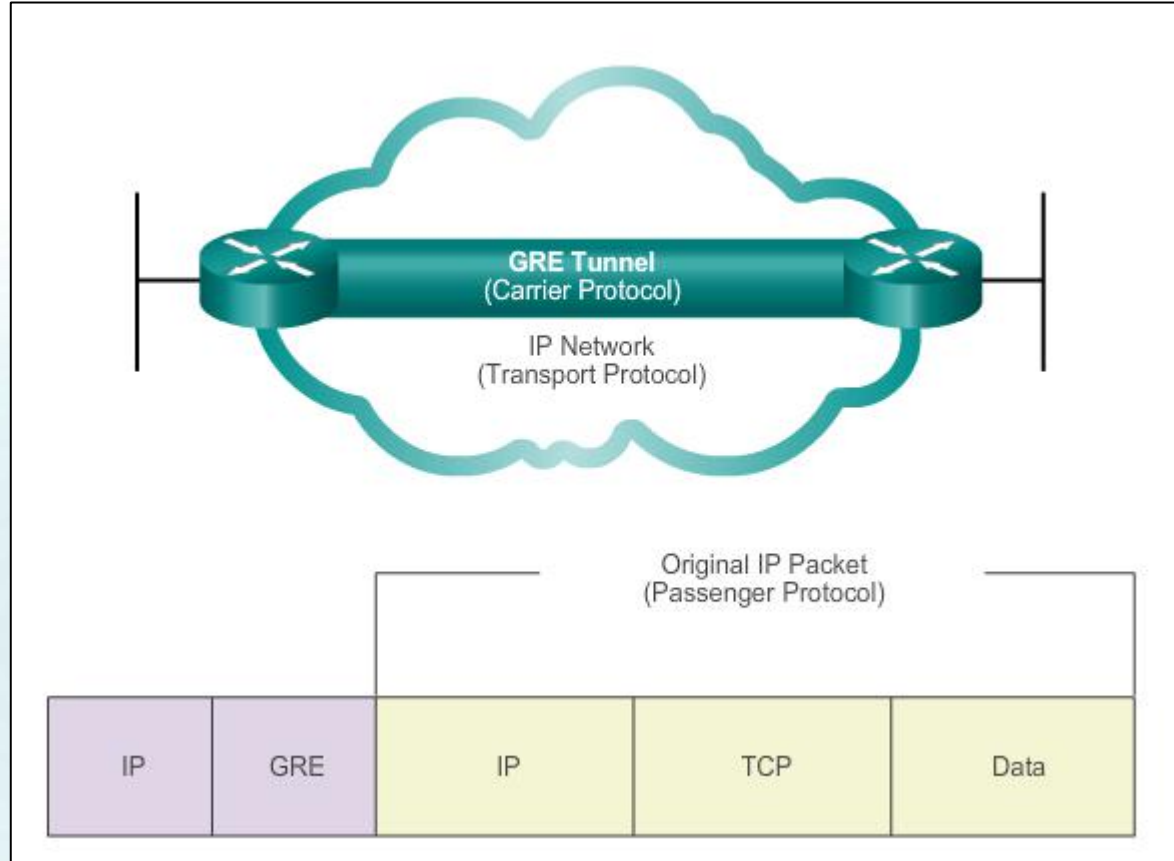


Site-to-Site GRE Tunnels



Fundamentals of Generic Routing Encapsulation

Introduction to GRE



- Basic, non-secure, site-to-site VPN tunneling protocol developed by Cisco
- Encapsulates a wide variety of protocol packet types inside IP tunnels
- Creates a virtual point-to-point link to routers at remote points, over an IP internetwork

Characteristics of GRE

GRE has these characteristics:

- GRE is defined as an IETF standard.
- IP protocol 47 is used to identify GRE packets.
- GRE encapsulation uses a protocol type field in the GRE header to support the encapsulation of any OSI Layer 3 protocol.
- GRE itself is stateless; it does not include any flow-control mechanisms, by default.
- GRE does not include any strong security mechanisms to protect its payload.
- The GRE header, together with the tunneling IP header, creates at least 24 bytes of additional overhead for tunneled packets.



Introducing IPsec



IPsec VPNs

- Information from a private network is securely transported over a public network.
- Forms a virtual network instead of using a dedicated Layer 2 connection.
- To remain private, the traffic is encrypted to keep the data confidential.



IPsec Functions

- Defines how a VPN can be configured in a secure manner using IP.
- Framework of open standards that spells out the rules for secure communications.
- Not bound to any specific encryption, authentication, security algorithms, or keying technology.
- Relies on existing algorithms to implement secure communications.
- Works at the network layer, protecting and authenticating IP packets between participating IPsec devices.
- Secures a path between a pair of gateways, a pair of hosts, or a gateway and host.
- All implementations of IPsec have a plaintext Layer 3 header, so there are no issues with routing.
- Functions over all Layer 2 protocols, such as Ethernet, ATM, or Frame Relay.



IPsec Characteristics

IPsec characteristics can be summarized as follows:

- IPsec is a framework of open standards that is algorithm-independent.
- IPsec provides data confidentiality, data integrity, and origin authentication.
- IPsec acts at the network layer, protecting and authenticating IP packets.



IPsec Security Services

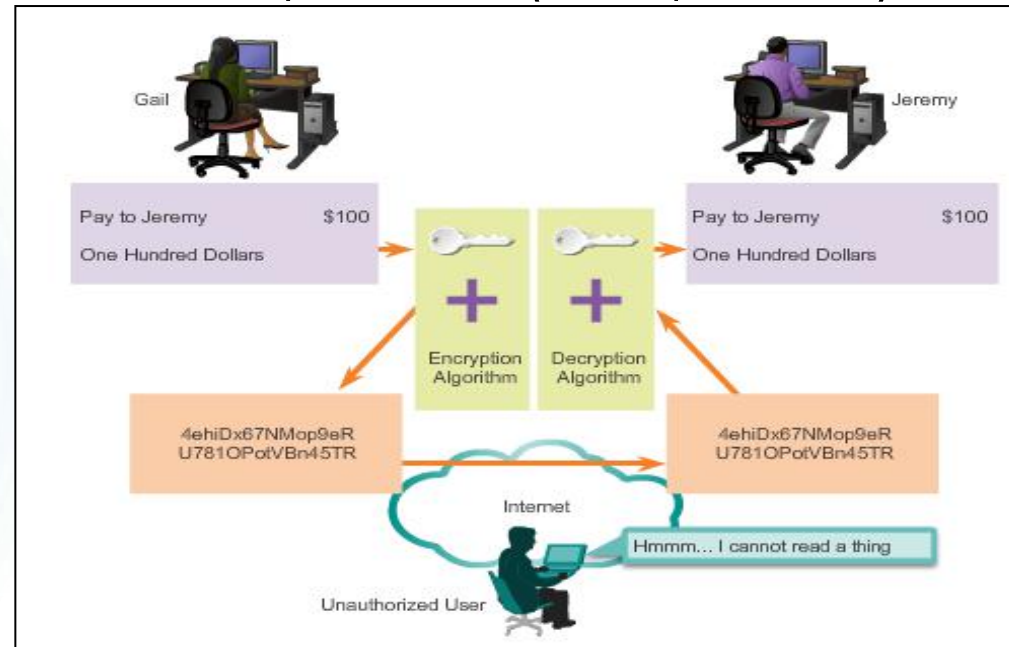
- **Confidentiality (encryption)** – encrypt the data before transmitting across the network
- **Data integrity** – verify that data has not been changed while in transit, if tampering is detected, the packet is dropped
- **Authentication** – verify the identity of the source of the data that is sent, ensures that the connection is made with the desired communication partner, IPsec uses Internet Key Exchange (IKE) to authenticate users and devices that can carry out communication independently.
- **Anti-Replay Protection** – detect and reject replayed packets and helps prevent spoofing

CIA: confidentiality, integrity, and authentication



Confidentiality with Encryption

- For encryption to work, both the sender and the receiver must know the rules used to transform the original message into its coded form.
- Rules are based on algorithms and associated keys.
- Decryption is extremely difficult (or impossible) without the correct key.



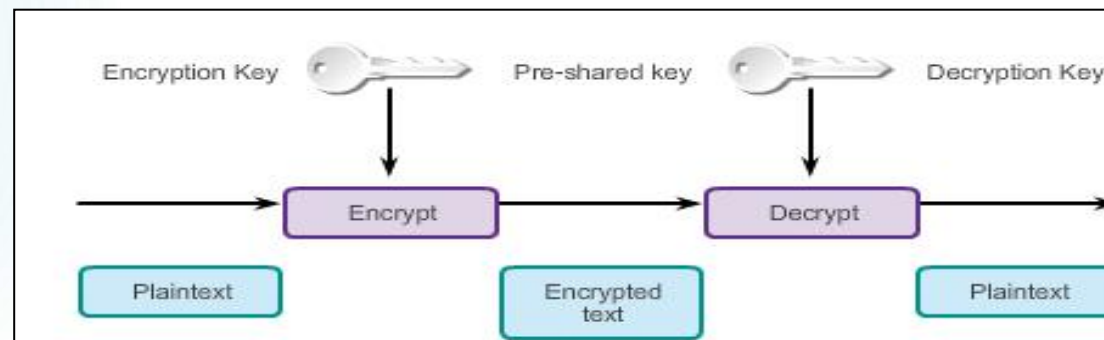
Encryption Algorithms

- As key length increases, it becomes more difficult to break the encryption. However, a longer key requires more processor resources when encrypting and decrypting data.
- Two main types of encryption are:
 - Symmetric Encryption
 - Asymmetric Encryption



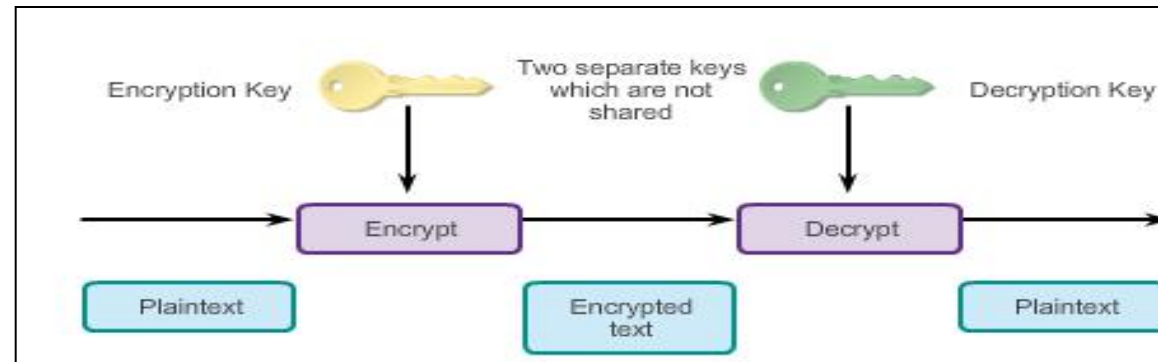
Symmetric Encryption

- Encryption and decryption use the same key.
- Each of the two networking devices must know the key to decode the information.
- Each device encrypts the information before sending it over the network to the other device.
- Typically used to encrypt the content of the message.
- Examples: DES and 3DES (no longer considered secure) and AES (256-bit recommended for IPsec encryption).



Asymmetric Encryption

- Uses different keys for encryption and decryption.
- Knowing one of the keys does not allow a hacker to deduce the second key and decode the information.
- One key encrypts the message, while a second key decrypts the message.
- Public key encryption is a variant of asymmetric encryption that uses a combination of a private key and a public key.
- Typically used in digital certification and key management
- Example: RSA

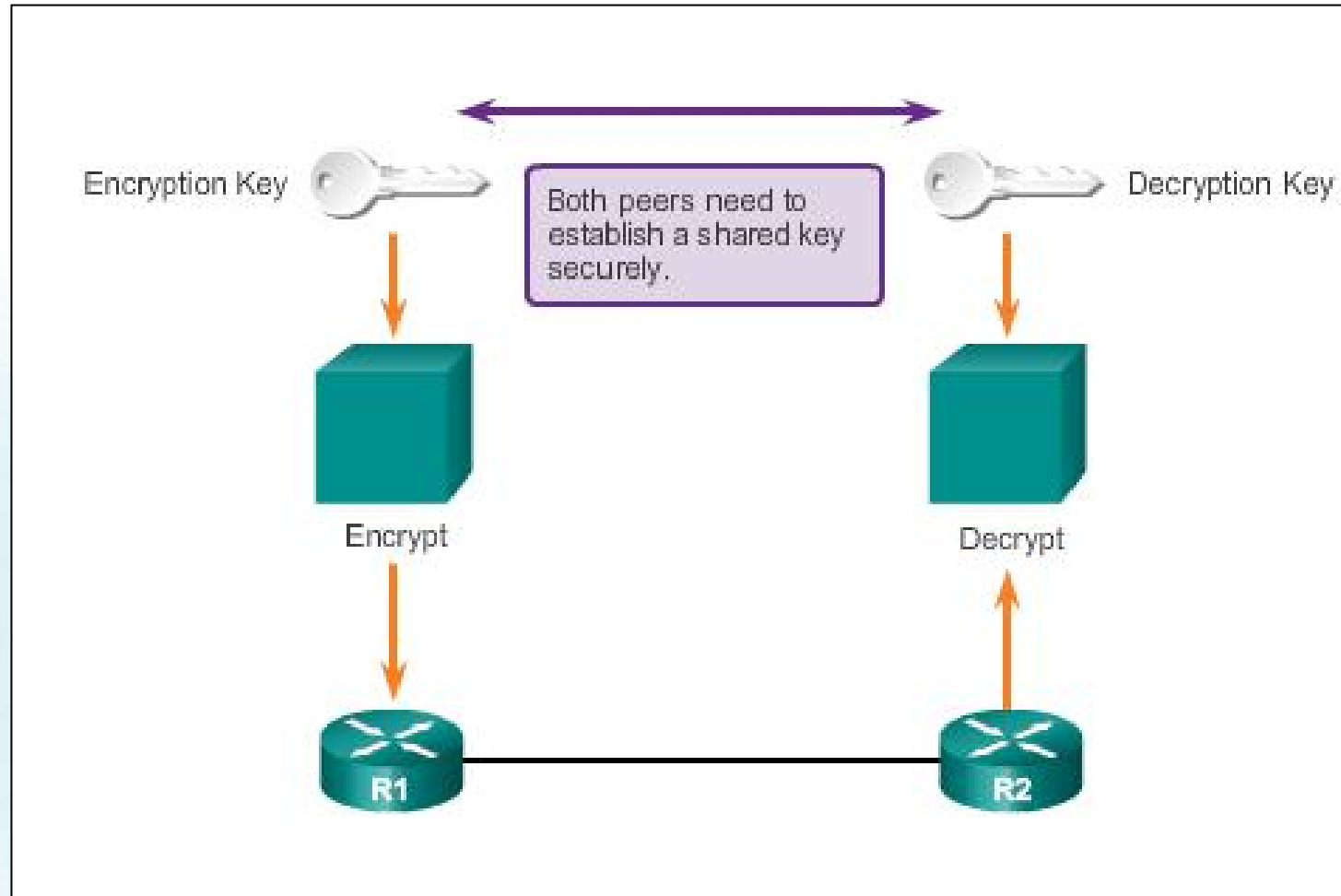


Diffie-Hellman Key Exchange

- Diffie-Hellman (DH) is not an encryption mechanism and is not typically used to encrypt data.
- DH is a method to securely exchange the keys that encrypt data.
- DH algorithms allow two parties to establish a shared secret key used by encryption and hash algorithms.
- DH is part of the IPsec standard.
- Encryption algorithms, such as DES, 3DES, and AES, as well as the MD5 and SHA-1 hashing algorithms, require a symmetric, shared secret key to perform encryption and decryption.
- DH algorithm specifies a public key exchange method that provides a way for two peers to establish a shared secret key that only they know, although they are communicating over an insecure channel.



Diffie-Hellman Key Exchange

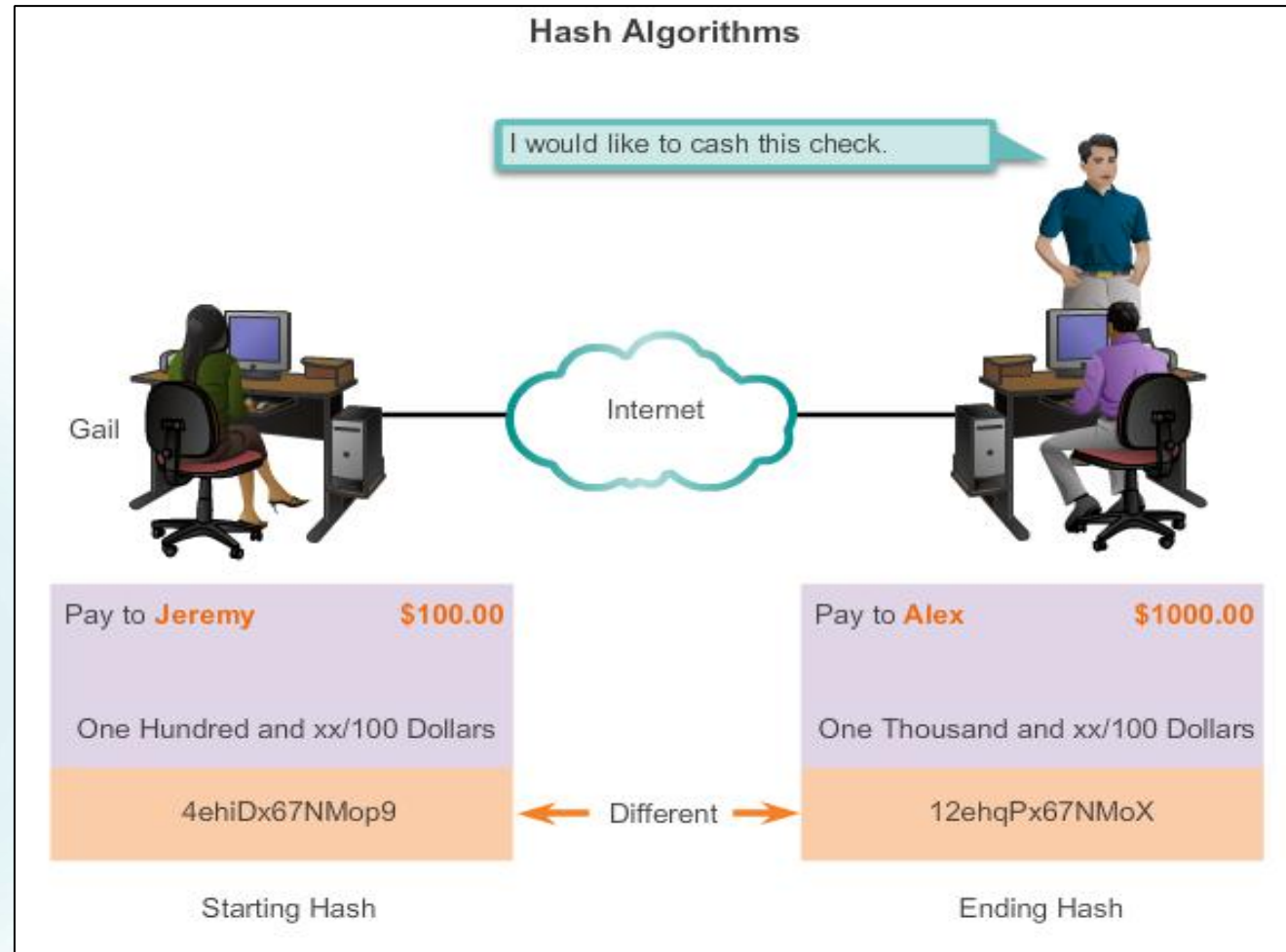


Integrity with Hash Algorithms

- The original sender generates a hash of the message and sends it with the message itself.
- The recipient parses the message and the hash, produces another hash from the received message, and compares the two hashes.
- If they are the same, the recipient can be reasonably sure of the integrity of the original message.



Integrity with Hash Algorithms (cont.)



Integrity with Hash Algorithms (cont.)

Hash-based Message Authentication Code (HMAC) is a mechanism for message authentication using hash functions.

- HMAC has two parameters: A message input and a secret key known only to the message originator and intended receivers.
- Message sender uses an HMAC function to produce a value (the message authentication code) formed by condensing the secret key and the message input.
- Message authentication code is sent along with the message.
- Receiver computes the message authentication code on the received message using the same key and HMAC function as the sender used.
- Receiver compares the result that is computed with the received message authentication code.
- If the two values match, the message has been correctly received and the receiver is assured that the sender is a user community member who share the key.



Integrity with Hash Algorithms (cont.)

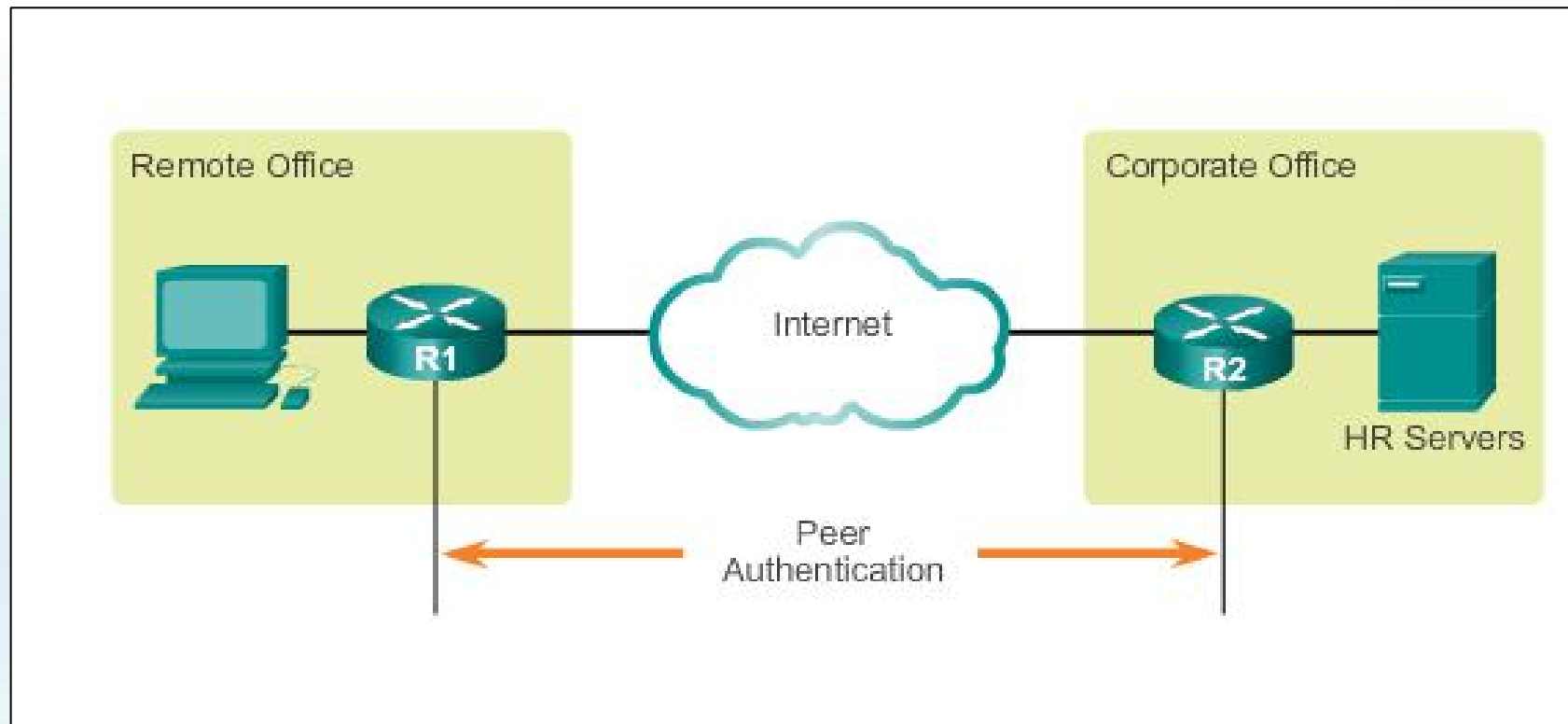
There are two common HMAC algorithms:

- **MD5** – Uses a 128-bit shared secret key. The variable-length message and 128-bit shared secret key are combined and run through the HMAC-MD5 hash algorithm. The output is a 128-bit hash. The hash is appended to the original message and forwarded to the remote end.
- **SHA** – SHA-1 uses a 160-bit secret key. The variable-length message and the 160-bit shared secret key are combined and run through the HMAC-SHA1 hash algorithm. The output is a 160-bit hash. The hash is appended to the original message and forwarded to the remote end.



IPsec Authentication

- IPsec VPNs support authentication.
- Device on the other end of the VPN tunnel must be authenticated before the communication path is considered secure.



IPsec Authentication (cont.)

There are two peer authentication methods, PSK and RSA signatures:

- **PSK**

- A secret key shared between the two parties using a secure channel before it needs to be used.
- Use symmetric key cryptographic algorithms.
- A PSK is entered into each peer manually and is used to authenticate the peer.



IPsec Authentication (cont.)

- **RSA signatures**

- Digital certificates are exchanged to authenticate peers.
- Local device derives a hash and encrypts it with its private key.
- Encrypted hash, or digital signature, is attached to the message and forwarded to the remote end.
- At the remote end, the encrypted hash is decrypted using the public key of the local end.
- If the decrypted hash matches the recomputed hash, the signature is genuine.



IPsec Protocol Framework

Authentication Header (AH)

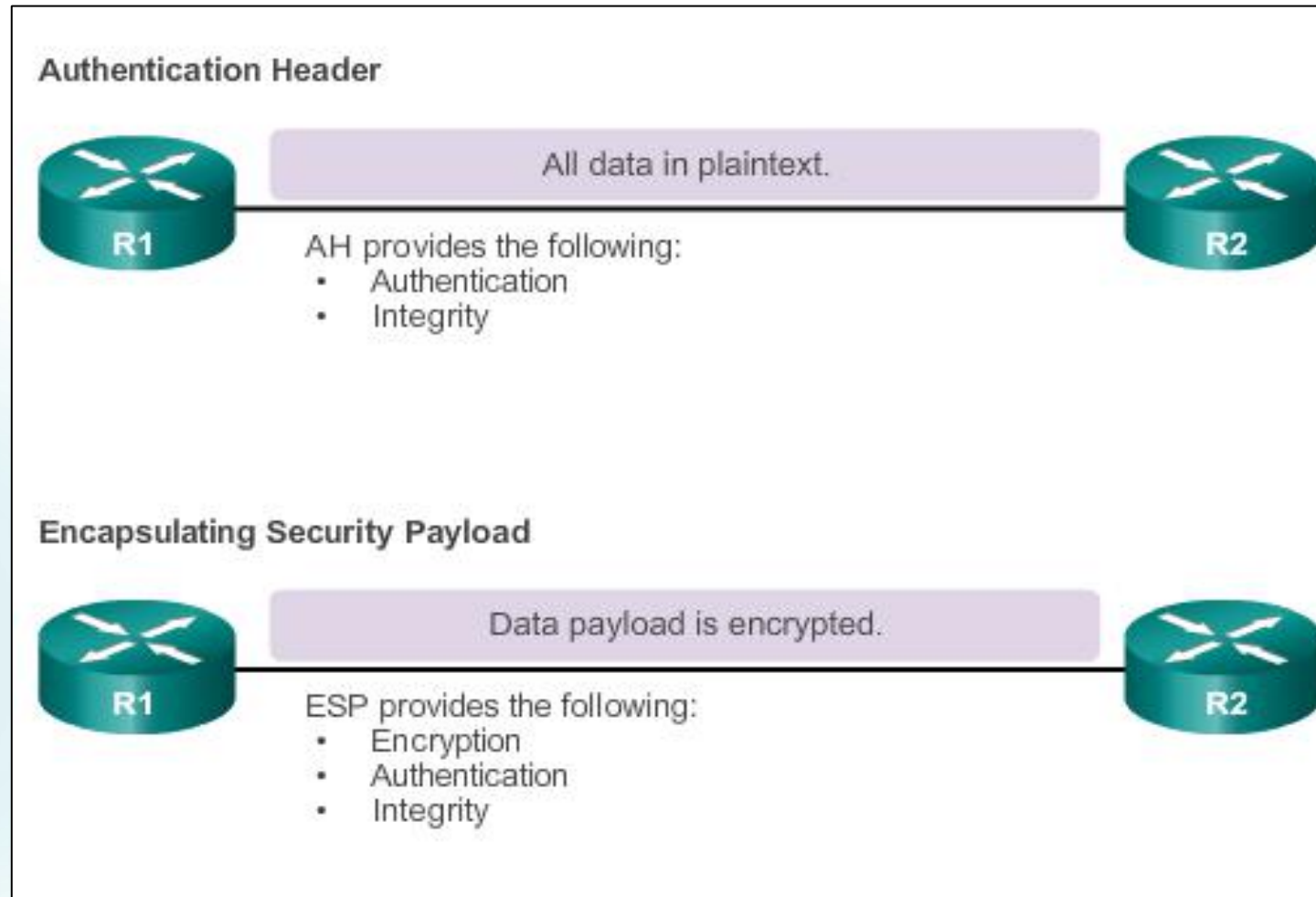
- Appropriate protocol to use when confidentiality is not required or permitted.
- Provides data authentication and integrity for IP packets that are passed between two systems.
- Does not provide data confidentiality (encryption) of packets.

Encapsulating Security Payload (ESP)

- A security protocol that provides confidentiality and authentication by encrypting the IP packet.
- Authenticates the inner IP packet and ESP header.
- Both encryption and authentication are optional in ESP, at a minimum, one of them must be selected.



IPsec Protocol Framework (cont.)



IPsec Protocol Framework (cont.)

Four basic building block of the IPsec framework that must be selected:

- **IPsec framework protocol** – A combination of ESP and AH, ESP or ESP+AH options are almost always selected because AH itself does not provide encryption.
- **Confidentiality** (if IPsec is implemented with ESP) – DES, 3DES, or AES, AES is strongly recommended since provides the greatest security.
- **Integrity** – Guarantees that the content has not been altered in transit using hash algorithms (MD5 or SHA).
- **Authentication** – Represents how devices on either end of the VPN tunnel are authenticated (PSK or RSA).
- **DH algorithm group** – Represents how a shared secret key is established between peers, DH24 provides the greatest security.



IPsec Protocol Framework (cont.)

