



Chapter 1: WAN Concepts



Connecting Networks

Cisco | Networking Academy®
Mind Wide Open™



Chapter 1 - Sections & Objectives

- 1.1 WAN Technologies Overview
 - Explain WAN access technologies available to small to medium-sized business networks.
- 1.2 Selecting a WAN Technology
 - Select WAN access technologies to satisfy business requirements.
- Contextual Examples
 - Choosing a WAN Link connection
 - Using VPNs to support WAN infrastructure



1.1 WAN Technologies Overview



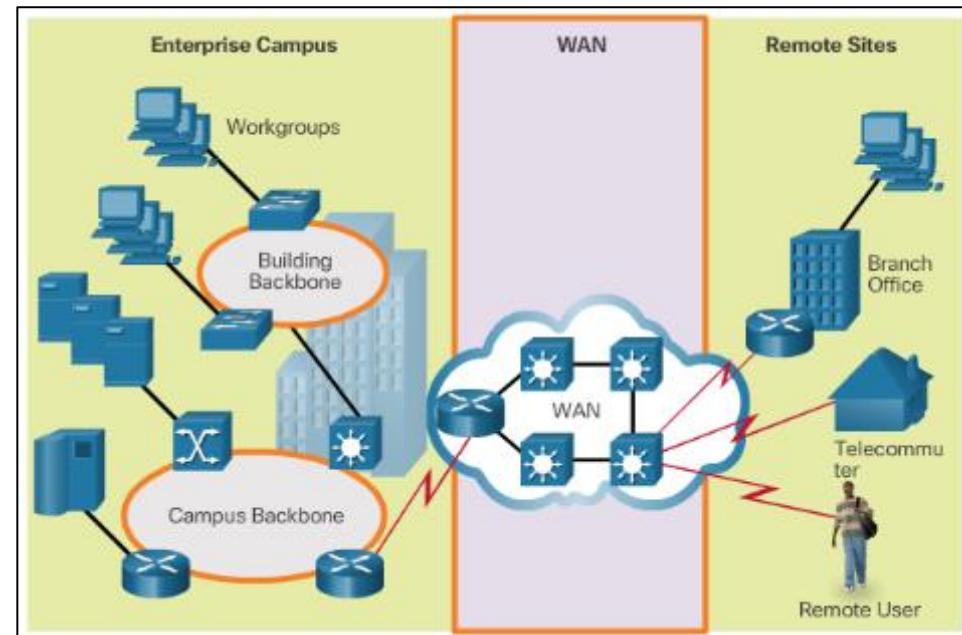
Cisco | Networking Academy®
Mind Wide Open™



WAN Technologies Overview

Purpose of WANs *

- WANs connect LANs
- WANs are used to **connect remote geographically separate sites to the enterprise network.**
 - e.g. connect remote branch offices to main enterprise network.
 - Support business communications requirements
- WANs connect home users to the Internet.
- Enterprise networks are using security and privacy solutions over the Internet to connect remote sites and users.





WAN Technologies Overview

Purpose of WANs *

- Common WAN topologies (advantages/disadvantages):: *

- Point-to-Point**

- Point-to-point circuit between two endpoints
- Usually dedicated leased-line (T1/E1)
- Expensive

- Hub-and-Spoke**

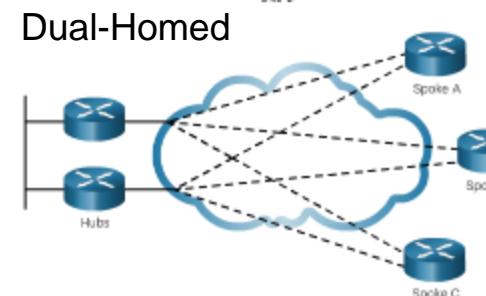
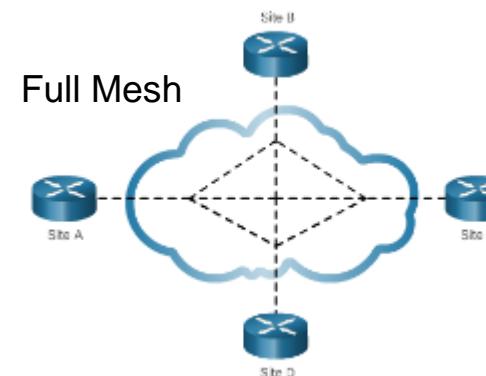
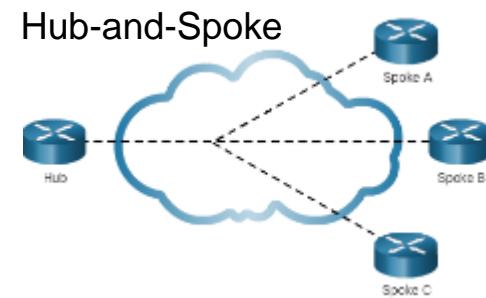
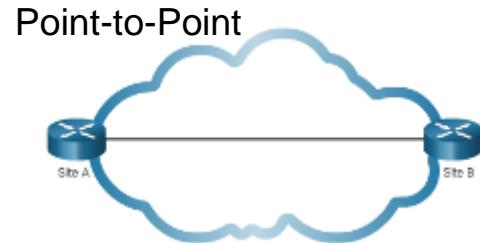
- A single-homed, point-to-multipoint topology
- Allows connection between multiple sites
- All spoke circuits share a single interface to the hub via virtual interfaces. All traffic goes through the hub
- Hub could be **single point of failure**

- Full Mesh**

- Each router has a connection to every other router; requires a **large number of virtual interfaces**
- Full mesh requires **a lot of maintenance** to configure virtual interfaces

- Dual-homed**

- Provides **redundancy** for a single-homed, hub-and-spoke topology by providing a second hub to connect to spoke routers
- Dual homed are more **expensive** and more **complex**.

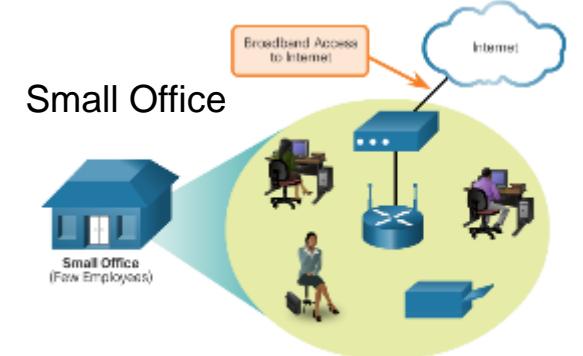




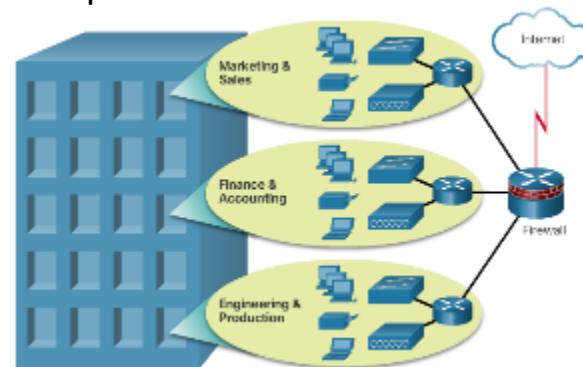
WAN Technologies Overview

Purpose of WANs

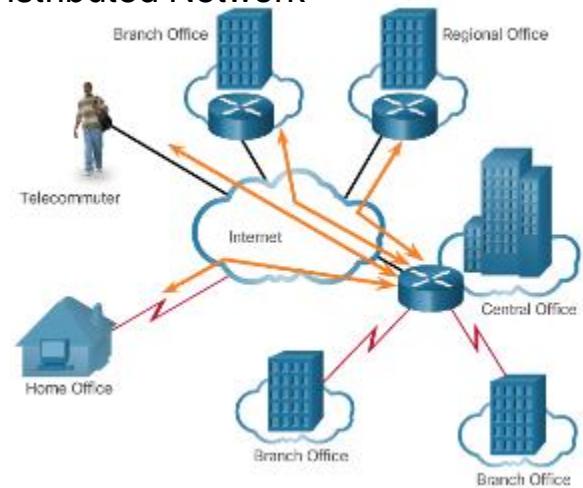
- As businesses grow, the topologies and WAN strategies change:
 - Small Office** – These businesses typically consist of one LAN at one location that connects to the Internet through a broadband technology.
 - Campus Network** – A small- to medium-sized business with one location and multiple LANs uses specialized equipment and technologies to connect to the Internet.
 - Branch Networks** – As the business grows, it adds more branch offices, each with its own campus network. WAN contracts to connect the remote networks are negotiated.
 - Distributed Network** – A multinational business has a network distributed across the globe. These businesses have complex WAN strategies to securely connect to regional offices, branch offices, partners, and telecommuters.



Campus Network



Distributed Network

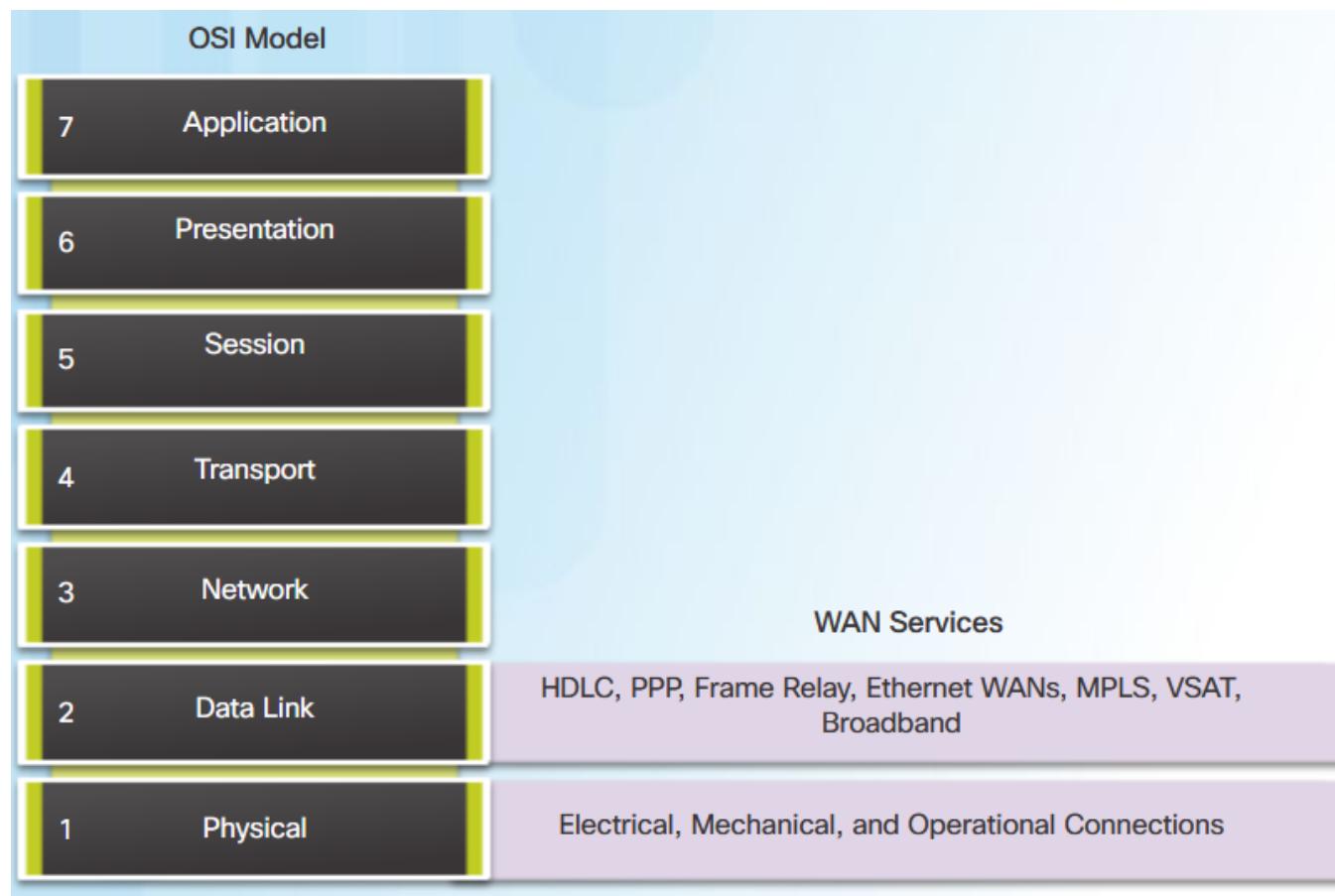




WAN Operations

WANs in the OSI Model

WAN access standards typically describe both **physical** layer delivery methods and **data link** layer requirements, including physical addressing, flow control, and encapsulation.





WAN Operations

WANs in the OSI Model

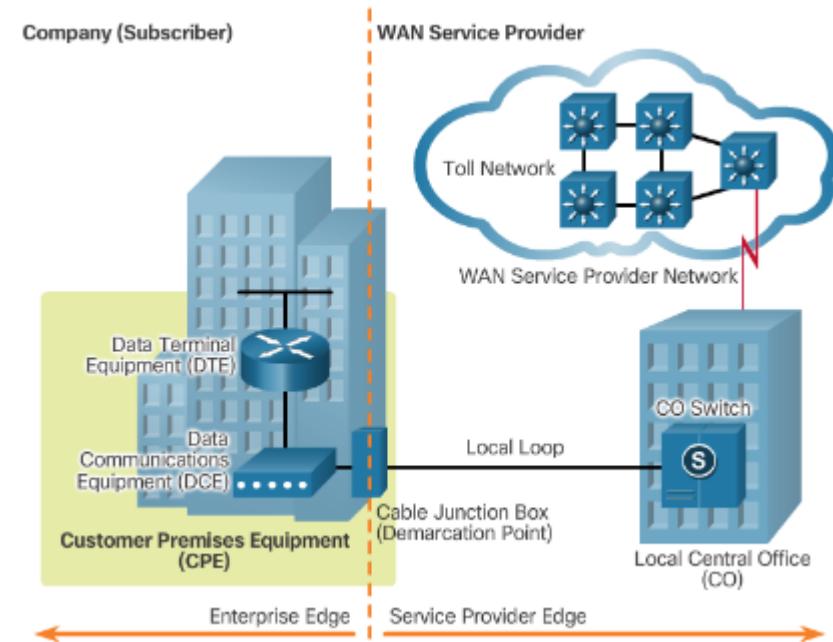
- Layer 1 protocols describe how to provide electrical, mechanical, operational, and functional connections to the services of a communications service provider.
- Layer 2 protocols define how data is **encapsulated** for transmission toward a remote location, and the mechanisms for transferring the resulting frames.
- A variety of different technologies are used, such as the **Point-to-Point Protocol (PPP)**, **Frame Relay**, and **ATM**. Some of these protocols use the same basic framing or a subset of the **High-Level Data Link Control (HDLC)** mechanism.
- Most WAN links are point-to-point. For this reason, the address field in the Layer 2 frame is usually not used.



WAN Technologies Overview

WAN Operations

- WAN operations focus primarily on the physical layer (OSI Layer 1) and the data link layer (OSI Layer 2).
 - Layer 1 protocols describe how to provide electrical, mechanical, operational, and functional connections
 - Layer 2 protocols define how data is encapsulated
- WAN Terms include:
 - **Customer Premises Equipment (CPE)** – owned by the business or leased from the service provider.
 - **Data Communications Equipment (DCE)** – provides an interface to connect subscribers to a communication link on the WAN cloud.
 - **Data Terminal Equipment (DTE)** – connects to the local loop through the DCE.
 - **Demarcation Point** – separates customer equipment from service provider equipment and is the place where the responsibility for the connection changes from the user to the service provider.
 - **Local Loop** – cable that connects the CPE to the CO of the service provider (last mile).
 - **Central Office (CO)** – local service provider facility or building that connects the CPE to the provider network.
 - **Toll network** – all the cabling and equipment inside the WAN provider network.

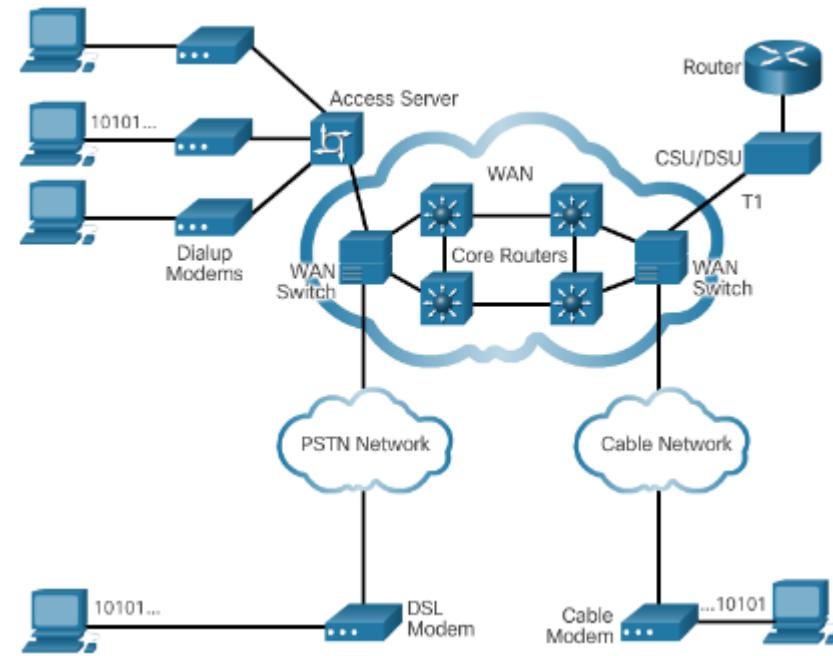




WAN Technologies Overview

WAN Operations

- WAN devices include:
 - **Dialup modem** – legacy WAN technology that converts digital signals into voice frequencies to be transmitted over the analog lines of the public telephone network.
 - **Access server** – legacy WAN technology that coordinates dial-in and dial-out user communications.
 - **Broadband modem** – used with high-speed DSL or cable Internet service
 - **CSU/DSU** – used to convert digital, leased-line signals into frames that the LAN can interpret and vice versa.
 - **WAN switch** – multiport internetworking device used in service provider networks
 - **Router** – provides internetworking and WAN access interface ports to connect to the service provider network
 - **Core router/Multilayer switch** – resides within the backbone of the WAN, supports multiple interfaces, and forwards IP packets at full line speed



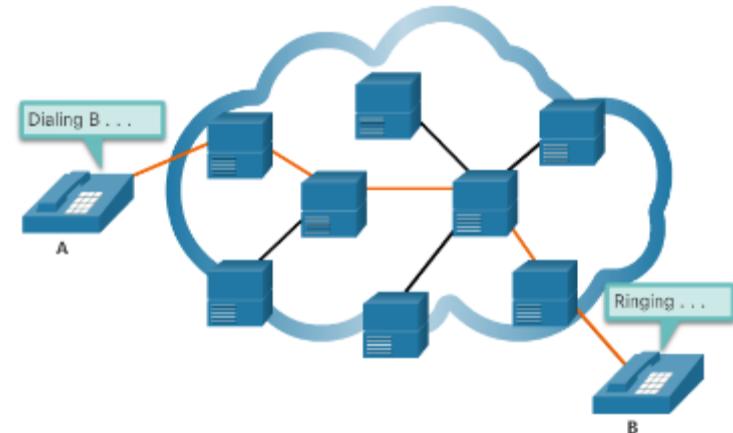


WAN Technologies Overview

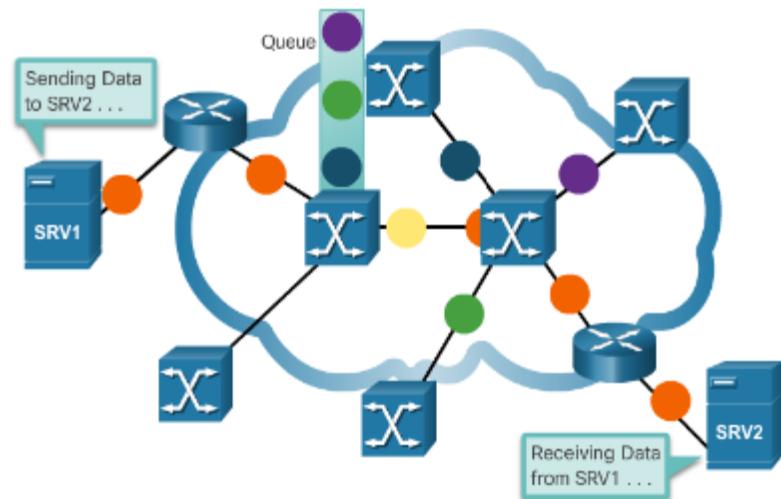
WAN Operations

- WANs can operate as circuit-switched or packet-switched networks:
 - **Circuit-switched Networks** – establish a **dedicated circuit** between source and destination before the users may communicate, such as making a telephone call
 - **Packet-Switched Networks** – **split traffic into packets** that are routed over a shared network and do not require a dedicated circuit between source and destination

Circuit-Switched



Packet-Switched



1.2 Selecting a WAN Technology



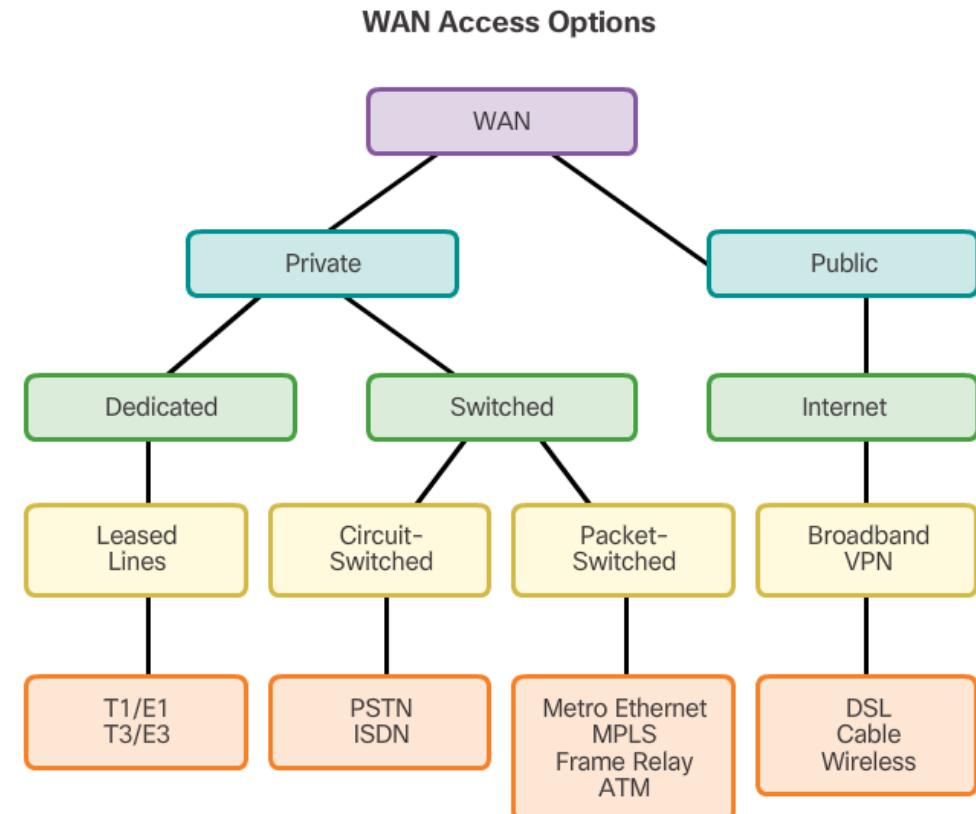


Selecting a WAN Technology

WAN Services

Two ways that a business can get WAN access:

- Private WAN Infrastructure
 - The business negotiates for dedicated or switched WAN access with a service provider.
- Public WAN Infrastructure
 - WAN access is achieved through the Internet using broadband connections.
VPNs secure the connections.

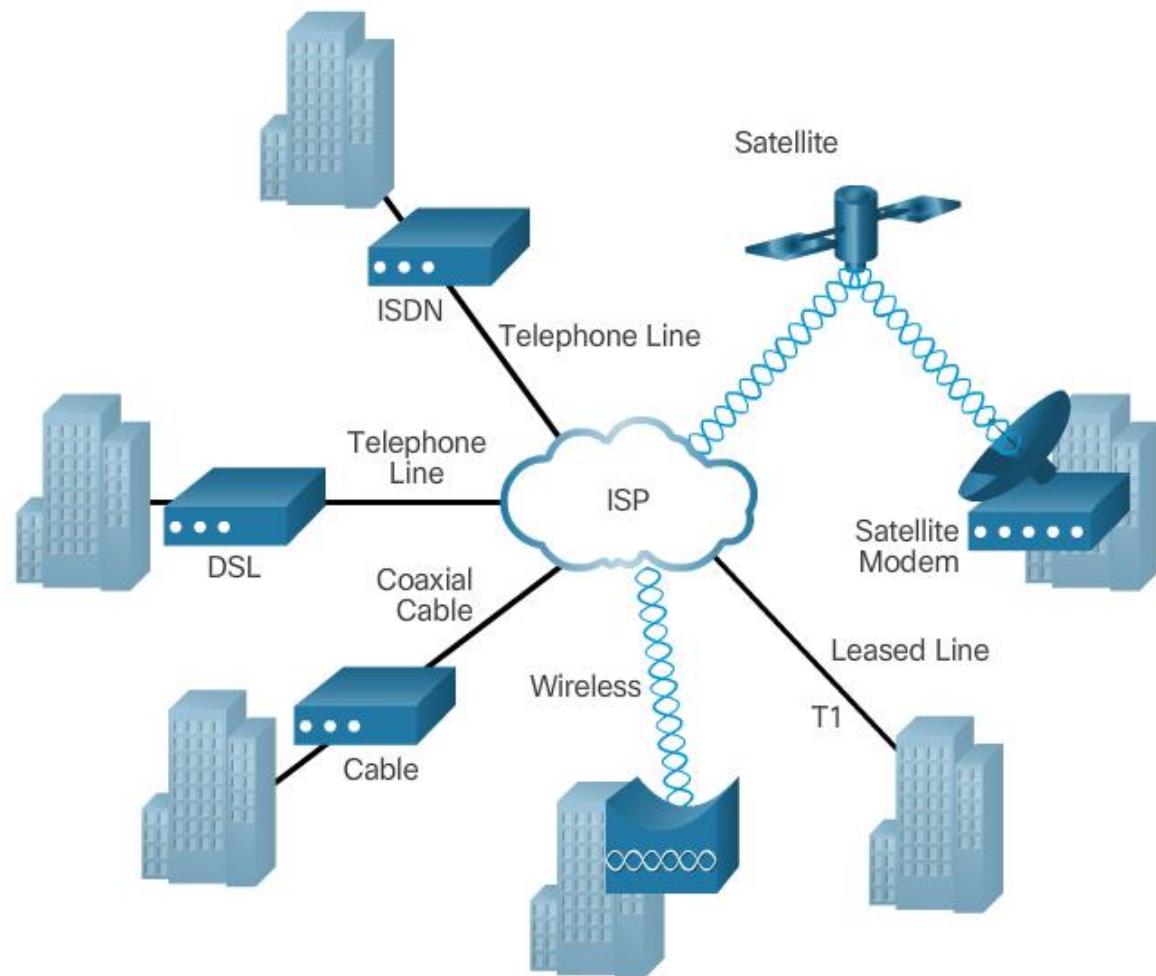




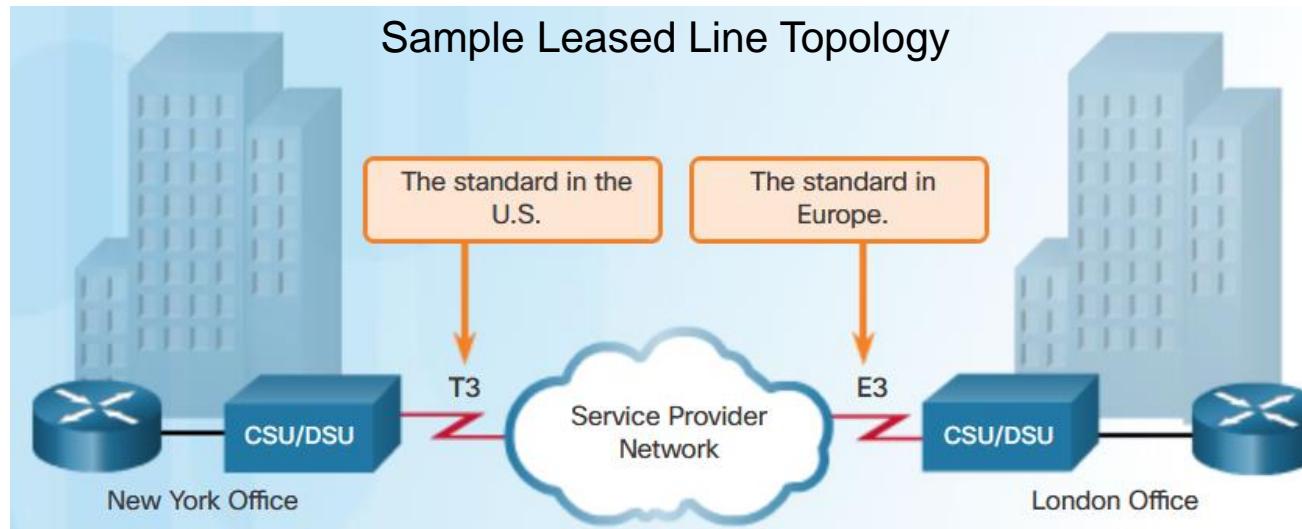
Selecting a WAN Technology

WAN Services (cont.)

This topology illustrates some of these WAN access technologies.



Leased Lines



- When **permanent dedicated connections** are required, a **point-to-point** link is used to provide a pre-established WAN communications path from the customer premises through the provider network to a remote destination.
- A point-to-point link is used to provide a pre-established WAN communications path from the customer premises through the provider network to a remote destination.
- Point-to-point links are usually more expensive than **shared** services such as Frame Relay.
- The Layer 2 protocol is usually HDLC or PPP.



Private WAN Infrastructures

Leased Lines

Advantages:

- **Simplicity** - Point-to-point communication links require minimal expertise to install and maintain.
- **Quality** - Point-to-point communication links usually offer high service quality, if they have adequate bandwidth. The dedicated capacity removes latency or jitter between the endpoints.
- **Availability** - Constant availability is essential for some applications, such as e-commerce. Point-to-point communication links provide permanent, dedicated capacity which is required for VoIP or Video over IP.

Disadvantages:

- **Cost** - Point-to-point links are generally the most expensive type of WAN access. The cost of leased line solutions can become significant when they are used to connect many sites over increasing distances. In addition, each endpoint requires an interface on the router, which increases equipment costs.
- **Limited flexibility** - WAN traffic is often variable, and leased lines have a fixed capacity, so that the bandwidth of the line seldom matches the need exactly. Any change to the leased line generally requires a site visit by ISP personnel to adjust capacity.



Private WAN Infrastructures Leased Lines

Some Interesting Links:

<https://business.bt.com/products/broadband/bt-leased-lines/>

<https://www.submarinecablemap.com/>

<http://www.aquacomms.com/>

Source: D. Clarke 2017



Selecting a WAN Technology

Private WAN Infrastructures

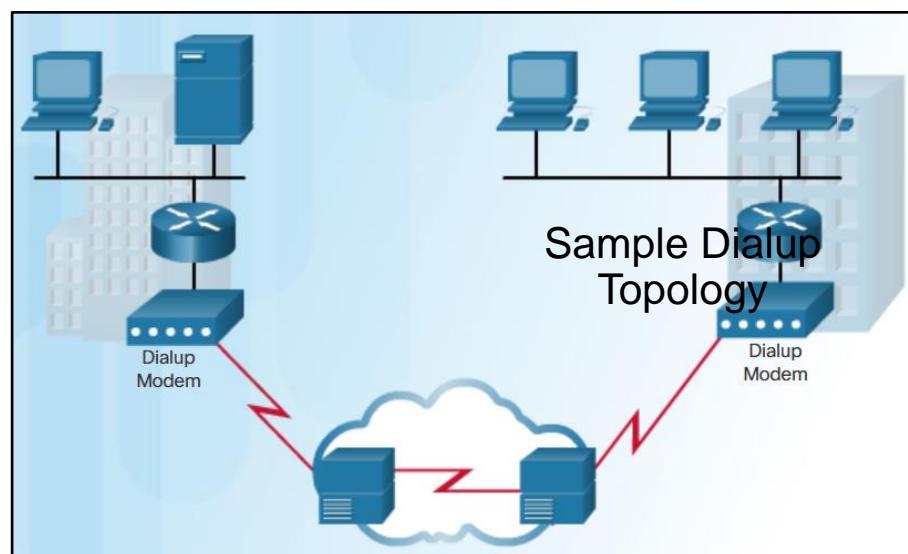
Dialup

Advantages:

- Simplicity
- Availability
- Low implementation costs

Disadvantages:

- relatively long connection time
- low data rates
- voice or video traffic does not work well at low bit rates



WAN built with an on-demand connection using a modem and the PSTN.



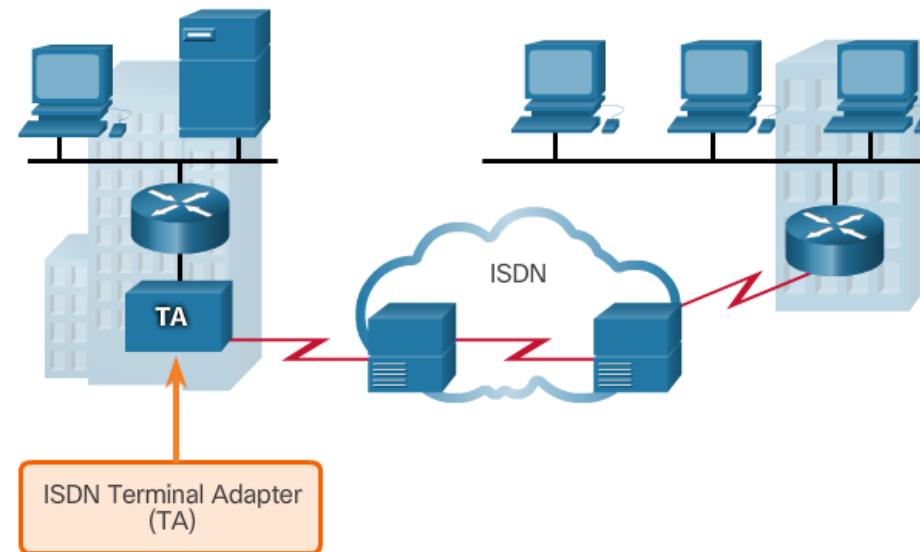
Selecting a WAN Technology

Private WAN Infrastructures (Cont.)

ISDN Integrated Services Digital Network

ISDN is a circuit-switching technology that enables the local loop of a PSTN to carry digital signals, resulting in higher capacity switched connections.

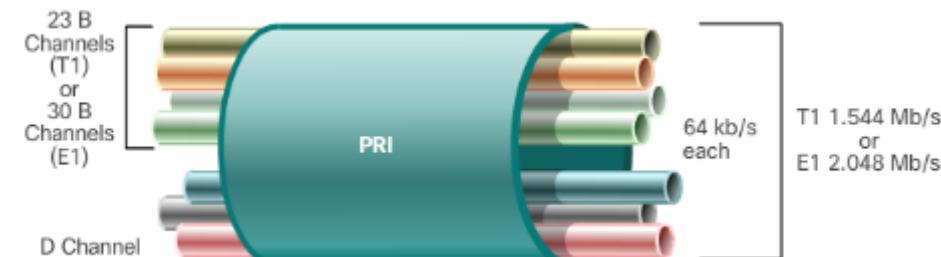
ISDN has declined in popularity as an Internet connection option with the introduction of high-speed DSL and other broadband services.



ISDN BRI



ISDN PRI

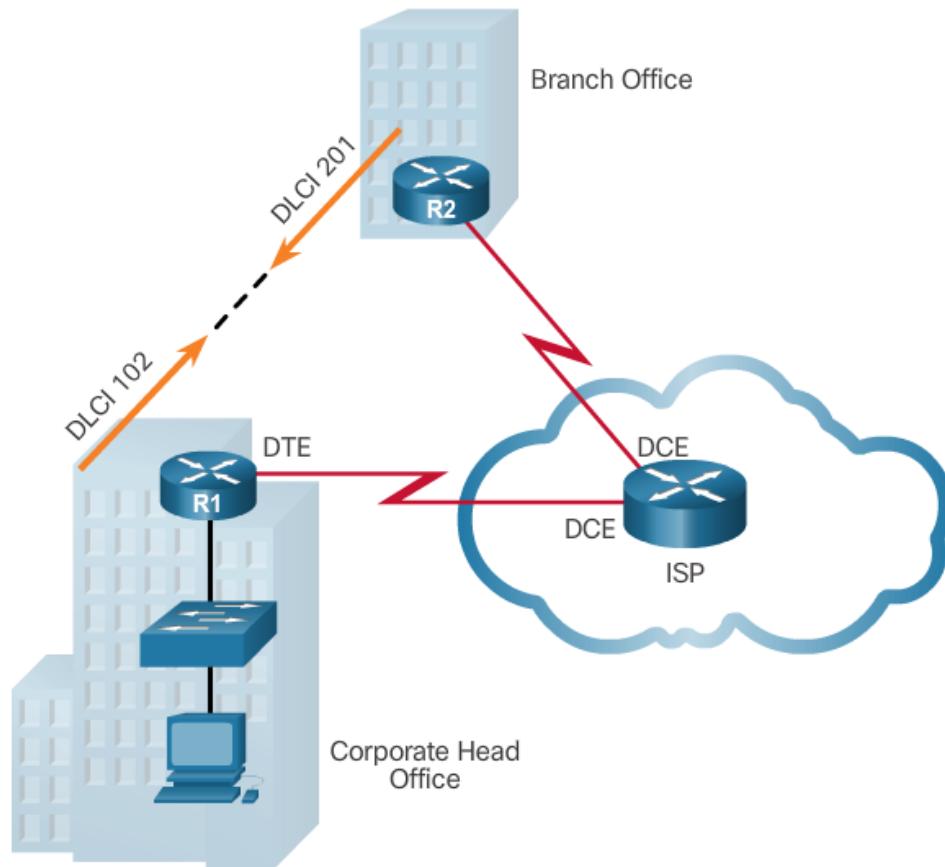




Selecting a WAN Technology

Private WAN Infrastructures (Cont.)

Frame Relay (Obsolete)



- 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.

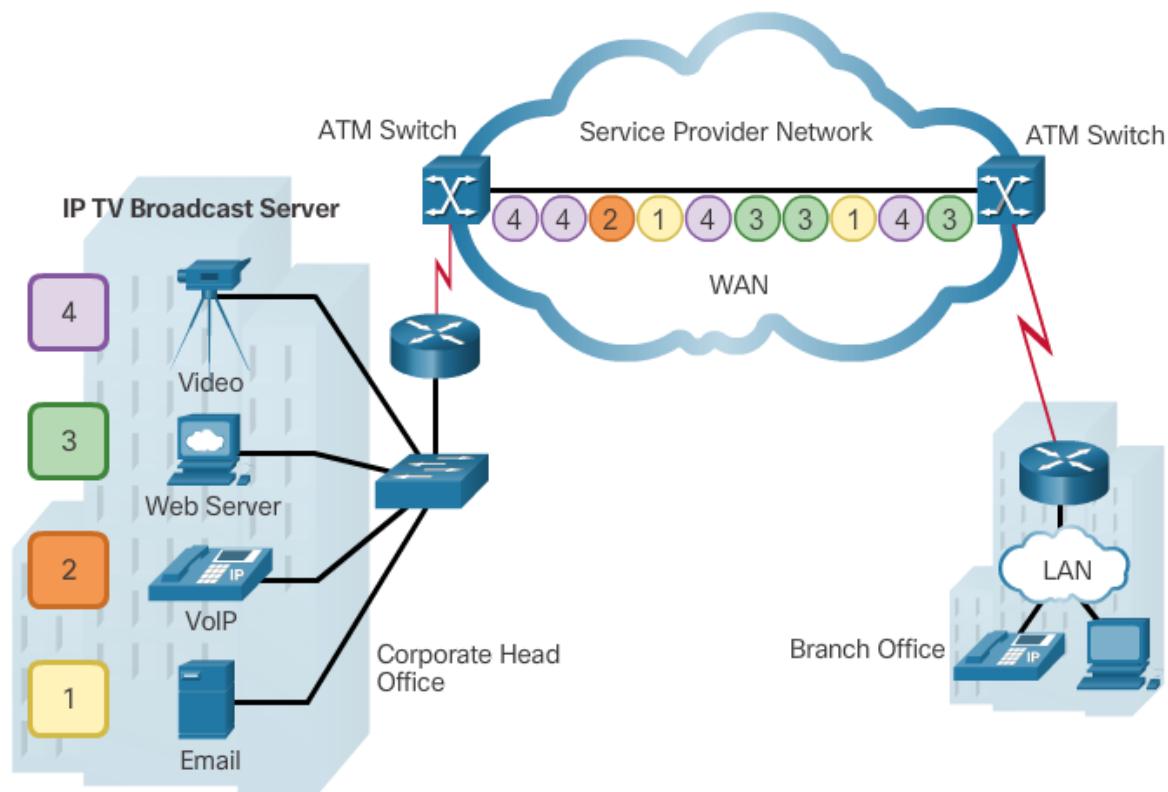


Selecting a WAN Technology

Private WAN Infrastructures (Cont.)

ATM (Obsolete)

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





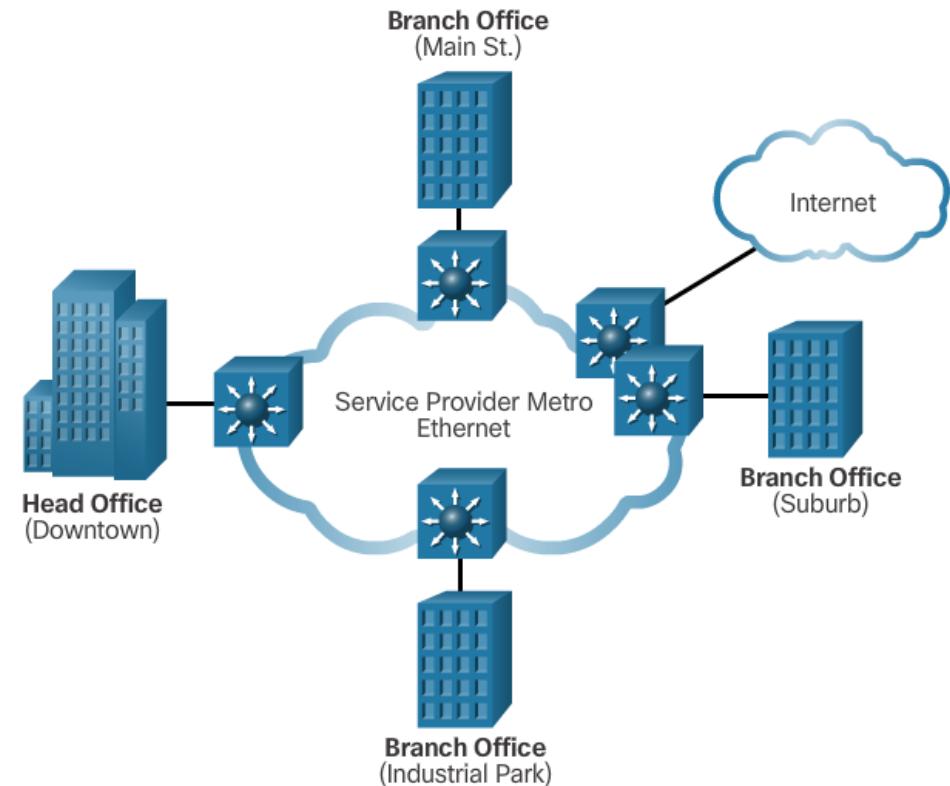
Selecting a WAN Technology

Private WAN Infrastructures (Cont.)

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.

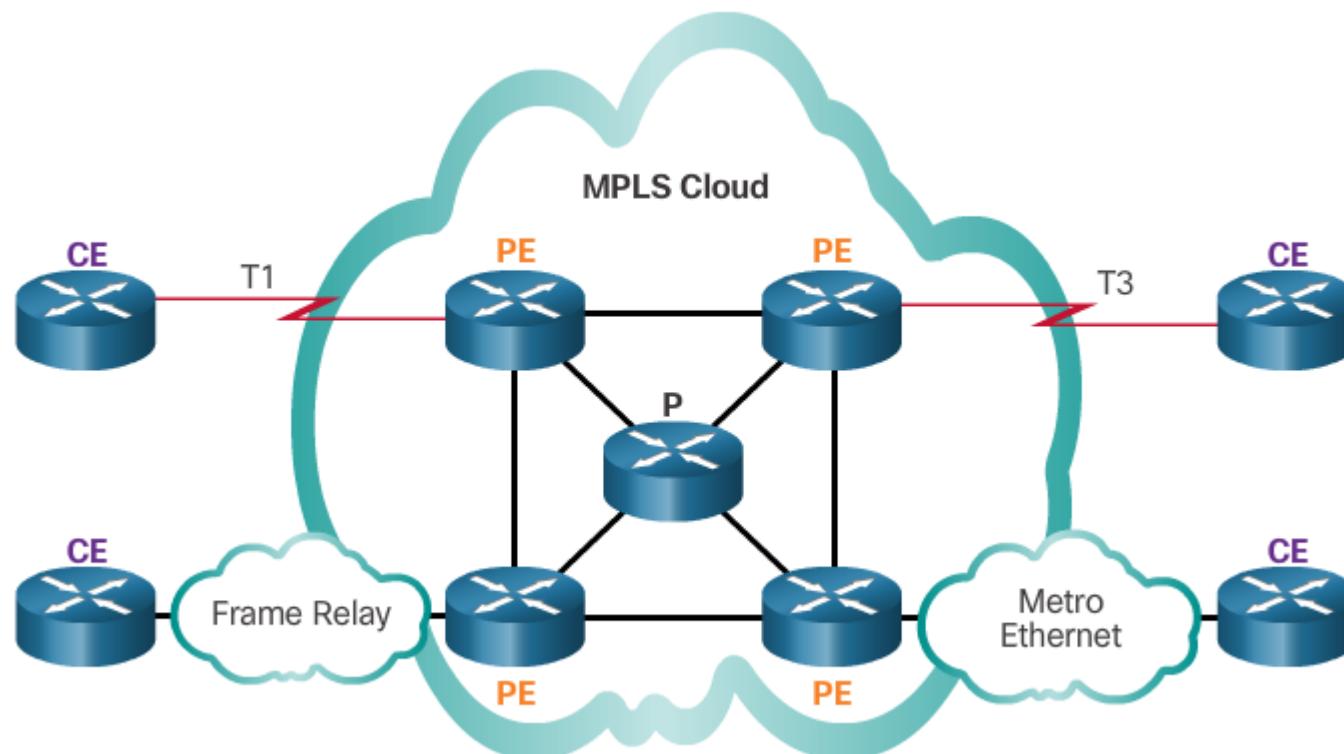


Selecting a WAN Technology

Private WAN Infrastructures (Cont.)

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.



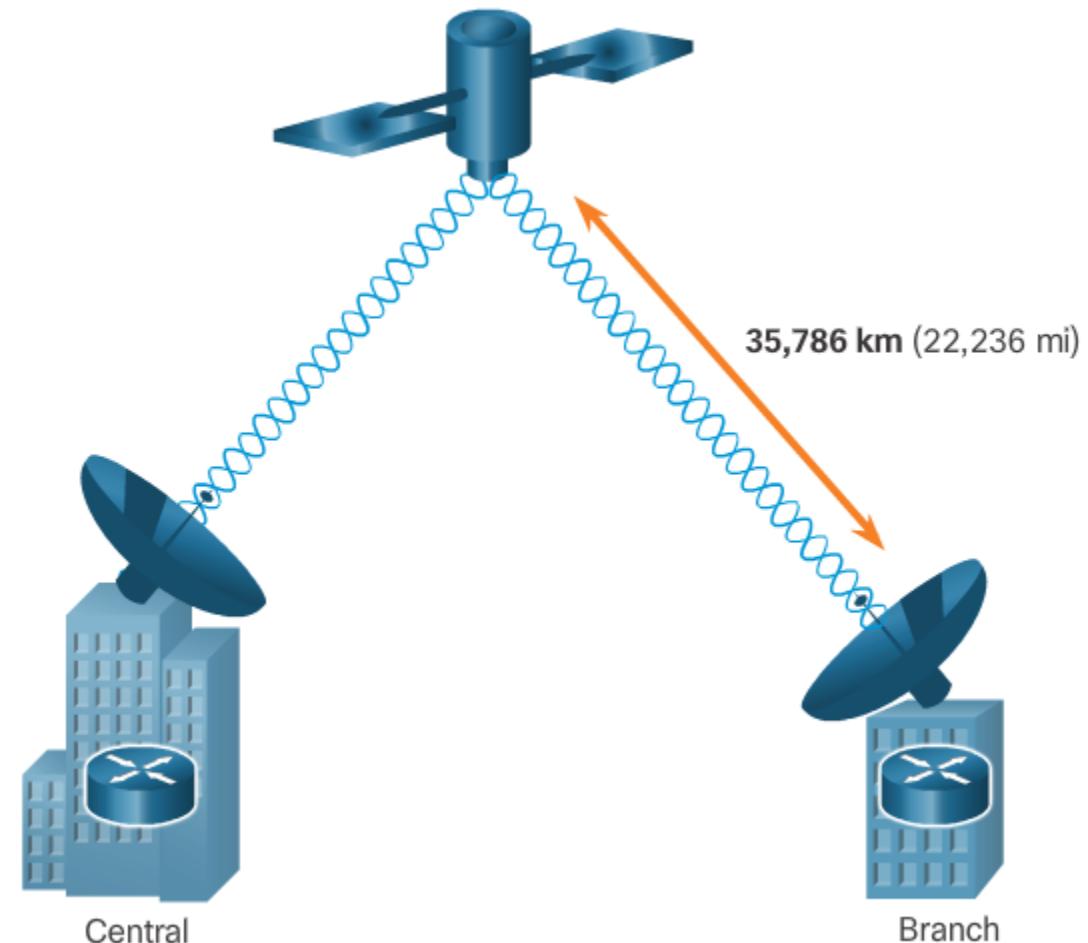


Selecting a WAN Technology

Private WAN Infrastructures (Cont.)

VSAT

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



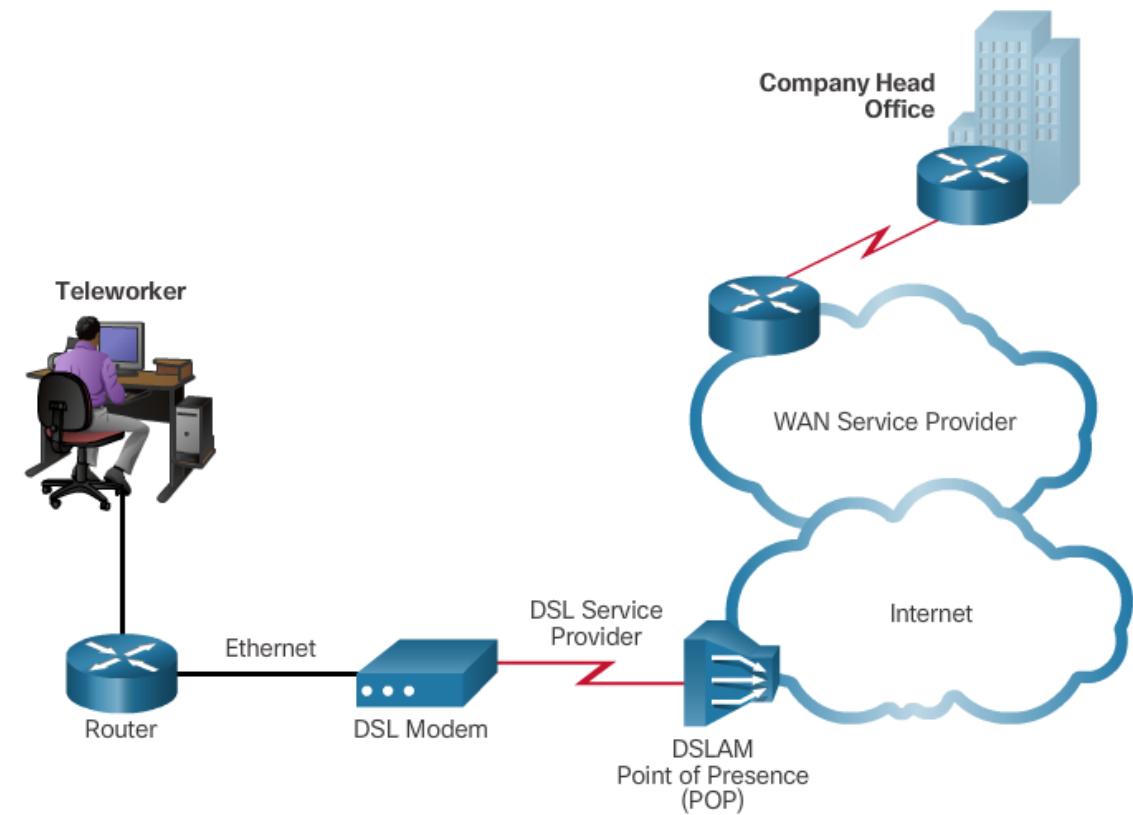


Selecting a WAN Technology

Public 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.



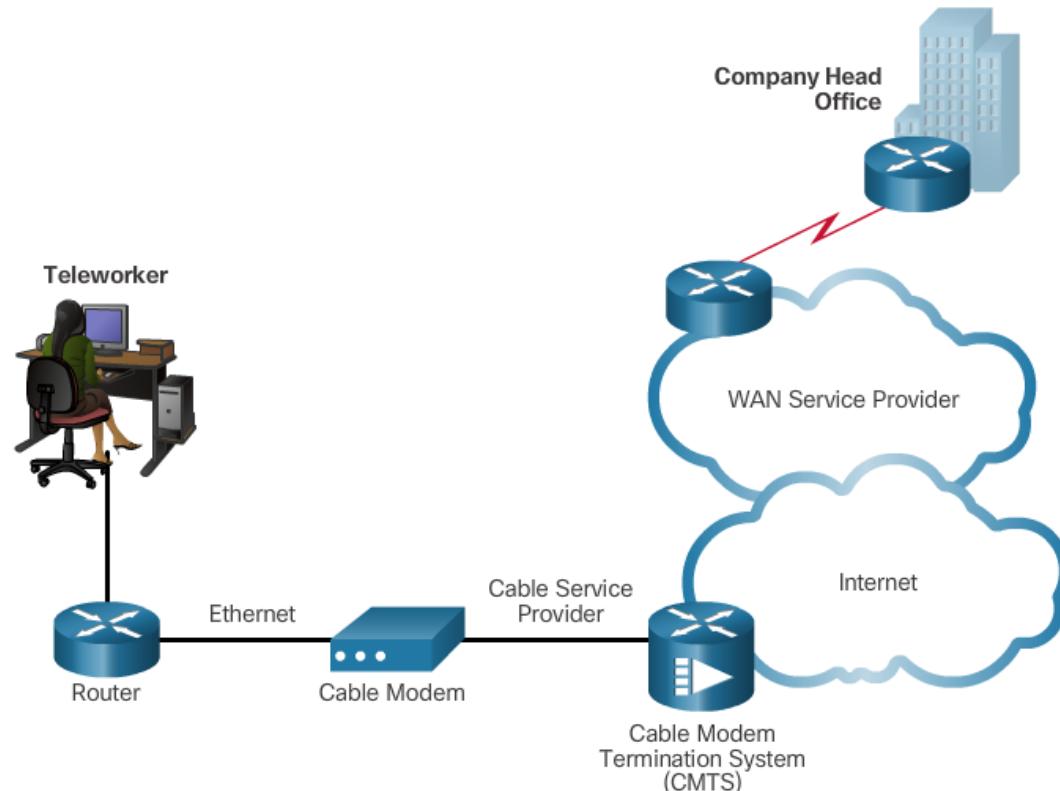


Selecting a WAN Technology

Public WAN Infrastructures (Cont.)

Cable

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





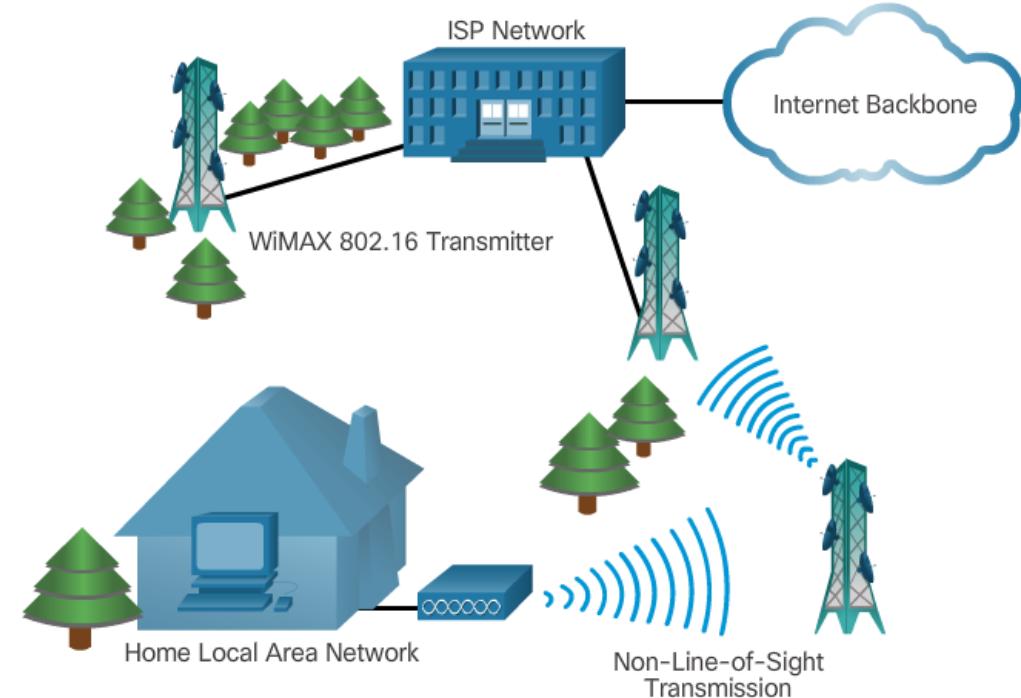
Selecting a WAN Technology

Public WAN Infrastructures (Cont.)

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** - Typically used by rural users where cable and DSL are not available.





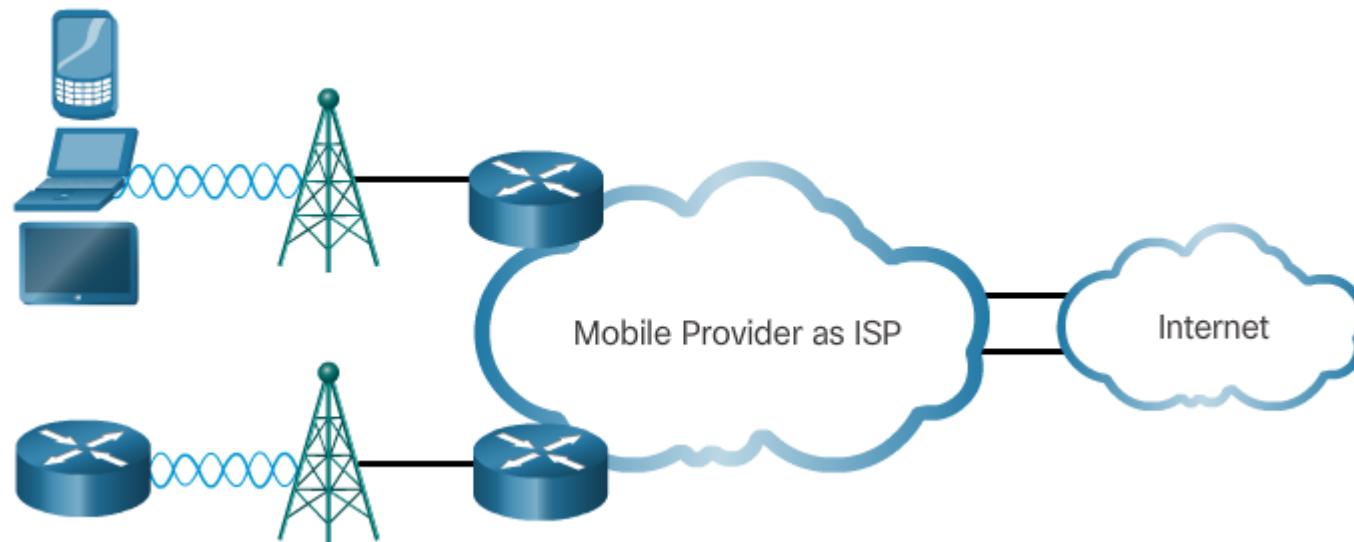
Selecting a WAN Technology

Public WAN Infrastructures (Cont.)

3G/4G

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.

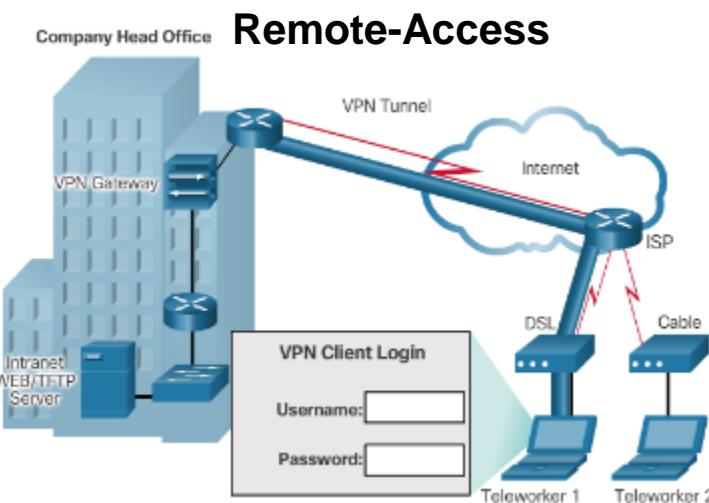
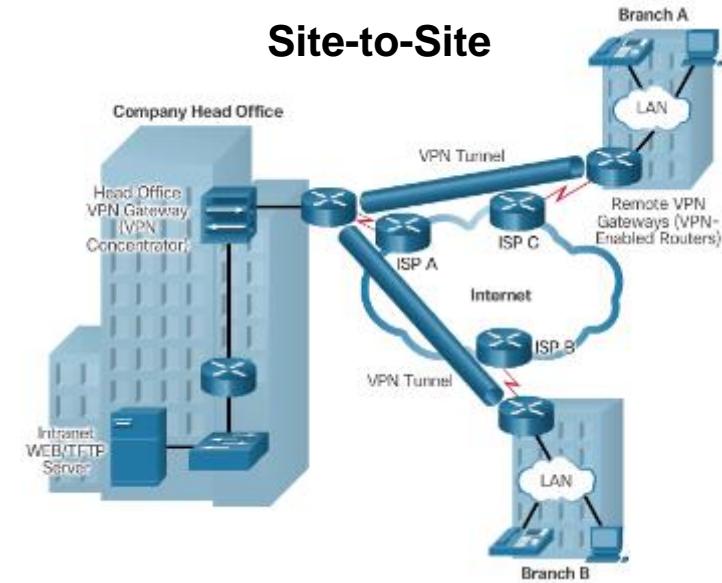




Selecting a WAN Technology

Public WAN Infrastructures (Cont.) *

- A VPN is a private network created via **tunneling** over a public network, such as the Internet.
 - VPNs establish a virtual point-to-point connection that enables hosts to send and receive data securely across public networks using dedicated connections and encryption.
 - VPNs provide a secure, reliable, and cost-effective method of interconnecting multiple networks to allow remote access to company resources.



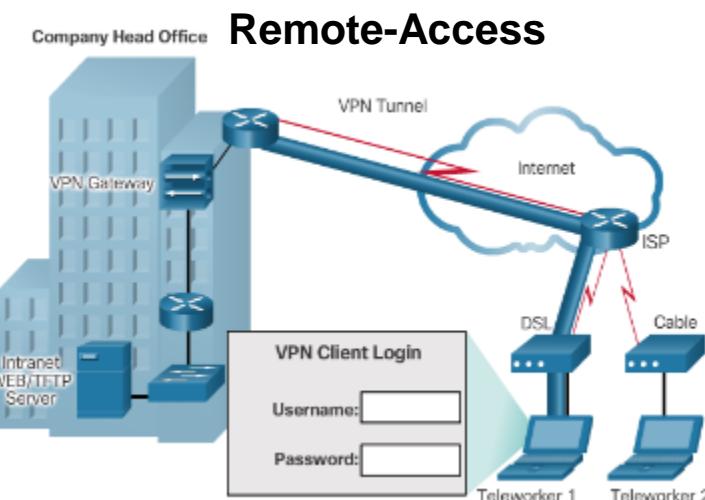
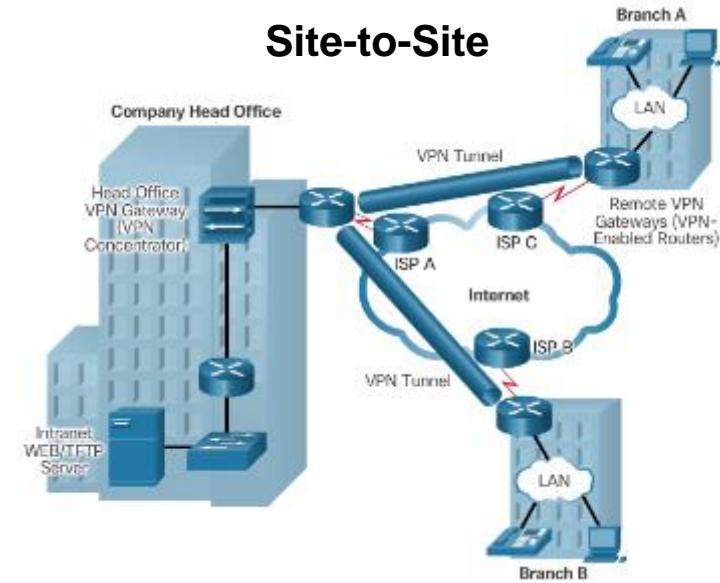
VPN = Virtual Private Network



Selecting a WAN Technology

Public WAN Infrastructures (Cont.)

- Public WANs rely on VPNs for securing data between private networks as it crosses a public network, such as the Internet.
- Benefits:
 - Cost savings
 - Security
 - Scalability
 - Compatibility with broadband technology
- Two types of VPN:
 - Site-to-site VPNs
 - Remote-access VPNs

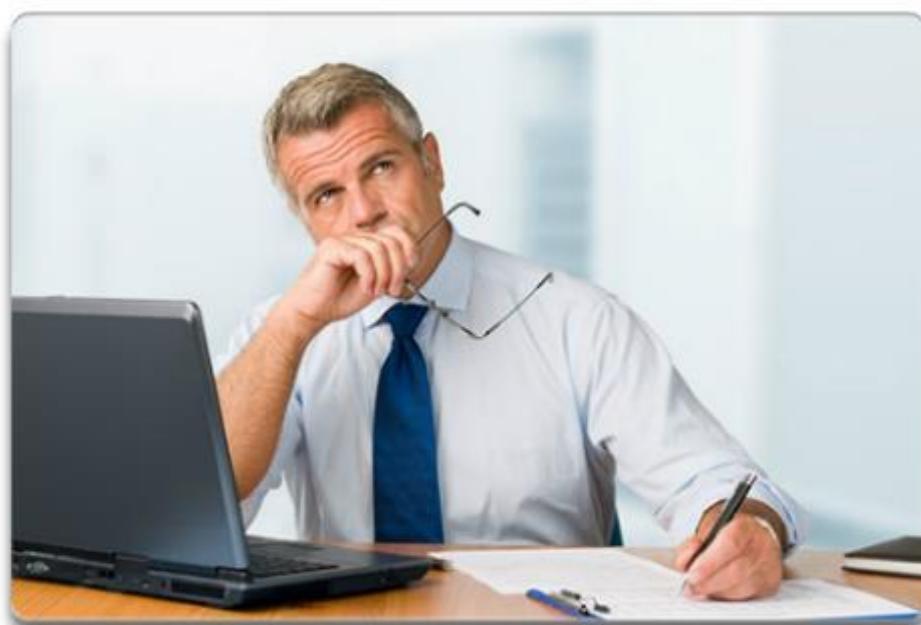




Selecting a WAN Technology

Selecting WAN Services

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?
- 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?



Choosing a WAN Link Connection *

- What is the purpose of the WAN?
 - Do you want to connect local branches, connect remote branches, connect to business partners?
- What is the geographic scope?
 - Depending on the range, some WAN connection options may be better than others.
- What are the traffic requirements?
 - Traffic type (data only, VoIP, video, large files) determines performance requirements.
- Should the WAN use a private or public infrastructure?
 - A private infrastructure offers the best security, whereas the public Internet offers lowest expense.
- For a private WAN, should it be dedicated or switched?
- For a public WAN, what type of VPN access do you need?
- Which connection options are available locally?
- What is the cost of the available connection options?

Source: D. Clarke 2017



Choosing a WAN Link Connection *

- **Contextual Example:**
- Your company is opening a new branch office and wishes to provide the branch office with Web Conferencing, IP telephony, video on demand, wireless services and TelePresence (Video Conferencing). What questions would you ask to help choose a suitable WAN Link connection to the new branch office?.
- **What is the purpose of the WAN?**
 - Will the business be connecting to a local branch in the same area, or to remote branch, (..one branch now, more branches later)?
 - Will the WAN connect to customers, business partners, or employees or a combination of all three?
 - Will the WAN provide full or limited access the business intranet for authorized users?
- **What is the geographic scope?**
 - Local WAN, regional WAN, or global WAN?
 - One-to-one (single branch), one-to-many branches, or many-to-many (distributed)?
 - (..one branch now, more branches later)?



Choosing a WAN Link Connection *

- **Contextual Example:** (continued)
- Your company is opening a new branch office and wishes to provide the branch office with Web Conferencing, IP telephony, video on demand, wireless services and TelePresence (Video Conferencing). What questions would you ask to help choose a suitable WAN Link connection to the new branch office.
- **What are the traffic requirements?**
 - Traffic type?
 - What type of traffic must be supported (data only, VoIP, video, large files, streaming files).
 - Traffic volume?
 - What volume of traffic type (voice, video, or data) must be supported for each destination?
 - This determines the bandwidth capacity required for the WAN connection to the ISP.
 - Quality of Service?
 - What Quality of Service is required? This may limit the choices. If the traffic is highly sensitive to latency and jitter, eliminate any WAN connection options that cannot provide the required quality.



Choosing a WAN Link Connection *

- **Contextual Example:** (continued)
- Your company is opening a new branch office and wishes to provide the branch office with Web Conferencing, IP telephony, video on demand, wireless services and TelePresence (Video Conferencing). What questions would you ask to help choose a suitable WAN Link connection to the new branch office.
- **What are the traffic requirements? (continued)**
 - Security?
 - What are the security requirements (data integrity, confidentiality, and security)? Traffic volume?
 - The security requirements are important if the traffic is of a highly confidential nature.
- **Private WAN - should it be dedicated or switched?**
- **Public WAN - what type of VPN access do you need?**
- **Which connection options are available locally?**
- **What is the **cost** of the available connection options?**



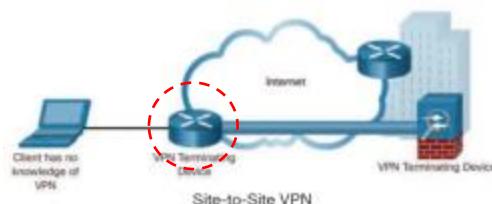
Choosing a WAN Link Connection - VPN Access*

- **Contextual Example:** (continued)
- The company intends to use Virtual Private Networks (VPNs) to support secure access by teleworkers, employees, vendors and clients. How would a VPN benefit the company?
 - Cost savings?
 - Security?
 - Scalability?
 - Compatibility with broadband technology?
- Cost savings?
 - Use of VPNs over the public Internet infrastructure to support secure remote access by teleworkers, vendors and clients reduces costs for the company.
 - Remote access via DSL instead of expensive dedicated WAN links reduces connection costs, while increasing remote connection bandwidth.
- Security?
 - VPNs can protect company data from unauthorized access during transmission across the public Internet using advanced encryption and authentication protocols.



Choosing a WAN Link Connection- VPN Access*

- **Contextual Example:** (continued)
- The company has two types of VPN (VPNs) available - Site-toSite VPNs and Remote-Access-VPNs How would they be used to support the company's WAN infrastructure?.



- **Site-to-Site VPNs?**
 - Site-to-site VPNs connect entire networks to each other such as the company's branch office network at one site to the company's headquarters network at another site.
 - Both sides of the VPN connection are aware of the VPN configuration in advance.
 - The VPN remains static.
 - Internal hosts have no knowledge that a VPN exists.
 - VPN gateway encapsulates and encrypts outbound traffic from a network site.
 - VPN gateway sends the traffic through a VPN tunnel over the Internet to a peer VPN gateway at the target site.
 - Peer VPN gateway strips the headers, decrypts the content, and relays the packet toward the target host inside its private network.



Choosing a WAN Link Connection- VPN Access*

- **Contextual Example:** (continued)
- The company has two types of VPN (VPNs) available - Site-toSite VPNs and Remote-Access-VPNs How would they be used to support the company's WAN infrastructure?



- **Remote-Access VPN?**
 - Remote-access VPNs securely connect individual teleworker hosts to the company network, usually via an Internet broadband connections.
 - The VPN is dynamic. VPN 'torn' down when communication session ends.
 - VPN Client software installed on teleworker host encapsulates, encrypts, and sends the traffic through a VPN tunnel over the Internet to the destination VPN gateway.
 - VPN gateway strips the headers, decrypts the content, and relays the packet toward the target host inside its private network.

1.3 Summary





Chapter Summary

Summary

- WAN access standards operate at Layers 1 and 2 of the OSI model.
- Permanent, dedicated point-to-point connections are provided by using leased lines.
- Private WAN connections include:
 - Dialup
 - ISDN
 - Frame Relay (Obsolete)
 - ATM (Obsolete)
 - Metro Ethernet
 - MPLS
 - VSAT
- Public WAN connections include:
 - DSL
 - Cable
 - Wireless
 - Cellular
- Security over public infrastructure connections can be provided by using remote-access or site-to-site Virtual Private Networks (VPNs).



Reminder

Lab on Friday

- This lab will help you check your skills from the previous courses. Refer to your notes and previous content if necessary.
- Revise how to configure the following on a Router before the Lab
- SSH
- DHCPv4
- NAT
- PAT
- Default routes IPv4 and IPv6
- OSPF.

Cisco | Networking Academy®

Mind Wide Open™





Chapter 2: Point-to-Point Connections



Connecting Networks

Cisco | Networking Academy®
Mind Wide Open™



Chapter 2 - Sections & Objectives

- 2.1 Serial Point-to-Point Overview
 - Serial vs. Parallel Transmission.
 - Configure HDLC encapsulation.
- 2.2 PPP Operation
 - Explain how PPP operates across a point-to-point serial link.
- 2.3 PPP Implementation
 - Configure PPP encapsulation.
- 2.4 Troubleshoot WAN Connectivity
 - Troubleshoot PPP.



2.1 Serial Point-to-Point Overview

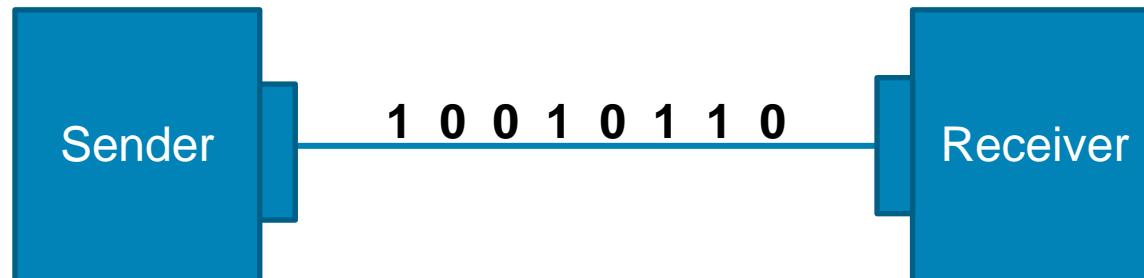


Cisco | Networking Academy®
Mind Wide Open™

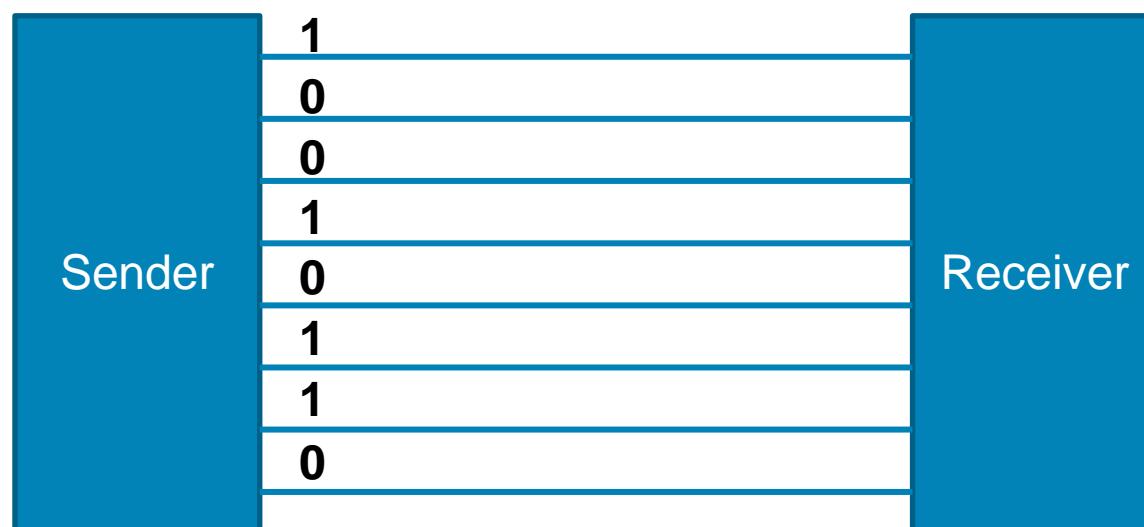


Serial Point-to-Point Overview

Serial vs. Parallel Transmission



Serial: bits are transmitted sequentially over a single channel.



Parallel: bits are transmitted simultaneously over multiple wires.
In reality, the wires are enclosed within a single physical cable.



Serial Point-to-Point Overview

Serial vs. Parallel Transmission

- Parallel Transmission - High throughput.
 - Can send N bits at the same time. Parallel interface can send N bits in the time that it takes serial interface to send 1 bit.
 - For N = 8, parallel interface can send 8 bits in the time that it takes serial interface to send 1 bit.
 - The parallel connection theoretically transfers data 8 times faster than a serial connection.
 - Based on this theory, a parallel connection sends a byte (8 bits) in the time that a serial connection sends a single bit.
 - **See the animation in Figure 2 Serial and Parallel Communication** Section 2.1.1.1 in Chapter 2 Point-to-Point Connections in NetAcad online.
- Parallel Transmission – issues
 - Crosstalk across wires...especially as the wire length increases.
 - Clock skew. Data across the various parallel wires does not arrive at the same time. Creates synchronization issues.
 - Many parallel ports are simplex (one-direction, outbound comms only). Some support half-duplex communication (two-way communication, but only one way at a time).
- => **Serial Transmission preferred**



Serial Point-to-Point Overview

Serial vs. Parallel Transmission

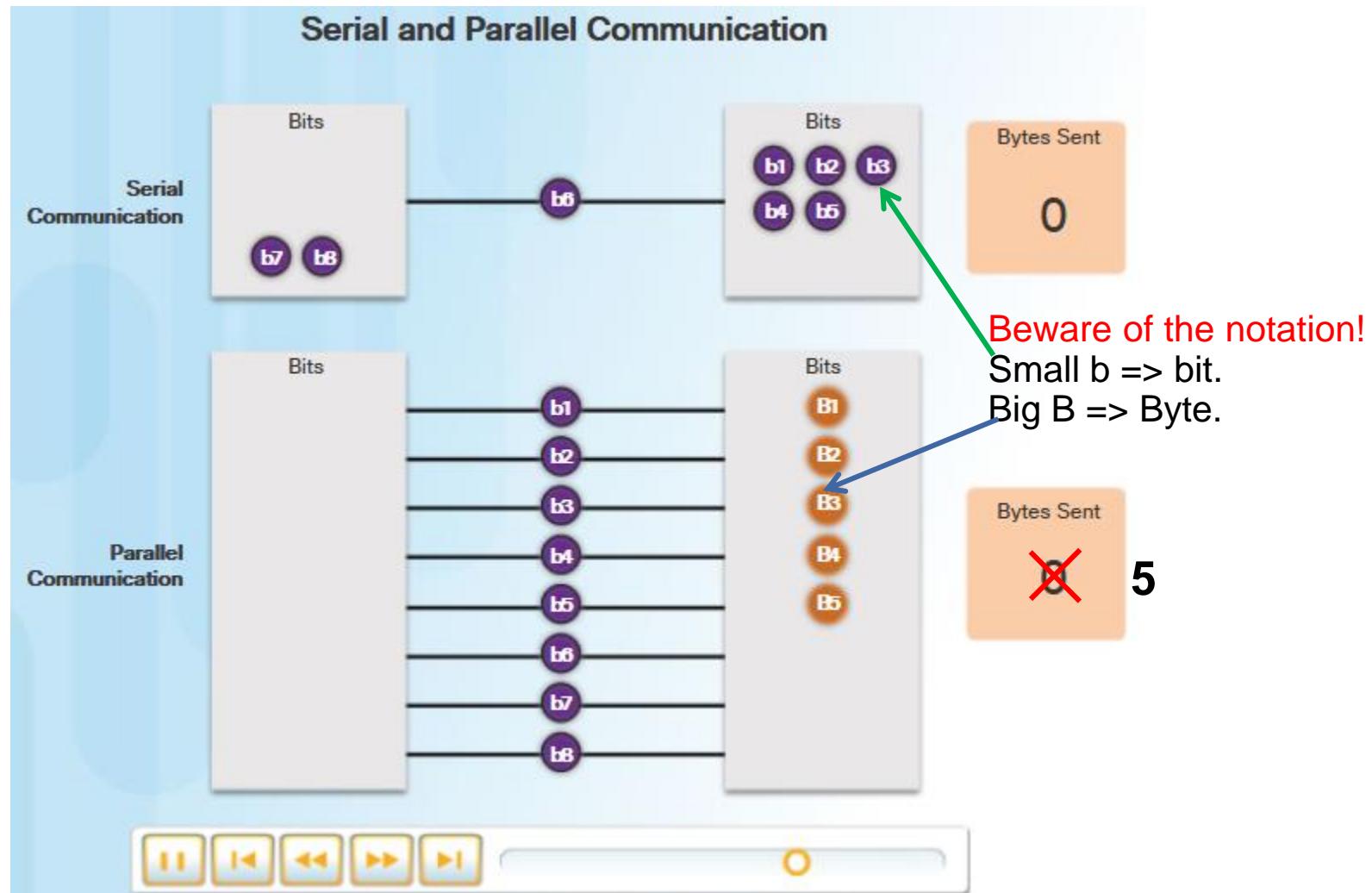


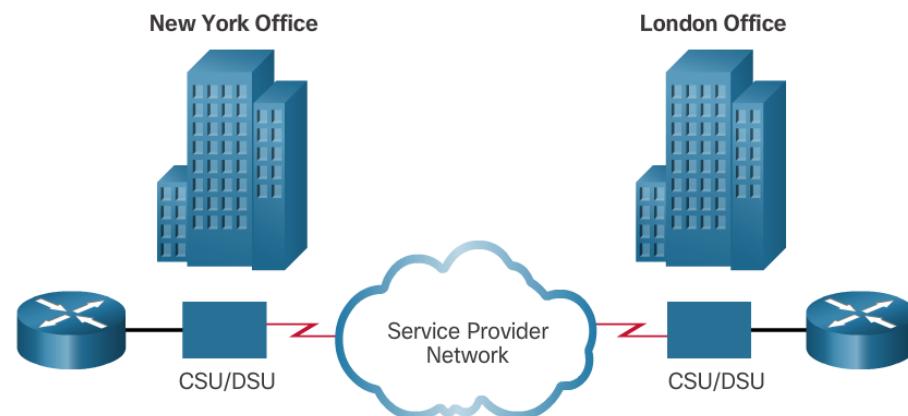
Figure 2 Animation Serial and Parallel Comms Section 2.1.1.1 Chapter 2 Point-to-Point Connections NetAcad online.



Serial Point-to-Point Overview

Serial Communications

- Point-to-point connections are used to connect LANs to service provider WANs, and to connect LAN segments within an enterprise network.
- A point-to-point link can connect two **geographically distant sites**, such as a corporate office in New York and a regional office in London.



- Point-to-point connections cross both land and sea. Undersea fiber-optic cables connect countries and continents.
- See <https://www.submarinecablemap.com/>



Serial Point-to-Point Overview

Serial Communications

- Point-to-point links are usually more expensive than shared services.
 - The cost of leased-line solutions can become significant when used to connect many sites over increasing distances.
- Sometimes the benefits outweigh the cost of the leased line.
 - The dedicated capacity removes **latency** or **jitter** between the endpoints.
 - Constant availability is essential for some applications such as VoIP or video over IP.



Serial Point-to-Point Overview

Serial Communications

- **Bandwidth (BW)** refers to the rate at which data is transferred over the communication link.
- The underlying carrier technology will dictate how much bandwidth is available.
- Serial connection bandwidths can be incrementally increased to accommodate the need for faster transmission.
- Most fundamental line speed is 64 kb/s, or DS0.
 - 64 kb/s (BW) needed for an uncompressed, digitized telephone phone call.
- 24 DS0s bundled to get a DS1 line (aka T1 line). T1 speed of 1.544 Mb/s.

North American:

Carrier Transmission Rates

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

European: E1 (2.048 Mb/s) and E3 (34.368 Mb/s). Similar to T1 and T3. But different bandwidths and frame structures.



Serial Point-to-Point Overview

HDLC Encapsulation

- On each WAN connection, data is encapsulated into frames before crossing the WAN link.
 - HDLC is the default encapsulation type on point-to-point connections, dedicated links, and circuit-switched connections when the link uses two Cisco devices.
- HDLC defines a Layer 2 framing structure that allows for flow control and error control through the use of acknowledgments.
 - HDLC uses a frame delimiter, or flag, to mark the beginning and the end of each frame
 - Cisco HDLC frames contain a field for identifying the network protocol being encapsulated.

Standard HDLC

Flag	Address	Control	Data	FCS	Flag
------	---------	---------	------	-----	------

Supports only single-protocol environments.

Cisco HDLC

Flag	Address	Control	Protocol	Data	FCS	Flag
------	---------	---------	----------	------	-----	------

Uses a protocol data field to support multiprotocol environments.





Serial Point-to-Point Overview

Which Encapsulation is in use?

- **show interface serial0/0/0**

```
R1# show interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
Hardware is GT96K Serial
Internet address is 172.16.0.1/30
MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set
Keepalive set (10 sec)
```

```
R1#sh int serial 0/0/0
Serial0/0/0 is up, line protocol is up (connected)
Hardware is HD64570
Internet address is 192.168.10.1/30
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, loopback not set, keepalive set (10 sec)
LCP Open
Open: IPCP, CDPCP
Last input never, output never, output hang never
```

- Re-enable HDLC encapsulation – Two steps
 - **Step 1.** Enter the interface configuration mode of the serial interface.
 - **Step 2.** Enter the **encapsulation hdlc** command to specify the encapsulation protocol on the interface.



Serial Point-to-Point Overview

Troubleshooting Serial Lines

- The **show interfaces serial** command returns one of six possible states:

- Serial x is up, line protocol is up

'up up' = correct state for serial line...working

- Serial x is down, line protocol is down

- Serial x is up, line protocol is down

- Serial x is up, line protocol is up (looped)

5 x Problem states

- Serial x is up, line protocol is down (disabled)

- Serial x is administratively down, line protocol is down

- 5 x Problem States

- See Figure 2, Section 2.1.2.4 Troubleshooting a Serial Interface in NetAad. Explains the issues & how to troubleshoot them



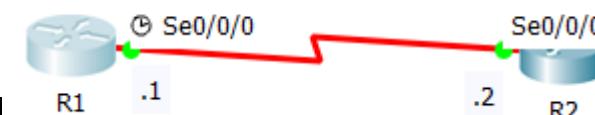
Serial Point-to-Point Overview

Troubleshooting Serial Lines

- The **show controllers** command is another important diagnostic tool when troubleshooting serial lines.
 - The output indicates the state of the interface channels and whether a cable is attached to the interface.

R1

```
R1#show controllers serial 0/0/0
Interface Serial0/0/0
Hardware is PowerQUICC MPC860
DCE V.35, clock rate 2000000
idb at 0x81081AC4, driver data structure at 0x81084AC0
SCC Registers:
General [GSMR]=0x2:0x00000000, Protocol-specific [PSMR]=0x8
Events [SCCE]=0x0000, Mask [SCCM]=0x0000, Status [SCCS]=0x00
Transmit on Demand [TODR]=0x0, Data Sync [DSR]=0x7E7E
Interrupt Registers:
```



R2

```
R2#show controllers serial0/0/0
Interface Serial0/0/0
Hardware is PowerQUICC MPC860
DTE V.35, TX and RX clocks detected
idb at 0x81081AC4, driver data structure at 0x81084AC0
SCC Registers:
General [GSMR]=0x2:0x00000000, Protocol-specific [PSMR]=0x8
Events [SCCE]=0x0000, Mask [SCCM]=0x0000, Status [SCCS]=0x00
Transmit on Demand [TODR]=0x0, Data Sync [DSR]=0x7E7E
Interrupt Registers:
```

2.2 PPP Operation





PPP Operation Benefits of PPP

- Use **PPP** encapsulation to **connect a Cisco router to a non-Cisco router**.
- **PPP Advantages**
 - The **link quality** management feature monitors the quality of the link. If too many errors are detected, PPP takes the link down.
 - PPP supports PAP and CHAP **authentication**.

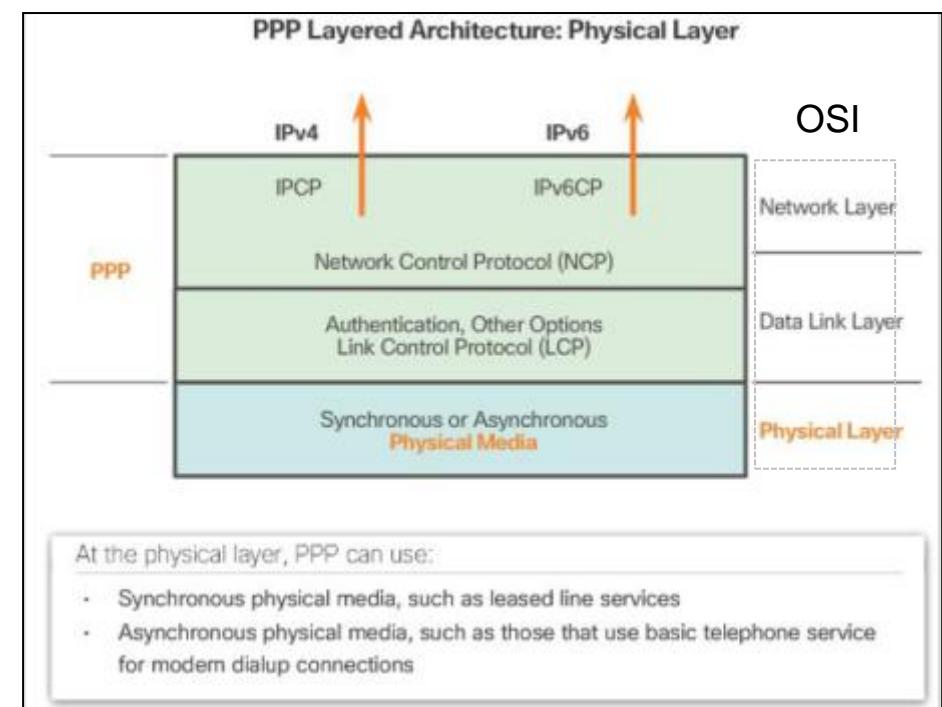




PPP Operation LCP and NCP

■ PPP Layered Architecture *

- PPP and OSI share the same physical layer, but PPP distributes the functions of LCP and NCP differently.
- The only absolute requirement imposed by PPP is a full-duplex circuit, either dedicated or switched, that can operate in an asynchronous or synchronous bit-serial mode.
- Most of the work done by PPP happens at the data link and network layers, by LCP and NCPs.





PPP Operation

LCP and NCP

■ Link Control Protocol

- LCP establishes the point-to-point link.
- LCP also negotiates and sets up control options on the WAN data link, which are handled by the NCPs.
- After the link is established, PPP also uses LCP to agree automatically on encapsulation formats such as authentication, compression, and error detection.



PPP Operation LCP and NCP

■ Network Control Protocol

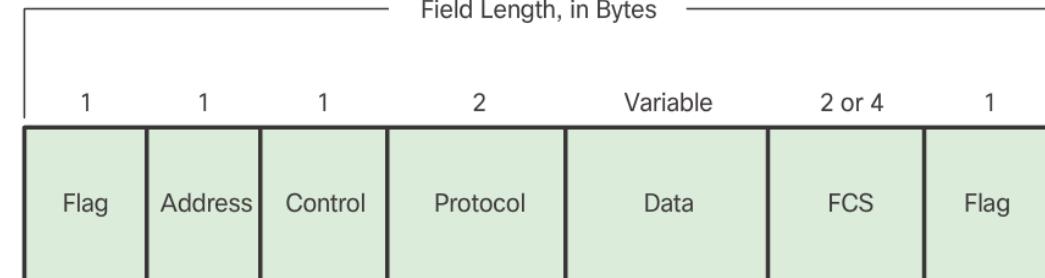
- PPP permits multiple network layer protocols to operate on the same communications link.
- For every network layer protocol used, PPP uses a separate NCP
- Each NCP manages the specific needs required by its respective network layer protocols.



PPP Operation

PPP Frame

- A PPP frame - six fields:



- **Flag** - A single byte that indicates the beginning or end of a frame. The Flag field consists of the binary sequence 01111110.
- **Address** - A single byte that contains the binary sequence 11111111, the standard broadcast address. PPP does not assign individual station addresses.
- **Control** - A single byte that contains the binary sequence 00000011, which calls for transmission of user data in an unsequenced frame.
- **Protocol** - Two bytes that identify the protocol encapsulated in the information field of the frame. The 2-byte Protocol field identifies the protocol of the PPP payload.
- **Data** - Zero or more bytes that contain the datagram for the protocol specified in the protocol field.
- **Frame Check Sequence (FCS)** – This is normally 16 bits (2 bytes). If the receiver's calculation of the FCS does not match the FCS in the PPP frame, the PPP frame is silently discarded.



PPP Operation

PPP Sessions

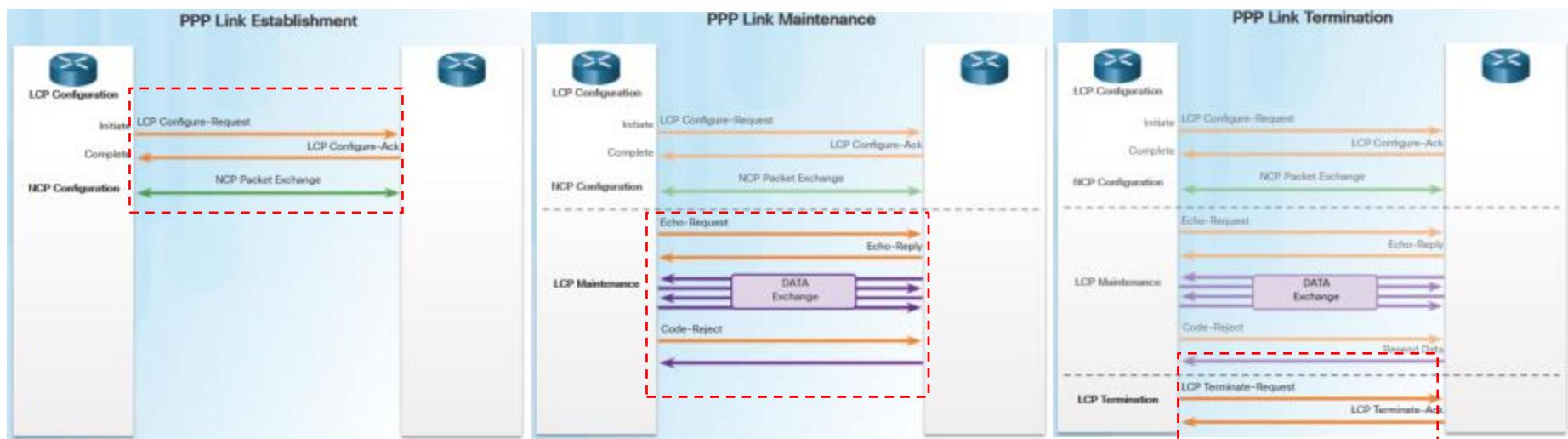
- There are **four** phases of establishing a PPP session
 - Phase 1: Link establishment and configuration negotiation
 - The originating PPP node sends LCP frames to configure and establish the data link.
 - Phase 2: Link quality determination (**optional-phase**)
 - The link is tested to determine whether the link quality is sufficient to bring up network layer protocols
 - Phase 3: Network layer protocol configuration negotiation
 - The originating PPP node sends NCP frames to choose and configure the network-layer protocols
 - Phase 4: Link termination negotiation
 - Link remains configured for communications until LCP or NCP frames close the link or until some external event occurs



PPP Operation

PPP Sessions

- 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.
 - Link-maintenance frames manage and debug a link.
 - Link-termination frames terminate a link.



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**).

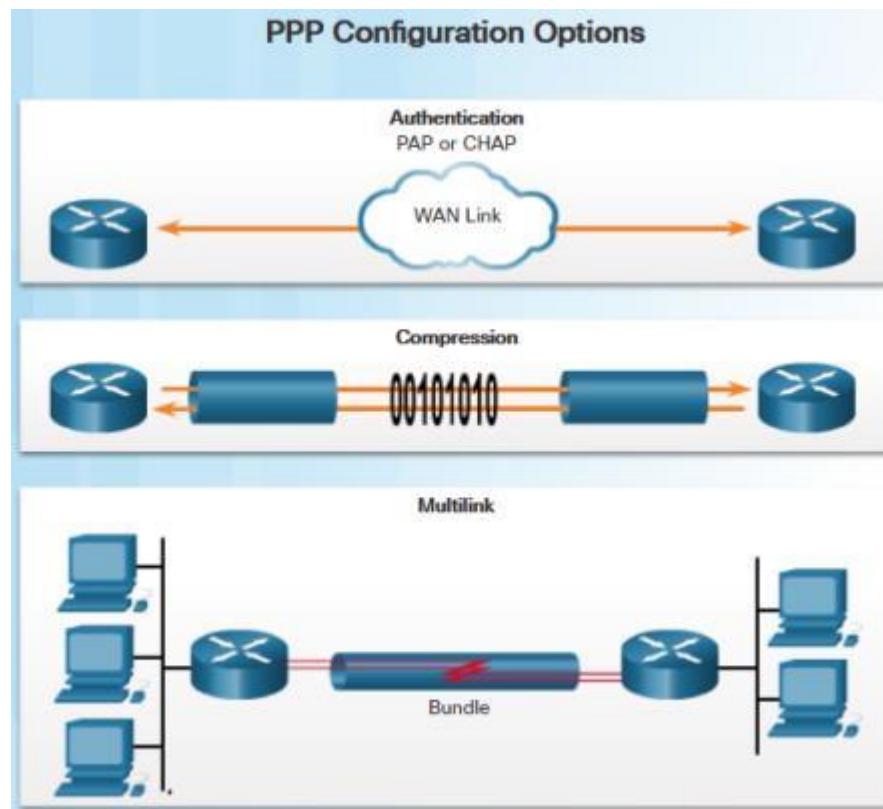
Link-termination frames terminate a link (**Terminate-Request** and **Terminate-Ack**).



PPP Operation

PPP Sessions

- PPP can be configured to support optional functions:
 - Authentication - either PAP or CHAP
 - Compression - either Stacker or Predictor
 - Multilink – combine two or more channels to increase the WAN bandwidth





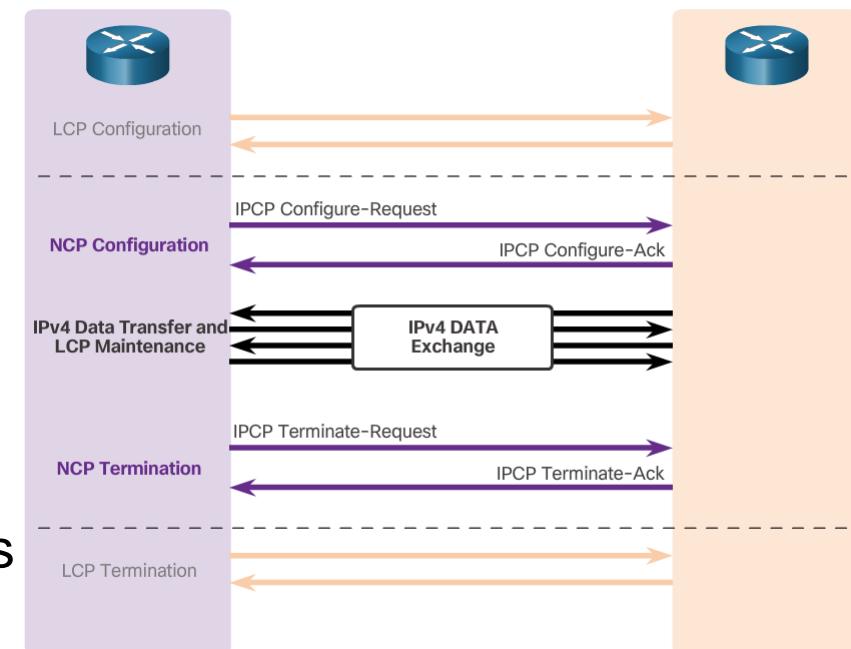
PPP Operation

PPP Sessions

- After LCP has established the link, the routers exchange IPCP messages
- IPCP negotiates 2 options

- Compression – saves BW
 - Devices negotiate compression algorithm. Van Jacobson TCP/IP header compression reduces TCP/IP header size to as few as 3 bytes. Improves slow serial lines for interactive traffic.

- IPv4-Address
 - IPv4-Address - Allows the initiating device to specify an IPv4 address to use for routing IP over the PPP link, or to request an IPv4 address for the responder. Before broadband (DSL and cable modem services), dialup network devices commonly used the IPv4 address option.



2.3 PPP Implementation





PPP Implementation Configure PPP

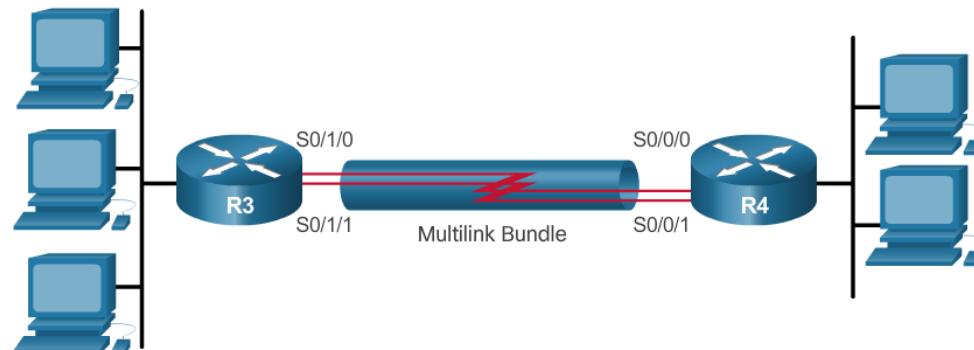
- PPP may include several LCP options:
 - Authentication, Compression, Error detection, PPP Callback, and Multilink
- To set PPP as the encapsulation method used by a serial interface, use the **encapsulation ppp** interface configuration command.
- Point-to-point software compression on serial interfaces can be configured after PPP encapsulation is enabled with the **compress** command.
- The **ppp quality percentage** command ensures that the link meets the quality requirement set; otherwise, the link closes down.



PPP Implementation

Configure PPP

- MPPP allows packets to be fragmented and sends these fragments simultaneously over multiple point-to-point links to the same remote address.
- Configuring MPPP requires two steps:
 - Step 1. Create a multilink bundle.
 - Step 2. Assign interfaces to the multilink bundle.



- Use the **show interfaces serial** command to verify proper configuration of HDLC or PPP encapsulation



PPP Implementation

Configure PPP Authentication

- RFC 1334, PPP Authentication Protocols, defines two protocols for authentication, PAP and CHAP.
 - PAP is a very basic two-way process. There is no encryption. The username and password are sent in plaintext.
 - **CHAP is more secure than PAP.** It involves a three-way exchange of a shared secret.
 - To specify the order in which the CHAP or PAP protocols are requested on the interface, use the **ppp authentication** interface configuration command. Use the **no** form of the command to disable this authentication.
 - The PAP username and password that each router sends must match those specified with the **username name password** *password* command of the other router.

We will look at CHAP Authentication in Friday's Lab



2.4 Troubleshoot WAN Connectivity



Cisco | Networking Academy®
Mind Wide Open™



Troubleshoot WAN Connectivity

Troubleshoot PPP

- A **debug** output displays information about various router operations, related traffic generated or received by the router, and any error messages.
- Debug ppp
 - Use the **debug ppp** command to display information about the operation of PPP.
 - A good command to use when troubleshooting serial interface encapsulation is the **debug ppp packet** command.
 - The **debug ppp negotiation** command enables the network administrator to view the PPP negotiation transactions, identify the problem or stage when the error occurs, and develop a resolution.
 - The **debug ppp error** command is used to display protocol errors and error statistics associated with PPP connection negotiation and operation.

We will look at debug ppp output in Friday's Lab



Troubleshoot WAN Connectivity

Troubleshoot PPP

- Debug PPP Authentication
 - Always verify your configuration with the **show interfaces serial** command, in the same way as you did without authentication.
 - Never assume your authentication configuration works without testing it using the previously covered show commands
 - For debugging PPP authentication, use the **debug ppp authentication** command.

```
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
```

2.4 Chapter Summary





Chapter Summary

Summary

- Serial transmissions sequentially send **one bit at a time over a single channel**. A serial port is bidirectional. Synchronous serial communications require a **clocking signal**.
- 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. In the United States, OC transmission rates are standardized specifications for SONET.
- The bandwidth hierarchy used by carriers is different in North America (T-carrier) and Europe (E-carrier). In North America, the fundamental line speed is 64 kbps, or DS0. Multiple DS0s are **bundled** together to provide higher line speeds.
- 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.



Summary Continued

- 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. PPP uses HDLC for encapsulating datagrams.
- **LCP** is the PPP protocol used to establish, configure, test, and terminate the data link connection.
- LCP can optionally authenticate a peer using PAP or CHAP.
- A family of **NCPs** are used by the PPP protocol to simultaneously support multiple network layer protocols.



Summary Continued

- **Multilink** PPP spreads traffic across bundled links by fragmenting packets and simultaneously sending these fragments over multiple links to same remote address, where they are reassembled.
- **PPP optionally supports authentication** using **PAP**, **CHAP**, or both PAP and CHAP protocols.
- **PAP** sends authentication data in plaintext.
- **CHAP** uses a 3-way handshake, periodic challenge messaging, and a one-way hash that helps protect against playback attacks.



Reminder

Lab on Friday

- In this lab, you will configure PPP encapsulation on dedicated serial links between two routers. PPP CHAP will also be configured on the PPP serial links.
- You will also examine the effects of the encapsulation and authentication changes on the status of the serial link and use **debug ppp** commands below to observe the effects of changing the PPP configurations on both routers.
- **debug ppp**
- **debug ppp negotiation**
- **debug ppp packet**
- **debug ppp authentication**





What does UP UP Mean?

Serial0/0/0 is **up**, line protocol is **up** (connected)

Line Status

Layer 1

Physical Layer

'Hardware'

Carrier Signal

NB Line must be up before protocol can be up as protocol is carried on the line. No physical connection...No line protocol.

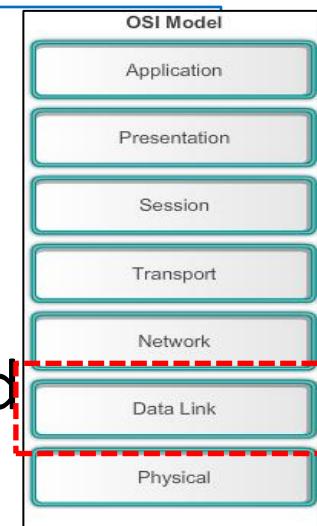


Protocol Status

Layer 2

Data Link Layer

Keep-Alive msgs Tx'd
(Heart-beat msgs)



NB Line protocol down means software processes 'say' line not useable. Interface mis-config'd? duplex?, clock rate?

Typical meanings when a ping does not work (Source: Odom 2013, p.325)

Line Status

Admin Down

Down

Up

Up

Protocol Status

Down

Down

Down

Up

Likely General Reason/Layer

Interface shutdown

Layer 1

Layer 2

Layer 3



Chapter 3: Branch Connections



Connecting Networks

Cisco | Networking Academy®
Mind Wide Open™



Chapter 3- Sections & Objectives

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



3.1 Remote Access Connections



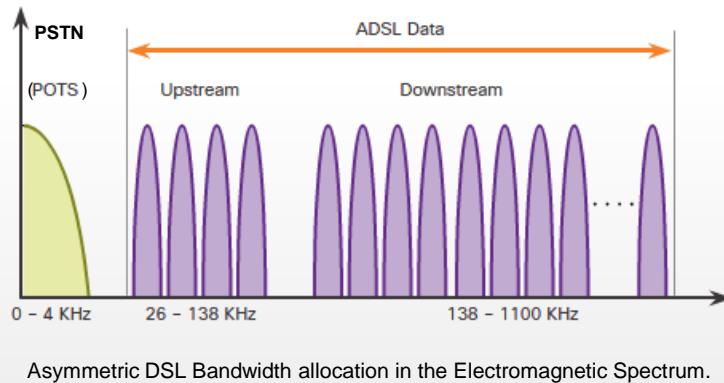
Cisco | Networking Academy®
Mind Wide Open™



Remote Access Connections

Broadband Connections - DSL

- Bandwidth allocation on copper wire for Asymmetric DSL (ADSL).

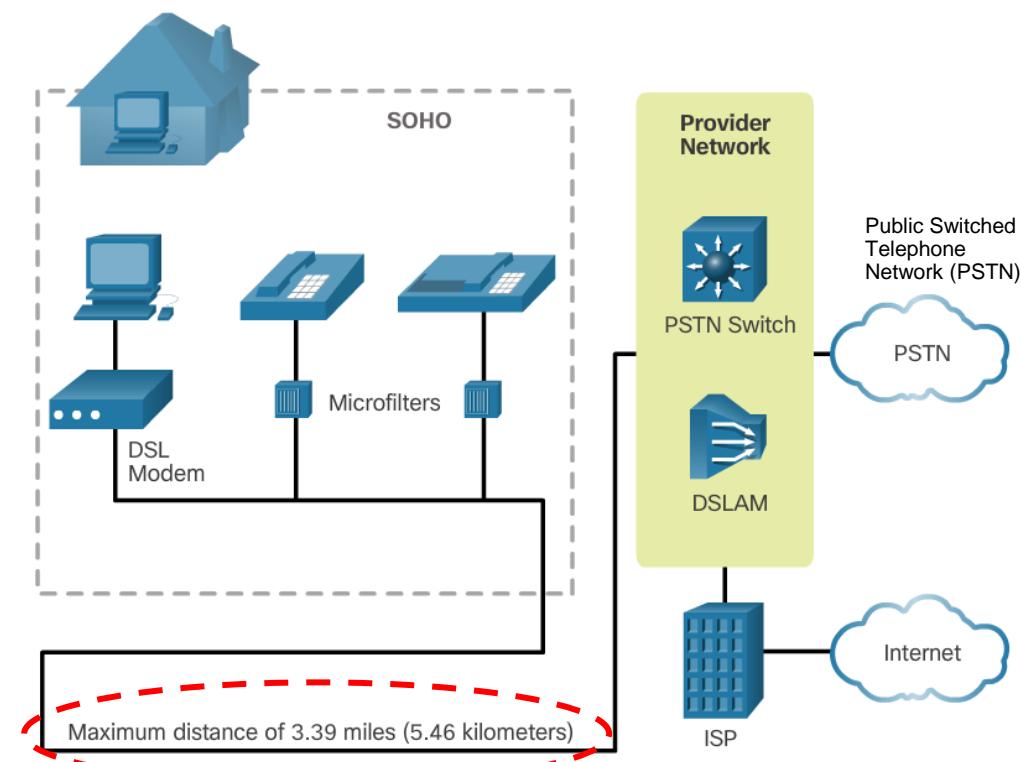


The above Figure shows bandwidth space allocation on a copper wire for asymmetric DSL (ADSL).

PSTN shows frequency range used by the voice-grade telephone service

ADSL shows the frequency space used by the upstream and downstream DSL signals.

The PSTN area plus the ADSL area shows the entire frequency range supported by the copper wire pair.

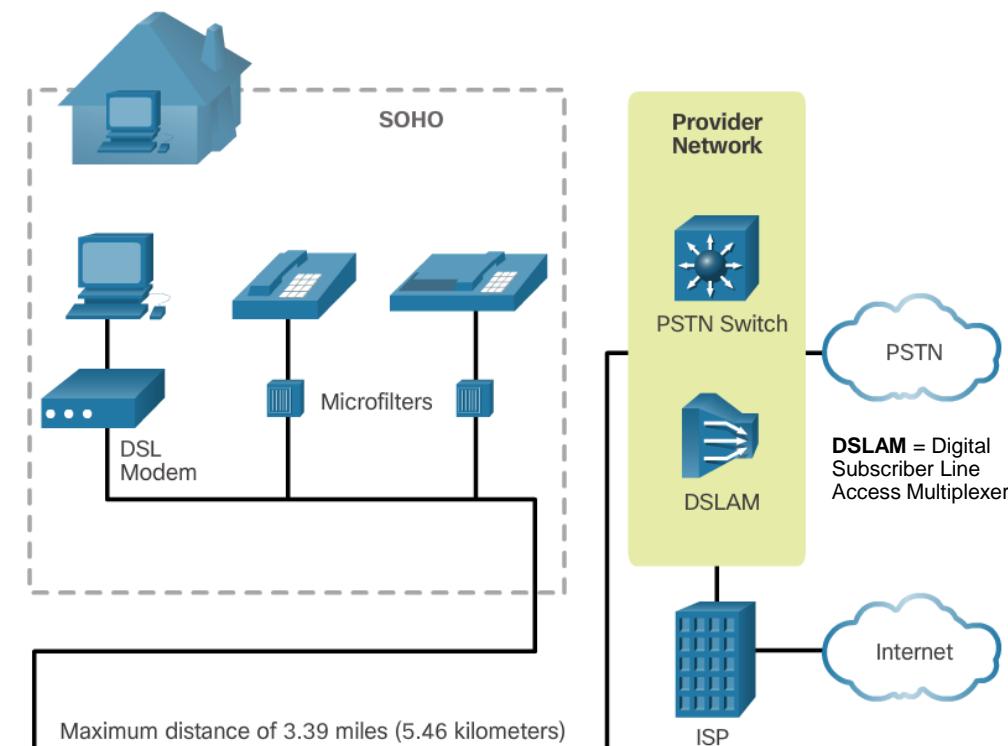




Remote Access Connections

Broadband Connections - DSL

- A Digital Subscriber Line (DSL) is a means of **providing high-speed connections over installed copper wires.**
- The two important components are the DSL transceiver and the DSLAM
- The **advantage** that DSL has over cable technology is that DSL is **not a shared medium**. Each user has a separate direct connection to the DSLAM.
- Transfer rates dependent length of local loop, type and condition of the cabling.
- **Loop < 3.39 miles (5.46Km)**



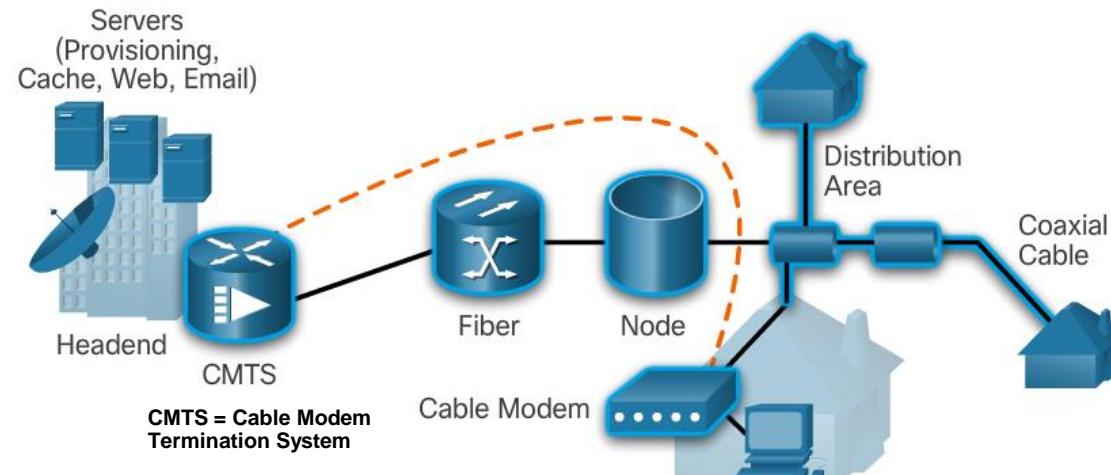


Remote Access Connections

Broadband Connections - CABLE

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

HFC = hybrid fibre coaxial





Remote Access Connections

Broadband Connections

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



Remote Access Connections

Select a Broadband Connection

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



3.2 PPPoE



Cisco | Networking Academy®
Mind Wide Open™

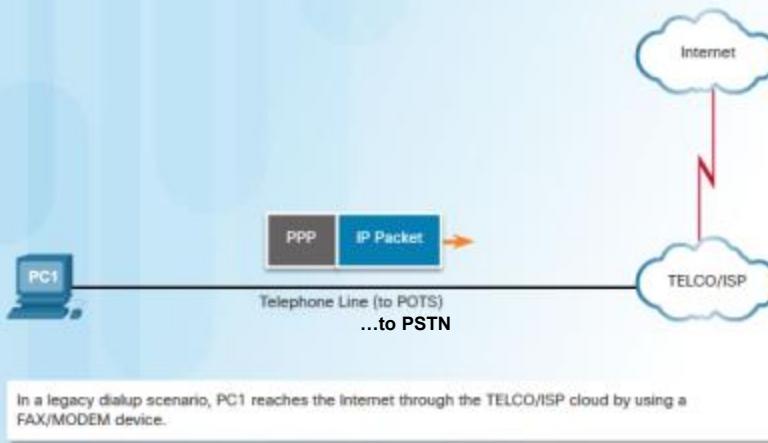


PPPoE

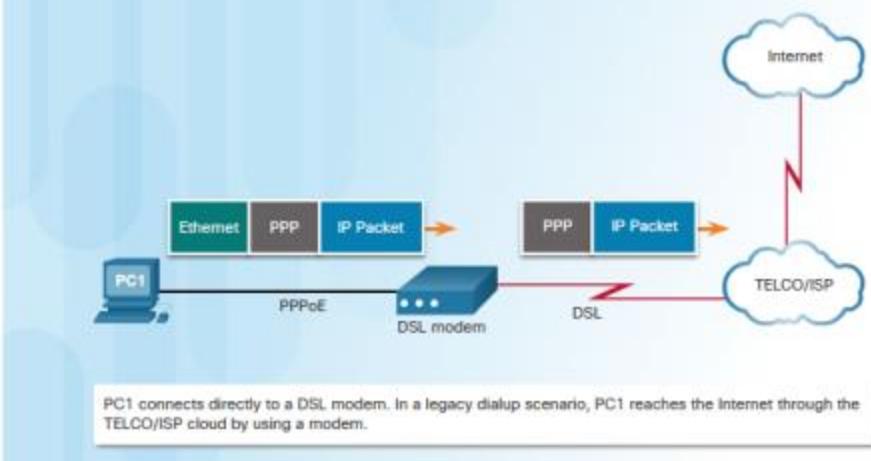
PPPoE Overview

- PPP can be used on all serial links including those links created with dial-up analog and ISDN modems.

PPP Frames Over Legacy Dialup Connection



PPP Frames Over an Ethernet Connection (PPPoE)



PPP supports authentication...Have you paid your phone bill?



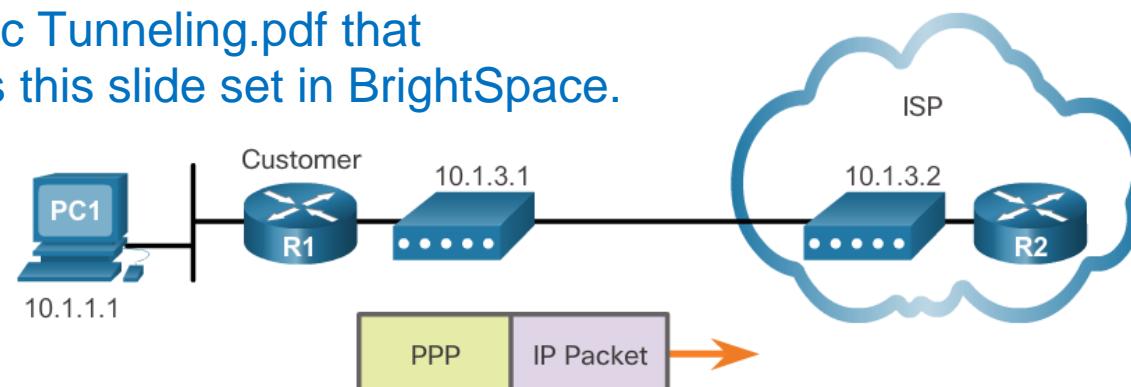
PPPoE

PPPoE Overview

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

Tunneling as a general concept:

– See the doc Tunneling.pdf that accompanies this slide set in BrightSpace.



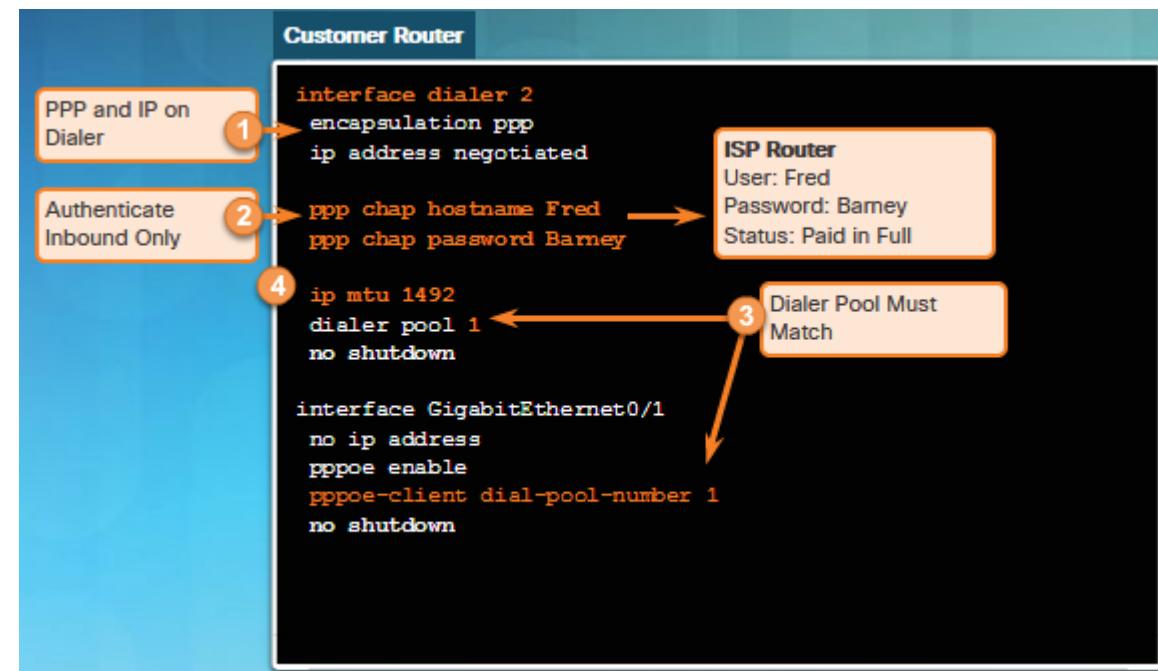


PPPoE

Implement PPPoE

■ PPPoE Configuration

- **Dialer interface:** 'Dialer' = old telephony term for dialing on a rotary telephone.
- Dialer interfaces have been in Cisco IOS for a long time. In the past routers used dial-up technology to make a phone call to another router to make a physical link.
- Nowadays, dialer interfaces are used as logical interfaces which may be dynamically bound, to use another interface.



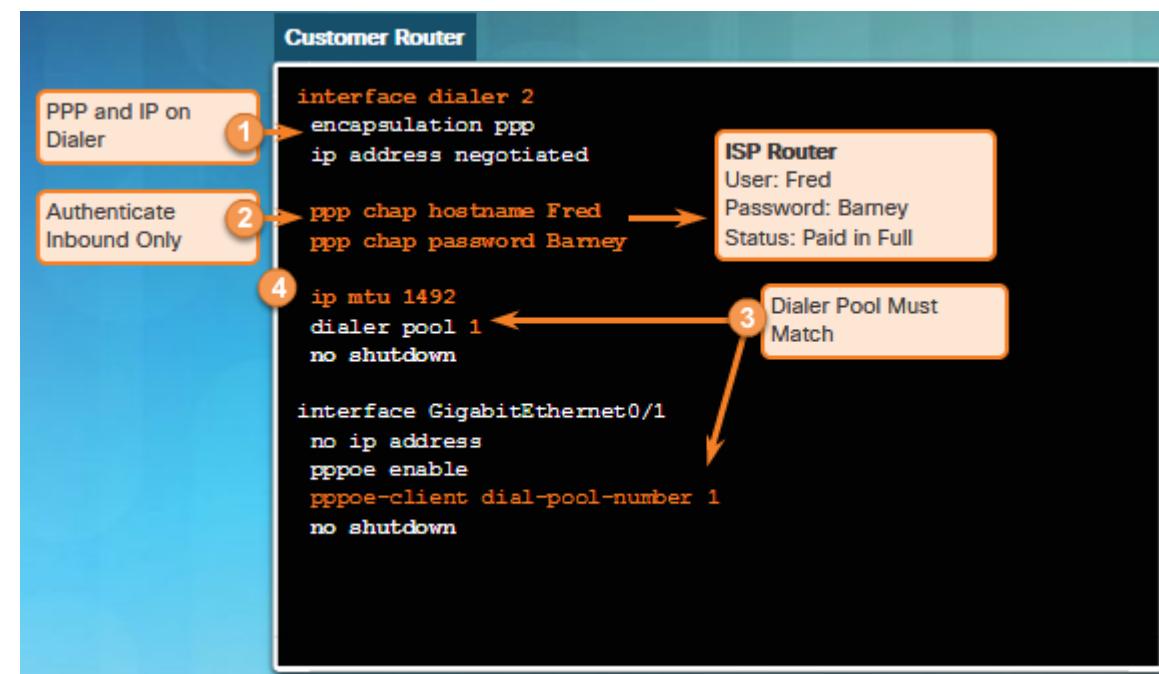


PPPoE

Implement PPPoE

■ PPPoE Configuration

- The dialer interface is created using the **interface dialer number** command.
- The PPP CHAP configuration usually defines one-way authentication; therefore, the ISP authenticates the customer. (Have you paid your bill?)
- The physical Ethernet interface that connects to the DSL modem is then enabled with the command **pppoe enable**.
- The dialer interface is linked to the Ethernet interface with the **dialer pool** and **pppoe-client** commands, using the same number.
- The **maximum transmission unit (MTU)** should be set down to **1492**, versus the default of 1500, to accommodate the PPPoE headers.





PPPoE

Implement PPPoE

■ PPPoE Verification

- The **show ip interface brief** command is issued to verify the IPv4 address automatically assigned to the dialer interface by the ISP router.
- The **show interface dialer** command verifies the MTU and PPP encapsulation configured on the dialer interface.
- The **show pppoe session** command is used to display information about currently active PPPoE sessions.
- The Ethernet MAC addresses can be verified by using the **show interfaces** command on each router.

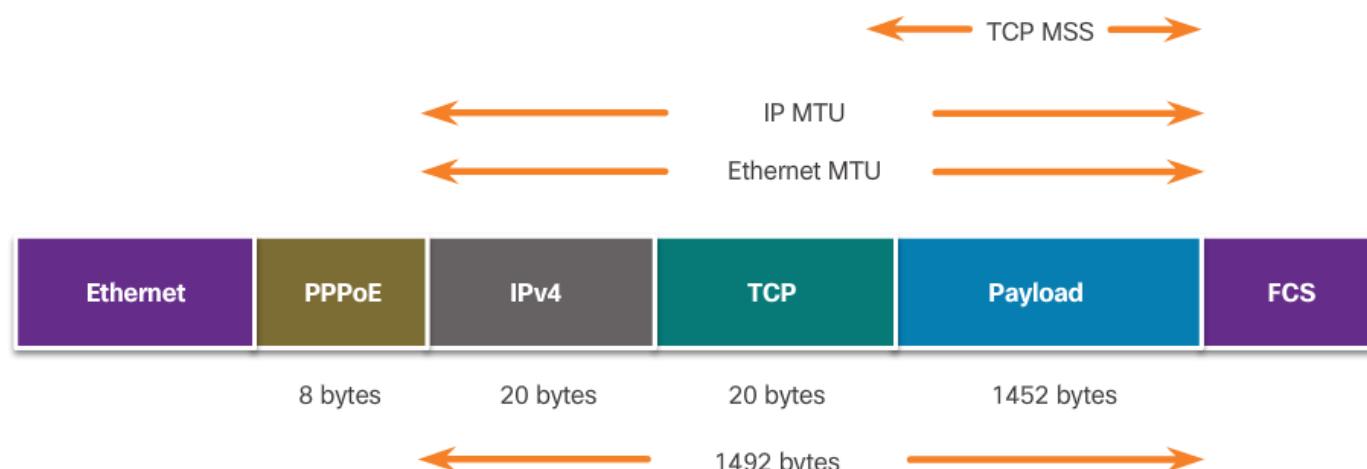


PPPoE

Implement PPPoE

■ PPPoE Troubleshooting

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





3.3 VPNs



Cisco | Networking Academy®
Mind Wide Open™



VPNs

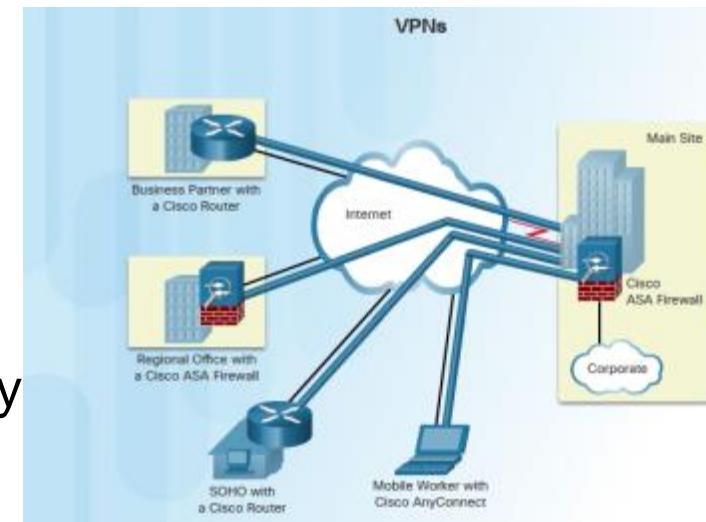
Fundamentals of VPNs

■ Introducing VPNs

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

■ Benefits of VPNs *

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

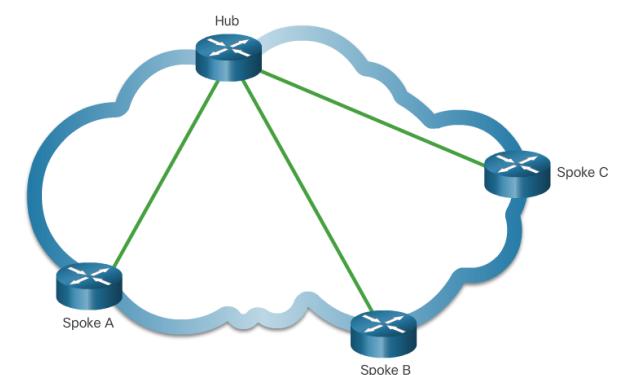
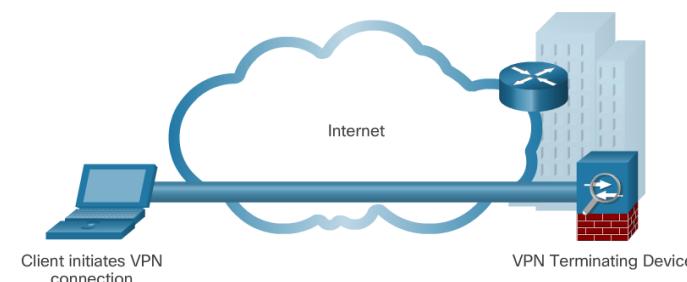
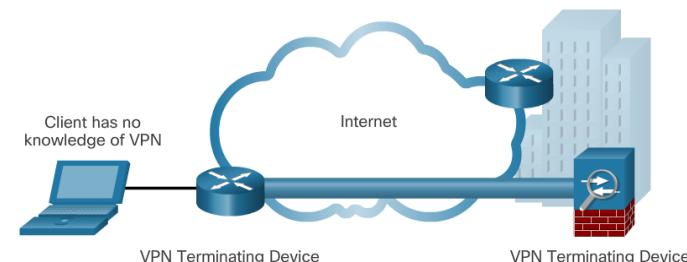




VPNs

Types of VPNs *

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





3.4 GRE: Generic Routing Encapsulation



Cisco | Networking Academy®
Mind Wide Open™

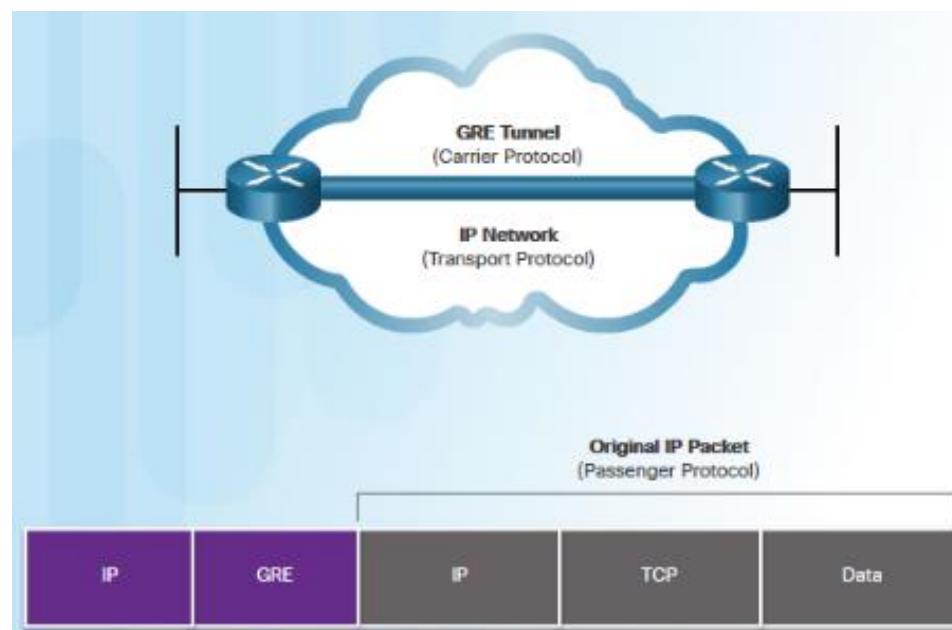


GRE

GRE Overview

■ GRE Introduction

- Generic Routing Encapsulation (GRE) – a basic, non-secure, site-to-site VPN **tunneling** protocol.
- GRE is designed to manage the transportation of multiprotocol and IP multicast traffic between two or more sites, that may only have IP connectivity. GRE is a **tunnelling** protocol developed by Cisco..



Tunneling as a general concept:
– See the doc Tunneling.pdf that accompanies this slide set in BrightSpace.

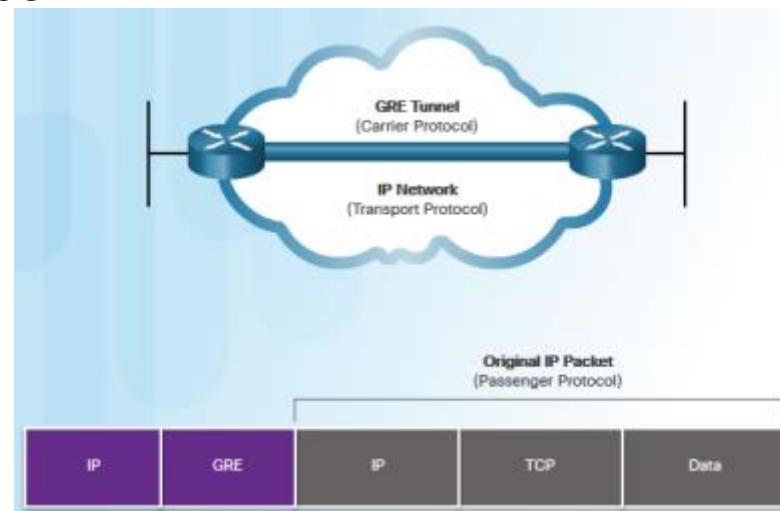


GRE

GRE Overview

■ GRE Introduction

- A tunnel interface supports a header for each of the following:
 - **Passenger protocol:** The original IPv4 or IPv6 packet that will be encapsulated by the carrier protocol.
 - **Carrier protocol:** The encapsulation protocol such as GRE that encapsulates the passenger protocol.
 - **Transport protocol:** The delivery protocol such as IP that carries the carrier protocol.



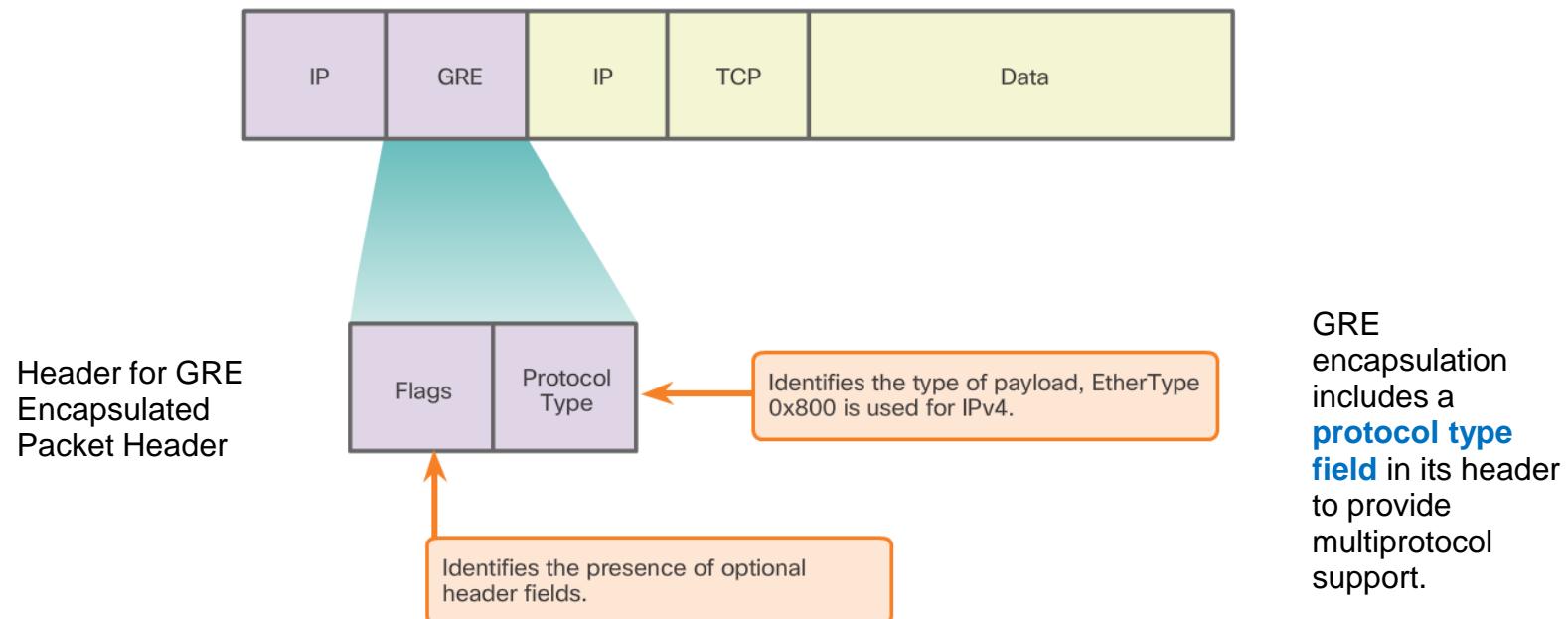


GRE

GRE Overview

■ GRE Characteristics

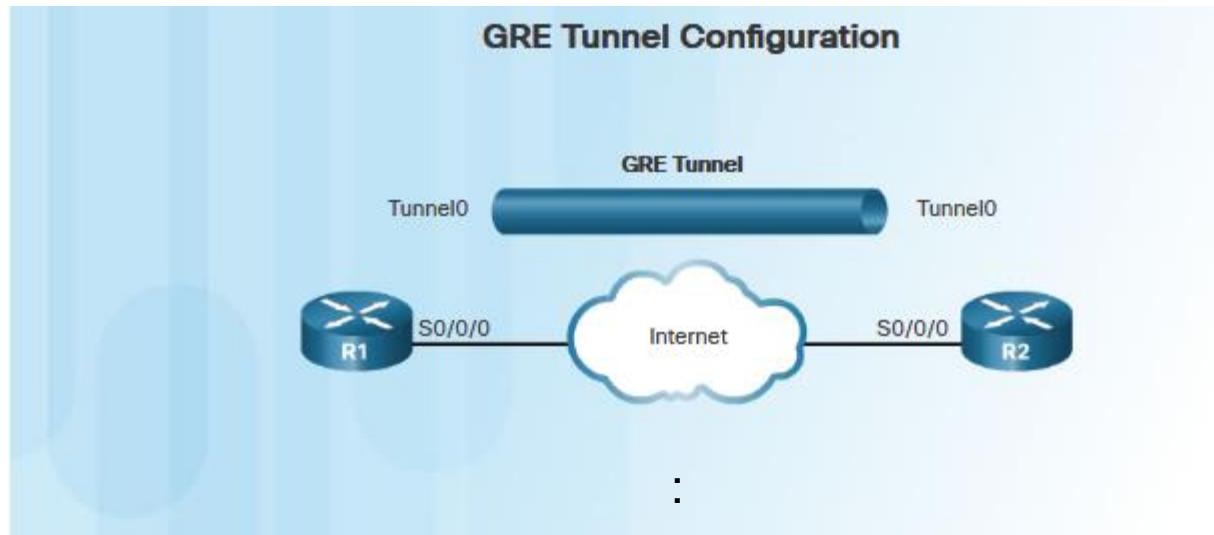
- IP **tunneling** using GRE enables *network expansion across a single-protocol backbone* environment.
- GRE is stateless. No flow-control mechanisms included by default.
- GRE does not include any strong security mechanisms to protect its payload.





GRE

Implementing GRE

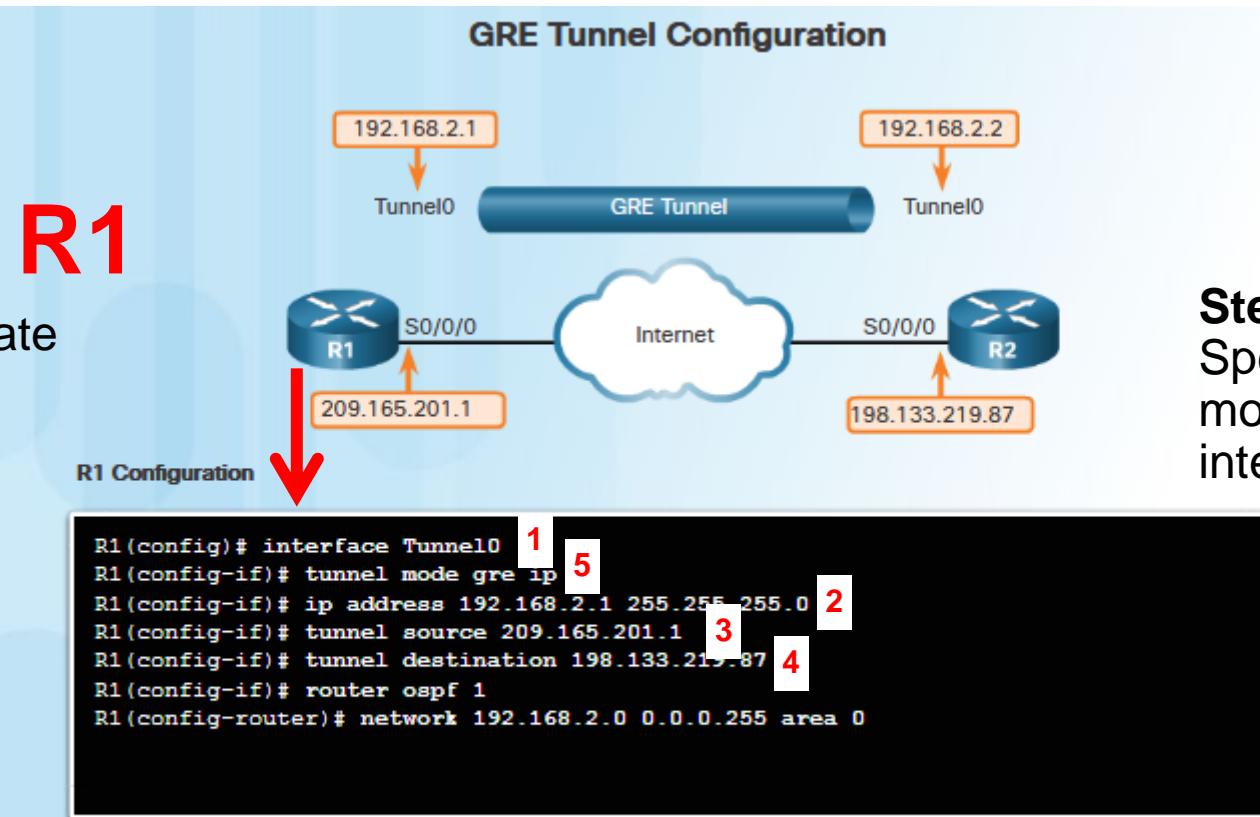


Five steps to configuring a GRE tunnel:

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



GRE Implementing GRE



Step 2. Configure an IP address for the tunnel interface

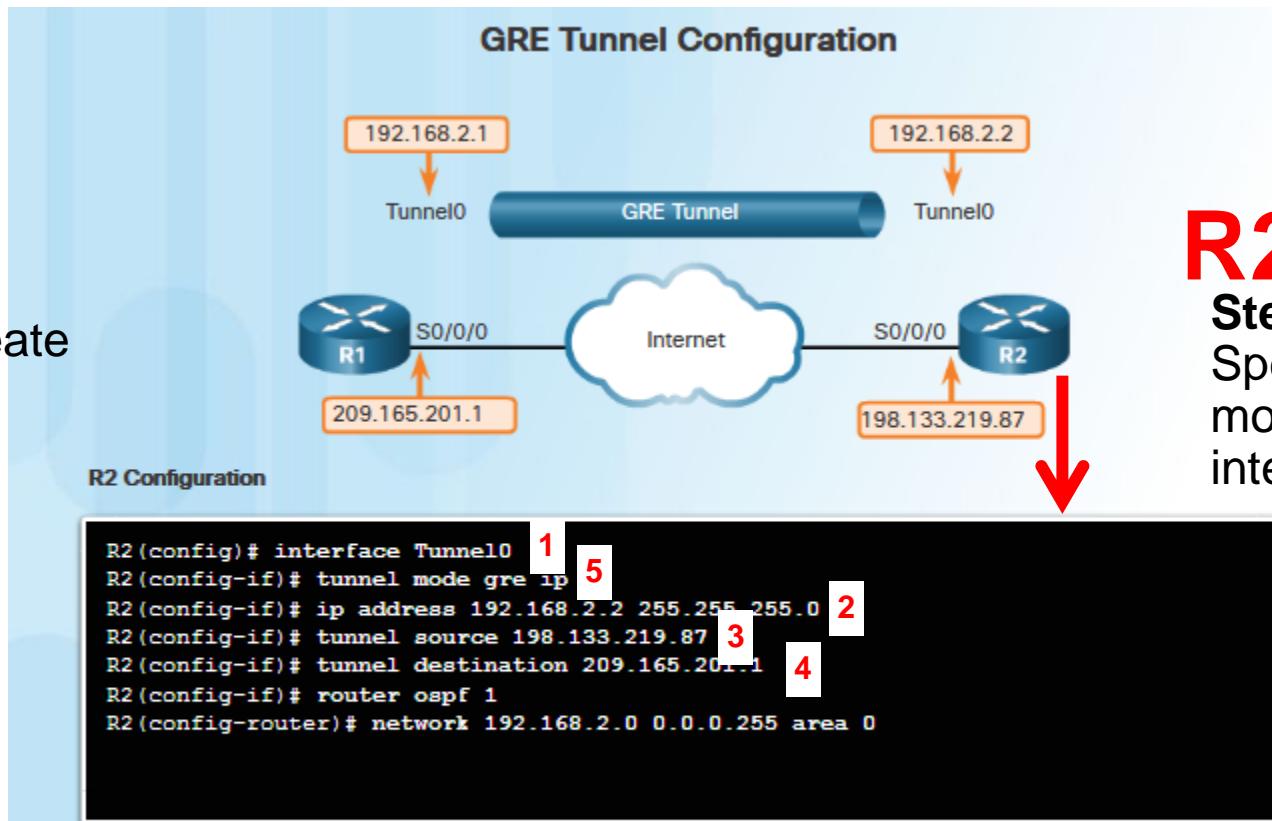
Step 3. Specify the tunnel source IP address

Step 4. Specify the tunnel destination IP address



GRE

Implementing GRE



Step 1. Create a tunnel interface

Step 2. Configure an IP address for the tunnel interface

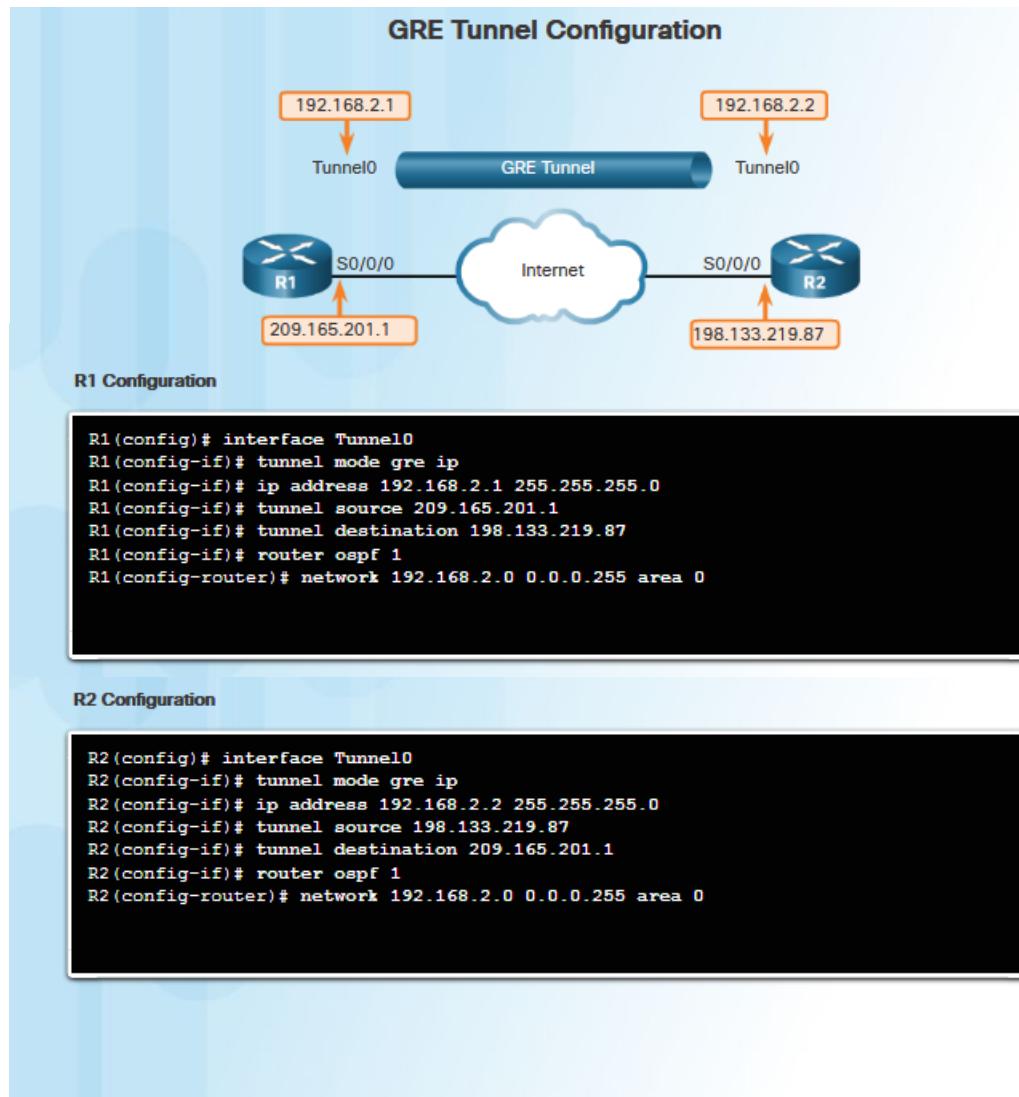
Step 3. Specify the tunnel source IP address

Step 4. Specify the tunnel destination IP address



GRE

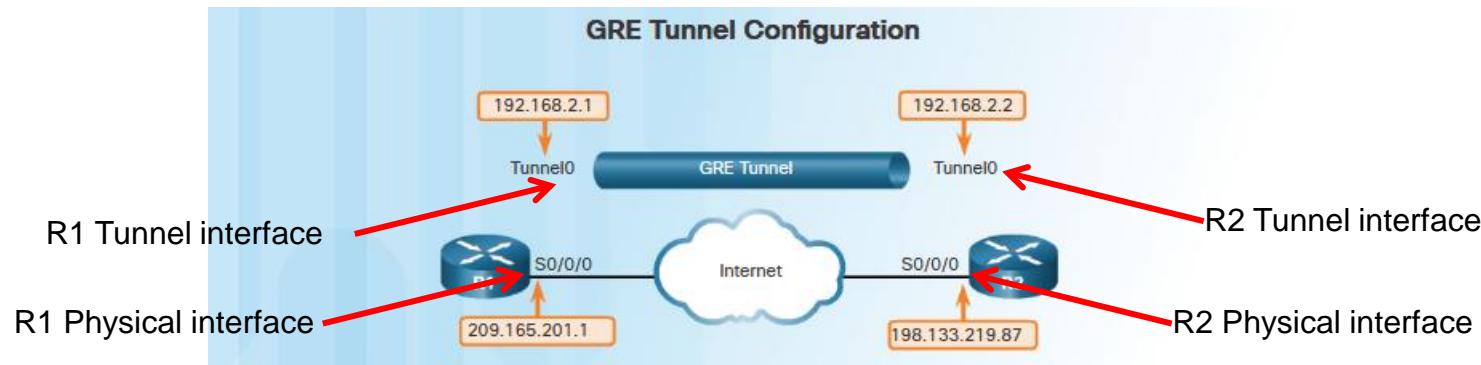
Implementing GRE





GRE

Implementing GRE



- Difficult to remember which IP addresses are on the physical interfaces and which IP addresses are on the tunnel interfaces..
- The below may help...
 - The physical interfaces are configured before the GRE tunnel interfaces are created.
 - The IP addresses in the tunnel **source** and tunnel **destination** commands refer to the IP addresses of the **physical interfaces**.
 - The IP addresses in the ip address command on the tunnel interfaces are from the private IP network specifically selected for the GRE tunnel.



GRE

Implementing GRE

- GRE tunnel commands used in the previous slides..

Command	Description
<code>tunnel mode gre ip</code>	Specifies that the mode of the tunnel interface is GRE over IP.
<code>tunnel source ip_address</code>	Specifies the tunnel source address.
<code>tunnel destination ip_address</code>	Specifies the tunnel destination address.
<code>ip address ip_address mask</code>	Specifies the IP address of the tunnel interface.



GRE

Implement GRE

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



3.5 eBGP



Cisco | Networking Academy®
Mind Wide Open™



eBGP BGP Overview

■ IGP and EGP

- Interior Gateway Protocols (IGPs) are used to exchange routing information within a company network or an autonomous system (AS).
- Exterior Gateway Protocols (EGPs) are used for the exchange of routing information between autonomous systems.

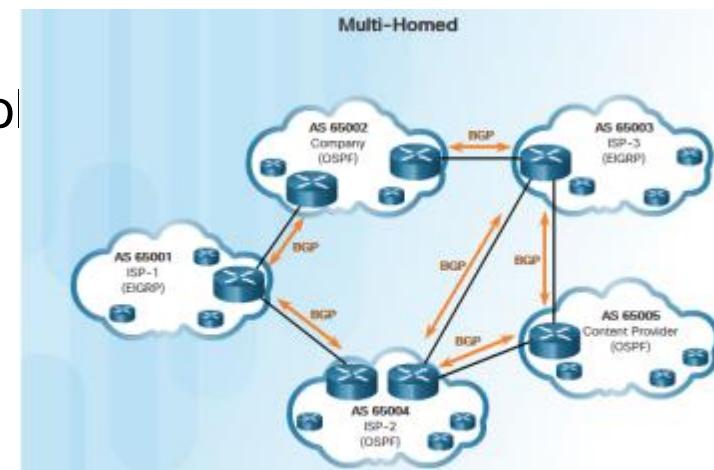
■ eBGP and iBGP

- External BGP (eBGP) is the routing protocol used between routers in different autonomous systems.
- Internal BGP (iBGP) is the routing protocol used between routers in the same AS.

■ This course focuses on eBGP only.

IGP – Move packets efficiently

BGP – Political, security, economic, policies. ISP may not wish to carry another ISP's traffic, (unless fee involved). See Tannenbaum pp.497-502.



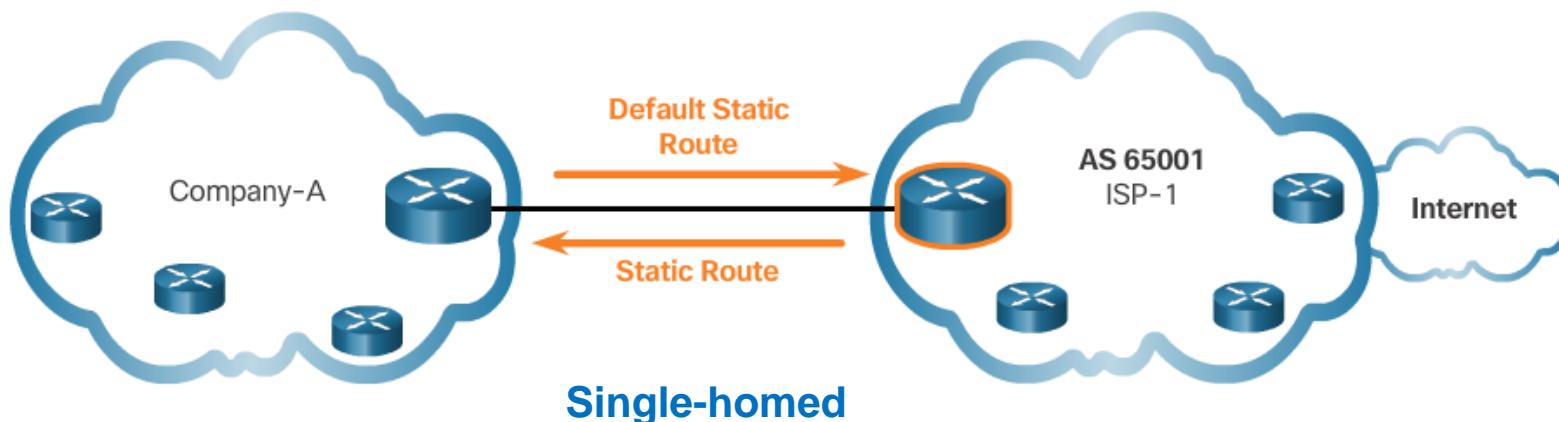


eBGP

BGP Design Considerations

■ When to use BGP

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





eBGP

BGP Design Considerations

■ BGP Options

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



eBGP

BGP Branch Configuration

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

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

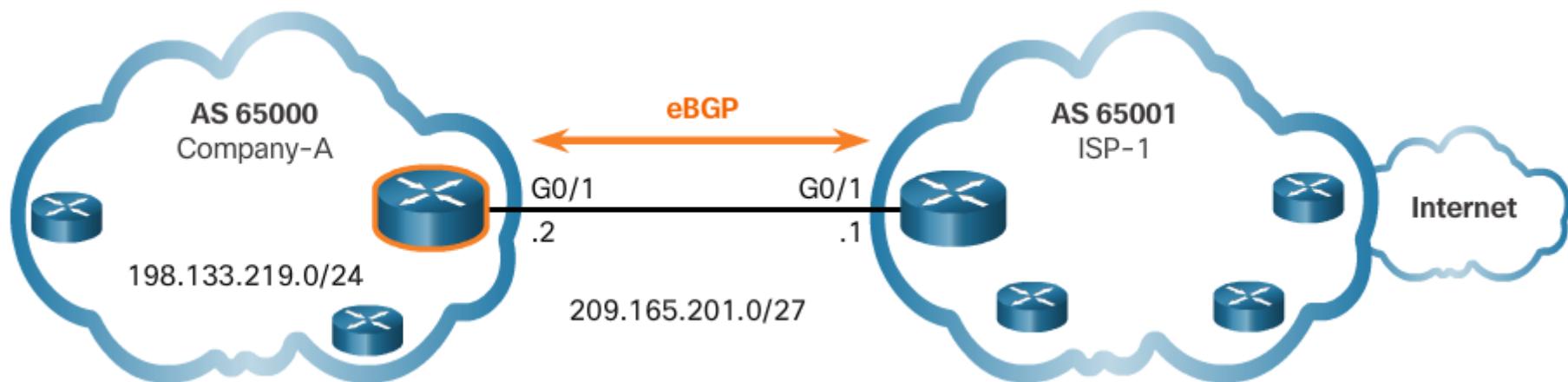


eBGP

BGP Branch Configuration

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

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



3.6 Chapter Summary





Chapter Summary

Summary

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



Chapter Summary

Summary Continued

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



Reminder

Lab on Friday

- In this lab, you will configure a GRE VPN tunnel. Verify that network traffic is using the tunnel. Configure OSPF inside GRE VPN tunnel.

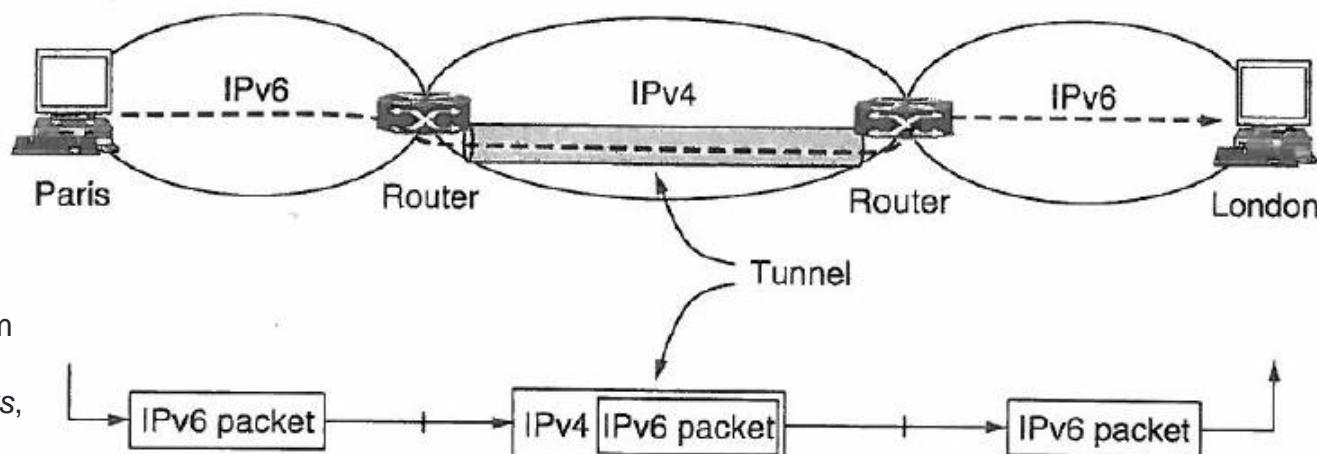




Tunneling

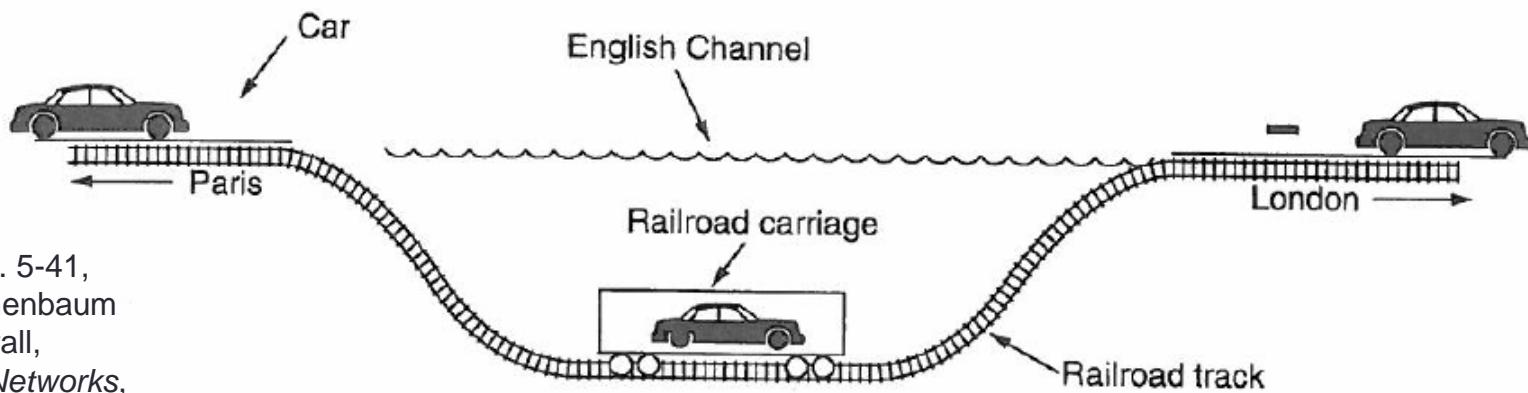
- Problem...
 - Source host and destination host are both on the same type of network, but connected by different type of network. How to make them inter-work?
- Solution...
 - Tunneling
- Concept used in
 - ‘IPv6 over IPv4’
<https://tunnelbroker.net/> Your own tunnel?
 - PPPoE
 - GRE
 - VPNs

Tunneling



Source: Fig. 5-40,
p.448, Tannenbaum
and Wetherall,
Computer Networks,
5th Ed. 2011.

Figure 5-40. Tunneling a packet from Paris to London.



Source: Fig. 5-41,
p.449, Tannenbaum
and Wetherall,
Computer Networks,
5th Ed. 2011.

Figure 5-41. Tunneling a car from France to England.

Tunneling

- Path = one big tunnel (London to Paris Office)
 - Between two multi-protocol routers across the IPv4 internet
 - Similar to a hop over a single link
 - IPv6 packet encapsulated inside IPv4 packet IPv6 ‘**IPv6 over IPv4**’.
- Tunneling widely used technique
 - Connect networks of one protocol type using a network of another protocol type.
 - Resulting network is an **overlay** network...overlaid on the base network.

Tunneling

- A Disadvantage/Advantage
 - Disadvantage
 - Hosts on the underlying network can't 'see' the packets. The packets can't 'break out' in middle of tunnel.
 - Advantage (for VPN)
 - Hosts on the underlying network can't 'see' the packets. Hence 'private' network.
 - VPN is an 'overlay' used to give 'some' security.

Note: VPNs are implemented with encryption such as IPsec.

Tunneling

- Reference

Tannenbaum and Wetherall, *Computer Networks*, 5th Ed.
2011,
Section 5.5.3, pp. 447-449.



Chapter 4: Access Control Lists



Cisco | Networking Academy®
Mind Wide Open™



Chapter 4 - Sections & Objectives

- 4.1 Standard ACL Operation and Configuration
 - Configure standard IPv4 ACLs.
- 4.2 Extended IPv4 ACLs
 - Configure extended IPv4 ACLs.
- 4.3 IPv6 ACLs
 - Configure IPv6 ACLs.
- 4.4 Troubleshoot ACLs
 - Troubleshoot ACLs.



4.1 Standard ACL Operation and Configuration Review



Cisco | Networking Academy®
Mind Wide Open™



ACL Operation Overview

ACLs and the Wildcard Mask

- An ACL is a sequential list of permit or deny statements, known as access control entries (ACEs).
- As network traffic passes through an interface configured with an ACL, the router compares the information within the packet against each ACE.
- An IPv4 ACE includes the use of a wildcard mask to filter IPv4 addresses.
- Calculate wildcard mask... just subtract subnet mask from 255

NWK = 10.0.0.0 SNM = 255.0.0.0

255.255.255.255

255. 0. 0. 0

0.255.255.255

WCM = 0.255.255.255

NWK = 192.168.10.0 SNM = 255.255.255.0

255.255.255.255

255.255.255. 0

0. 0. 0.255

WCM = 0.0.0.255



ACL Operation Overview

ACLs and the Wildcard Mask cont...

Wildcard Masking

Octet Bit Position and Address Value for Bit



Examples

0 0 0 0 0 0 0 0	= Match All Address Bits (Match All)
0 0 1 1 1 1 1 1	= Ignore Last 6 Address Bits
0 0 0 0 1 1 1 1	= Ignore Last 4 Address Bits
1 1 1 1 1 1 0 0	= Ignore First 6 Address Bits
1 1 1 1 1 1 1 1	= Ignore All Bits in Octet

0 means to match the value of the corresponding address bit

1 means to ignore the value of the corresponding address bit



ACL Operation Overview

ACLs and the Wildcard Mask cont...

Wildcard Masks to Match IPv4 Hosts and Subnets

Example 1

	Decimal	Binary
IP Address	192.168.1.1	11000000.10101000.00000001.00000001
Wildcard Mask	0.0.0.0	00000000.00000000.00000000.00000000
Result	192.168.1.1	11000000.10101000.00000001.00000001

Example 2

	Decimal	Binary
IP Address	192.168.1.1	11000000.10101000.00000001.00000001
Wildcard Mask	255.255.255.255	11111111.11111111.11111111.11111111
Result	0.0.0.0	00000000.00000000.00000000.00000000

Example 3

	Decimal	Binary
IP Address	192.168.1.1	11000000.10101000.00000001.00000001
Wildcard Mask	0.0.0.255	00000000.00000000.00000000.11111111
Result	192.168.1.0	11000000.10101000.00000001.00000000



ACL Operation Overview

Applying ACLs to an Interface

Inbound and Outbound ACLs



An inbound ACL filters packets coming into a specific interface and before they are routed to the outbound interface.

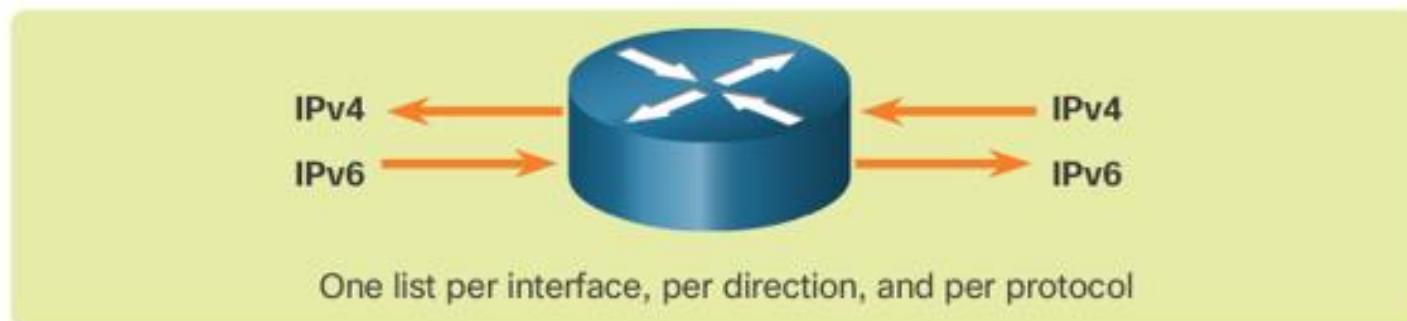
An outbound ACL filters packets after being routed, regardless of the inbound interface.



ACL Operation Overview

Applying ACLs to an Interface cont...

ACL Traffic Filtering on a Router



- **One ACL per interface:** ACLs control traffic for an interface, for example, GigabitEthernet 0/0.
- **One ACL per protocol:** To control traffic flow on an interface, an ACL must be defined for each protocol enabled on the interface.
- **One ACL per direction:** ACLs control traffic in one direction at a time on an interface. Two separate ACLs must be created to control inbound and outbound traffic.



ACL Operation Overview

Applying ACLs to an Interface cont...

ACL Traffic Filtering on a Router



One list per interface, per direction, and per protocol

With two interfaces and two protocols running, this router could have a total of 8 separate ACLs applied.

The Rules for Applying ACLs

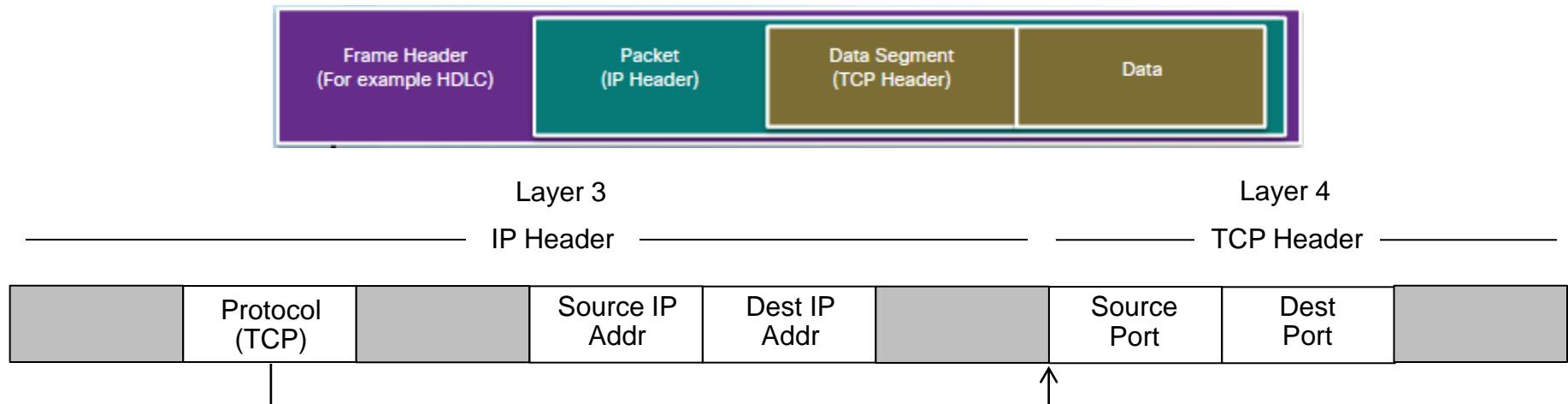
You can only have one ACL per protocol, per interface, and per direction:

- One ACL per protocol (e.g., IPv4 or IPv6)
- One ACL per direction (i.e., IN or OUT)
- One ACL per interface (e.g., GigabitEthernet0/0)



ACL Operation Overview

Packet Filtering - Controlling Network Traffic

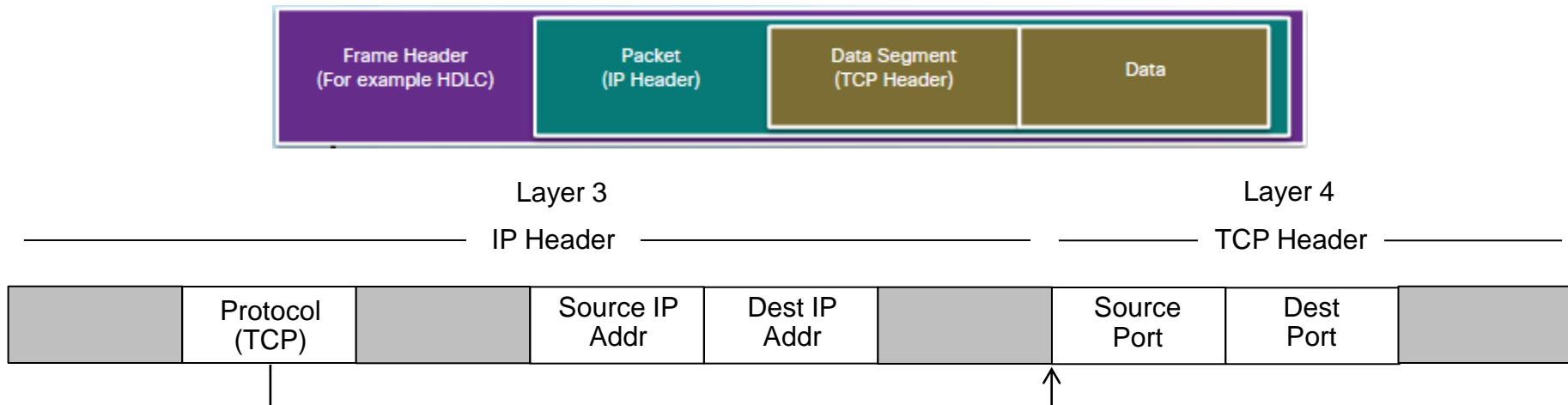


- Packet Filtering either at Layer 3 of Layer 4
 - Filtering - analyzing incoming and outgoing packets
 - Standard ACLs - filter at Layer 3 only
 - Extended ACLs - filter at Layer 3 and Layer 4



ACL Operation Overview

Packet Filtering - Controlling Network Traffic

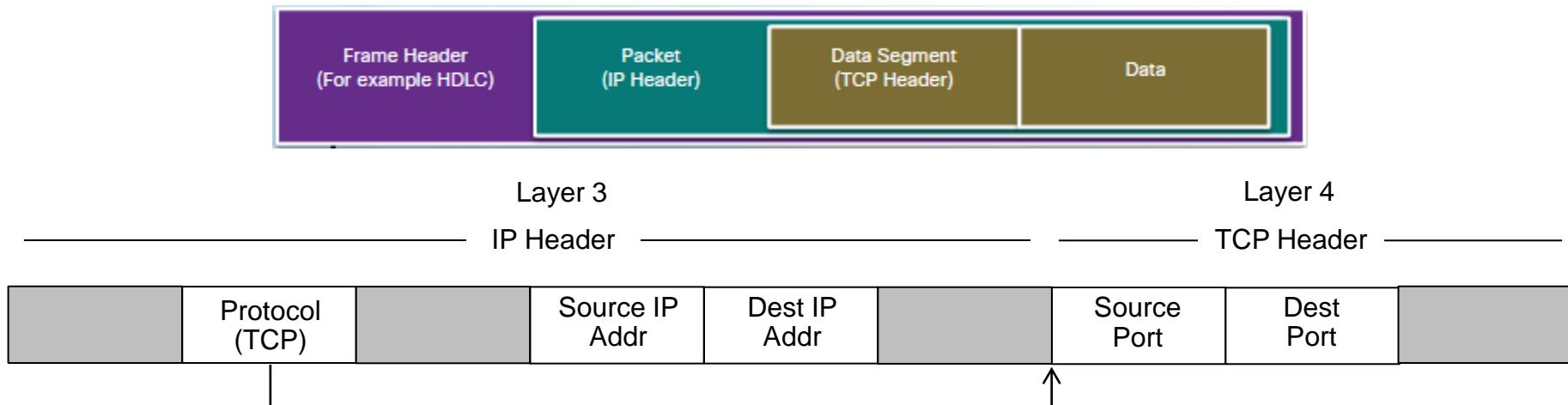


- An ACL statement examines the contents of the packet header fields. It looks inside the packet header fields for a set of values and if found, permits or denies the packet.
- An extended ACL statement examines a number of fields in the packet header. All the values in those fields must match the values in the extended ACL statement to permit the packet. If all values do not match, the packet is denied.



ACL Operation Overview

Packet Filtering - Controlling Network Traffic



- The Header fields are the Protocol, Source IP address, Destination IP address in the IP Packet header plus the TCP or UDP source and destination port numbers in the Data Segment Header.
- Port numbers identify the application that sends or receives data.
- We can use port numbers to permit or deny access to applications and services.
- Web servers use well-known port 80 by default.



ACL Operation Overview

A TCP Conversation



TCP segments are marked with flags that denote their purpose:

- a SYN starts (synchronizes) the session
- an ACK is an acknowledgment that an expected segment was received
- a FIN finishes the session.



ACL Operation Overview

A TCP Conversation cont...

- The TCP data segment also identifies the port which matches the requested service.

Port Numbers

Port Number Range	Port Group
0 to 1023	Well-known Ports
1024 to 49151	Registered Ports
49152 to 65535	Private and/or Dynamic Ports

Well-Known Port Numbers

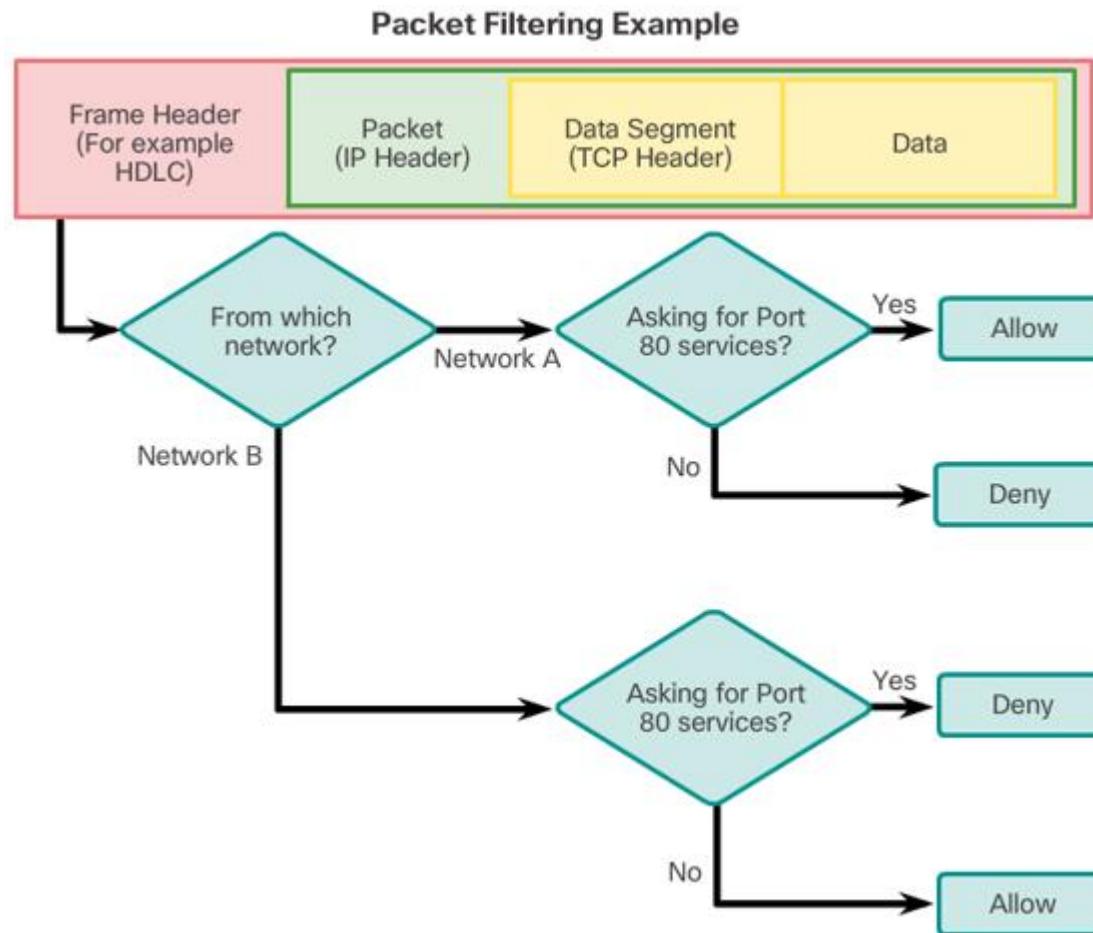
Port Number	Protocol	Application	Acronym
20	TCP	File Transfer Protocol (data)	FTP
21	TCP	File Transfer Protocol (control)	FTP
22	TCP	Secure Shell	SSH
23	TCP	Telnet	-
25	TCP	Simple Mail Transfer Protocol	SMTP
53	UDP, TCP	Domain Name Service	DNS
67	UDP	Dynamic Host Configuration Protocol (server)	DHCP
68	UDP	Dynamic Host Configuration Protocol (client)	DHCP
69	UDP	Trivial File Transfer Protocol	TFTP
80	TCP	Hypertext Transfer Protocol	HTTP
110	TCP	Post Office Protocol version 3	POP3
143	TCP	Internet Message Access Protocol	IMAP
161	UDP	Simple Network Management Protocol	SNMP
443	TCP	Hypertext Transfer Protocol Secure	HTTPS



ACL Operation Overview

ACL Packet Filtering

- Packet filtering controls access to a network by analyzing the incoming and outgoing packets and forwarding them or discarding them based on given criteria.





Types of IPv4 ACLs

Standard and Extended IPv4 ACLs

- History
 - Standard ACLs [IOS 8.3]
 - Standard ACLs are the **oldest type of ACL**. They date back to as early as Cisco IOS Software Release 8.3. Standard ACLs control traffic by the comparison of the source address of the IP packets to the addresses configured in the ACL.
 - **Compare source address only.**
 - Extended ACLs [IOS 8.3]
 - Extended ACLs were introduced in Cisco IOS Software Release 8.3. Extended ACLs control traffic by the comparison of the source and destination addresses of the IP packets to the addresses configured in the ACL.
 - **Compare source and destination addresses.**
 - IP Named ACLs [IOS 11.2]
 - IP named ACLs were introduced in Cisco IOS Software Release 11.2. This allows standard and extended ACLs to be given names instead of numbers..

<https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html>



Types of IPv4 ACLs

Standard and Extended IPv4 ACLs

- Two types of Cisco IPv4 ACLs:
 - Standard
 - **Standard ACLs** can be used to permit or deny traffic only from source IPv4 addresses. The destination of the packet and the ports involved are not evaluated
 - Extended
 - **Extended ACLs** filter IPv4 packets based on **several attributes**:
 - Protocol type
 - Source IPv4 address
 - Destination IPv4 address
 - Source TCP or UDP ports
 - Destination TCP or UDP ports
 - Optional protocol type information for finer control



Types of IPv4 ACLs

Standard and Extended IPv4 ACLs cont...

Standard ACLs

```
access-list 10 permit 192.168.30.0 0.0.0.255
```

Extended ACLs

```
access-list 103 permit tcp 192.168.30.0 0.0.0.255 any eq 80
```

Extended ACLs filter IP packets based on several attributes, including the following:

- Source and destination IP addresses
- Source and destination TCP and UDP ports
- Protocol type/Protocol number (example: IP, ICMP, UDP, TCP, etc.)



Types of IPv4 ACLs

Numbered and Named ACLs

- Standard and extended ACLs can be created using either a number or a name to identify the ACL.

Numbered ACL:

Assign a number based on protocol to be filtered.

- (1 to 99) and (1300 to 1999): Standard IP ACL
- (100 to 199) and (2000 to 2699): Extended IP ACL

Named ACL:

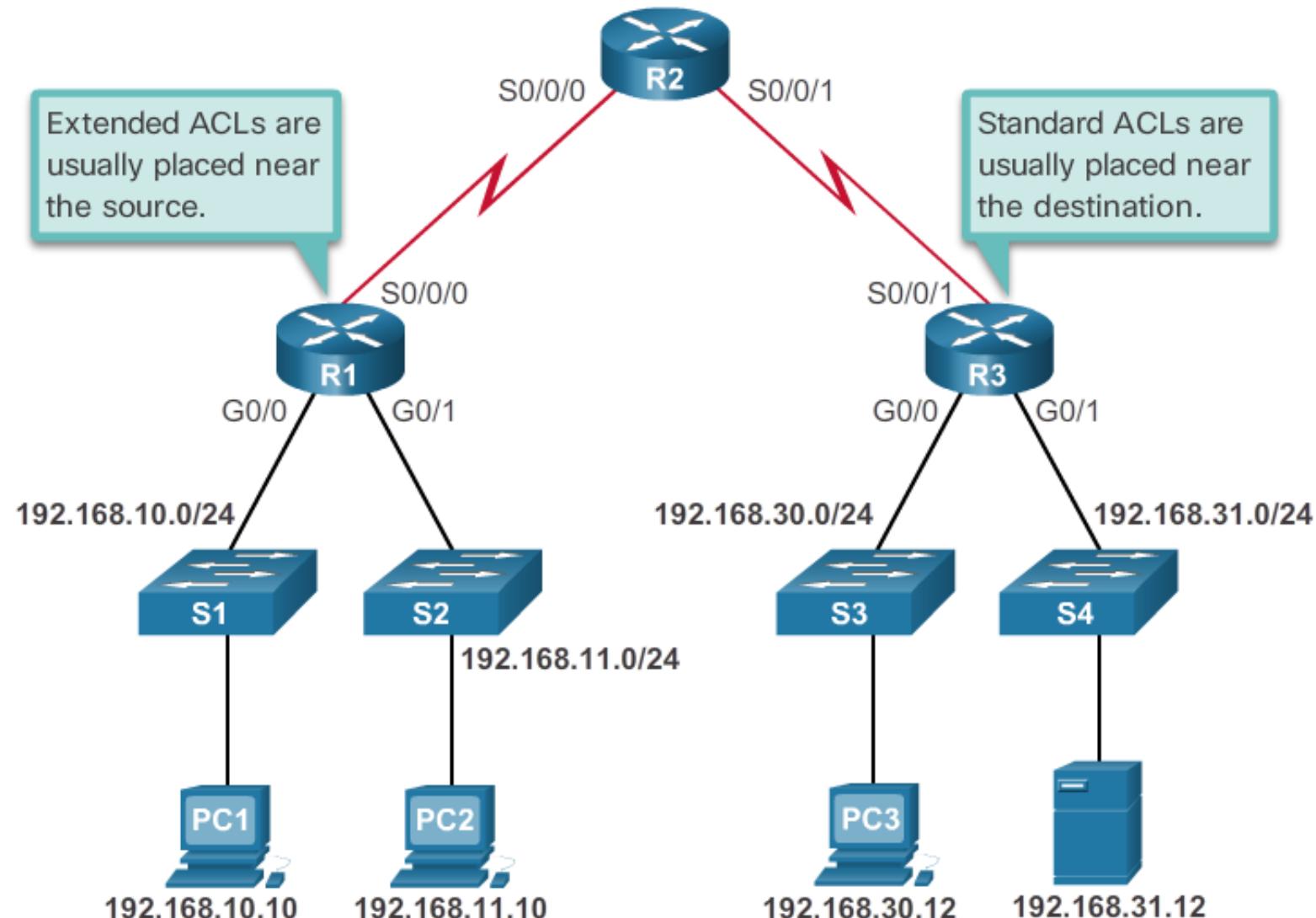
Assign a name to identify the ACL.

- Names can contain alphanumeric characters.
- It is suggested that the name be written in CAPITAL LETTERS.
- Names cannot contain spaces or punctuation.
- Entries can be added or deleted within the ACL.



Types of IPv4 ACLs

Where to Place ACLs





Types of IPv4 ACLs

Where to Place ACLs cont...

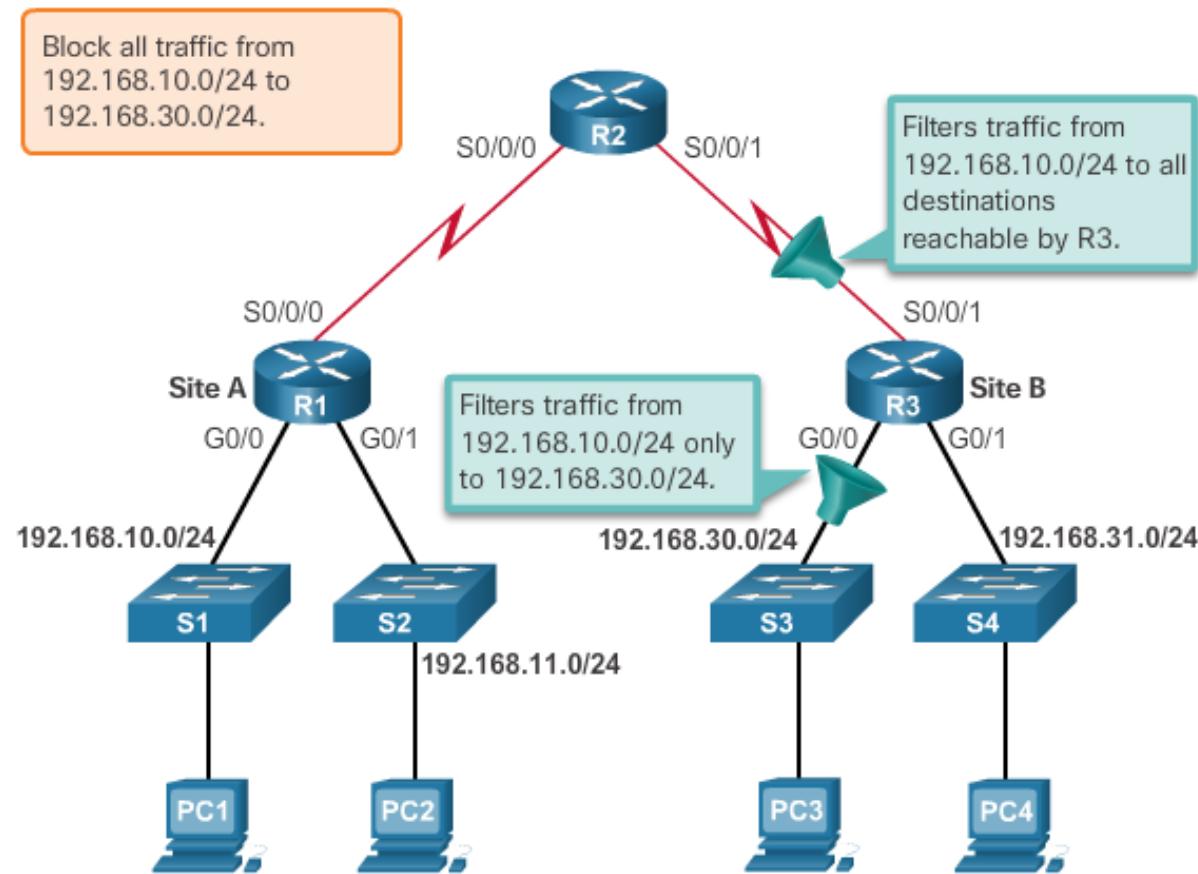
- Every ACL should be placed where it has the **greatest impact on efficiency**. The basic rules are:
 - **Standard** ACLs - Because standard ACLs do not specify destination addresses, place them as **close as possible to the destination** as possible.
 - **Extended** ACLs - Locate extended ACLs as **close as possible to the source** of the traffic to be filtered.
 - Placement of the ACL, and therefore the type of ACL used, may also depend on: the extent of the network administrator's control, bandwidth of the networks involved, and ease of configuration.



Types of IPv4 ACLs

Standard ACL Placement Example

- The administrator wants to prevent traffic originating in the 192.168.10.0/24 network from reaching the 192.168.30.0/24 network.

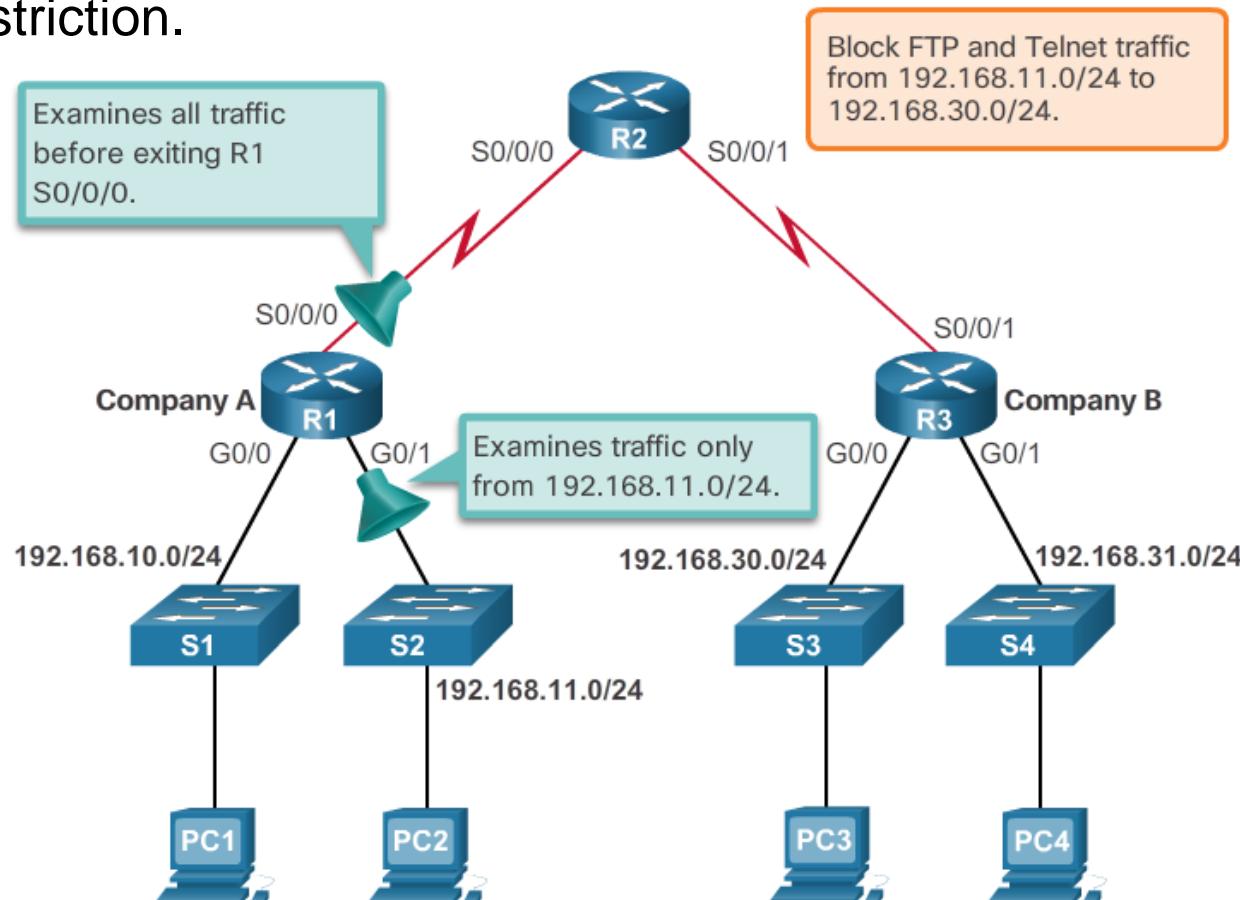




Types of IPv4 ACLs

Extended ACL Placement Example

- The administrator wants to deny Telnet and FTP traffic from the 192.168.11.0/24 network to Company B's 192.168.30.0/24 network. All other traffic from the .11 network must be permitted to leave Company A without restriction.





Standard IPv4 ACL Configuration

Configure a Standard IPv4 ACL

- Router(config)# **access-list access-list-number { deny | permit | remark } source [source-wildcard] [log]**

```
R1(config)# access-list 10 permit 192.168.10.0 0.0.0.255
R1(config)# exit
R1# show access-lists
Standard IP access list 10
    10 permit 192.168.10.0, wildcard bits 0.0.0.255
R1# conf t
Enter configuration commands, one per line. End with
CTRL/Z.
R1(config)# no access-list 10
R1(config)# exit
R1# show access-lists
R1#
```

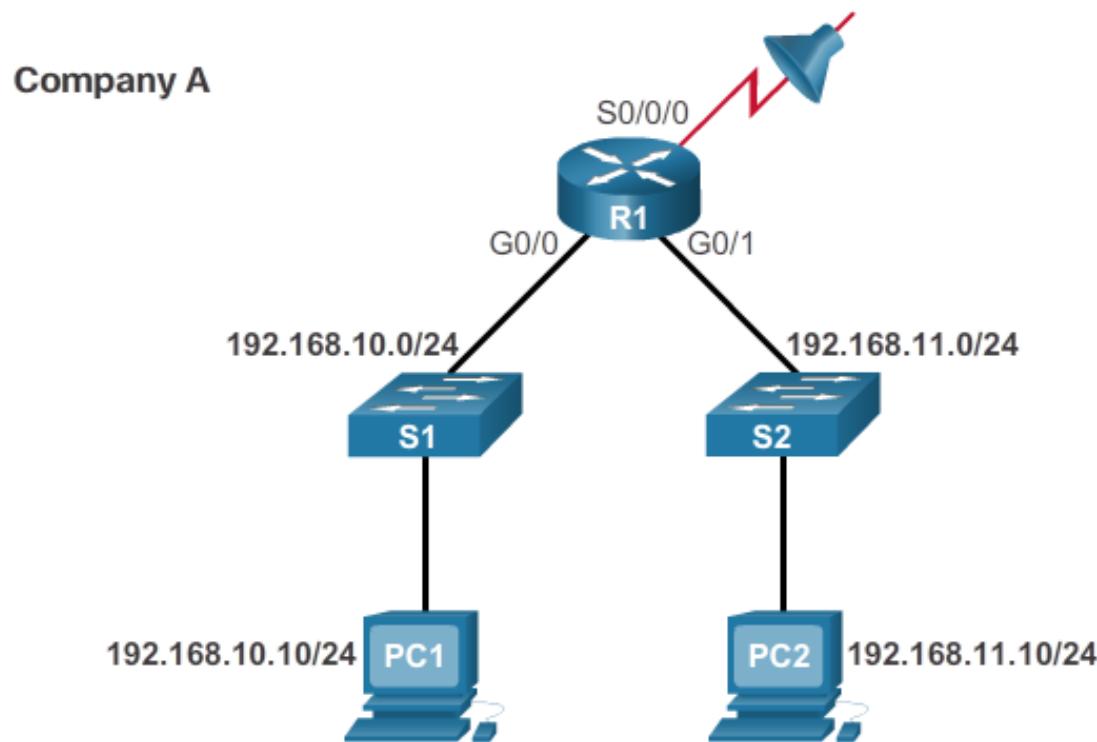
```
R1(config)# access-list 10 remark Permit hosts from the
192.168.10.0 LAN
R1(config)# access-list 10 permit 192.168.10.0 0.0.0.255
R1(config)# exit
R1# show running-config | include access-list 10
access-list 10 remark Permit hosts from the 192.168.10.0 LAN
access-list 10 permit 192.168.10.0 0.0.0.255
R1#
```



Standard IPv4 ACL Configuration

Apply a Standard IPv4 ACL

Permit a Specific Subnet



```
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)# interface s0/0/0
R1(config-if)# ip access-group 1 out
```



Standard IPv4 ACL Configuration Named Standard IPv4 ACLs

Named ACL Example

```
Router(config)# ip access-list [standard | extended] name
```

Alphanumeric name string must be unique and cannot begin with a number.

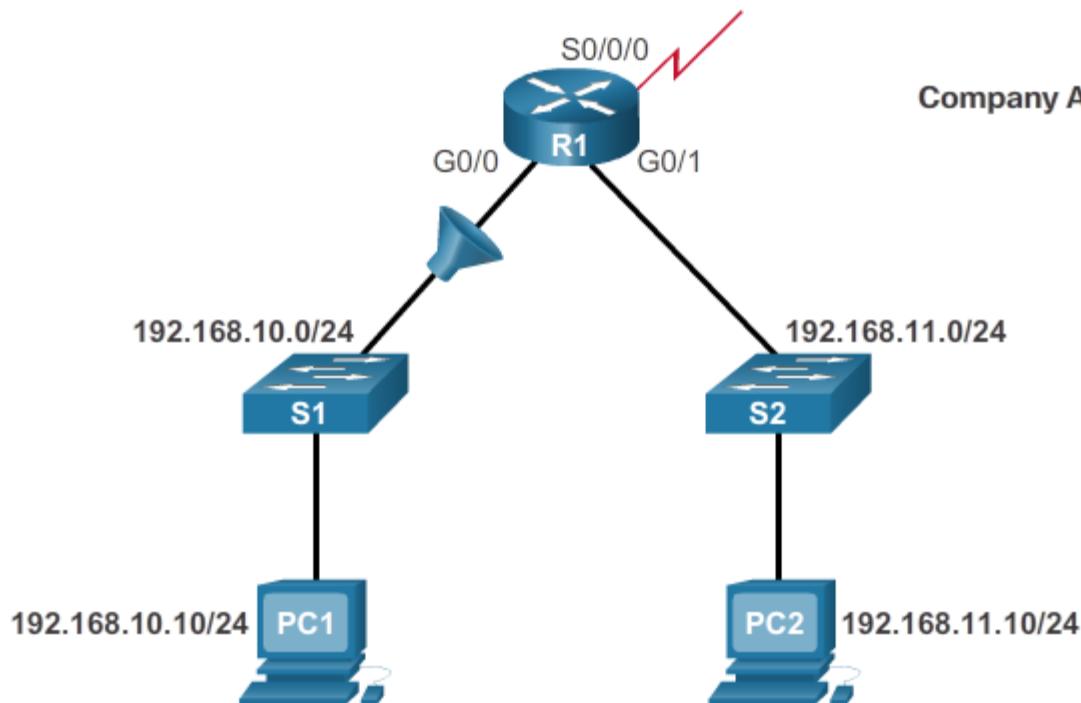
```
Router(config-std-nacl)# [permit | deny | remark] {source  
[source-wildcard]} [log]
```

```
Router(config-if)# ip access-group name [in | out]
```

Activates the named IP ACL on an interface.



Standard IPv4 ACL Configuration Named Standard IPv4 ACLs cont...



```
R1(config)# ip access-list standard NO_ACCESS
R1(config-std-nacl)# deny host 192.168.11.10
R1(config-std-nacl)# permit any
R1(config-std-nacl)# exit
R1(config)# interface g0/0
R1(config-if)# ip access-group NO_ACCESS out
```



Standard IPv4 ACL Configuration

Verify ACLs

```
R1# show ip interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Internet address is 10.1.1.1/30
<output omitted>
  Outgoing access list is 1
    Inbound  access list is not set
<output omitted>

R1# show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
<output omitted>
  Outgoing access list is NO_ACCESS
    Inbound  access list is not set
<output omitted>
```

```
R1# show access-lists
Standard IP access list 1
  10 deny   192.168.10.10
  20 permit  192.168.0.0, wildcard bits 0.0.255.255
Standard IP access list NO_ACCESS
  15 deny   192.168.11.11
  10 deny   192.168.11.10
  20 permit  192.168.11.0, wildcard bits 0.0.0.255
R1#
```

4.2 Extended IPv4 ACLs





Structure of an Extended IPv4 ACLs

Extended ACLs

- Extended ACLs are used more often than standard ACLs because they provide a greater degree of control.



Extended ACLs can filter on:

- Source address
- Destination address
- Protocol
- Port number



Structure of an Extended IPv4 ACLs

Filtering Ports and Services

- The ability to filter on protocol and port number allows network administrators to build very specific extended ACLs.
- An application can be specified by configuring either the port number or the name of a well-known port.

Using Port Numbers

```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 23
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 21
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 20
```

Using Keywords

```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq telnet
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp-data
```



Configure Extended IPv4 ACLs

Configuring Extended ACLs

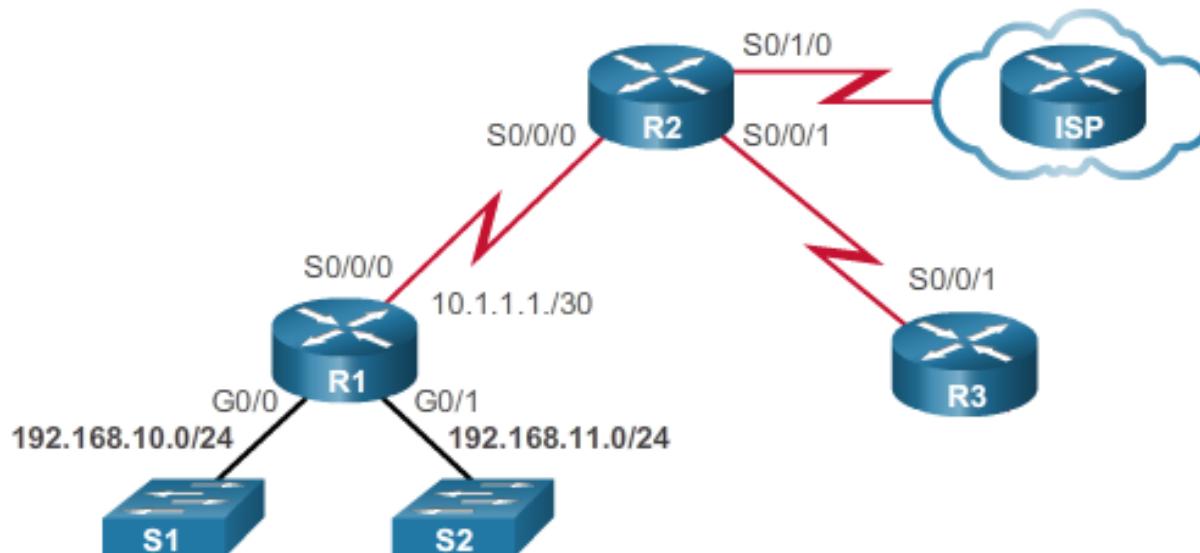
- The procedural steps for configuring extended ACLs are the same as for standard ACLs. The extended ACL is **first configured**, and **then** it is **activated** on an interface. However, the command syntax and parameters are more complex to support the additional features provided by extended ACLs.

```
access-list access-list-number {deny | permit | remark} protocol  
{source source-wildcard} [operator port [port-number or name]]  
{destination destination-wildcard} [operator port [port-number or  
name]]
```



Configure Extended IPv4 ACLs

Configuring Extended ACLs cont...



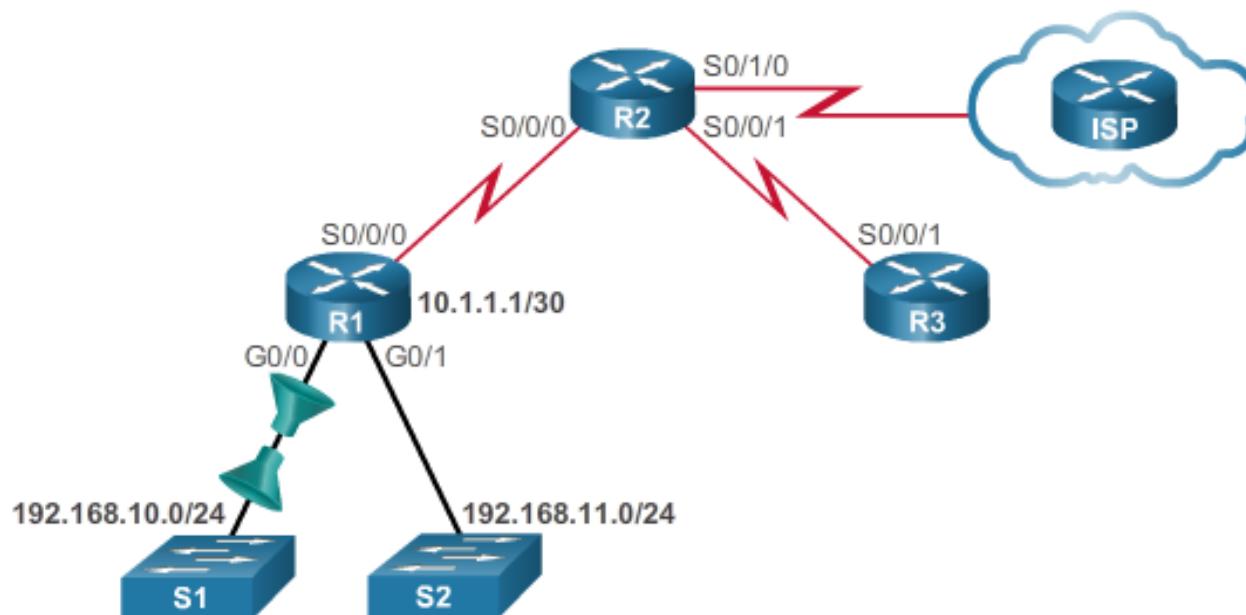
```
R1(config)# access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config)# access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config)# access-list 104 permit tcp any 192.168.10.0 0.0.0.255
      established
```

- ACL 103 allows requests to ports 80 and 443.
- ACL 104 allows established HTTP and HTTPS replies.



Configure Extended IPv4 ACLs

Applying Extended ACLs to Interfaces

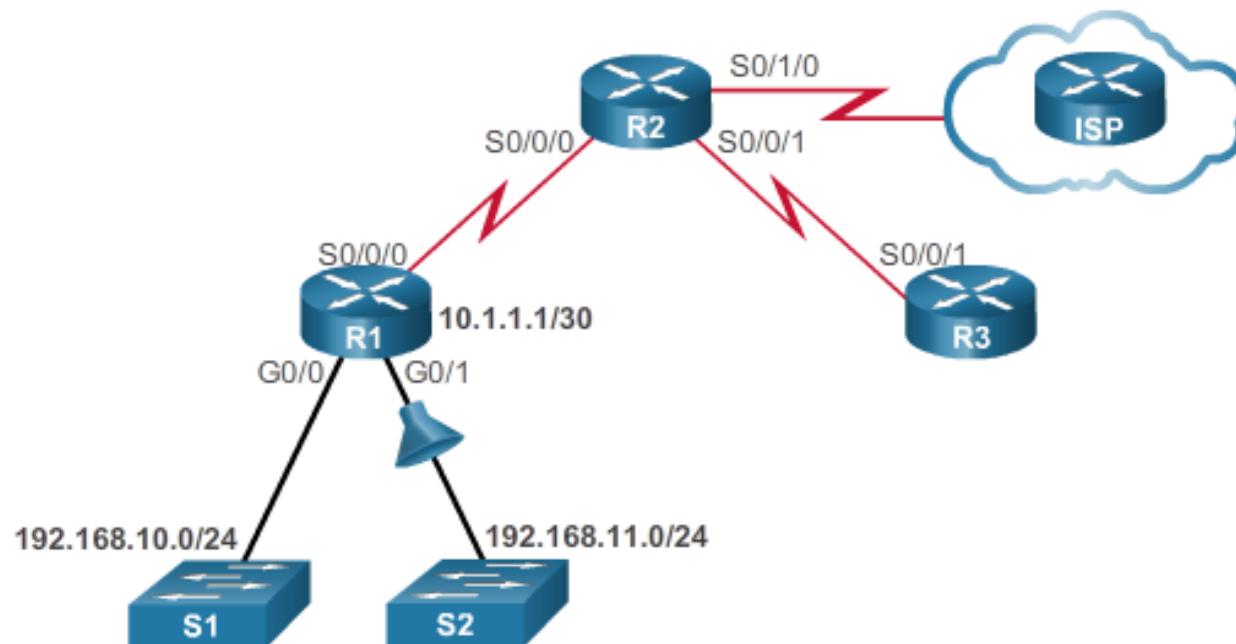


```
R1(config)# access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config)# access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config)# access-list 104 permit tcp any 192.168.10.0 0.0.0.255 established
R1(config)# interface g0/0
R1(config-if)# ip access-group 103 in
R1(config-if)# ip access-group 104 out
```



Configure Extended IPv4 ACLs

Filtering Traffic with Extended ACLs

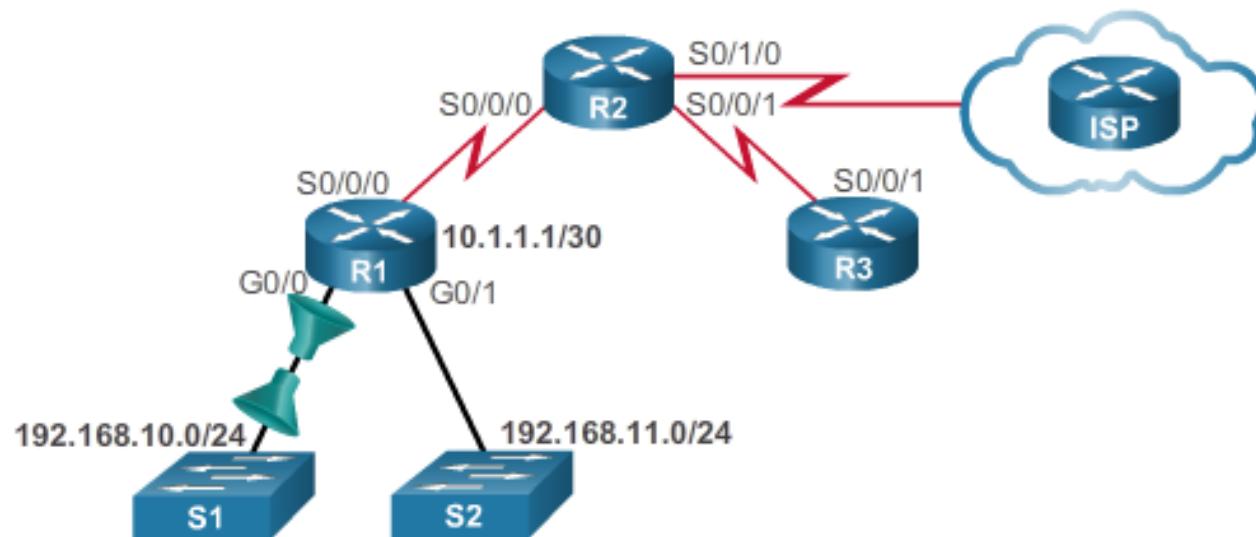


```
R1(config) # access-list 101 deny tcp 192.168.11.0 0.0.0.255  
192.168.10.0 0.0.0.255 eq ftp  
R1(config) # access-list 101 deny tcp 192.168.11.0 0.0.0.255  
192.168.10.0 0.0.0.255 eq ftp-data  
R1(config) # access-list 101 permit ip any any  
R1(config) # interface g0/1  
R1(config-if) # ip access-group 101 in
```



Configure Extended IPv4 ACLs

Creating Named Extended ACLs



```
R1(config)# ip access-list extended SURFING
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config-ext-nacl)# exit
R1(config)# ip access-list extended BROWSING
R1(config-ext-nacl)# permit tcp any 192.168.10.0 0.0.0.255 established
R1(config-ext-nacl)# exit
R1(config)# interface g0/0
R1(config-if)# ip access-group SURFING in
R1(config-if)# ip access-group BROWSING out
```



Configure Extended IPv4 ACLs

Verifying Extended ACLs

```
R1#show access-lists
Extended IP access list BROWSING
    10 permit tcp any 192.168.10.0 0.0.0.255 established
Extended IP access list SURFING
    10 permit tcp 192.168.10.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1#
R1#show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up
    Internet address is 192.168.10.1/24
<output omitted for brevity>
    Outgoing access list is BROWSING
    Inbound access list is SURFING
<output omitted for brevity>
```



Configure Extended IPv4 ACLs

Editing Extended ACLs

- Editing an extended ACL can be accomplished using the same process as editing a standard. An extended ACL can be modified using:
 - Method 1 - Text editor
 - The ACL is copied and pasted into the text editor where the changes are made. The current access list is removed using the **no access-list** command. The modified ACL is then pasted back into the configuration.
 - Method 2 – Sequence numbers
 - Sequence numbers can be used to delete or insert an ACL statement.



Configure Extended IPv4 ACLs

Editing Extended ACLs cont...

- Editing an extended ACL via Sequence Numbers:

```
R1# show access-lists
Extended IP access list BROWSING
    10 permit tcp any 192.168.10.0 0.0.0.255 established
Extended IP access list SURFING
    10 permit tcp 192.168.11.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1#
R1# configure terminal
R1(config)# ip access-list extended SURFING
R1(config-ext-nacl)# no 10
R1(config-ext-nacl)# 10 permit tcp 192.168.10.0 0.0.0.255 any eq
www
R1(config-ext-nacl)# end
R1#
R1# show access-lists
Extended IP access list BROWSING
    10 permit tcp any 192.168.10.0 0.0.0.255 established
Extended IP access list SURFING
    10 permit tcp 192.168.10.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443
```

A callout box with an orange arrow points from the highlighted IP address '192.168.11.0' in the ACL output to the text 'Should be 192.168.10.0'.

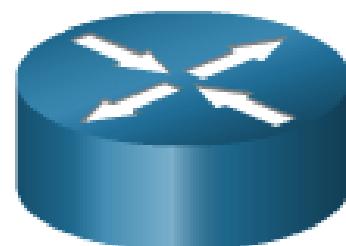
4.3 IPv6 ACLs





IPv6 ACL Creation

Types of IPv6 ACLs



IPv4 ACLs

- Standard
 - Numbered
 - Named
- Extended
 - Numbered
 - Named

IPv6 ACLs

- Named only
- Similar in functionality to IPv4 Extended ACL



IPv6 ACL Creation

Comparing IPv4 and IPv6 ACLs

Although IPv4 and IPv6 ACLs are very similar, there are three significant differences between them.

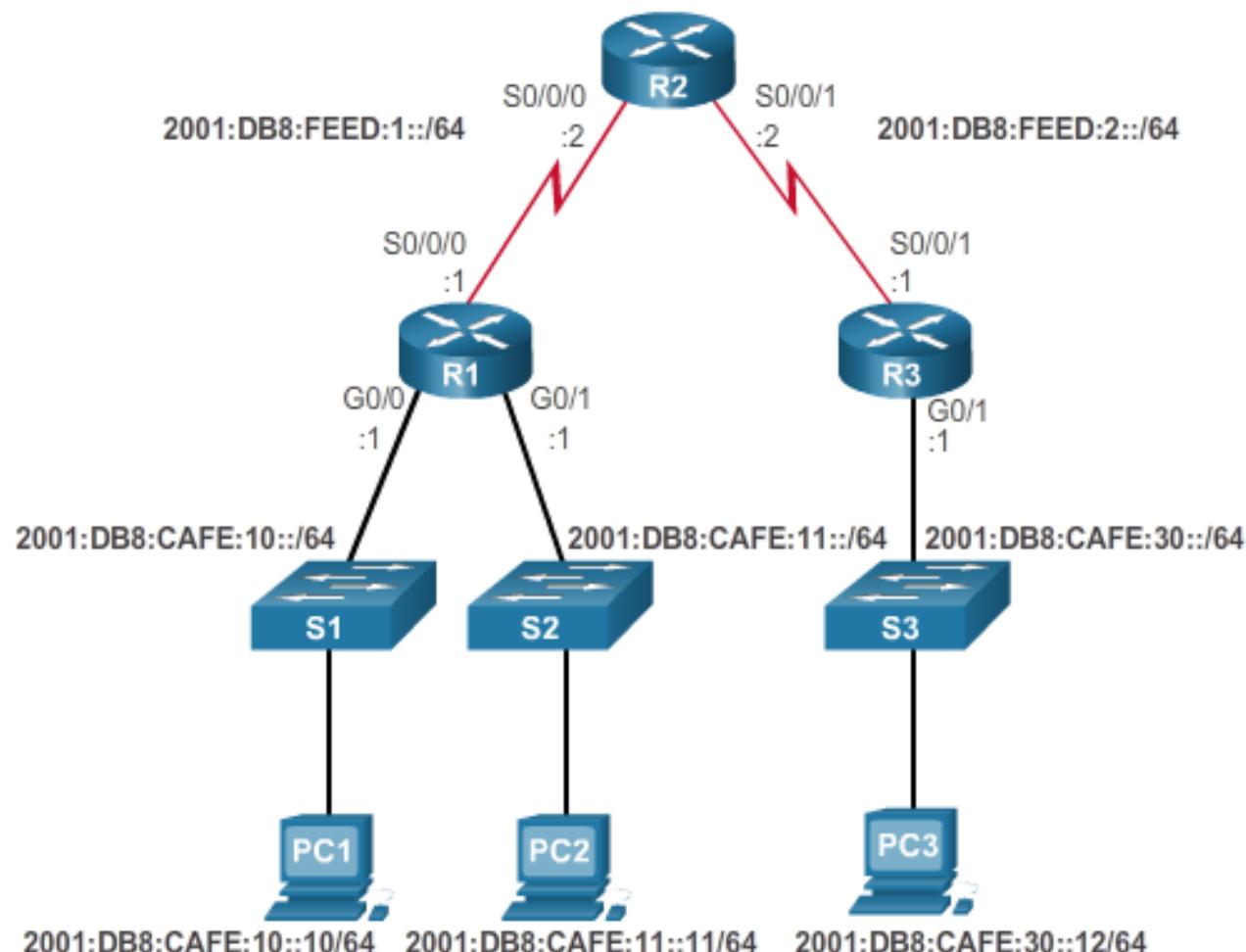
- Applying an IPv6 ACL
 - IPv6 uses the **ipv6 traffic-filter** command to perform the same function for IPv6 interfaces.
- No Wildcard Masks
 - The prefix-length is used to indicate how much of an IPv6 source or destination address should be matched.
- Additional Default Statements
 - **permit icmp any any nd-na** ND-NA Neighbour Advertisement Messages
 - **permit icmp any any nd-ns** ND-NS = Neighbour Solicitation Messages

ICMPv6 uses Neighbor Discovery (ND) messages to resolve Layer 3 addresses to Layer 2 MAC addresses. IPv6 uses Layer 3 service for neighbor discovery. IPv6 ACLs need to **implicitly permit** ND packets to be sent and received on an interface.



Configuring IPv6 ACLs

Configuring IPv6 Topology





Configuring IPv6 ACLs

Configuring IPv6 ACLs

There are three basic steps to configure an IPv6 ACL:

1. From global configuration mode, use the **ipv6 access-list *name*** command to create an IPv6 ACL.
2. From the named ACL configuration mode, use **permit** or **deny** statements to specify one or more conditions to determine if a packet is forwarded or dropped.
3. Return to privileged EXEC mode

```
R1(config)# ipv6 access-list access-list-name
R1(config-ipv6-acl)# deny | permit protocol {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address} [operator [port-number]]
```



Configuring IPv6 ACLs

Configuring IPv6 ACLs cont...

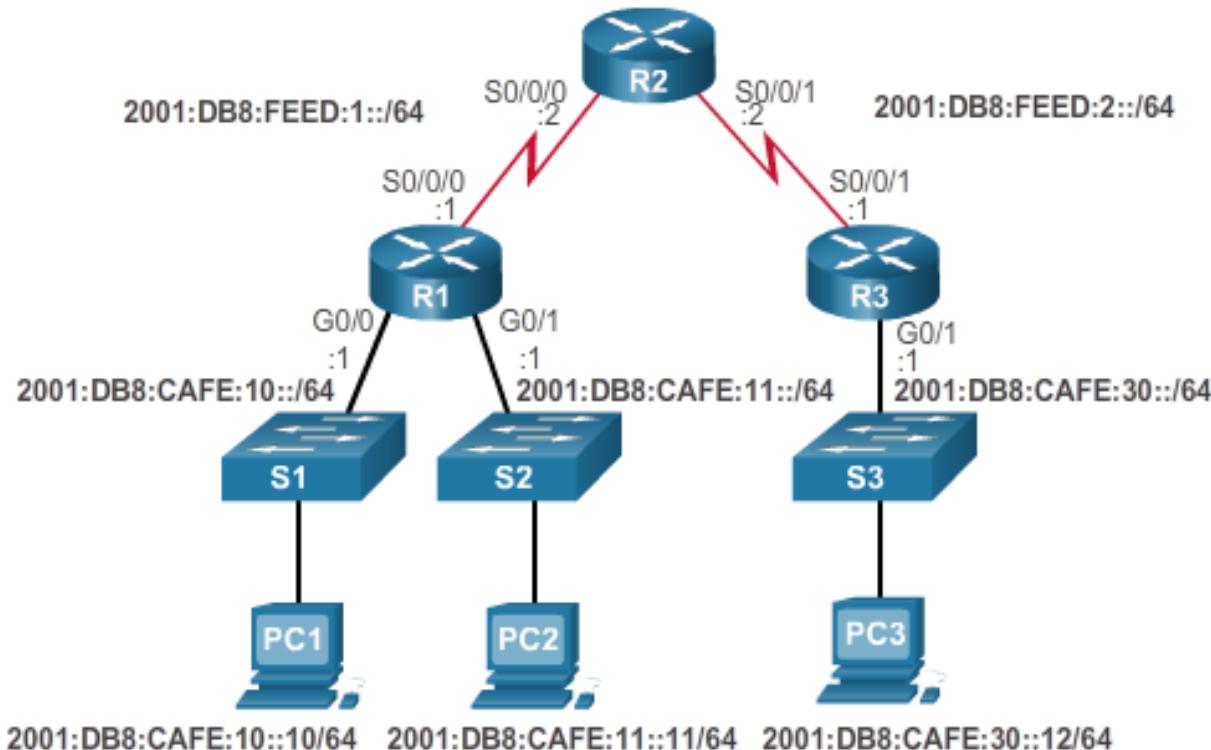
- This IPv6 ACL does the following:
 - The first statement names the IPv6 access list NO-R3-LAN-ACCESS.
 - The second statement denies all IPv6 packets from the 2001:DB8:CAFE:30::/64 destined for any IPv6 network.
 - The third statement allows all other IPv6 packets.

```
R1(config)# ipv6 access-list NO-R3-LAN-ACCESS
R1(config-ipv6-acl)# deny ipv6 2001:db8:cafe:30::/64 any
R1(config-ipv6-acl)# permit ipv6 any any
R1(config-ipv6-acl)# end
R1#
```



Configuring IPv6 ACLs

Configuring IPv6 ACLs cont...

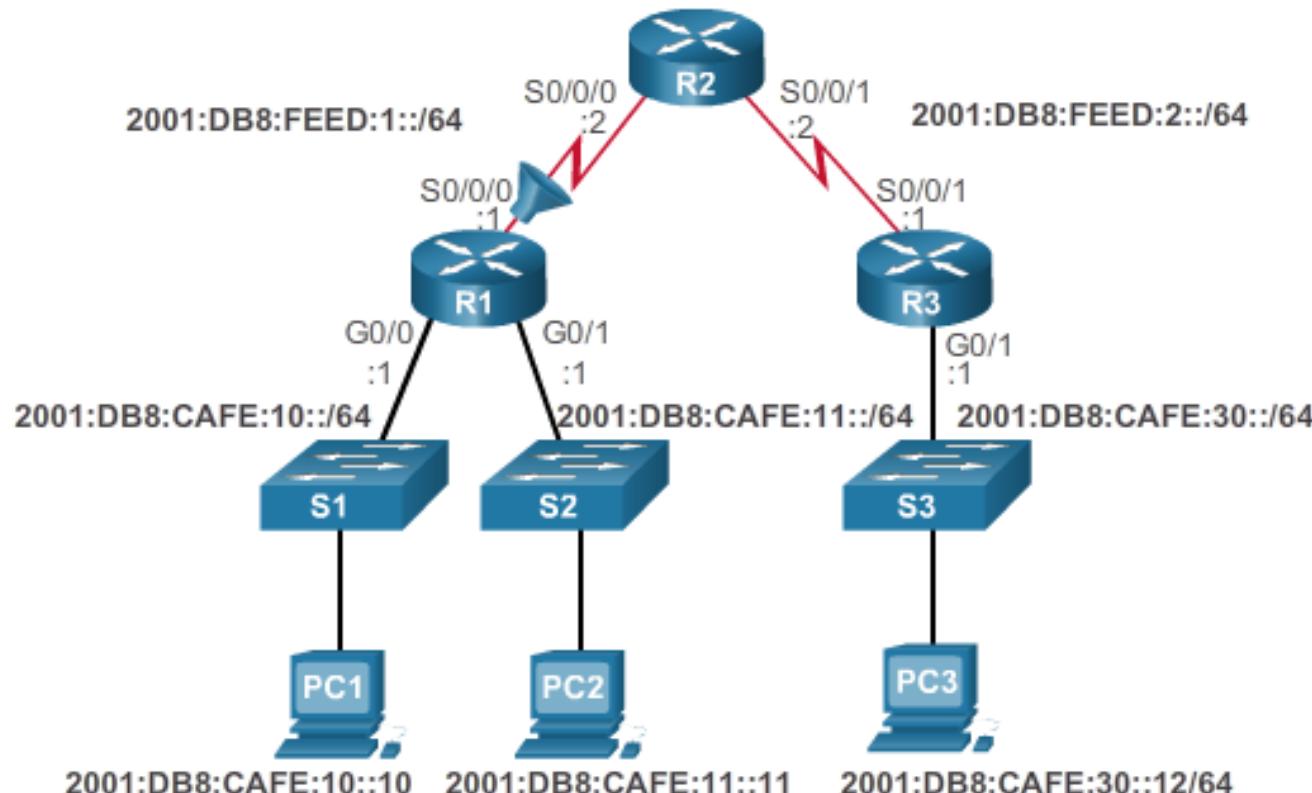


```
R1 (config) # ipv6 access-list NO-R3-LAN-ACCESS
R1 (config-ipv6-acl) # deny ipv6 2001:db8:cafe:30::/64 any
R1 (config-ipv6-acl) # permit ipv6 any any
R1 (config-ipv6-acl) # end
R1#
```



Configuring IPv6 ACLs

Applying an IPv6 ACL to an Interface

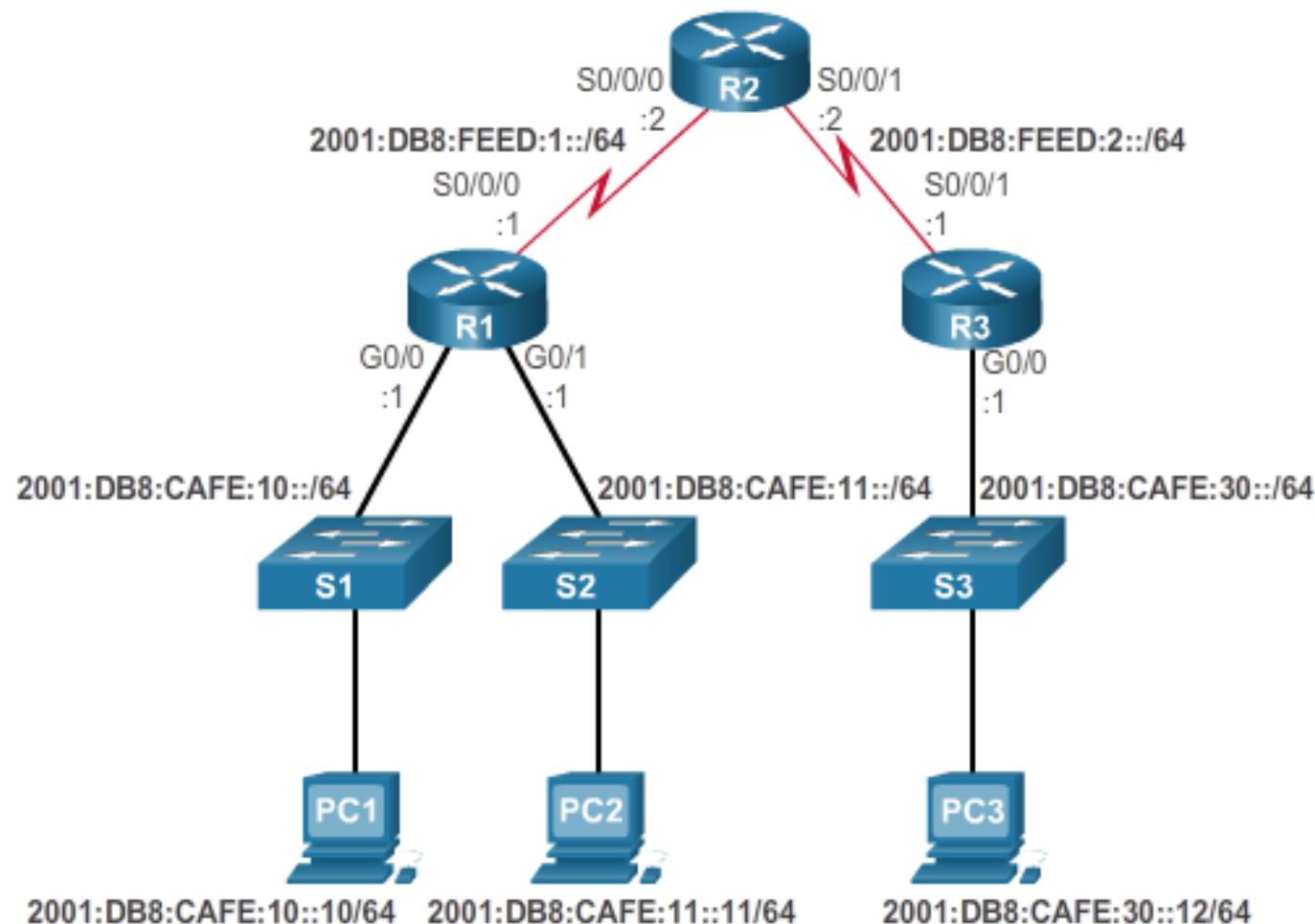


```
R1(config)# interface s0/0/0
R1(config-if)# ipv6 traffic-filter NO-R3-LAN-ACCESS in
```



Configuring IPv6 ACLs

IPv6 ACL Examples





Configuring IPv6 ACLs

IPv6 ACL Examples cont...

- Router R1 is configured with an IPv6 access list to deny FTP traffic to 2001:DB8:CAFE:11::/64. Ports for both FTP data (port 20) and FTP control (port 21) need to be blocked.
- Because the filter is applied inbound on the G0/0 interface on R1, only traffic from the 2001:DB8:CAFE:10::/64 network will be denied.

```
R1(config)# ipv6 access-list NO-FTP-TO-11
R1(config-ipv6-acl)# deny tcp any 2001:db8:cafe:11::/64 eq ftp
R1(config-ipv6-acl)# deny tcp any 2001:db8:cafe:11::/64 eq ftp-data
R1(config-ipv6-acl)# permit ipv6 any any
R1(config-ipv6-acl)# exit
R1(config)# interface g0/0
R1(config-if)# ipv6 traffic-filter NO-FTP-TO-11 in
R1(config-if)#

```



Configuring IPv6 ACLs

IPv6 ACL Examples cont...

1. The first two permit statements allow access from any device to the web server at 2001:DB8:CAFE:10::10.
2. All other devices are denied access to network 2001:DB8:CAFE:10::/64.
3. PC3 at 2001:DB8:CAFE:30::12 is permitted Telnet access to PC2 which has the IPv6 address 2001:DB8:CAFE:11::11.

```
R3(config)# ipv6 access-list RESTRICTED-ACCESS
R3(config-ipv6-acl)# remark Permit access only HTTP and HTTPS to Network 10
R3(config-ipv6-acl)# permit tcp any host 2001:db8:cafe:10::10 eq 80 ] 1
R3(config-ipv6-acl)# permit tcp any host 2001:db8:cafe:10::10 eq 443
R3(config-ipv6-acl)# remark Deny all other traffic to Network 10
R3(config-ipv6-acl)# deny ipv6 any 2001:db8:cafe:10::/64 2
R3(config-ipv6-acl)# remark Permit PC3 telnet access to PC2
R3(config-ipv6-acl)# permit tcp host 2001:DB8:CAFE:30::12 host 2001:DB8:CAFE:11::11 eq 23 3
R3(config-ipv6-acl)# remark Deny telnet access to PC2 for all other devices
R3(config-ipv6-acl)# deny tcp any host 2001:db8:cafe:11::11 eq 23 4
R3(config-ipv6-acl)# remark Permit access to everything else
R3(config-ipv6-acl)# permit ipv6 any any 5
R3(config-ipv6-acl)# exit
R3(config)# interface g0/0
R3(config-if)# ipv6 traffic-filter RESTRICTED-ACCESS in 6
R3(config-if)#

```



Configuring IPv6 ACLs

IPv6 ACL Examples cont...

4. All other devices are denied Telnet access to PC2.
5. All other IPv6 traffic is permitted to all other destinations.
6. The IPv6 access list is applied to interface G0/0 in the inbound direction, so only the 2001:DB8:CAFE:30::/64 network is affected.

```
R3(config)# ipv6 access-list RESTRICTED-ACCESS
R3(config-ipv6-acl)# remark Permit access only HTTP and HTTPS to Network 10
R3(config-ipv6-acl)# permit tcp any host 2001:db8:cafe:10::10 eq 80 ] 1
R3(config-ipv6-acl)# permit tcp any host 2001:db8:cafe:10::10 eq 443
R3(config-ipv6-acl)# remark Deny all other traffic to Network 10
R3(config-ipv6-acl)# deny ipv6 any 2001:db8:cafe:10::/64 2
R3(config-ipv6-acl)# remark Permit PC3 telnet access to PC2
R3(config-ipv6-acl)# permit tcp host 2001:DB8:CAFE:30::12 host 2001:DB8:CAFE:11::11 eq 23 3
R3(config-ipv6-acl)# remark Deny telnet access to PC2 for all other devices
R3(config-ipv6-acl)# deny tcp any host 2001:db8:cafe:11::11 eq 23 4
R3(config-ipv6-acl)# remark Permit access to everything else
R3(config-ipv6-acl)# permit ipv6 any any 5
R3(config-ipv6-acl)# exit
R3(config)# interface g0/0
R3(config-if)# ipv6 traffic-filter RESTRICTED-ACCESS in 6
R3(config-if)#

```



Configuring IPv6 ACLs

Verifying IPv6 ACLs

```
R3# show ipv6 interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Global unicast address(es):
    2001:DB8:CAFE:30::1, subnet is 2001:DB8:CAFE:30::/64
  Input features: Access List
  Inbound access list RESTRICTED-ACCESS
<output omitted>
```



Configuring IPv6 ACLs

Verifying IPv6 ACLs cont...

```
R3# show access-lists
IPv6 access list RESTRICTED-ACCESS
    permit tcp any host 2001:DB8:CAFE:10::10 eq www sequence 20
    permit tcp any host 2001:DB8:CAFE:10::10 eq 443 sequence 30
    deny ipv6 any 2001:DB8:CAFE:10::/64 sequence 50
    permit tcp host 2001:DB8:CAFE:30::12 host 2001:DB8:CAFE:11::11 eq
        telnet sequence 70
    deny tcp any host 2001:DB8:CAFE:11::11 eq telnet sequence 90
    permit ipv6 any any sequence 110
R3#
```



Configuring IPv6 ACLs

Verifying IPv6 ACLs cont...

```
R3# show running-config
<output omitted>
ipv6 access-list RESTRICTED-ACCESS
  remark Permit access only HTTP and HTTPS to Network 10
  permit tcp any host 2001:DB8:CAFE:10::10 eq www
  permit tcp any host 2001:DB8:CAFE:10::10 eq 443
  remark Deny all other traffic to Network 10
  deny ipv6 any 2001:DB8:CAFE:10::/64
  remark Permit PC3 telnet access to PC2
  permit tcp host 2001:DB8:CAFE:30::12 host 2001:DB8:CAFE:11::11
    eq telnet
  remark Deny telnet access to PC2 for all other devices
  deny tcp any host 2001:DB8:CAFE:11::11 eq telnet
  remark Permit access to everything else
  permit ipv6 any any
```

4.4 Troubleshoot ACLs

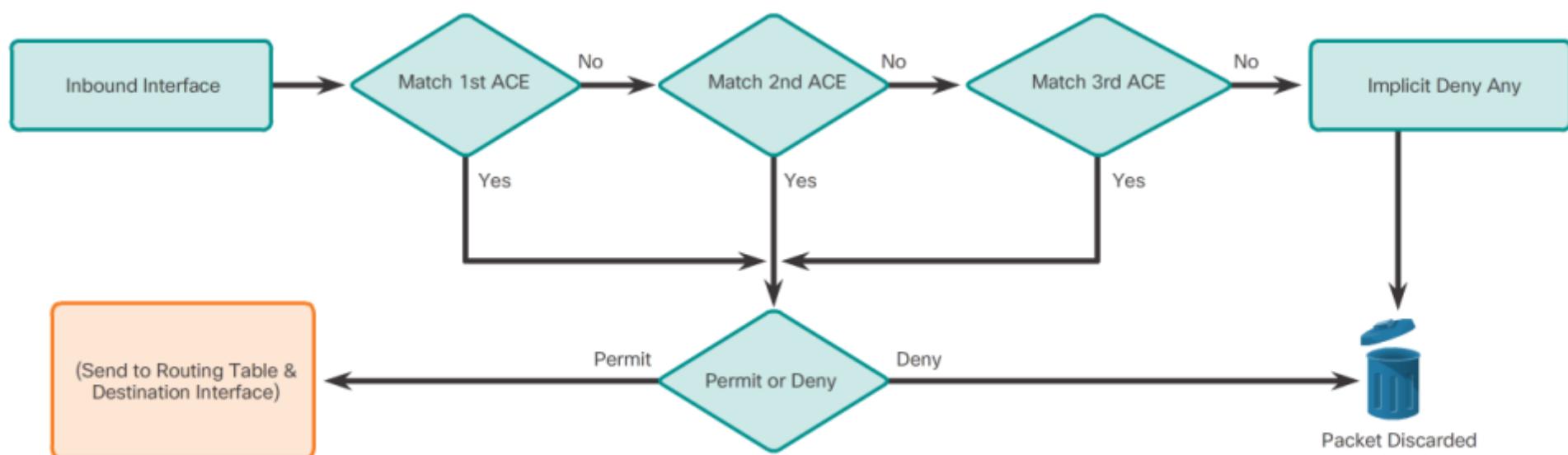




Processing Packets with ACLs

Inbound and Outbound ACL Logic

Inbound ACL Process

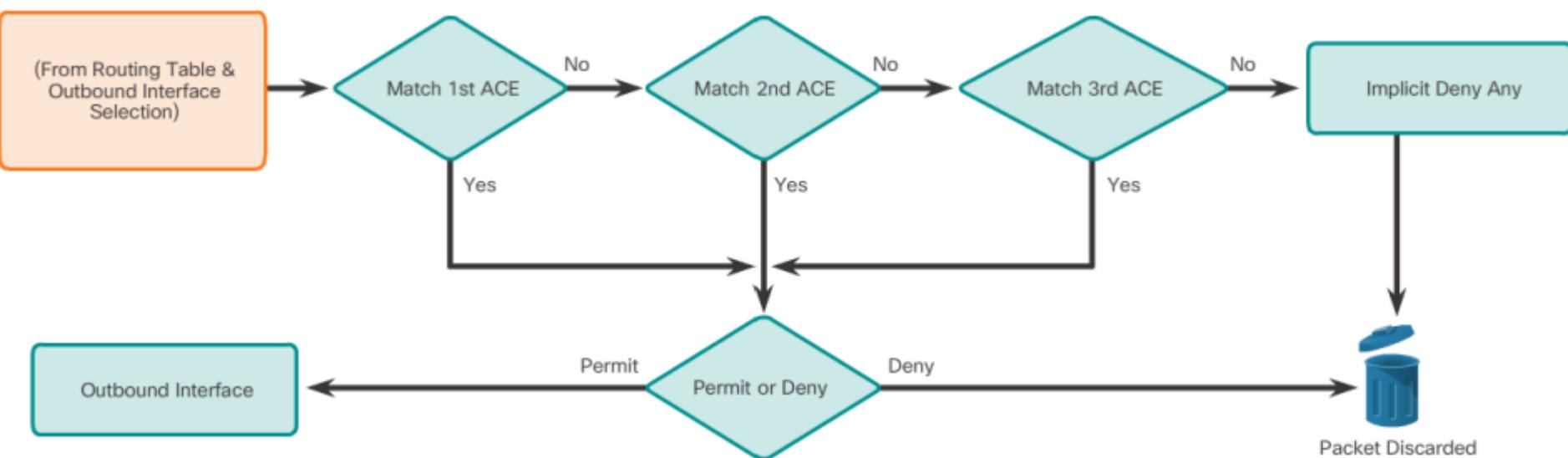




Processing Packets with ACLs

Inbound and Outbound ACL Logic

Outbound ACL Process

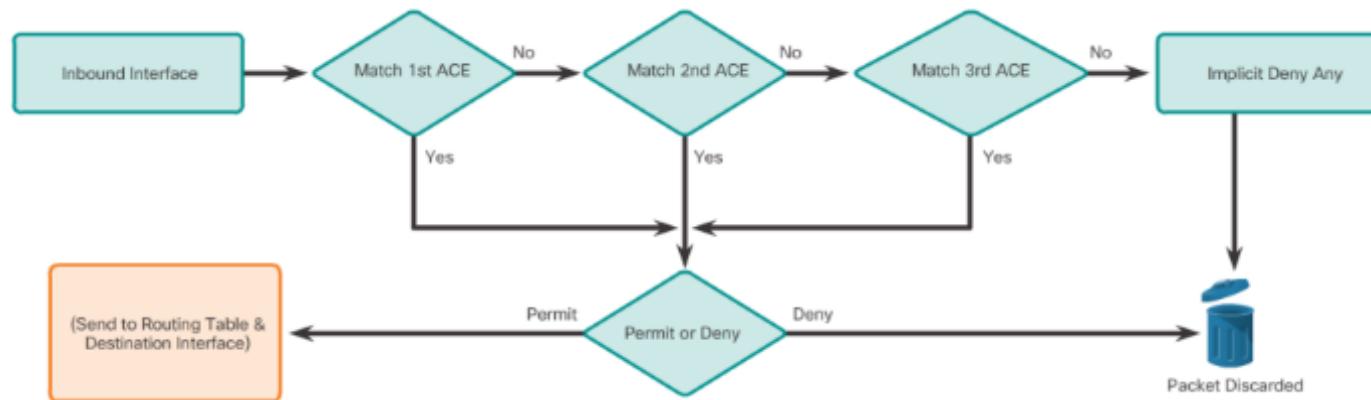




Processing Packets with ACLs

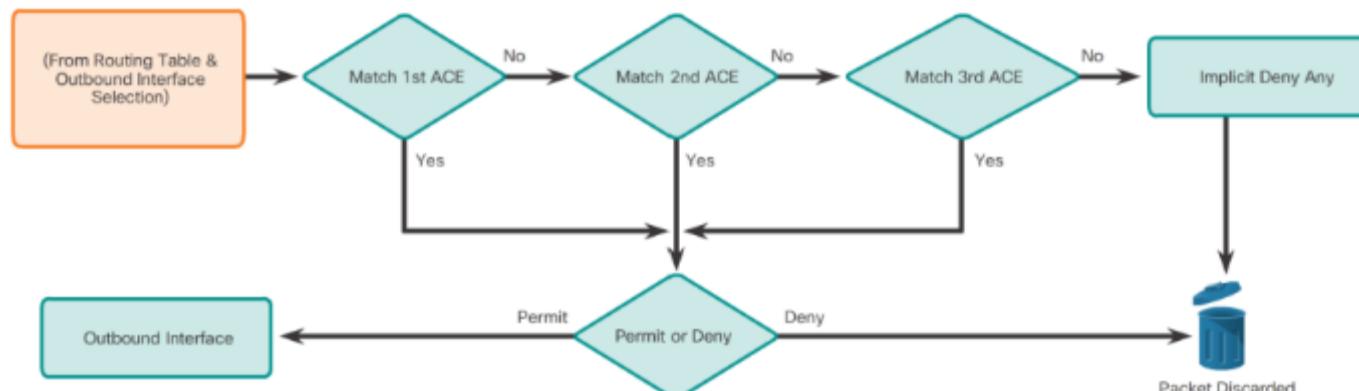
Inbound and Outbound ACL Logic

Inbound ACL Process.



Compare
the two
diagrams.

Outbound ACL Process.





Processing Packets with ACLs

ACL Logic Operations

- As a frame enters an interface, the router checks to see whether the destination Layer 2 address matches its interface Layer 2 address, or whether the frame is a broadcast frame.
- If the frame address is accepted, the frame information is stripped off and the router checks for an ACL on the inbound interface.
- If an ACL exists, the packet is tested against the statements in the list.
- If the packet matches a statement, the packet is either permitted or denied.
- If the packet is accepted, it is then checked against routing table entries to determine the destination interface.
- If a routing table entry exists for the destination, the packet is then switched to the outgoing interface, otherwise the packet is dropped.
- Next, the router checks whether the outgoing interface has an ACL. If an ACL exists, the packet is tested against the statements in the list. If the packet matches a statement, it is either permitted or denied.
- If there is no ACL or the packet is permitted, the packet is encapsulated in the new Layer 2 protocol and forwarded out the interface to the next device.

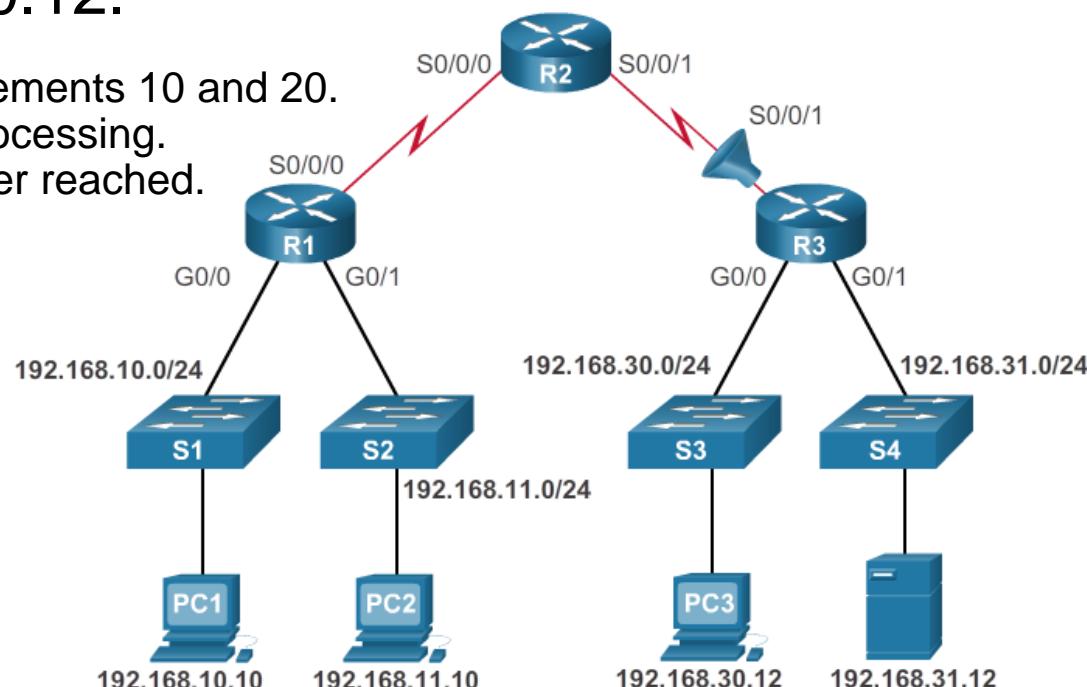


Common ACL Errors

Troubleshooting IPv4 ACLs- Example 1

- Host 192.168.10.10 has no Telnet connectivity with 192.168.30.12.

Reverse ACL statements 10 and 20.
ACL Top Down processing.
Statement 20 never reached.



```
R3# show access-lists
Extended IP access list 110
  10 deny tcp 192.168.10.0 0.0.0.255 any (12 match(es))
  20 permit tcp 192.168.10.0 0.0.0.255 any eq telnet
  30 permit ip any any
```

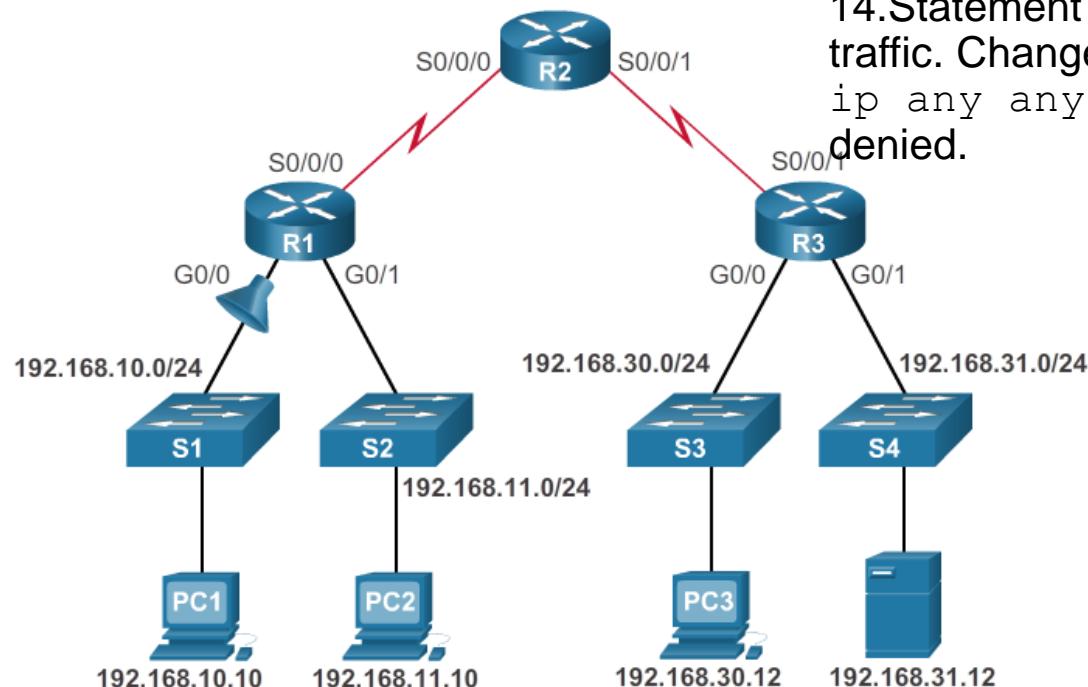


Common ACL Errors

Troubleshooting IPv4 ACLs- Example 2

- The 192.168.10.0/24 network cannot use TFTP to connect to the 192.168.30.0/24 network.

TFTP uses UDP. Not TCP. See Slide 14. Statement 30 allows all other TCP traffic. Change statement 30 to ip any any. As UDP implicitly denied.



```
R1# show access-lists 120
Extended IP access list 120
    10 deny tcp 192.168.10.0 0.0.0.255 any eq telnet
    20 deny tcp 192.168.10.0 0.0.0.255 host 192.168.31.12 eq smtp
    30 permit tcp any any
```

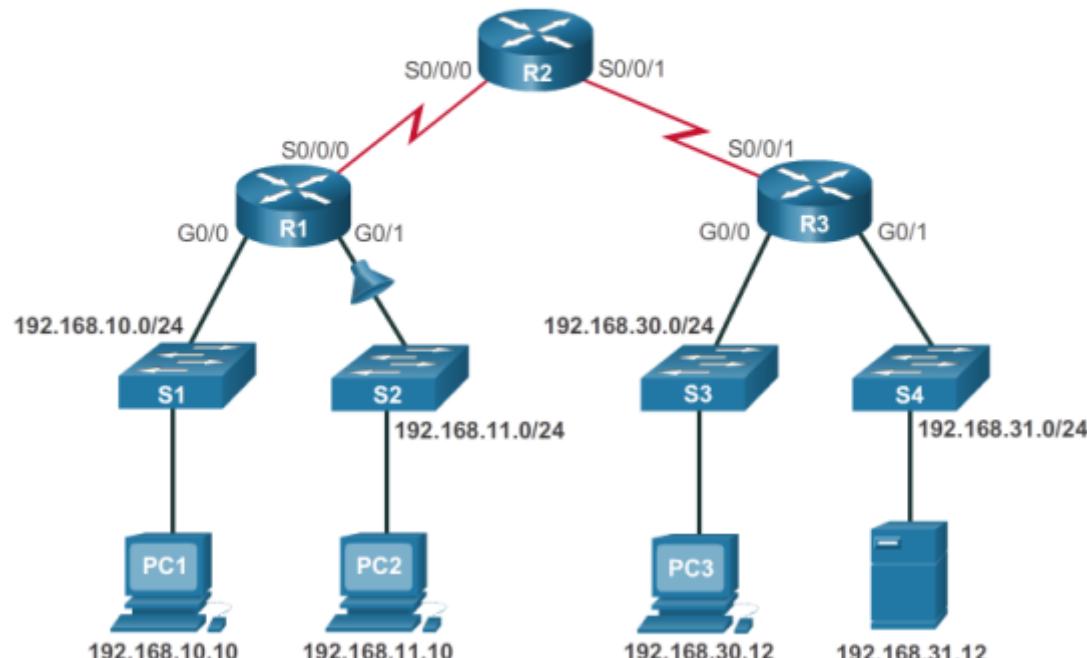


Common ACL Errors

Troubleshooting IPv4 ACLs- Example 3

- The 192.168.11.0/24 network can use Telnet to connect to 192.168.30.0/24, but this connection should not be allowed.

```
R1# show access-lists 130
Extended IP access list 130
  10 deny tcp any eq telnet any
  20 deny tcp 192.168.11.0 0.0.0.255 host 192.168.31.12 eq smtp
  30 permit tcp any any (12 match(es))
```



Telnet port number in wrong position in ACL statement 10. Any source packet with telnet port number is denied. Change statement to
deny tcp any any eq telnet

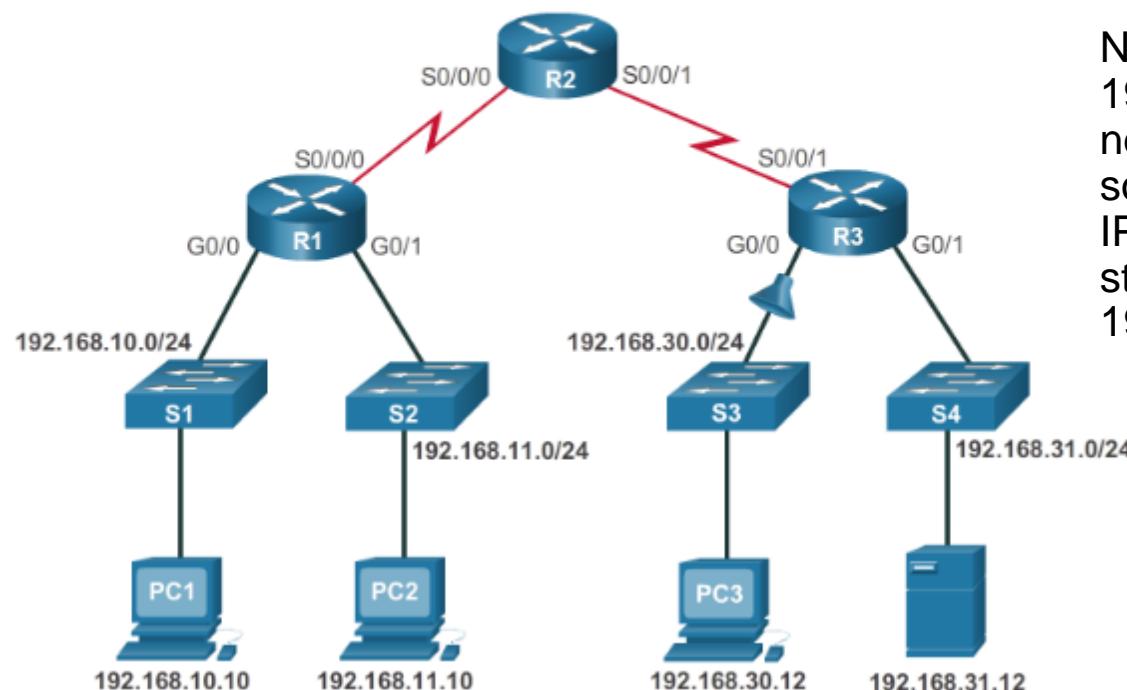


Common ACL Errors

Troubleshooting IPv4 ACLs- Example 4

- Host 192.168.30.12 is able to Telnet to connect to 192.168.31.12, but this connection should not be allowed.

```
R3# show access-lists 140
Extended IP access list 140
  10 deny tcp host 192.168.30.1 any eq telnet
  20 permit ip any any (5 match(es))
```



No rules to deny host 192.168.30.12 or its network as the source. Change host IPv4 address in statement 10 to 192.168.30.12.

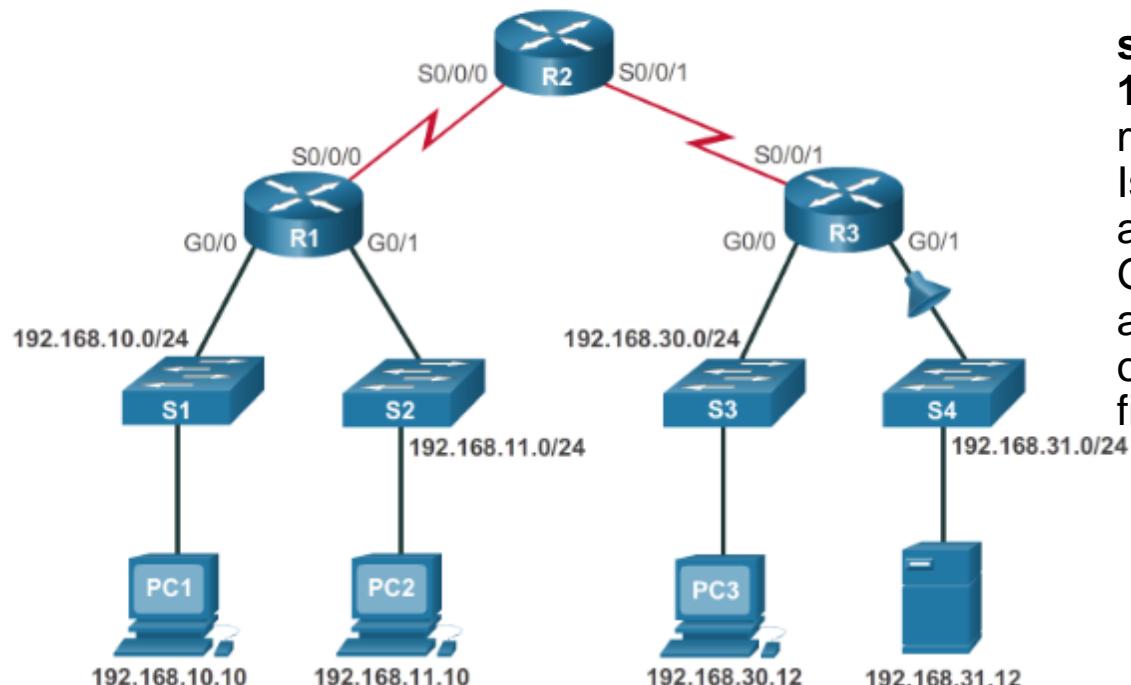


Common ACL Errors

Troubleshooting IPv4 ACLs- Example 5

- Host 192.168.30.12 can use Telnet to connect to 192.168.31.12, but this connection should not be allowed.

```
R2# show access-lists 150
Extended IP access list 150
  10 deny tcp any host 192.168.31.12 eq telnet
  20 permit ip any any
```



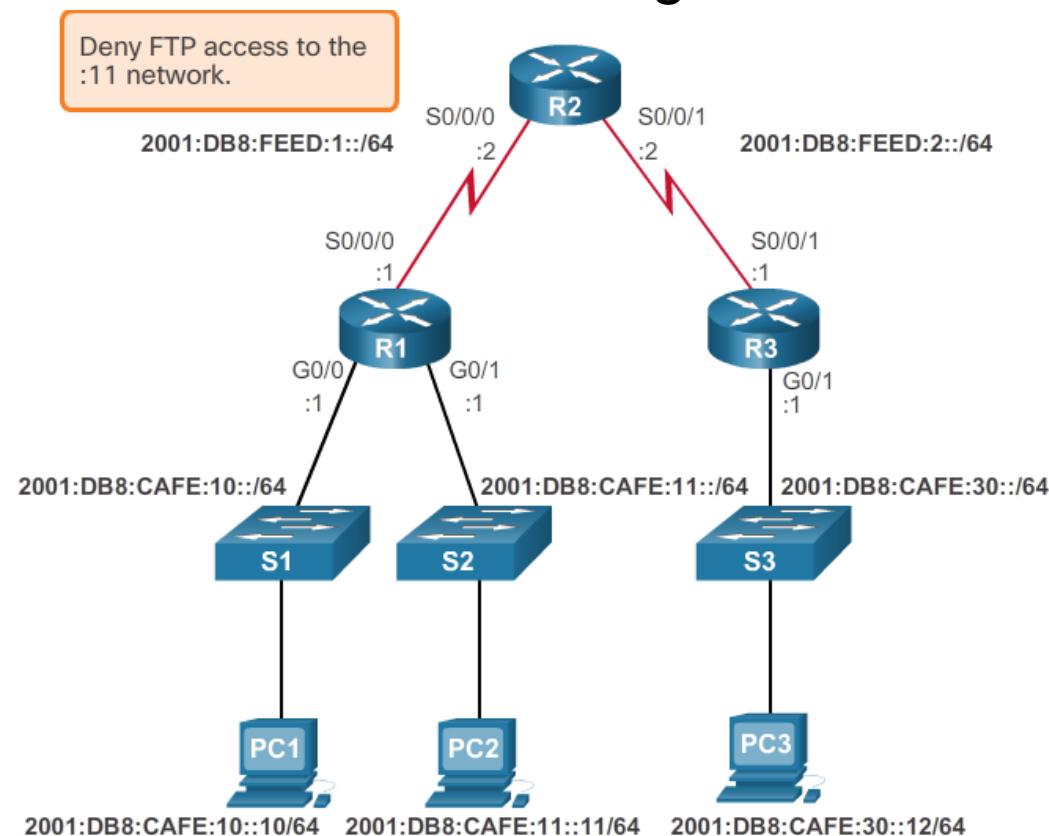
show access-list 150
150 output shows no matches. Problem is ACL direction. ACL applied inbound on G0/1. ACL should be applied outbound on G0/1 for correct filtering.



Common ACL Errors

Troubleshooting IPv6 ACLs- Example 1

- R1 is configured with an IPv6 ACL to deny FTP access from the :10 network to the :11 network, but PC1 is still able to connect to the FTP server running on PC2.





Common ACL Errors

Troubleshooting IPv6 ACLs- Example 1 cont...

Verify the IPv6 ACL Configuration and Application

```
R1# show ipv6 access-list
IPv6 access list NO-FTP-TO-11
    deny tcp any 2001:DB8:CAFE:11::/64 eq ftp sequence 10
    deny tcp any 2001:DB8:CAFE:11::/64 eq ftp-data sequence 20
    permit ipv6 any any (11 matches) sequence 30
R1# show running-config | begin interface G
interface GigabitEthernet0/0
    no ip address
    ipv6 traffic-filter NO-FTP-TO-11 out
    duplex auto
    speed auto
    ipv6 address FE80::1 link-local
    ipv6 address 2001:DB8:1:10::1/64
    ipv6 eigrp 1
<output omitted>
R1#
```



Common ACL Errors

Troubleshooting IPv6 ACLs- Example 1 cont...

Correct and Verify the IPv6 ACL

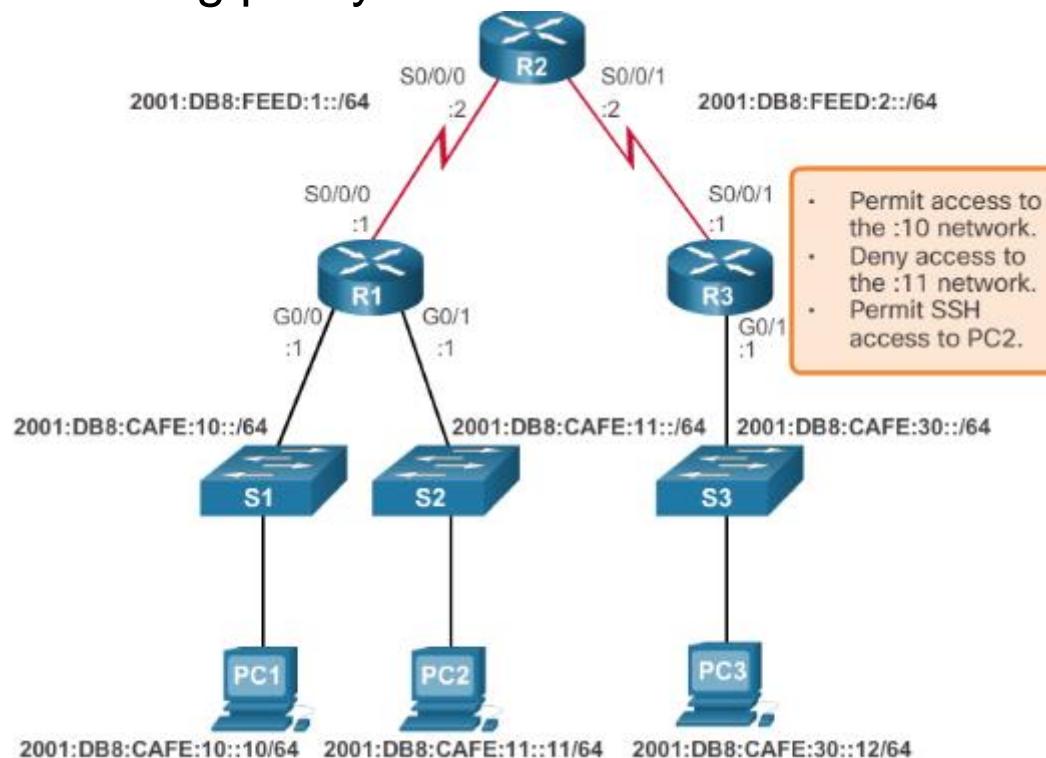
```
R1(config)# interface g0/0
R1(config-if)# no ipv6 traffic-filter NO-FTP-TO-11 out
R1(config-if)# ipv6 traffic-filter NO-FTP-TO-11 in
R1(config-if)# end
R1#
!PC1 attempts to access the FTP server again.
R1# show ipv6 access-list
IPv6 access list NO-FTP-TO-11
    deny tcp any 2001:DB8:CAFE:11::/64 eq ftp (37 matches) sequence 10
    deny tcp any 2001:DB8:CAFE:11::/64 eq ftp-data sequence 20
    permit ipv6 any any (11 matches) sequence 30
```



Common ACL Errors

Troubleshooting IPv6 ACLs- Example 2

- R3 is configured with IPv6 ACL RESTRICTED-ACCESS that should enforce the following policy for the R3 LAN:



- However, after configuring the ACL, PC3 cannot reach the 10 network or the 11 network, and it cannot SSH into the host at 2001:DB8:CAFE:11::11.



Common ACL Errors

Troubleshooting IPv6 ACLs- Example 2 cont...

Verify the IPv6 ACL Configuration and Application

```
R3# show running-config | section interface GigabitEthernet0/0
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
ipv6 address FE80::3 link-local
ipv6 address 2001:DB8:1:30::1/64
ipv6 eigrp 1
ipv6 traffic-filter RESTRICTED-ACCESS in
R3# show ipv6 access-list
IPv6 access list RESTRICTED-ACCESS
    permit ipv6 any host 2001:DB8:CAFE:10:: sequence 10
    deny ipv6 any 2001:DB8:CAFE:11::/64 sequence 20
    permit tcp any host 2001:DB8:CAFE:11::11 eq 22 sequence 30
R3#
```



Common ACL Errors

Troubleshooting IPv6 ACLs- Example 2 cont...

```
R3(config)# ipv6 access-list RESTRICTED-ACCESS
R3(config-ipv6-acl)# permit ipv6 any 2001:db8:cafe:10::/64 sequence 10
R3(config-ipv6-acl)# end
R3# show access-list
IPv6 access list RESTRICTED-ACCESS
    permit ipv6 any 2001:DB8:CAFE:10::/64 sequence 10
    deny ipv6 any 2001:DB8:CAFE:11::/64 sequence 20
    permit tcp any host 2001:DB8:CAFE:11::11 eq 22 sequence 30
R3#
```



Common ACL Errors

Troubleshooting IPv6 ACLs- Example 2 cont...

Replace the IPv6 ACL Host Statement

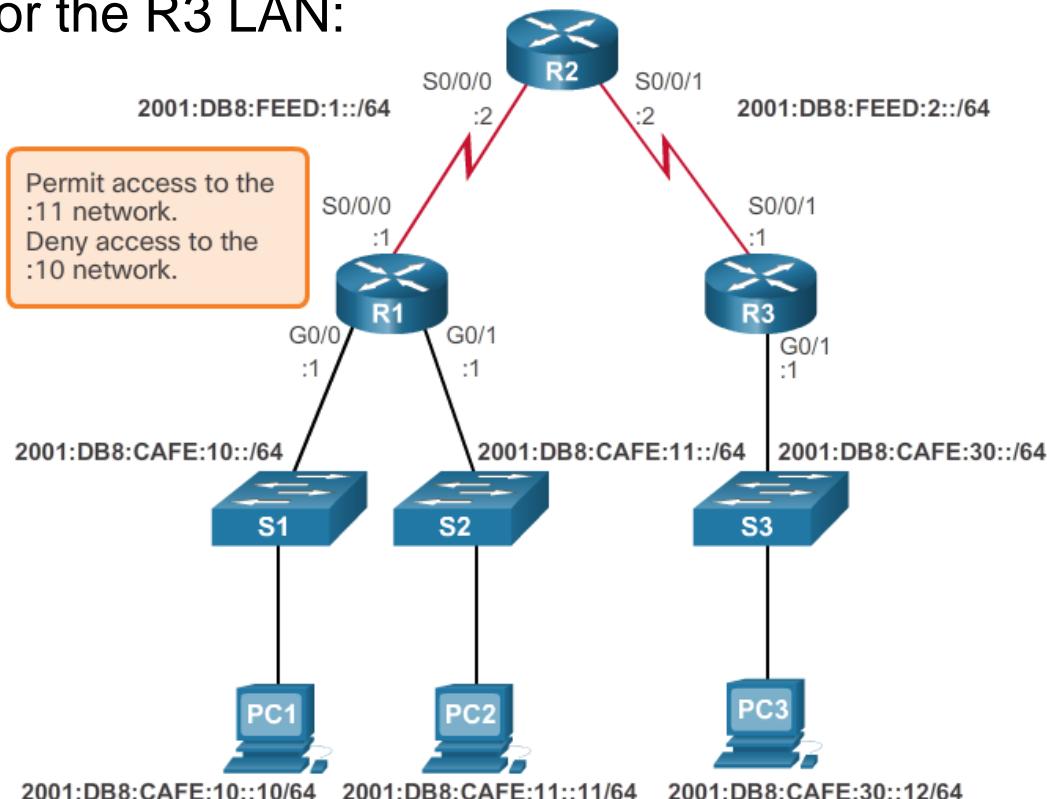
```
R3(config)# ipv6 access-list RESTRICTED-ACCESS
R3(config-ipv6-acl)# no deny ipv6 any 2001:DB8:CAFE:11::/64
R3(config-ipv6-acl)# no permit tcp any host 2001:DB8:CAFE:11::11 eq 22
R3(config-ipv6-acl)# permit tcp any host 2001:DB8:CAFE:11::11 eq 22
R3(config-ipv6-acl)# deny ipv6 any 2001:DB8:CAFE:11::/64
R3(config-ipv6-acl)# end
R3# show access-list
IPv6 access list RESTRICTED-ACCESS
    permit ipv6 any 2001:DB8:CAFE:10::/64 sequence 10
    permit tcp any host 2001:DB8:CAFE:11::11 eq 22 sequence 20
    deny ipv6 any 2001:DB8:CAFE:11::/64 sequence 30
R3#
```



Common ACL Errors

Troubleshooting IPv6 ACLs- Example 3

- R1 is configured with IPv6 ACL DENY-ACCESS that should enforce the following policy for the R3 LAN:



- However, after applying the ACL to the interface the :10 network is still reachable from the :30 network.



Common ACL Errors

Troubleshooting IPv6 ACLs- Example 3 cont...

Verify the IPv6 ACL Configuration and Application

```
R1# show access-list
IPv6 access list DENY-ACCESS
    permit ipv6 any 2001:DB8:CAFE:11::/64 sequence 10
    deny ipv6 any 2001:DB8:CAFE:10::/64 sequence 20
R1# show running-config | section interface GigabitEthernet0/1
interface GigabitEthernet0/1
    no ip address
    duplex auto
    speed auto
    ipv6 address FE80::1 link-local
    ipv6 address 2001:DB8:CAFE:11::1/64
    ipv6 eigrp 1
    ipv6 traffic-filter DENY-ACCESS out
R1#
```



Common ACL Errors

Troubleshooting IPv6 ACLs- Example 3 cont...

Remove ACL on R1, then Configure and Apply ACL on R2

```
R1(config)# no ipv6 access-list DENY-ACCESS
R1(config)# interface g0/1
R1(config-if)# no ipv6 traffic-filter DENY-ACCESS out
R1(config-if)#
!-----
R3(config)# ipv6 access-list DENY-ACCESS
R3(config-ipv6-acl)# permit ipv6 any 2001:DB8:CAFE:11::/64
R3(config-ipv6-acl)# deny ipv6 any 2001:DB8:CAFE:10::/64
R3(config-ipv6-acl)# exit
R3(config)# interface g0/0
R3(config-if)# ipv6 traffic-filter DENY-ACCESS in
R3(config-if)#

```

4.5 Chapter Summary





Chapter Summary

Summary

- By default a router does not filter traffic. Traffic that enters the router is routed solely based on information within the routing table.
- An ACL is a sequential list of permit or deny statements. The last statement of an ACL is always an implicit deny any statement which blocks all traffic. To prevent the implied deny any statement at the end of the ACL from blocking all traffic, the **permit ip any any** statement can be added.
- When network traffic passes through an interface configured with an ACL, the router compares the information within the packet against each entry, in sequential order, to determine if the packet matches one of the statements. If a match is found, the packet is processed accordingly.
- ACLs can be applied to inbound traffic or to outbound traffic.
- **Standard ACLs** can be used to permit or deny traffic **only from a source IPv4 addresses**. The basic **rule for placing a standard ACL** is to place it **close to the destination**.
- **Extended ACLs** filter packets based on several attributes: protocol type, source or destination IPv4 address, and source or destination ports. The **basic rule for placing an extended ACL** is to place it **as close to the source** as possible.



Summary Continued

- The **access-list** global configuration command defines a standard ACL with a number in the range of 1 through 99 or an extended ACL with numbers in the range of 100 to 199. The **ip access-list standard *name*** is used to create a standard named ACL, whereas the command **ip access-list extended *name*** is for an extended access list.
- After an ACL is configured, it is linked to an interface using the **ip access-group** command in interface configuration mode. A device can only have one ACL per protocol, per direction, per interface.
- To remove an ACL from an interface, first enter the **no ip access-group** command on the interface, and then enter the global **no access-list** command to remove the entire ACL.
- The **show running-config** and **show access-lists** commands are used to verify ACL configuration. The **show ip interface** command is used to verify the ACL on the interface and the direction in which it was applied.
- The **access-class** command configured in line configuration mode is used to link an ACL to a particular VTY line.



Summary Continued

- Unlike IPv4, IPv6 ACLs do not have support for a standard or extended option.
- From global configuration mode, use the **ipv6 access-list name** command to create an IPv6 ACL.
- Unlike IPv4 ACLs, IPv6 ACLs do not use wildcard masks. Instead, the prefix-length is used to indicate how much of an IPv6 source or destination address should be matched.
- After an IPv6 ACL is configured, it is linked to an interface using the **ipv6 traffic-filter** command.



Reminder

Lab on Friday

- In this lab we will be configuring and verifying Access Control Lists
- In preparation for the lab, look at the following two videos in Chapter 4 of the NetAcad online course. **Good videos.**

4.1.3.6 Video Demonstration - Standard ACL Configuration Part 1
(Length: 7:38)

4.1.3.7 Video Demonstration - Standard ACL Configuration Part 2
(Length: 7:25)







Chapter 5: Network Security and Monitoring



Connecting Networks

Cisco | Networking Academy®
Mind Wide Open™



Chapter 5 - Sections & Objectives

- 5.1 LAN Security
 - Explain how to mitigate common LAN security issues.
- 5.2 SNMP
 - Configure SNMP to monitor network operations in a small to medium-sized business network.
- 5.3 Cisco Switch Port Analyzer (SPAN)
 - Troubleshoot a network problem using SPAN.



5.1 LAN Security



Cisco | Networking Academy®
Mind Wide Open™

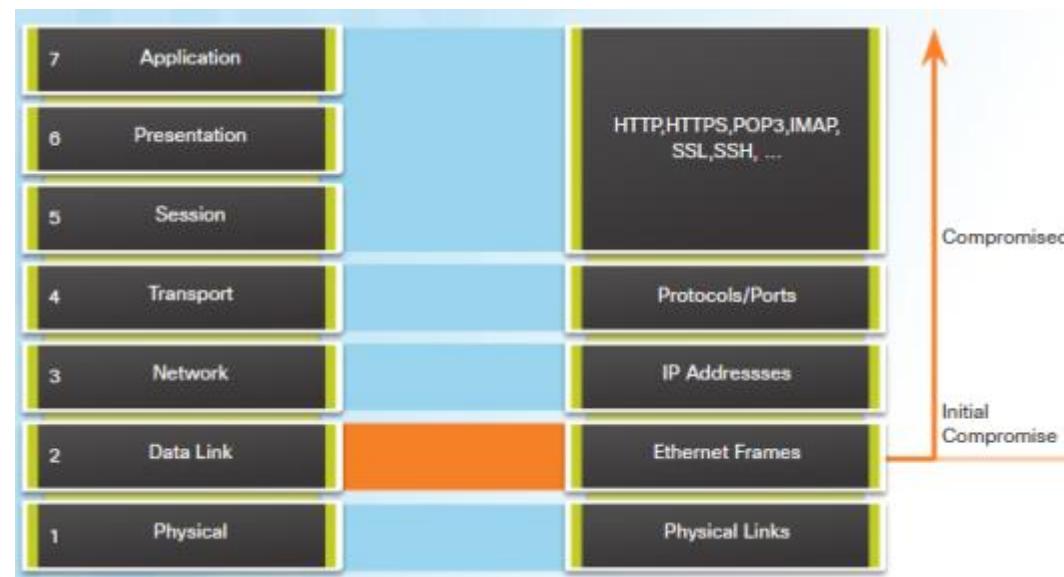


LAN Security

LAN Security Attacks *

- Common attacks against the Layer 2 LAN infrastructure include:
 - MAC Address Table Flooding Attacks
 - VLAN Attacks
 - DHCP Attacks
 - CDP Reconnaissance Attacks
 - Telnet Attacks

If Layer 2 compromised,
then all layers above
Layer 2 are also affected.





LAN Security

LAN Security Best Practices *

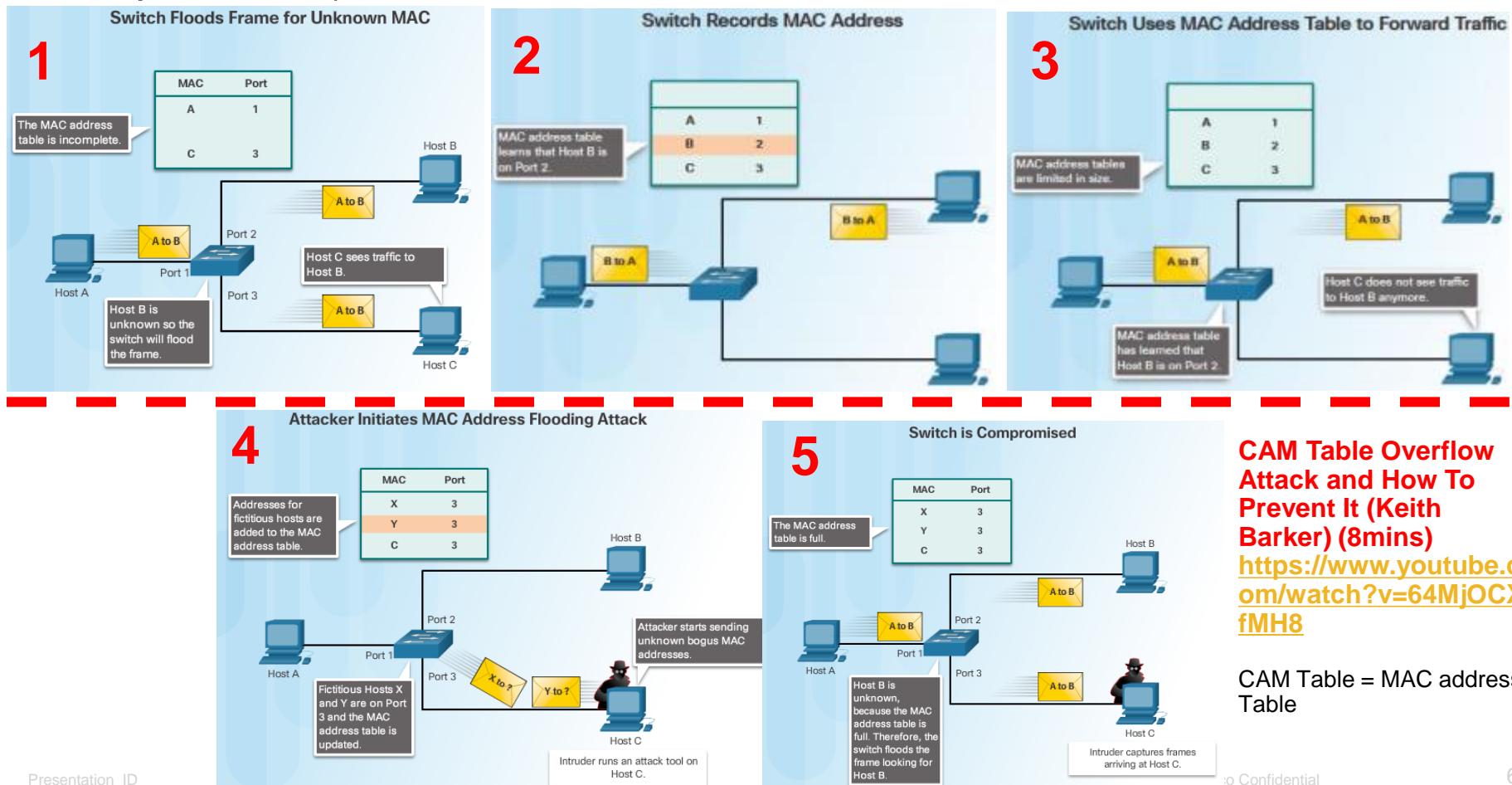
- This topic covers several Layer 2 security solutions:
 - MAC address table flooding attacks
 - Mitigate using port security (fail-open mode)
 - VLAN attacks (switch spoofing)
 - Mitigate disable auto trunking...
 - DHCP attacks (spoofing and starvation)
 - Mitigate using DHCP snooping
 - Securing administrative access using AAA (local or server based)
 - Securing device access using IEEE 802.1X port authentication
 - 802.1X standard defines a port-based access control and authentication protocol. Restricts unauthorized workstations from connecting to a LAN through publicly accessible switch ports
 - An authentication server authenticates each workstation that is connected to a switch port before making available any services offered by the switch or the LAN.



LAN Security

LAN Security Best Practices

- This topic covers several Layer 2 security solutions:
 - Mitigating MAC address table flooding attacks using port security (fail-open mode)

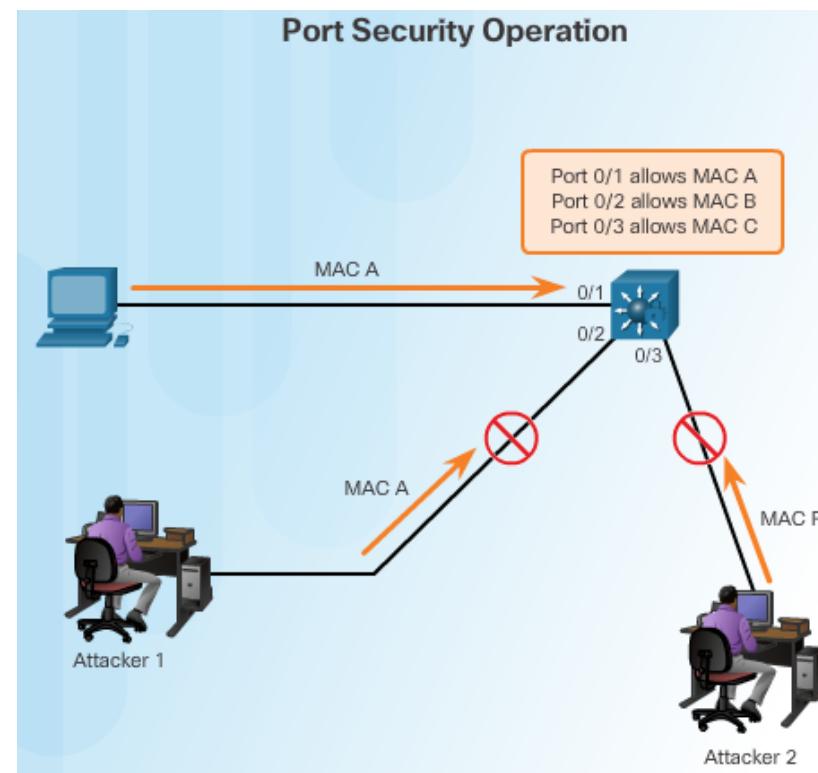




LAN Security

Mitigate MAC Address Attacks

- Enable port security
- Statically specify MAC addresses for a port
- Limit permitted MAC addresses



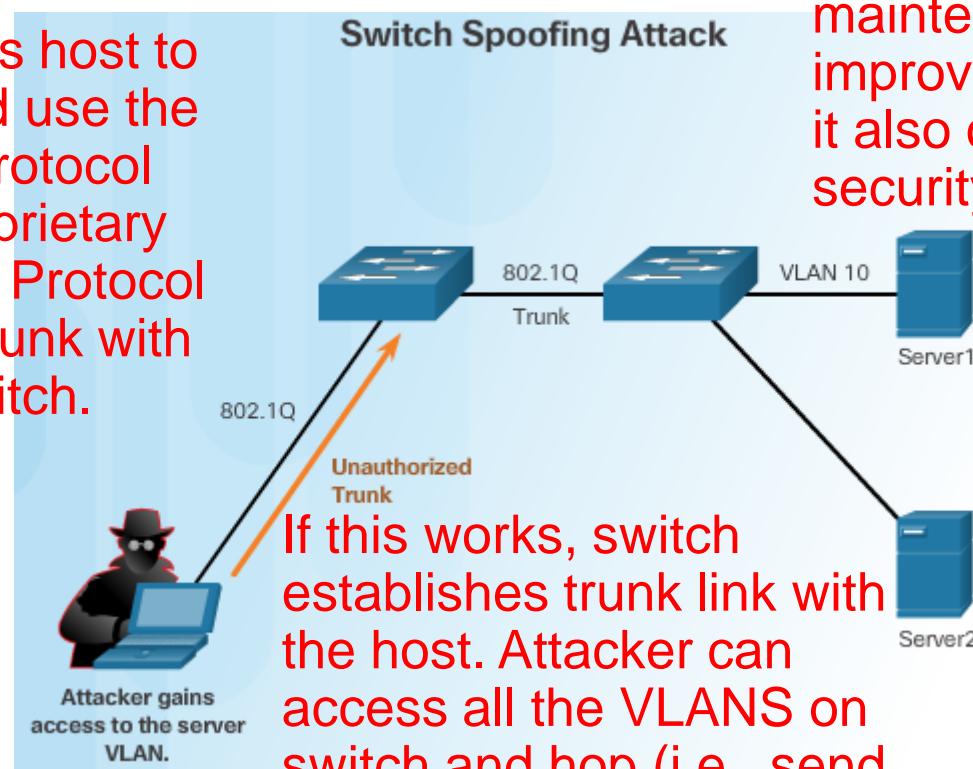


LAN Security

LAN Security Best Practices

- This topic covers several Layer 2 security solutions:
 - Mitigating VLAN attacks (switch spoofing)

Attacker configures host to spoof a switch and use the 802.1Q trunking protocol and the Cisco-proprietary Dynamic Trunking Protocol (DTP) feature to trunk with the connecting switch.



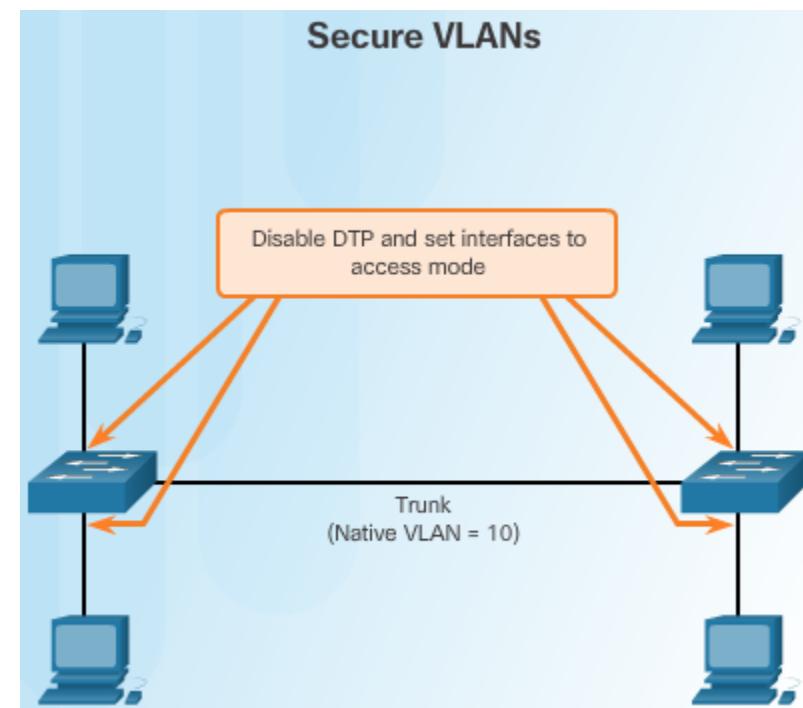
VLAN architecture simplifies network maintenance and improves performance, but it also opens the door to security risks.



LAN Security

Mitigate VLAN Attacks

- Disable DTP (Auto Trunking)
- Set native VLAN to something other than default VLAN 1
- Disable unused ports. Make them access ports, and assign them to a black hole VLAN.
- Enable port security





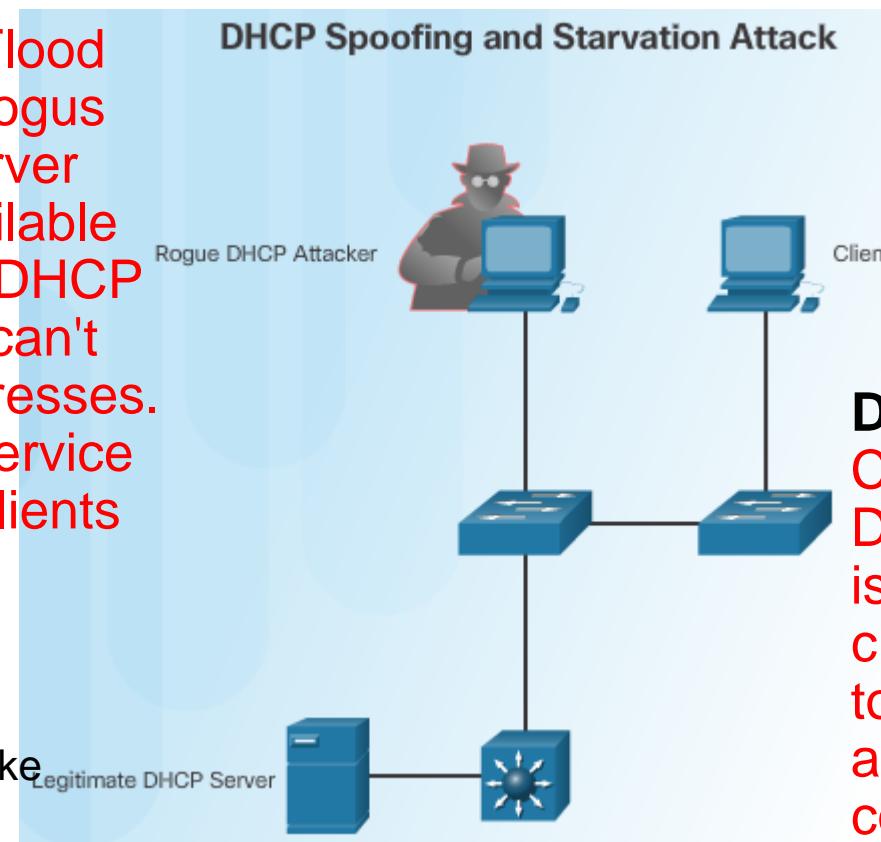
LAN Security

LAN Security Best Practices

- This topic covers several Layer 2 security solutions:
 - Mitigating DHCP attacks using DHCP snooping (spoofing and starvation)

DHCP starvation. Flood DHCP server with bogus DHCP requests. Server leases all of the available IP addresses in the DHCP server pool. Server can't issue any more addresses. Result is denial-of-service (DoS) attack. New clients cannot get network access.

DHCP starvation is often used before spoofing. Take 'out' legitimate server. Easier to introduce fake DHCP server.



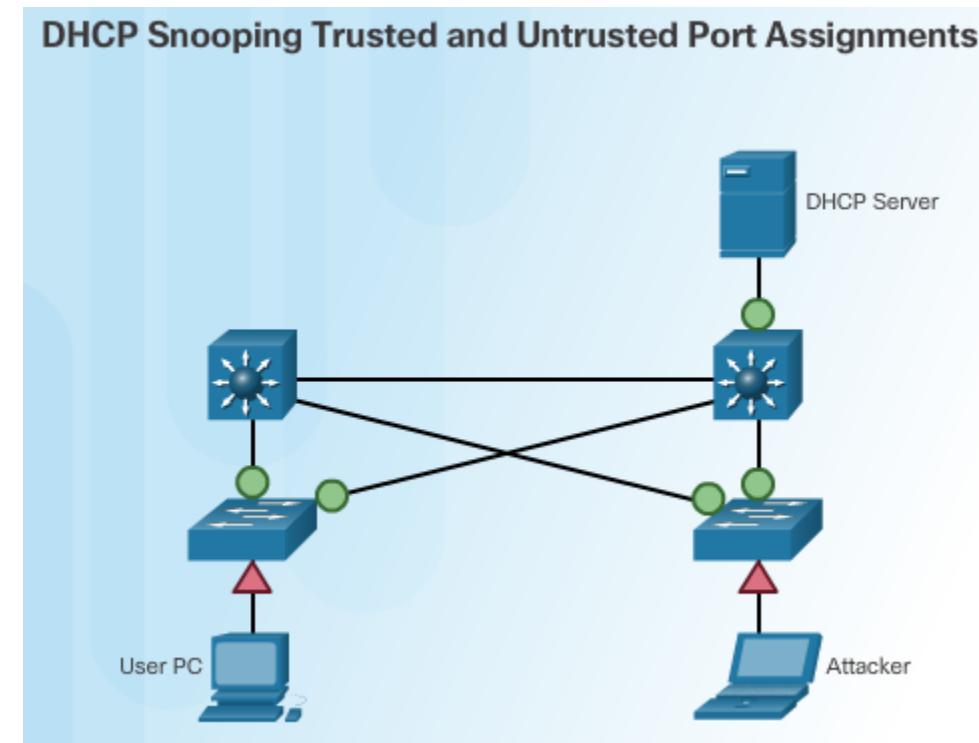
DHCP spoofing. Configures a fake DHCP server. Server issue IP addresses to clients. Forces clients to use false DNS server and computer under control of attacker default gateway.



LAN Security

Mitigate DHCP Attacks

- Use Port Security
- Use DHCP Snooping
- Compares the DHCP source packet information with that held in a binding database.
 - Switch builds a DHCP binding table that maps a client MAC address, IP address, VLAN and port ID.
 - When DHCP snooping is configured, switch ports are configured as either a trusted port or an untrusted port.
 - A device connected to a trusted port can send any type of DHCP message into the switch.
 - An untrusted port only allows incoming DHCP requests.



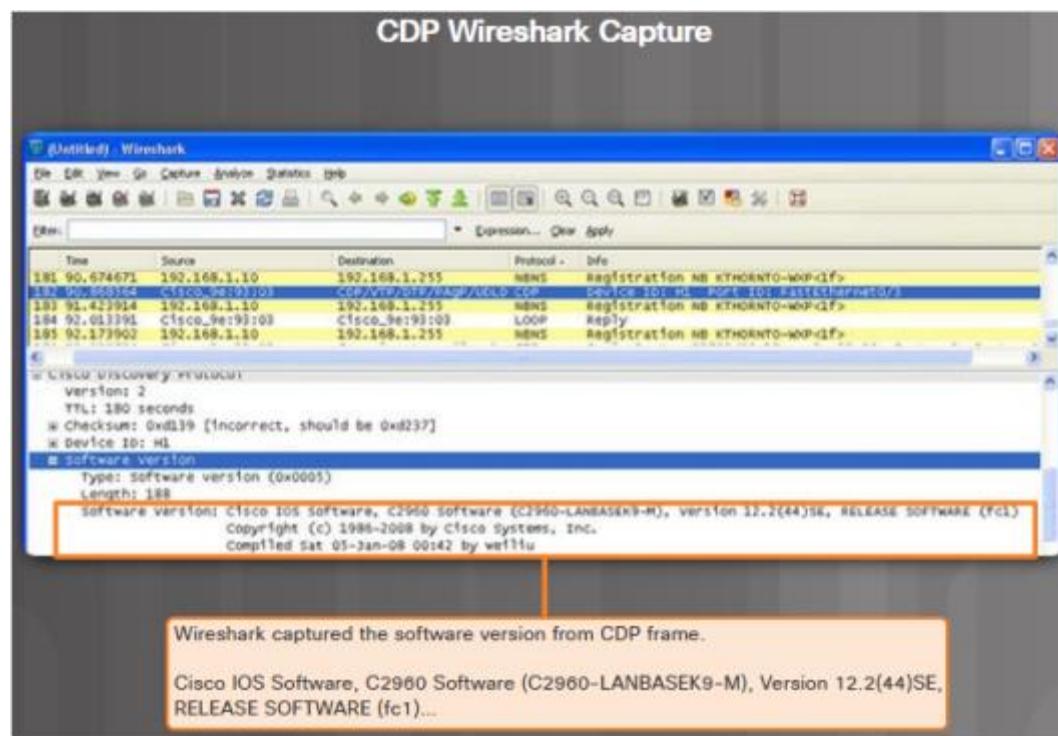


LAN Security

CDP Reconnaissance Attacks

- Common attacks against the Layer 2 LAN infrastructure include:

- CDP Reconnaissance Attacks
- CDP = Cisco Discovery Protocol



CDP: discover information about neighboring devices.

CDP: Useful for troubleshooting.

CDP: Useful for attackers
- discover network infrastructure vulnerabilities.

See Wireshark capture...can identify the Cisco IOS software version used by the device.

Attacker can see any security vulnerabilities specific to IOS version..



LAN Security

Mitigate CDP Reconnaissance Attacks

- Limit CDP on devices or ports.
- Disable CDP on edge ports that connect to untrusted devices

CDP globally disable: **no cdp run**

CDP globally enable: **cdp run**

CDP port disable: **no cdp enable** on interface

CDP port disable: **cdp enable** on interface

CDP Wireshark Capture

The screenshot shows a Wireshark capture window titled "CDP Wireshark Capture". The packet list pane displays several CDP frames (Protocol: CDP) between Cisco routers. The details pane shows the registration message for each router. The bytes pane shows the raw CDP frame structure. The bottom status bar indicates: "Wireshark captured the software version from CDP frame." A callout box highlights the software version information in the details pane: "Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(44)SE, RELEASE SOFTWARE (fc1)".

CDP Wireshark Capture

File Edit View Go Capture Analyze Statistics Help

Expression... Clear Apply

Time	Source	Destination	Protocol	Info
181 90.674671	192.168.1.10	192.168.1.255	MBNS	REGISTRATION NB KTHORONTO-NOP<1f>
182 90.685364	CISCO_9e:93:03	CISCO_9e:93:03	CDP	DEVICE ID: M1 PORT ID: F1/E1/E2/H1/H2
183 91.429914	192.168.1.10	192.168.1.255	MBNS	REGISTRATION NB KTHORONTO-NOP<1f>
184 92.013391	Cisco_9e:93:03	Cisco_9e:93:03	LOOP	Reply
185 92.177902	192.168.1.10	192.168.1.255	MBNS	REGISTRATION NB KTHORONTO-NOP<1f>

Wireshark captured the software version from CDP frame.

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(44)SE, RELEASE SOFTWARE (fc1)...
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Sat 03-Jan-08 00:14:22 by wmtlu



LAN Security

LAN Security Attacks *

- Common attacks against the Layer 2 LAN infrastructure include:
 - Telnet Attacks

Brute Force Password Attack

This screenshot shows a password auditing tool interface. The main window displays a table of user accounts with columns for User Name, Password, and Method used to crack the password. The 'Method' column indicates whether the password was cracked using a Dictionary attack or Precomputed Hashes. The right side of the interface shows a progress bar and a summary of the audit results, including the number of users audited, the number of users cracked, and the total audit time.

User Name	Password	Method
administrator	a	Precomputed Hash
charles	abc	Precomputed Hash
serge	aaaaaa	Precomputed Hash
reba	cccccc	Precomputed Hash
fred	crash007	Precomputed Hash
larry	123456	Precomputed Hash
jim	mmmm	Precomputed Hash
judith	aaa	Precomputed Hash
and	aaaa	Precomputed Hash
kathy	xxxxxx	Precomputed Hash
lupe	lupehoney	Precomputed Hash
factor	z	Precomputed Hash
jane	rr	Precomputed Hash
theresa	000	Precomputed Hash
wilma	empty	Precomputed Hash
Administrator	Solaris25	Precomputed Hash
root	a	Precomputed Hash
stake	"jazzing"	Dictionary
bill	nnn	Precomputed Hash
george	mmmm	Precomputed Hash
thomas	xxxxxxxx	Precomputed Hash
DerrickLee	aa	Precomputed Hash
rita	aaa	Precomputed Hash

05/19/2004 16:43:35 Cracked password for lupe with Precomputed Hashes.
 05/19/2004 16:43:36 Cracked password for lupe with Precomputed Hashes.
 05/19/2004 16:43:41 Cracked password for Theresa with Precomputed Hashes.
 05/19/2004 16:43:43 Cracked password for Bill with Precomputed Hashes.
 05/19/2004 16:43:47 Cracked password for Charles with Precomputed Hashes.
 05/19/2004 16:43:47 Cracked password for DerrickLee with Precomputed Hashes.
 05/19/2004 16:44:43 Cracked password for Tom with Precomputed Hashes.
 05/19/2004 16:44:43 Cracked password for User with Precomputed Hashes.
 05/19/2004 16:44:44 Auditing session completed.

Example of Password Auditing Tool.

Two types of Telnet attack

1. Brute Force Password Attack

- 1st Phase: Dictionary attack.
- 2nd Phase: Password auditing tools to create sequential character combinations to guess the password.

2 Telnet DoS Attack

- Continuously request Telnet connections. Makes Telnet service unavailable. No admin access to device(s)...
- Can be used with other direct attacks to stop the admin access during a breach.



LAN Security

LAN Security Best Practices *

- There are several strategies to help secure Layer 2 of a network:
 - Always use secure variants of these protocols such as SSH, SCP, SSL, SNMPv3, and SFTP.
 - Always use strong passwords and change them often. (**Users & usability issues?**)
 - Enable CDP on select ports only.
 - Secure Telnet access.
 - Use a dedicated management VLAN where nothing but management traffic resides.
 - Use ACLs to filter unwanted access on vty lines etc.
 - Authenticate and authorize administrative access to the device using **AAA** with either **TACACS+** or **RADIUS** protocols.

AAA: The Authentication, Authorization, and Accounting framework

TACACS+ : Terminal Access Controller Access Control System (TACACS+) protocol

RADIUS : Remote Authentication Dial-In User Service protocol



LAN Security

LAN Security Best Practices *

- AAA: The Authentication, Authorization, and Accounting framework
- Authentication = Who is the user?
- Authorization = What is the user allowed do?
- Accounting = What did the user do?



LAN Security

LAN Security Best Practices *

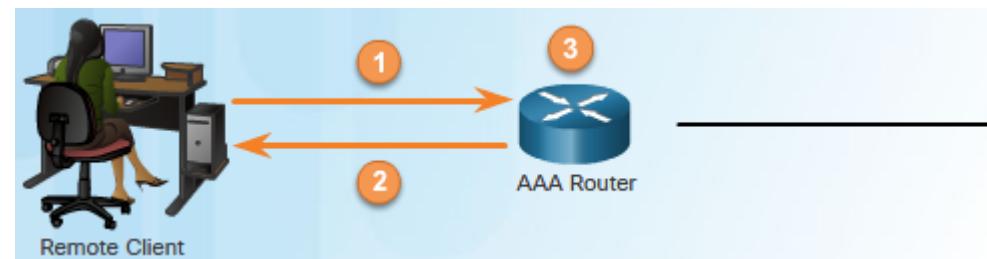
- AAA: The Authentication, Authorization, and Accounting framework
- Two common methods of implementing AAA
 - Local AAA Authentication –
 - **Local database for authentication** - stores usernames and passwords locally in the Cisco router, and users authenticate against the local database. Suitable for small networks.
 - Server-Based AAA Authentication –
 - Server-based AAA authentication - router accesses a **central AAA server** that contains the usernames and password for all users and serves as a central authentication system for all infrastructure devices.



LAN Security

LAN Security Best Practices *

- Local AAA Authentication



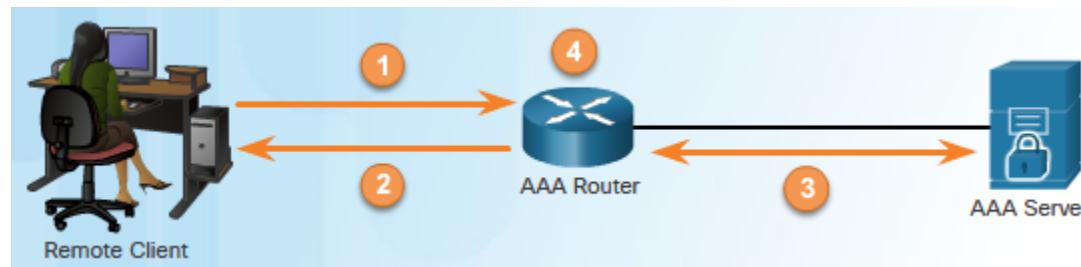
- 1 The client establishes a connection with the router.
- 2 The AAA router prompts the user for a username and password.
- 3 The router authenticates the username and password using the local database. User gets access to network based on the information in the local database.



LAN Security

LAN Security Best Practices *

■ Server-Based AAA Authentication



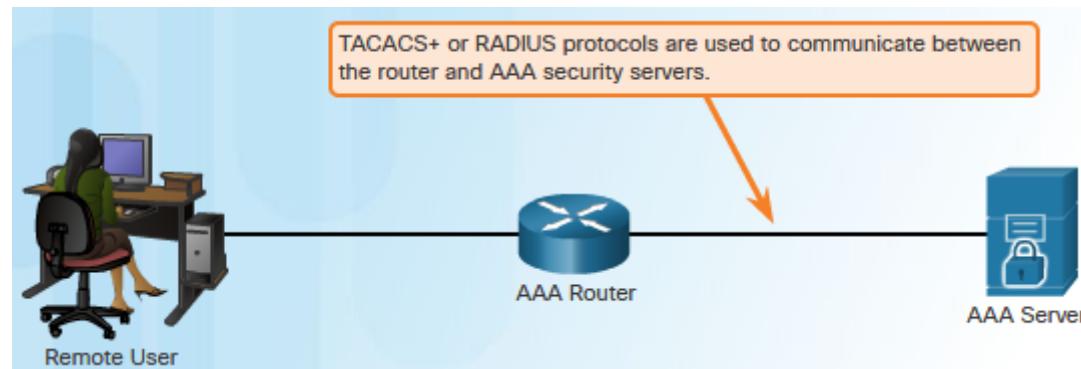
- 1 The client establishes a connection with the router.
- 2 The AAA router prompts the user for a username and password.
- 3 The router authenticates the username and password using a remote AAA server.
- 4 User gets access to network



LAN Security

LAN Security Best Practices *

■ Server-Based AAA Authentication: TACACS+ vs. RADIUS



- TACACS+ : Terminal Access Controller Access Control System (TACACS+) protocol
- RADIUS : Remote Authentication Dial-In User Service protocol

- Both TACACS+ and RADIUS protocols can be used to communicate between a router and AAA servers.
- TACACS+ is more secure. All TACACS+ protocol exchanges are encrypted.
- RADIUS only encrypts the user's password. User names & accounting not encrypted.

5.2 SNMP

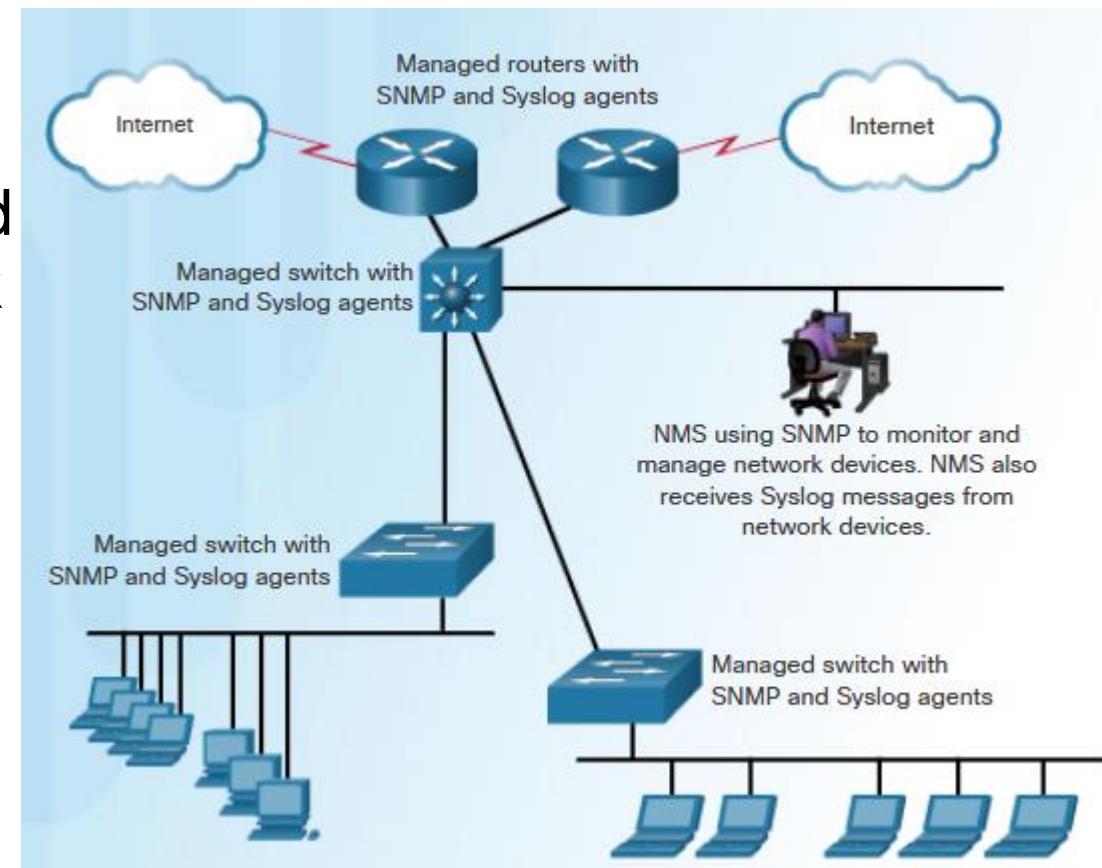




SNMP

SNMP Operation

- SNMP (Simple Network Management Protocol) is a network management protocol which can be used to **manage, monitor** and control clients on an IP network.
- SNMP can be used to **get** and **set** variables indicating the status and configuration of network hosts such routers and switches, and also network client computers.
- Can get info about 'system up time', for example.

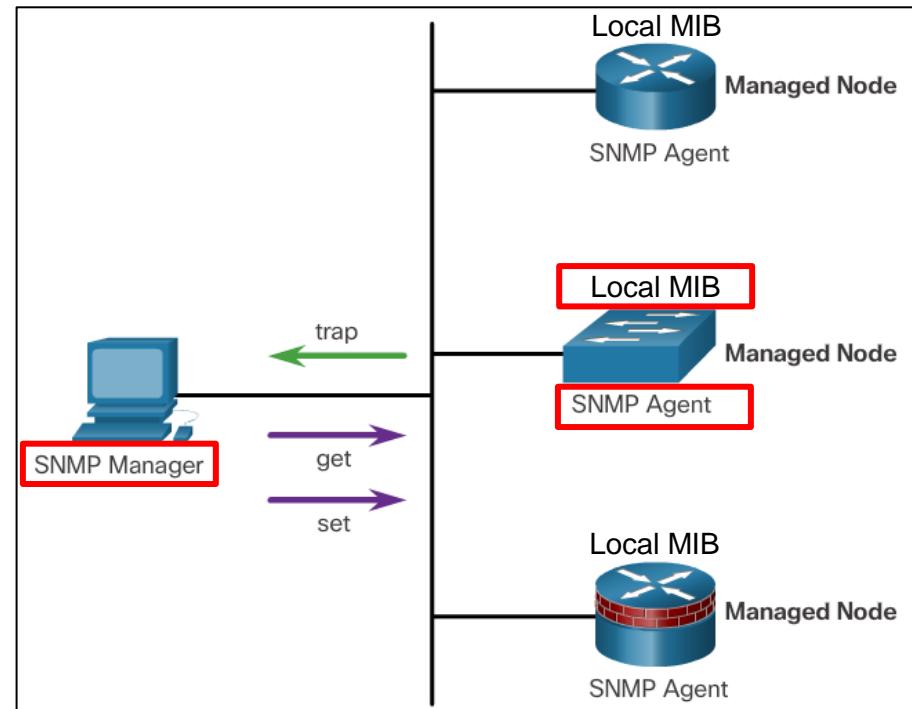




SNMP

SNMP Operation

- SNMP allows administrators to **manage** and **monitor** devices on an IP network.
- SNMP Elements
 - SNMP **Manager**
 - SNMP **Agent** (Nodes)
 - **MIB** (management Information base)
- SNMP Operation
 - Trap (Send info)
 - Get (Collect info)
 - Set (Change configuration)



Information about the status of network devices is stored in variables in a Management Information Base (MIB) on each device.

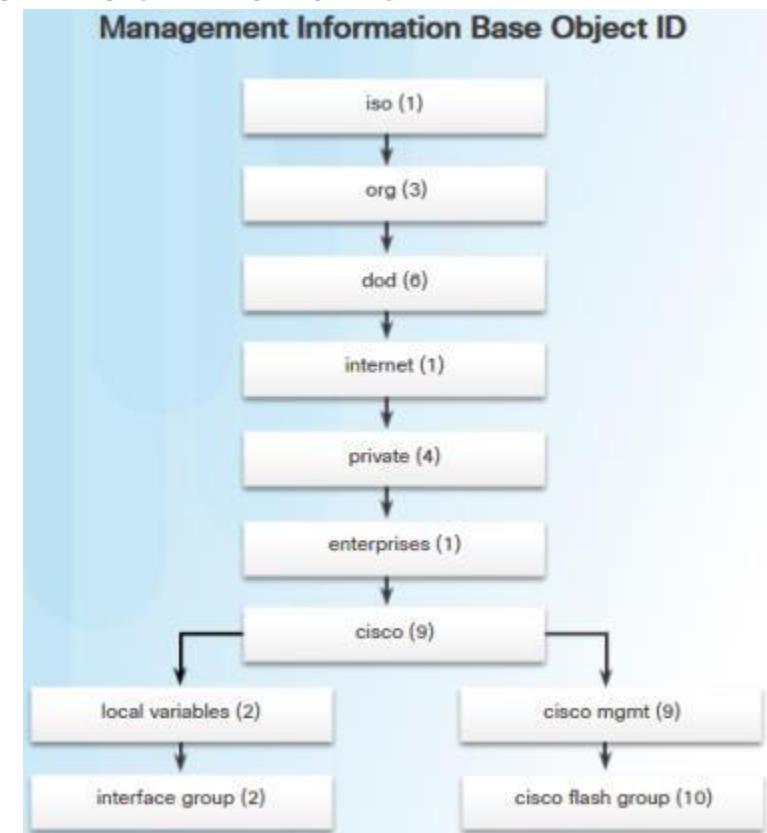
The Management software uses these variables to monitor and control network devices.



SNMP

SNMP Operation – MIB Object ID

- MIB exists on each device.
- MIB organizes **variables** hierarchically.
- MIB variables enable the management software to monitor and control the network device.
- Formally, the MIB defines each variable as an object ID (OID).
- OIDs uniquely identify managed objects in the MIB hierarchy.
- The MIB organizes the OIDs based on RFC standards into a hierarchy of OIDs, usually shown as a tree.

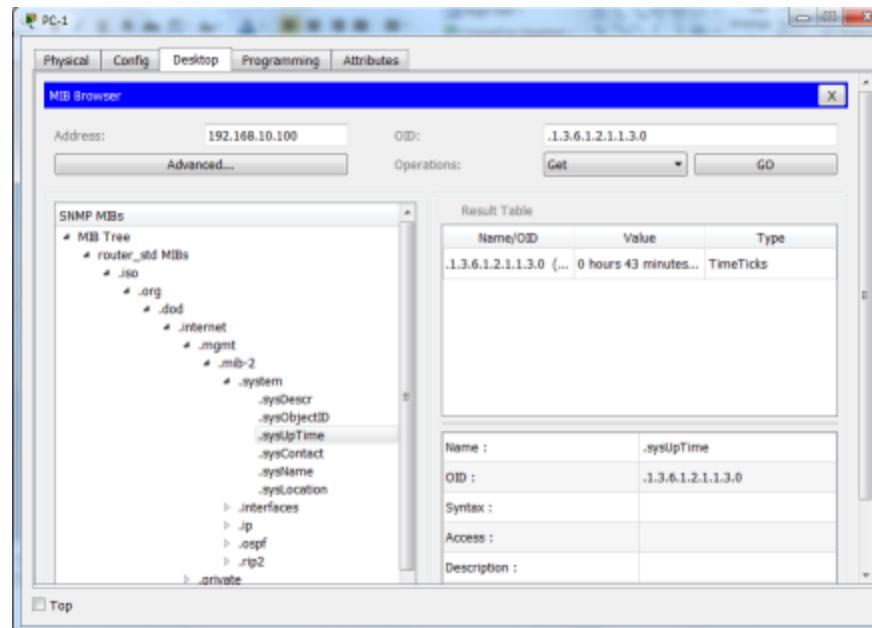




SNMP

SNMP Operation – MIB Object ID

- OIDs can be described in words and numbers to find a variable in the tree.



Example from MIB browser on a Packet Tracer PC

- (iso.org.dod.internet.mgmt.mib-2.system.sysUpTime
(0.1.3.6.1.2.1.1.3.0)
- OID = 0.1.3.6.1.2.1.1.3 describes the variable sysUpTime



SNMP

SNMP Operation

■ SNMP Security Model and Levels

Model	Level	Authentication	Encryption	Result
SNMPv1	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
SNMPv2c	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
SNMPv3	noAuthNoPriv	Username	No	Uses a username match for authentication (an improvement over SNMPv2c).
SNMPv3	authNoPriv	Message Digest 5 (MD5) or Secure Hash Algorithm (SHA)	No	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
SNMPv3	authPriv (requires the cryptographic software image)	MD5 or SHA	Data Encryption Standard (DES) or Advanced Encryption Standard (AES)	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.



SNMP

SNMP Operation – Community strings

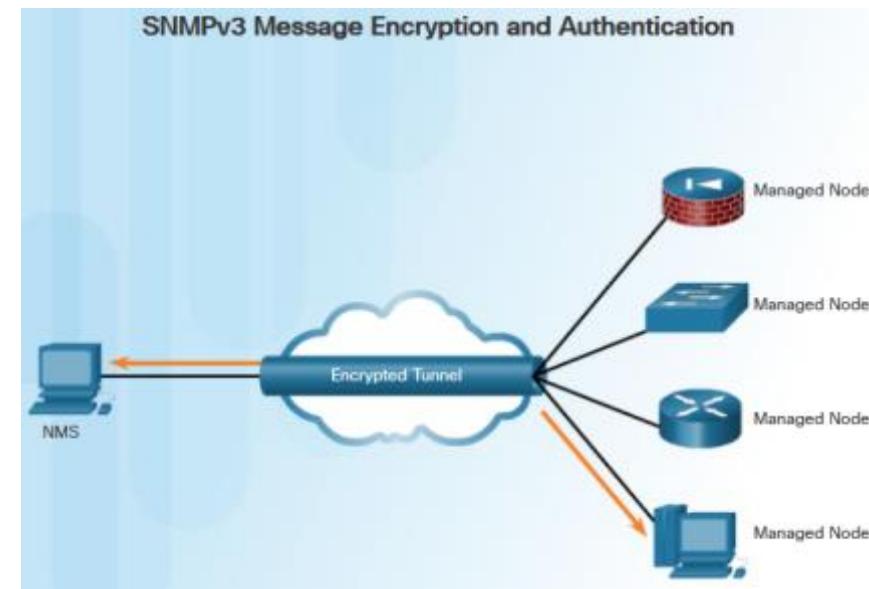
- Network management System access requests to MIB need authentication
- SNMPv1 and SNMPv2c use **community strings** authenticate access to MIB objects.
- Two types of community strings
 - **Read-only (ro)** - variables can't changed. Used in SNMPv2c as security is minimal
 - **Read-write (rw)** - Read and Write access to all objects in the MIB.
 - See animation in online course Section 5.2.1.5. Shows SNMP operating with community string.
 - Community strings are **plaintext passwords!**



SNMP

SNMP Operation – SNMPv3

- SNMPv3 authenticates and encrypts packets. Address the security issues with SNMPv1 and SNMPv2.
- SNMPv3 provides three security features:
 - Message integrity and authentication
 - Ensures no tampering in transit
 - Encryption
 - Packet contents scrambled
 - Access control
 - Restrict SNMP manager e.g. no full access to firewall device.





SNMP

SNMP Operation – Best Practices

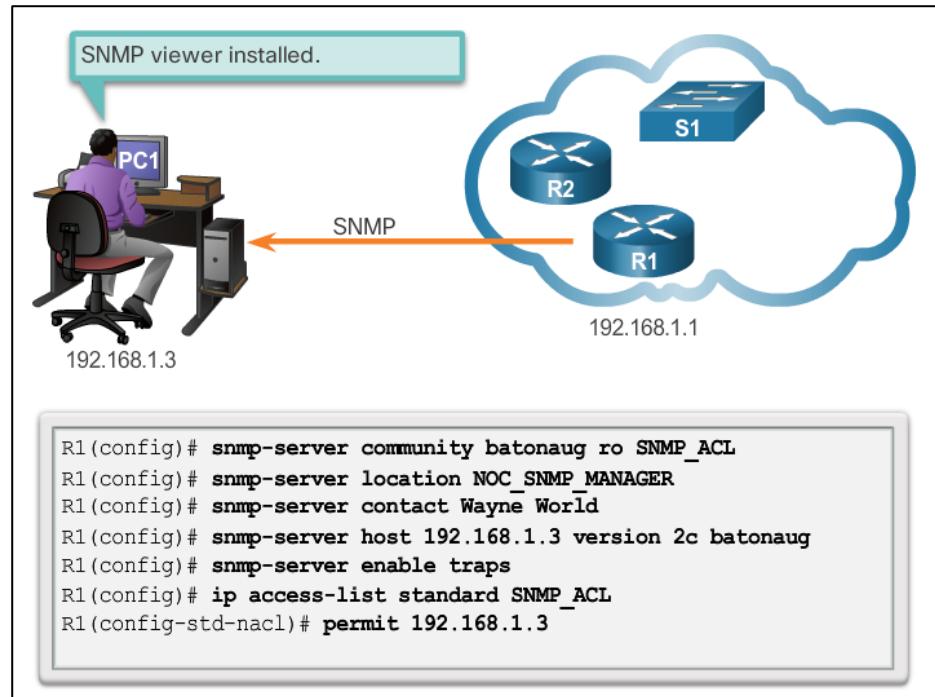
- SNMP can also have security vulnerabilities
- Both SNMPv1 and community strings should be carefully chosen and changed regularly.
- Ensure that SNMP messages do not spread beyond the management consoles.
 - ACLs to prevent SNMP messages going beyond the required devices.
 - ACLs on the monitored devices to limit access for management systems only.
- SNMPv3 is recommended because it provides security authentication and encryption.



SNMP

Configuring SNMP

- Configuration steps
 - Configure community string
 - Document location of device
 - Document system contact
 - Restrict SNMP Access
 - Specify recipient of SNMP Traps
 - Enable traps on SNMP agent



SNMP traps = Alert messages sent from SNMP agent to SNMP manager.



SNMP

Configuring SNMP

■ Securing SNMPv3

Step 1: Configure an ACL to permit access to the protected management network.

```
Router(config)# ip access-list standard acl-name  
Router(config-std-nacl)# permit source_net
```

Step 2: Configure an SNMP view.

```
Router(config)# snmp-server view view-name oid-tree
```

Step 3: Configure an SNMP group.

```
Router(config)# snmp-server group group-name v3  
priv read view-name access [acl-number | acl-name]
```

Step 4: Configure a user as a member of the SNMP group.

```
Router(config)# snmp-server user username group-name v3  
auth {md5 | sha} auth-password priv {des | 3des | aes  
{128 | 192 | 256}} privpassword
```



5.3 Cisco Switch Port Analyzer (SPAN)



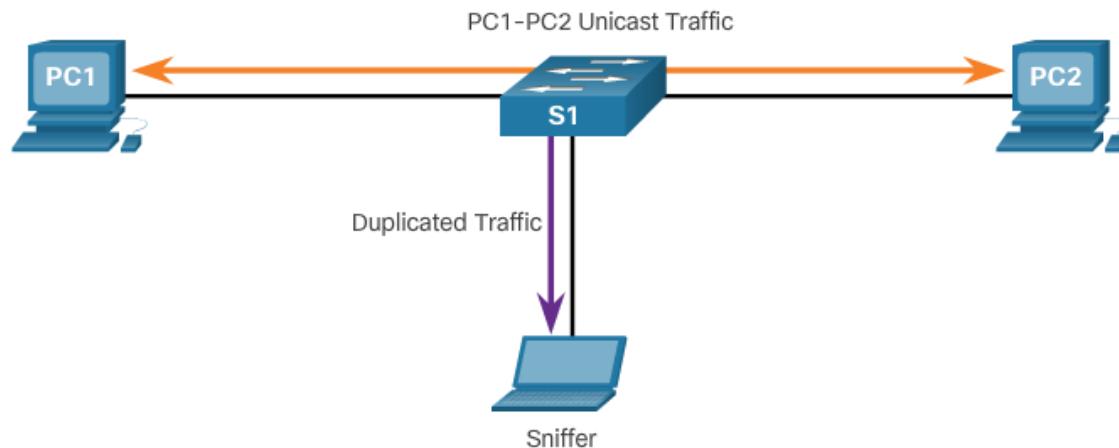
Cisco | Networking Academy®
Mind Wide Open™



Cisco Switch Port Analyzer SPAN Overview

■ Port mirroring

- The port mirroring feature allows a switch to **copy** and send Ethernet frames from specific ports to the destination port connected to a packet analyzer. The original frame is still forwarded in the usual manner.



Port Mirroring: Traffic between PC1 and PC2 is also sent to Laptop. Packet sniffer/analyser is installed on Laptop.



Cisco Switch Port Analyzer SPAN Overview

- Local SPAN
 - Traffic on a switch is mirrored to another port on the **same** switch.
 - Local because the monitored ports are all located on the **same** switch as the destination port (monitor port).
- Remote SPAN (RSPAN)
 - Source and destination ports can be in different switches.
 - Useful when the packet analyzer is on a different switch to the traffic being monitored.

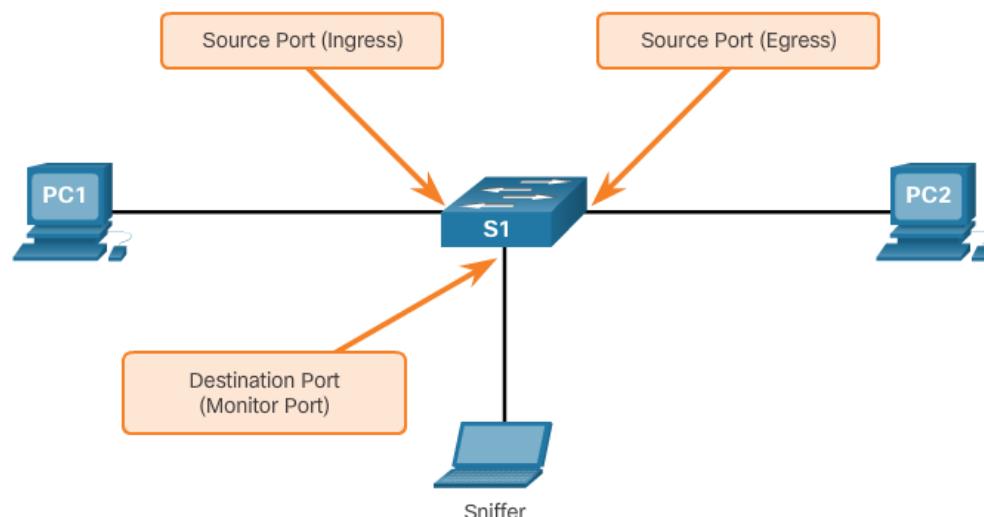


Cisco Switch Port Analyzer SPAN Overview

■ SPAN terminology

Term	Definition
Ingress traffic	This is traffic that enters the switch.
Egress traffic	This is traffic that leaves the switch.
Source (SPAN) port	This is a port that is monitored with use of the SPAN feature.
Destination (SPAN) port	This is a port that monitors source ports, usually where a packet analyzer, IDS or IPS is connected. This port is also called the monitor port.
SPAN session	This is an association of a destination port with one or more source ports.
Source VLAN	This is the VLAN monitored for traffic analysis.

IDS = intrusion detection system, IPS = intrusion prevention system

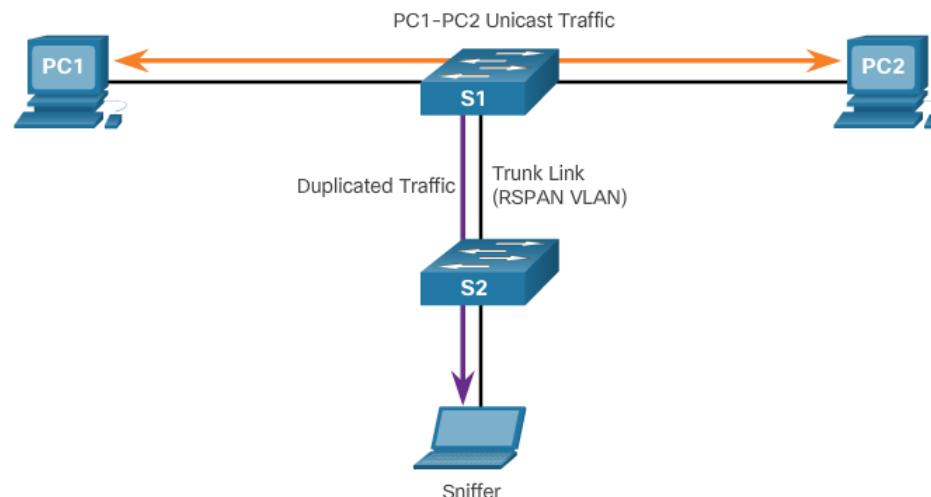




Cisco Switch Port Analyzer SPAN Overview

■ RSPAN terminology

Term	Definition
RSPAN source session	This is the source port/VLAN to copy traffic from.
RSPAN destination session	This is the destination VLAN/port to send the traffic to.
RSPAN VLAN	<ul style="list-style-type: none">A unique VLAN is required to transport the traffic from one switch to another.The VLAN is configured with the <code>remote-span vlan</code> configuration command.This VLAN must be defined on all switches in the path and must also be allowed on trunk ports between the source and destination.





Cisco Switch Port Analyzer SPAN Configuration

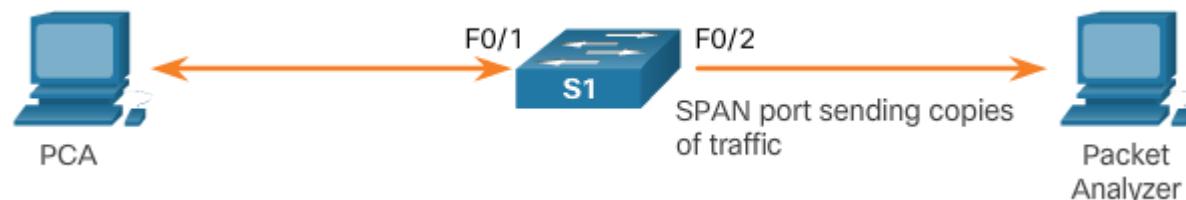
- Use **monitor session** global configuration command

Associate a SPAN session with a source port

```
Switch(config)# monitor session number source [ interface interface | vlan vlan ]
```

Associate a SPAN session with a destination port

```
Switch(config)# monitor session number destination [ interface interface | vlan vlan ]
```



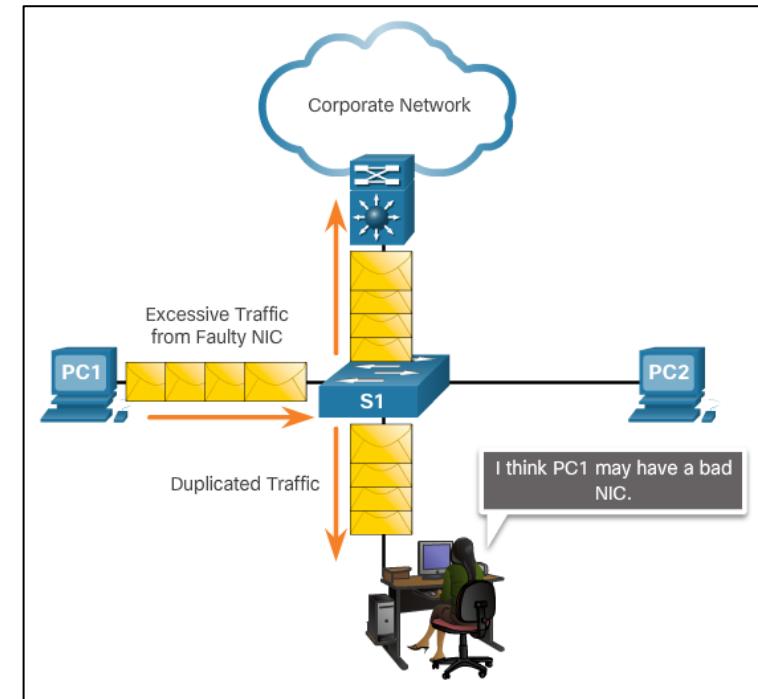
```
S1(config)# monitor session 1 source interface fastethernet 0/1
S1(config)# monitor session 1 destination interface fastethernet 0/2
```



Cisco Switch Port Analyzer

SPAN as a Troubleshooting Tool

- SPAN allows administrators to troubleshoot network issues
- Administrator can use SPAN to duplicate and redirect traffic to a packet analyzer (e.g. Wireshark)
- Administrator can analyze traffic from all devices to troubleshoot sub-optimal operation of network applications
- Find faulty NICs. Enable SPAN. Send traffic to a packet analyzer. Helps find and isolate the end device causing the excess traffic.



5.4 Chapter Summary





Chapter Summary

Summary

- At Layer 2, a number of vulnerabilities exist that require specialized mitigation techniques:
 - MAC address table flooding attacks are addressed with port security.
 - VLAN attacks are controlled by disabling DTP and following basic guidelines for configuring trunk ports.
 - DHCP attacks are addressed with DHCP snooping.
- The SNMP protocol has three elements: the Manager, the Agent, and the MIB. The SNMP manager resides on the NMS, while the Agent and the MIB are on the client devices.
 - The SNMP Manager can poll the client devices for information, or it can use a TRAP message that tells a client to report immediately if the client reaches a particular threshold. SNMP can also be used to change the configuration of a device.



Summary Continued

- SNMPv3 is the recommended version because it provides security.
- SNMP is a comprehensive and powerful remote management tool. Nearly every item available in a **show** command on a network device is available through SNMP.
- Switched Port Analyzer (SPAN) is used to mirror the traffic going to and/or coming from the host. It is commonly implemented to support traffic analyzers or IDS/IPS devices.



Reminder

Lab on Friday

- In this lab we will be investigating the operation of an SNMP for network monitoring and management,







Chapter 6: Quality of Service



Connecting Networks

Cisco | Networking Academy®
Mind Wide Open™



Chapter 6 - Sections & Objectives

- 6.1 QoS Overview
 - Explain the purpose and characteristics of QoS.
- 6.2 QoS Mechanisms
 - Explain how networking devices implement QoS.



Chapter 6 – QoS Video List on NetAcad

Watch the QoS Videos – they give a good summary.

- **6.1.1.1 Video Tutorial - The Purpose of QoS (3mins)**

- **6.1.2.1 Video Tutorial - Traffic Characteristics (2:43mins)**

- **6.1.3.1 Video Tutorial - QoS Algorithms (1:29mins)**

- **6.2.1.1 Video Tutorial - QoS Models (4:22mins)**

- **6.2.2.1 Video Tutorial - QoS Implementation Techniques (8:26mins).**

6.1 QoS Overview





QoS Overview

Introduction

- Quality of service (QoS) is an important network requirement.
- New applications (voice and live video) create higher expectations for quality delivery.
- Users expect content to be available 'immediately'.
- The quality of network transmission is affected by
 - Link bandwidth between source and destination
 - Delay as packets are routed to destination, and
 - Variation in delay of received packets, (jitter).
- Quality-of-service (QoS) mechanisms can be used to prioritize time-sensitive traffic (voice and video) over less time-sensitive traffic (email and web browsing) and ensure a quality experience for the user.



QoS Overview

Network Transmission Quality

■ Congestion

- Congestion occurs when multiple communication lines aggregate onto a single device such as a router, and then much of that data is placed on fewer outbound interfaces or onto a slower interface.
- When the volume of traffic is greater than the volume that can be transported across the network, devices **queue**, the packets in memory until resources become available to transmit them.
- Queuing packets causes **delay** because new packets cannot be transmitted until previous packets have been processed.
- If the number of packets to be queued continues to increase, the memory within the device fills up and packets are dropped.

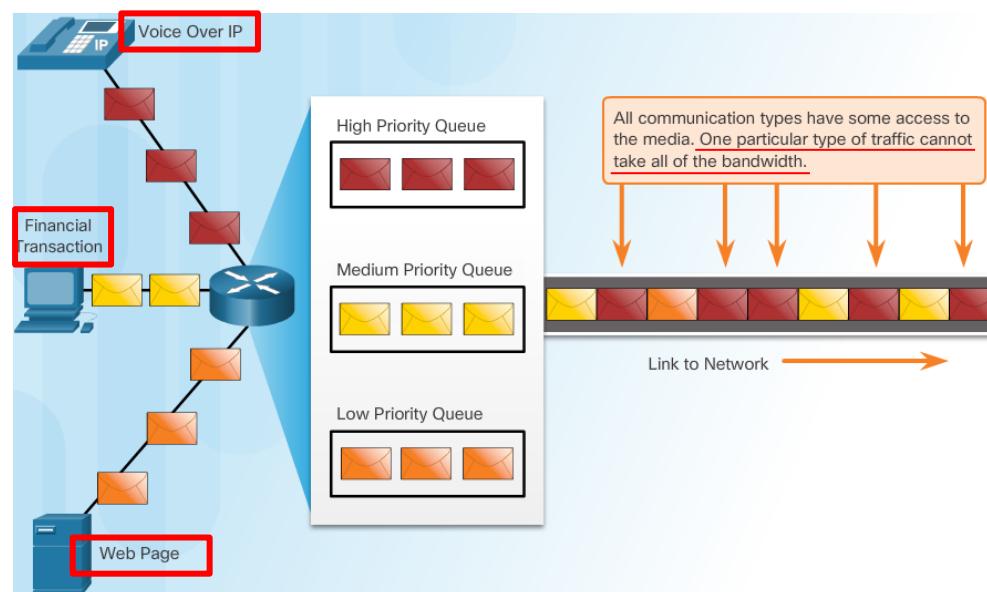


QoS Overview

Network Transmission Quality

■ Prioritizing Traffic

- One **QoS technique** that can help with this problem is to classify data into **multiple queues with different priority levels**.
- Time-sensitive traffic (voice and video) would be classified as high priority and put into the High Priority Queue, for example.
- Packets in the High Priority Queue will get preferential treatment vs. packets in the lower priority queues.



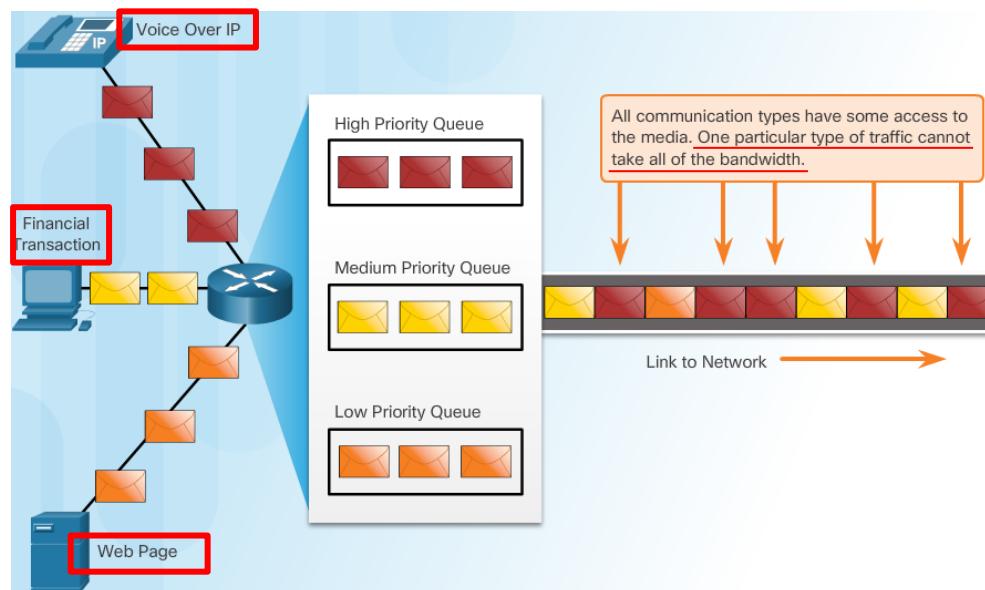


QoS Overview

Network Transmission Quality

■ Prioritizing Traffic

- High Priority Queue: Voice. High priority means more voice (VoIP) packets can be forwarded across the network.
- Medium Priority Queue: Financial Transaction. Also time sensitive. Need greater priority. More packets allowed also.
- Low Priority Queue: Web Page. Remaining bandwidth is used for the static web page.





QoS Overview

Network Transmission Quality

- Bandwidth, Congestion, Delay, and Jitter
 - Network bandwidth is measured in number of bits that can be transmitted in one second (bits per second, bps or b/s).
 - Network congestion causes delay.
 - **Delay** is the time it takes for a packet to travel from the source to the destination.
 - **Jitter** is the **variation** in the delay of received packets.
- Packet Loss
 - When congestion occurs, network devices such as routers and switches can drop packets.
 - Packet loss is a very common cause of voice quality problems on an IP network.
 - In a properly designed network, packet loss should be near zero.
 - Network engineers use QoS mechanisms to classify voice packets for zero packet loss.



QoS Overview

Traffic Characteristics

■ Network Traffic Trends

- The type of demands voice, video, and data traffic place on the network are very different.

■ Voice

- Voice is very sensitive to delays and dropped packets; there **is no reason to re-transmit voice** if packets are lost.
- Voice packets must receive a higher priority than other types of traffic.
- Voice can **tolerate a certain amount of latency**, jitter, and loss without any noticeable effects.

Voice

- Smooth
- Benign
- Drop sensitive
- Delay sensitive
- UDP priority





QoS Overview

Traffic Characteristics

■ Video

- Compared to voice, video is **less resilient to loss** and has a higher volume of data per packet.
- Video can tolerate a certain amount of latency, jitter, and loss without any noticeable affects.

■ Data

- Data applications that have **no tolerance for data loss**, such as email and web pages, use **TCP** to ensure that, if packets are lost in transit, they will be **resent**.
- Data traffic is relatively insensitive to drops and delays compared to voice and video.

Video

- Bursty
- Greedy
- Drop sensitive
- Delay sensitive
- UDP priority



Data

- Smooth/bursty
- Benign/greedy
- Drop insensitive
- Delay insensitive
- TCP retransmits





QoS Overview Queueing Algorithms

■ First In First Out (FIFO)

- FIFO has no concept of priority or classes of traffic and consequently, makes no decision about packet priority.
- FIFO, which is the fastest method of queuing, is effective for large links that have little delay and minimal congestion.



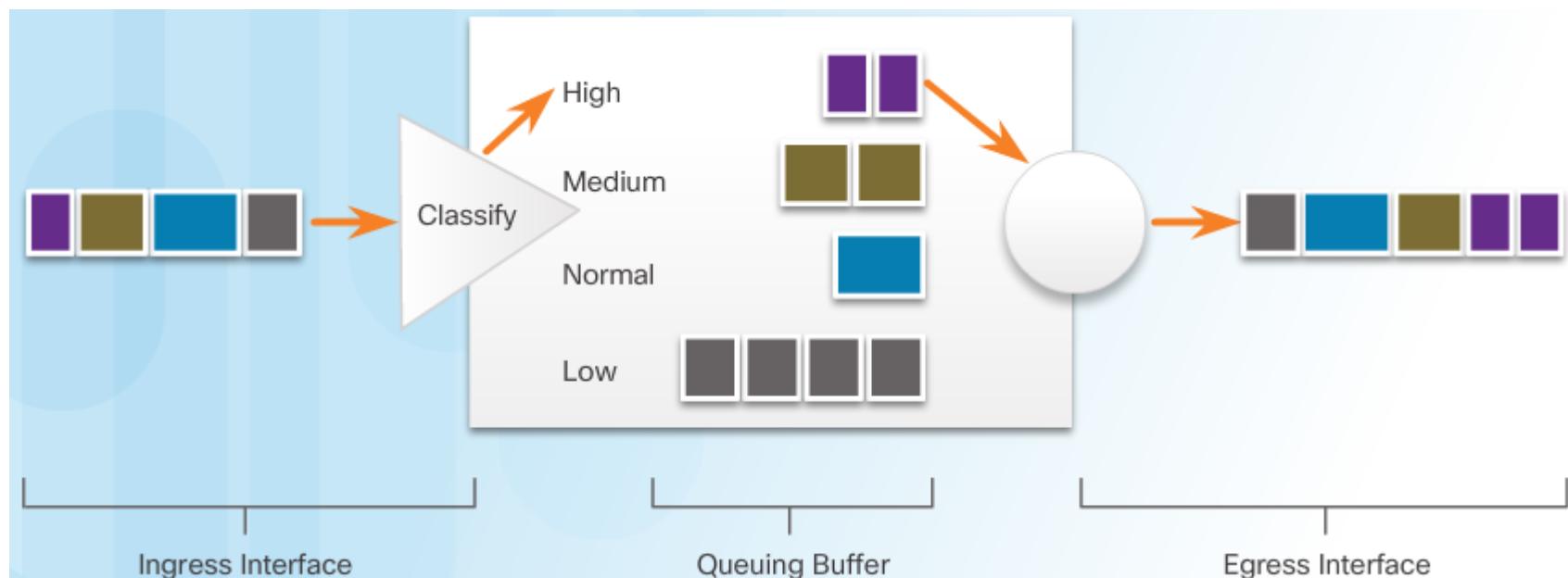


QoS Overview

Queueing Algorithms

■ Weighted Fair Queuing (WFQ)

- An automated scheduling method that provides fair bandwidth allocation to all network traffic.
- Applies priority, or weights, to identified traffic and classifies it into conversations or flows.
- WFQ is not supported with tunneling and encryption because these features modify the packet content information required

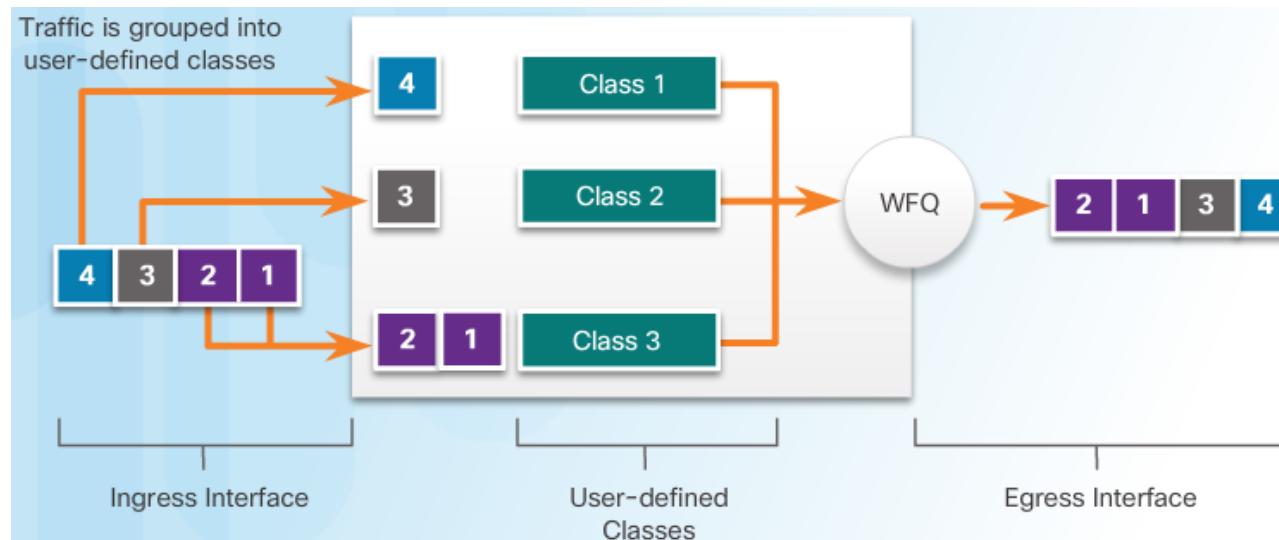




QoS Overview

Queueing Algorithms

- Class-Based Weighted Fair Queuing (CBWFQ)
 - Extends the standard WFQ functionality to provide support for user-defined traffic classes.
 - To characterize a class, you assign it bandwidth, weight, and maximum packet limit.
 - You also specify the queue limit for that class, which is the maximum number of packets allowed to accumulate in the queue for the class.
 - Packets belonging to a class are subject to the bandwidth and queue limits that characterize the class.



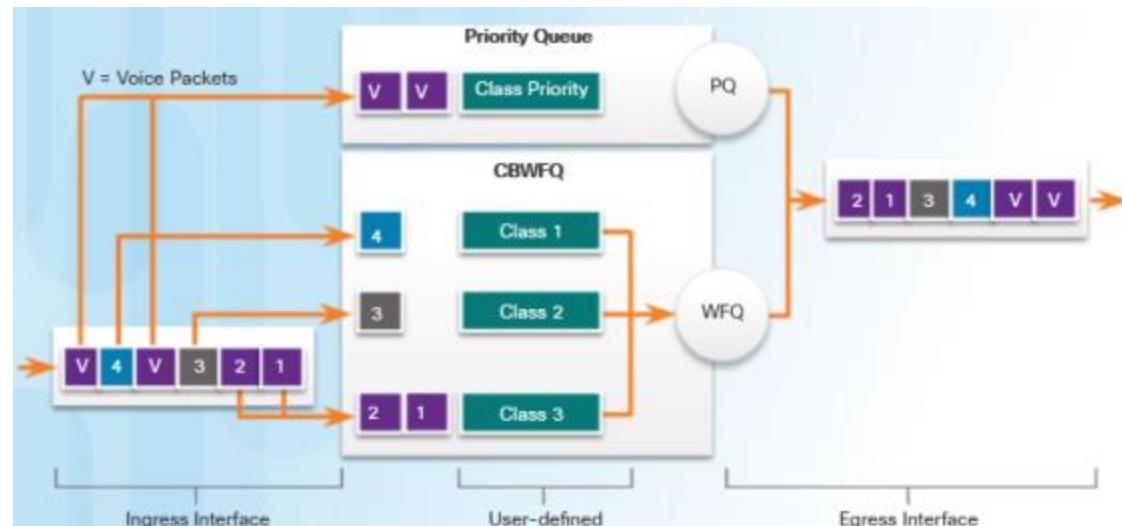


QoS Overview

Queueing Algorithms

■ Low Latency Queueing (LLQ)

- LLQ provides strict priority queuing for CBWFQ, reducing jitter in voice conversations.
- The bandwidth assigned to the packets of a class determines the order in which packets are sent.
- Without LLQ, all packets are serviced fairly based on weight; no class of packets may be granted strict priority.
- LLQ allows delay-sensitive data such as voice to be sent first.



6.2 QoS Mechanisms





QoS Mechanisms

QoS Models

- Selecting an Appropriate QoS Policy Model

Model	Description
Best-effort model	<ul style="list-style-type: none">• Not really an implementation as QoS is not explicitly configured.• Use when QoS is not required.
Integrated services (IntServ)	<ul style="list-style-type: none">• Provides very high QoS to IP packets with guaranteed delivery.• It defines a signaling process for applications to signal to the network that they require special QoS for a period and that bandwidth should be reserved.• However, IntServ can severely limit the scalability of a network.
Differentiated services (DiffServ)	<ul style="list-style-type: none">• Provides high scalability and flexibility in implementing QoS.• Network devices recognize traffic classes and provide different levels of QoS to different traffic classes.

- How can QoS be implemented in a network?
- Implemented using one of the following
 - **IntServ:** High guarantee of QoS, resource intensive, scalability issues
 - **DiffServ:** Less resource intensive, scales well
- Often co-deployed for network QoS



QoS Mechanisms

QoS Models

- Best-Effort

Benefits	Drawbacks
The model is the most scalable.	There are no guarantees of delivery.
Scalability is only limited by bandwidth limits, in which case all traffic is equally affected.	Packets will arrive whenever they can and in any order possible, if they arrive at all.
No special QoS mechanisms are required.	No packets have preferential treatment.
It is the easiest and quickest model to deploy.	Critical data is treated the same as casual email is treated.

- Basic design of the internet and still predominant
- Remains appropriate for most purpose
- All traffic treated in the same way

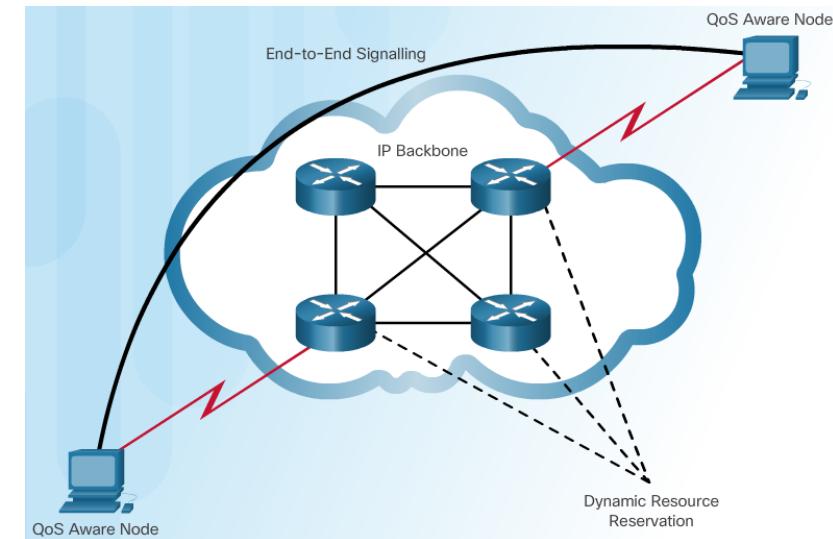


QoS Mechanisms

QoS Models

■ Integrated Services (IntServ)

- Uses **resource reservation** and **admission-control** mechanisms as building blocks to establish and maintain QoS.
- The edge router performs admission control to **ensure that available resources are sufficient** in the network.
- The IntServ standard assumes that routers along a path set and maintain the state for each individual communication.
- If network devices along the path can reserve the necessary bandwidth, the originating application can begin transmitting.
- If the requested reservation fails along the path, the originating application does not send any data.



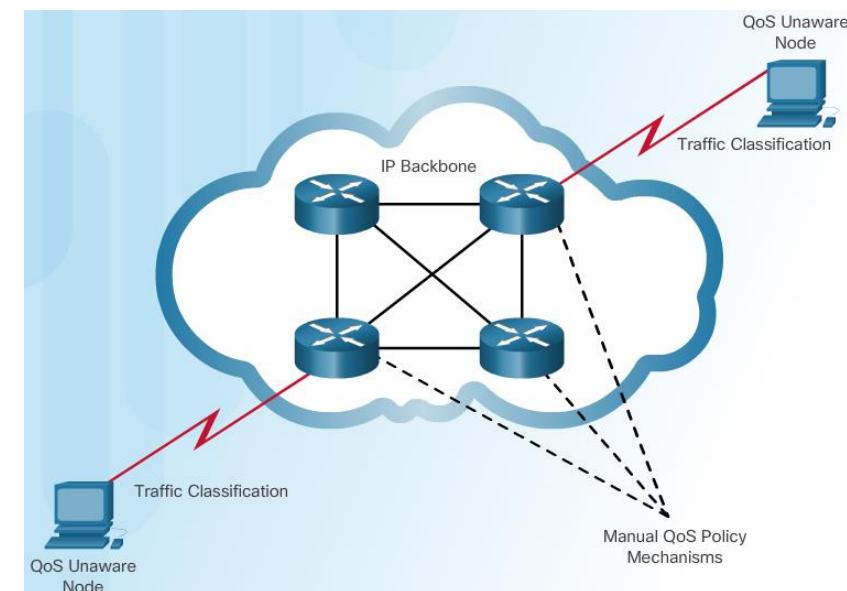


QoS Mechanisms

QoS Models

Differentiated Services (DiffServ)

- Specifies a simple and scalable mechanism for classifying and managing network traffic and providing QoS guarantees on modern IP networks.
- DiffServ can provide an “almost guaranteed” QoS while still being cost-effective and scalable.
- DiffServ uses a “soft QoS” approach. It works on the provisioned-QoS model, where network elements are set up to **service multiple classes** of traffic each with varying QoS requirements.
- DiffServ divides network traffic into **classes** based on business requirements.
- Each of the classes can then be assigned a **different level of service**.





QoS Mechanisms

QoS Implementation Techniques

- Avoiding Packet Loss
 - Dropped TCP segments cause TCP sessions to reduce their window sizes.
 - Some applications do not use TCP and cannot handle drops.
- The following solutions can prevent drops in sensitive apps:
 - Increase link capacity
 - Guarantee bandwidth (BW) and increase buffer space
 - Drop lower priority packets before congestion takes place



QoS Mechanisms

QoS Implementation Techniques

- QoS Tools

- Classification and marking tools
- Congestion avoidance tools
- Congestion management tools

QoS Tools	Description
Classification and marking tools	<ul style="list-style-type: none">• Sessions, or flows, are analyzed to determine what traffic class they belong to.• Once determined, the packets are marked.
Congestion avoidance tools	<ul style="list-style-type: none">• Traffic classes are allotted portions of network resources as defined by the QoS policy.• The QoS policy also identifies how some traffic may be selectively dropped, delayed, or re-marked to avoid congestion.• The primary congestion avoidance tool is WRED and is used to regulate TCP data traffic in a bandwidth-efficient manner before tail drops caused by queue overflows occur.
Congestion management tools	<ul style="list-style-type: none">• When traffic exceeds available network resources, traffic is queued to await availability of resources.• Common Cisco IOS-based congestion management tools include CBWFQ and LLQ algorithms.

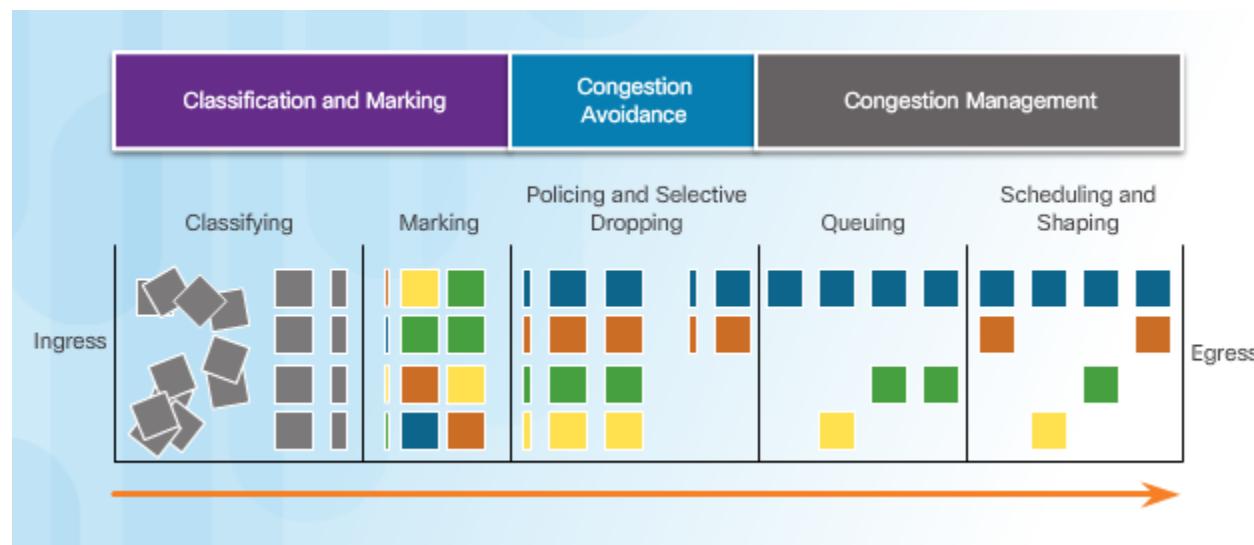
Source B. Keegan



QoS Mechanisms

QoS Implementation Techniques

- QoS Tools
 - Classification and marking tools
 - Congestion avoidance tools
 - Congestion management tools





QoS Mechanisms

QoS Implementation Techniques

Classification and Marking

- Before a packet can have a QoS policy applied to it, the packet has to be classified.
- Methods of classifying traffic flows at Layer 2 and 3 include using interfaces, ACLs, and class maps.

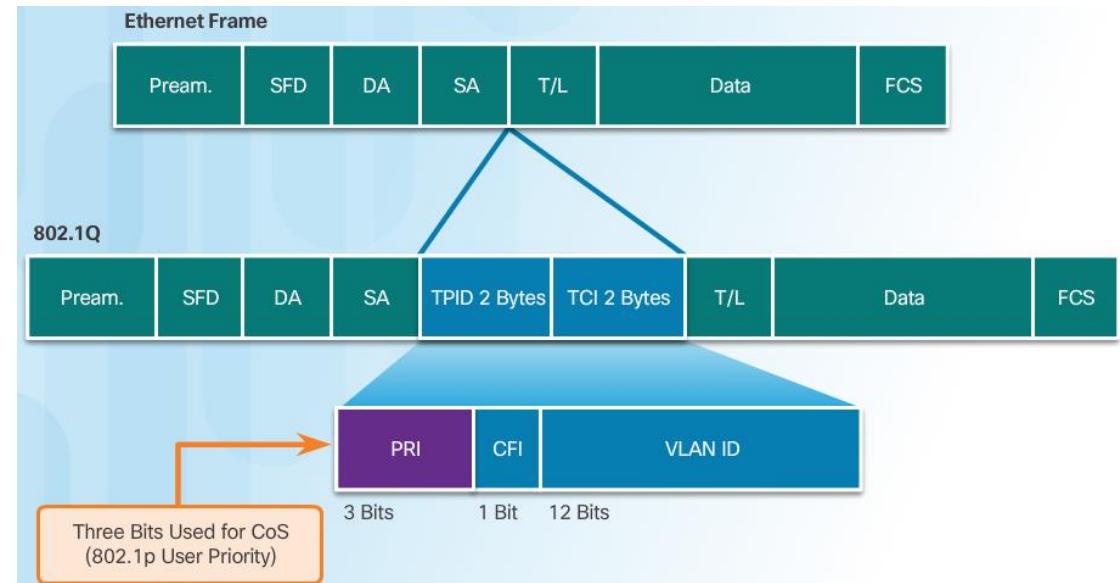
QoS Tools	Layer	Marking Field	Width in Bits
Ethernet (802.1Q, 802.1p)	2	Class of Service (CoS)	3
802.11 (Wi-Fi)	2	Wi-Fi Traffic Identifier (TID)	3
MPLS	2	Experimental (EXP)	3
IPv4 and IPv6	3	IP Precedence (IPP)	3
IPv4 and IPv6	3	Differentiated Services Code Point (DSCP)	6



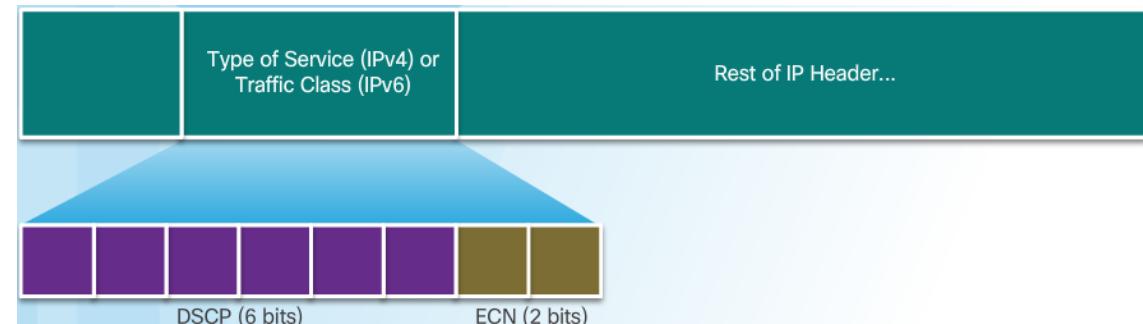
QoS Mechanisms

QoS Implementation Techniques

- **Marking at Layer 2**
 - 2 fields added
 - 3 bits used for CoS
 - How many levels?



- **Marking at Layer 3**
 - 8 bits available, 6 used
 - How many levels?

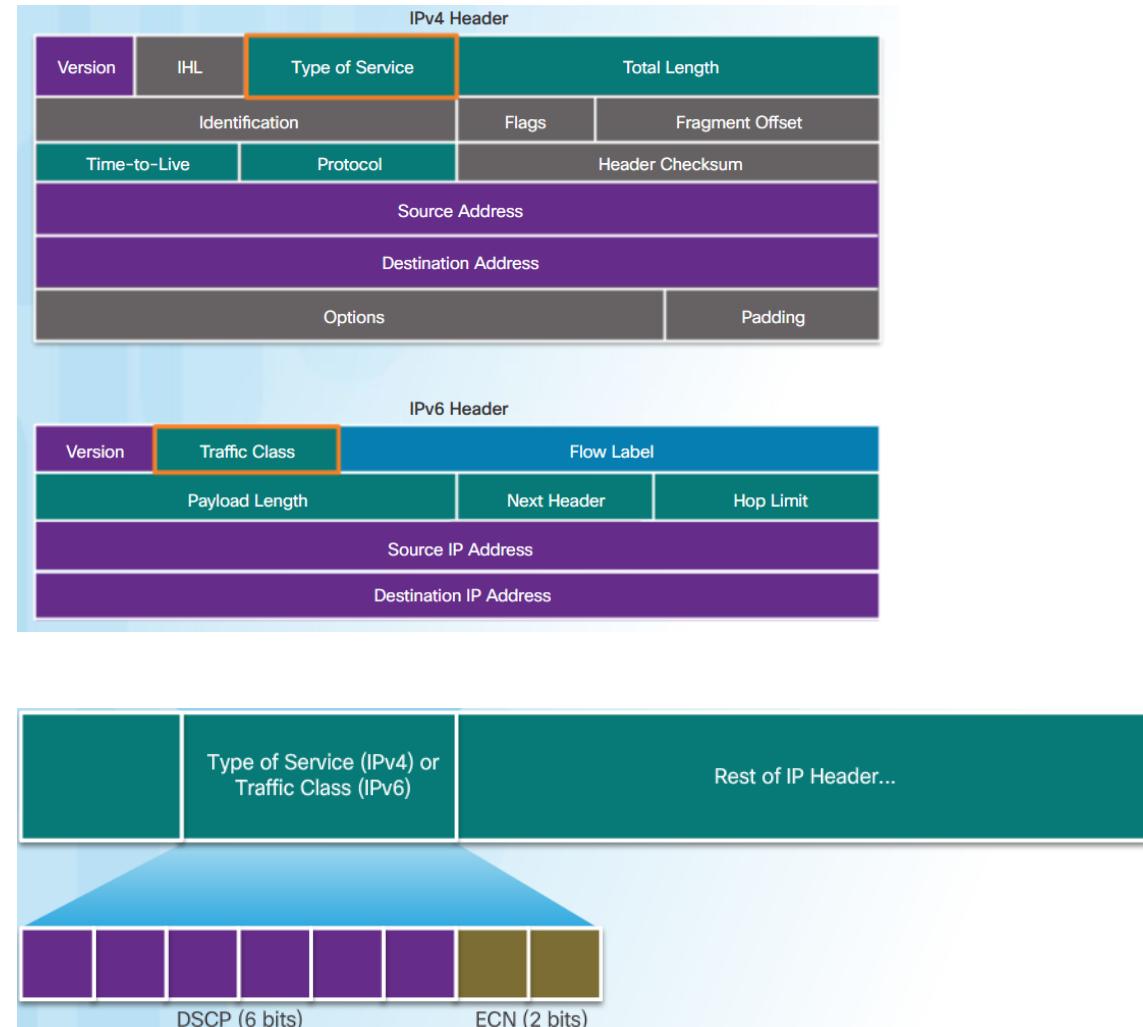




QoS Mechanisms

QoS Implementation Techniques

- **Marking at Layer 3**
 - IPv4 and IPv6 specify an 8-bit field in their packet headers to mark packets.
 - IPv4 – Type of Service field.
 - IPv6 – Traffic Class Field

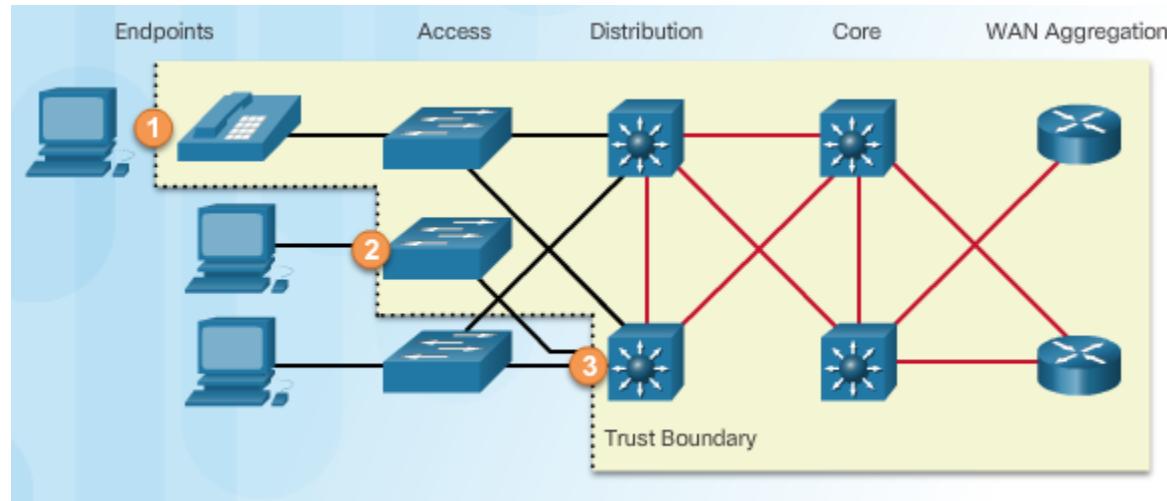




QoS Mechanisms

QoS Implementation Techniques

- Trust Boundaries
 - Traffic should be classified and marked as close to its source as technically and administratively feasible.



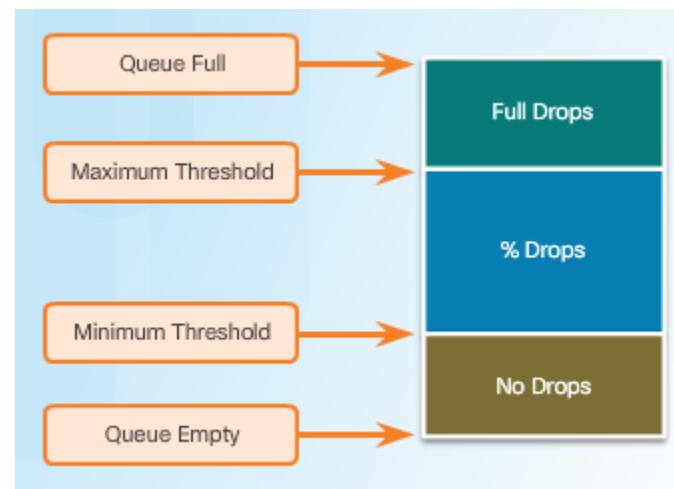


QoS Mechanisms

QoS Implementation Techniques

- **Congestion Avoidance**

- When the queue is below the minimum threshold, there are no drops.
- As the queue fills up to the maximum threshold, a small percentage of packets are dropped.
- When the maximum threshold is passed, all packets are dropped.



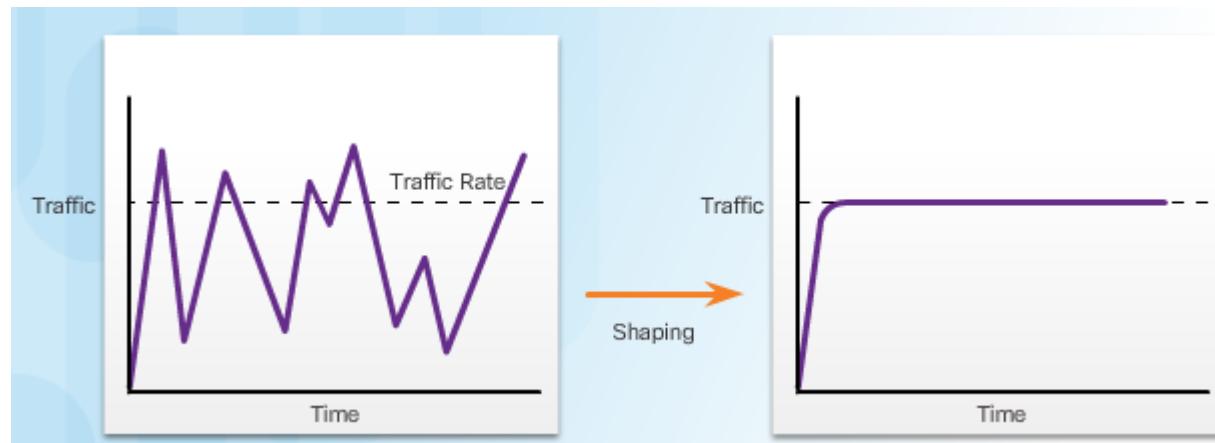


QoS Mechanisms

QoS Implementation Techniques

- Traffic Shaping

- Traffic **shaping** retains excess packets in a queue and then schedules the excess for **later transmission** over increments of time.
- Traffic shaping results in a smoothed packet output rate
- Shaping is applied to outbound traffic. Packets going out an interface get queued and can be shaped.





QoS Mechanisms

QoS Implementation Techniques

- Traffic Policing

- **Policing** is applied to inbound traffic on an interface.
- When the traffic rate reaches the configured maximum rate, excess traffic is either dropped or re-marked.



6.3 Chapter Summary





Chapter Summary

Summary

- The quality of network transmission is impacted by the **bandwidth** of the links between the source and destination, the sources of **delay** as packets are routed to the destination, and **jitter** or the variation in delay of the received packets. Without QoS mechanisms in place, packets are processed in the order in which they are received. When congestion occurs, time-sensitive packets will be dropped with the same frequency as packets that are not time-sensitive.
- **Voice packets** require latency of no more than 150 milliseconds (ms). Jitter should be no more than 30 ms, and voice packet loss should be no more than 1%. Voice traffic requires at least 30 Kb/s of bandwidth.
- **Video packets** require latency no more than 400 milliseconds (ms). Jitter should be no more than 50 ms, and video packet loss should be no more than 1%. Video traffic requires at least 384 Kb/s of bandwidth.
- For **data packets**, two factors impact the Quality of Experience (QoE) for end users:
 - Does the data come from an interactive application?
 - Is the data mission critical?



Chapter Summary

Summary Continued

- The **four queuing algorithms** discussed in this chapter are as follows:
 - **First in First Out (FIFO)** - Packets are forwarded in the order in which they are received.
 - **Weighted Fair Queuing (WFQ)** - Packets are classified into different flows based on header information including the ToS value
 - **Class-Based Weighted Fair Queuing (CBWFQ)** - Packets are assigned to user-defined classes based on matches to criteria such as protocols, ACLs, and input interfaces. The network administrator can assign bandwidth, weight, and maximum packet limit to each class.
 - **Low Latency Queuing (LLQ)** - Delay-sensitive data such as voice is added to a priority queue so that it can be sent first (before packets in other queues).
- The **three queuing models** discussed in the chapter are as follows:
 - **Best-Effort** - This is the default queuing model for interfaces. All packets are treated in the same way. There is no QoS.
 - **Integrated Services (IntServ)** - IntServ provides a way to deliver the end-to-end QoS that real-time applications require by explicitly managing network resources to provide QoS to specific user packet streams, sometimes called microflows.
 - **Differentiated Services (DiffServ)** - DiffServ uses a soft QoS approach that depends on network devices that are set up to service multiple classes of traffic each with varying QoS requirements. Although there is no QoS guarantee, the DiffServ model is more cost-effective and scalable than IntServ.



Chapter Summary

Summary Continued

- QoS tools include the following:
 - **Classification and Marking** - Classification determines the class of traffic to which packets or frames belong. Marking means that we are adding a value to the packet header. Devices receiving the packet look at this field to see if it matches a defined policy.
 - **Congestion Avoidance** - Congestion avoidance tools monitor network traffic loads in an effort to anticipate and avoid congestion. As queues fill up to the maximum threshold, a small percentage of packets are dropped. Once the maximum threshold is passed, all packets are dropped.
 - **Shaping and Policing** - Shaping retains excess packets in a queue and then schedules the excess for later transmission over increments of time. Shaping is used on outbound traffic. Policing either drops or remarks excess traffic. Policing is often applied to inbound traffic.



Reminder

Lab on Friday

- Networking 4 CA1 Quiz – this Friday 30/10/2020 during the Lab Time 2pm to 4pm.
- Quiz covers Chapter 1 to 4. Quiz is an online quiz using NetAcad
- Do the online Chapter Quizzes and Exams to review Chapters 1 to 4 material.
- **Can you make sure before this Friday that you can login to your NetAcad Account.**
- **You also need to be logged in to Bongo Virtual Classroom for the duration of the Quiz.**





Border Gateway Protocol (BGP)

- BGP4 de facto **inter**-AS routing protocol in Internet
- Determines optimal paths for source-destination pairs spanning multiple Autonomous Systems (AS)
- BGP allows each AS to
 1. Get subnet reachability info from neighbouring AS.
 2. Propagate reachability info to all routers internal to the AS.
 3. Determine ‘good’ routes to subnets based on reachability info and AS **policy**.
- BGP4 allows each subnet to advertise its existence to rest of the Internet
- BGP ensures that all the AS in the Internet know about the subnet and how to get there.
- BGP is the routing protocol that make the internet ‘work’.

Border Gateway Protocol (BGP)

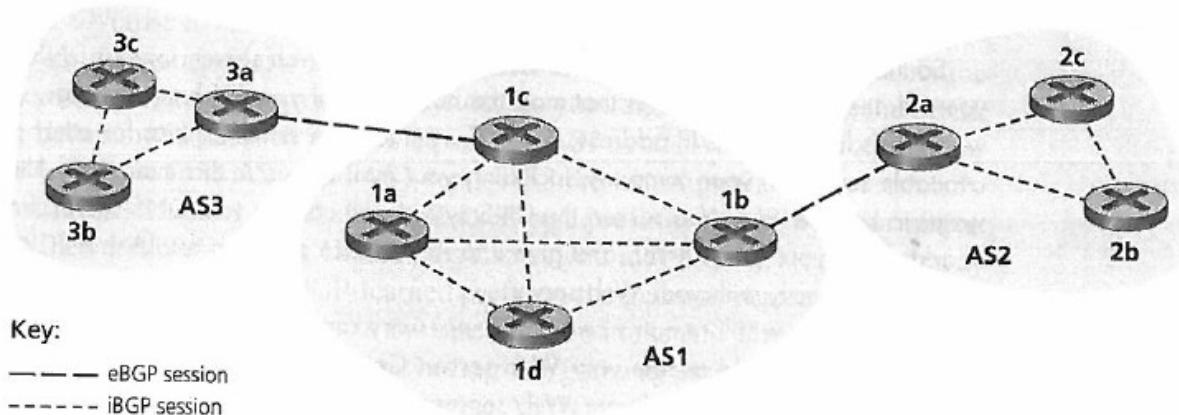
- Pairs of routers (**Gateway routers**) exchange routing info over semi-permanent TCP connections on port 179
- One BGP TCP connection for each link directly connecting two routers in two different AS
- Two routers at end of a connection are called **BGP peers**
- The TCP connection plus BGP messages sent over the connection is called a BGP session
- An **external BGP (eBGP) session** spans two AS
- An **internal BGP (iBGP) session** is between routers in same AS

Border Gateway Protocol (BGP)

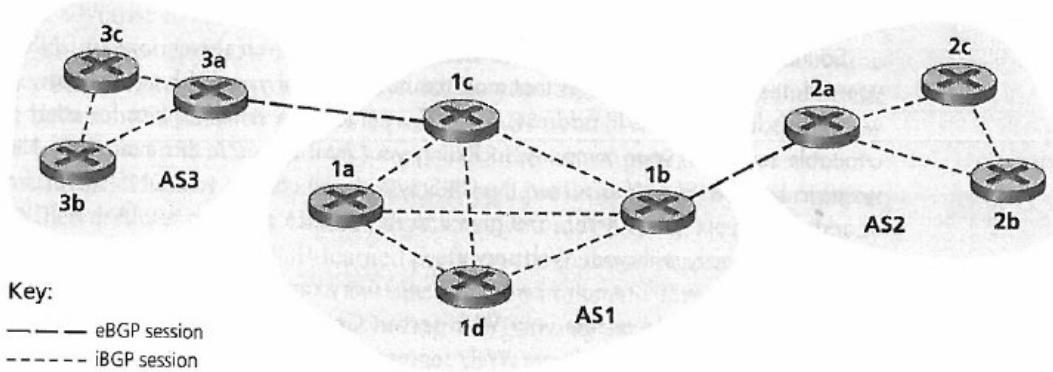
- BGP allows each AS to learn which destinations are reachable via neighbouring AS
- In BGP destinations are not hosts. They are CIDRized **prefixes**
- Each prefix represents a subnet or collection of subnets
- AS2 has 3 subnets
 138.16.64.0/24 138.16.65.0/24 138.16.66.0/24
- BGP could aggregate the prefixes and advertise the single prefix 138.16.64.0/22 to AS1
- See Route-summarization-example.txt file provided in BrightSpace

Border Gateway Protocol (BGP)

- How BGP distributes prefix reachability information over BGP sessions Fig. 4.40 p.417 K&R...per below
- Each AS exchanges prefix reachability information via their gateway routers.
- Gateway router send list of prefixes reachable via its AS to peer gateway routers in other AS
 - Using eBGP session between gateway routers 3a and 1c, AS3 sends AS1 the list of prefixes reachable from AS3



Border Gateway Protocol (BGP)



- When Gateway router receives eBGP learned prefixes it sends the prefixes via its iBGP session to the internal routers in the AS
 - So all routers in the AS learn about another AS prefixes.
 - And the other gateway routers in the AS learn about another AS prefixes
 - So the other gateway routers in the AS can re-advertise another AS prefixes
- When a Router (gateway or not) learns about a new prefix it creates an entry for the prefix in its routing table.

B

209.140.1.0/24 [20/0] via 209.20.1.5, 00:00:00

Border Gateway Protocol (BGP)

- Path Attributes and BGP routes...see below
- In BGP an AS is identified by its **autonomous system number (ASN)** HEANet = **AS1213** See the links on the end slide
- BGP peers advertise routes to each other
- Route = Prefix + BGP attributes
- BGP attributes = AS-PATH and NEXT-HOP
- PT example...

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 0.0.0.0	209.165.201.1	0		0	65001 i
*> 198.133.219.0/24	0.0.0.0	0		32768	i

- Real route server example from AI & I

```
147.252.0.0/16      *[BGP/170] 4w2d 12:06:52, localpref 100, from 12.122.159.217  
                      AS path: 7018 3356 1213 I, validation-state: unknown
```

Border Gateway Protocol (BGP)

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 0.0.0.0	209.165.201.1	0		0	65001 i
*> 198.133.219.0/24	0.0.0.0	0		32768	i

```
147.252.0.0/16      *[BGP/170] 4w2d 12:06:52, localpref 100, from 12.122.159.217
                     AS path: 7018 3356 1213 1213 I, validation-state: unknown
```

- Route = Prefix + BGP attributes
- BGP attributes = AS-PATH and NEXT-HOP
- AS-PATH attribute
 - Contains the AS the advertisement for the prefix passed through
 - When prefix passes into AS. AS adds its ASN to the PATH attribute
- NEXT-HOP attribute
 - NEXT-HOP is the router interface that begins the AS-PATH
 - Provides the important link between inter-AS and intra-AS routing protocols

Border Gateway Protocol (BGP)

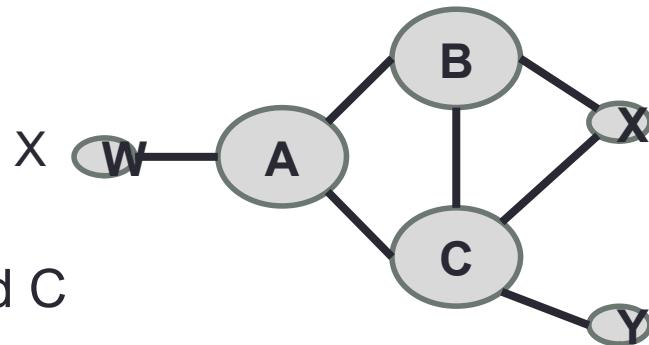
- Other BGP attributes...
 - Route Preference metric attribute
 - How prefix was inserted into BGP at the origin attribute
- Import policy
 - Used to decide to accept or filter the route or set attributes such as router preference metrics, when gateway router receives a route advertisement
 - Filter?
 - AS may not want to send traffic over an AS in the route's AS-PATH
(Policy decision by AS network admin)
 - Gateway may already know a better route to same prefix

Border Gateway Protocol (BGP)

- **BGP Route selection process**
- BGP uses eBGP and iBGP to distribute routes to all routers within an AS
- So a router may learn about more than one route to any prefix, so router must select a route
- Input to route selection process is set of all routes learned and accepted by the router
- If there are two or more routes to same prefix, BGP invokes elimination rules sequentially until one route remains

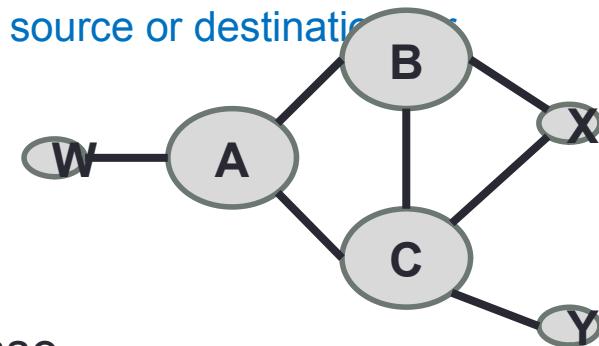
Border Gateway Protocol (BGP)

- **Routing Policy Concepts**
- Selective route advertising policy to implement customer/provider relationships
 - AS X = **stub network** =>
 - X must be the destination of all traffic entering X
 - X must be the source of all traffic leaving X
 - X = multi-homed to provider networks B and C
 - X is a customer of networks B and C
 - Technically X could forward traffic between B and C
 - Stop this by controlling how BGP routes are advertised
 - X can advertise it has no paths to other destinations except itself = selective route advertisement policy



Border Gateway Protocol (BGP)

- **Routing Policy Concepts**
- Control transit traffic between service providers
- **Rule of Thumb**
 - Traffic flowing across an ISP's backbone must have either a source or destination (or both) in a network that is a customer of the ISP.
 - A, B, and C = backbone ISP providers.
 - W = a customer of A. X = customer of B
 - B learns from A, a path AW to W
 - B installs the route BAW in its routing information base
 - B advertises path BAW to its customer X. Ok per Rule of Thumb
 - Should B advertise path BAW to provider C?
 - C could route traffic via path CBAW to A. Not Ok. Traffic is not from source or destination that is a customer of B. **Free transit traffic = cost to B.**
 - B can decide not to advertise path BAW to provider C = selective route advertisement policy



Border Gateway Protocol (BGP)

- Interesting Links
- [Hurricane Electric BGP Toolkit](#)
 - Click on ‘Your ISP is Asxxxx’. Then Click on the ‘Graph v4’ Tab.
- [ASN Lookup](#)
 - Type in an AS Number to get info on an Autonomous System
- Route servers
 - View BGP routes on the Internet
 - Public route servers accessible via telnet (...Use PuTTy)
 - Hurricane Electric US route-server.he.net
 - AT&T USA route-server.ip.att.net
 - Global Crossing UK. route-server.eu.gblx.net
 - [List of other route servers](#)

Reference

James Kurose and Keith W. Ross (2013)
Computer Networking: A Top-Down Approach, 6th Edition

Reminder

Lab on Friday

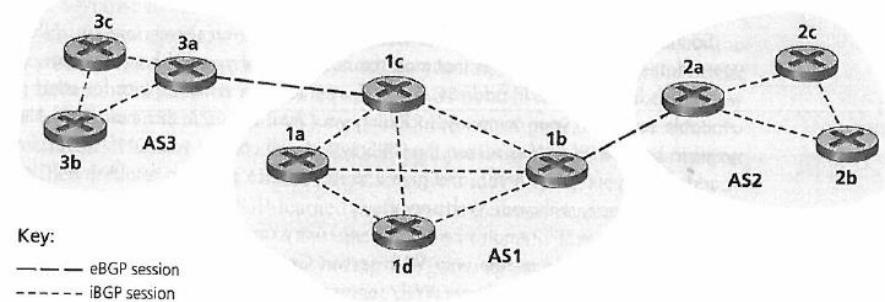
- The lab work from now on will be ‘gearing up’ towards the **Skills Based Assessment (SBA)** towards the end of the month, (Friday 27/11/20).
- It is important that you complete all the Labs including the remaining labs to iron out anything that may be unclear about the material to date.

Hierarchical Routing

- Autonomous Systems (AS)
- Interior Gateway Protocols (IGP) ...interior to what?
- Exterior Gateway Protocols (EGP) ...exterior to what?
- Difference between IGPs and EGPs

Hierarchical Routing

- A simplistic view of routing would be...
 - A network = a collection of interconnected routers
 - All routers run the same routing algorithm
 - Each router knows about all routes
- Simplistic view... Why? ... Two Problems...
 1. Scale
 - As the number of routers increase => greater overheads
 - Computing, storing, & communicating routing info gets prohibitive
 - Bigger routing Tables => more storage memory, more CPU scan time, more bandwidth needed for updates
 - Not possible for every router to have an entry for every other router
 2. Administrative Autonomy
 - Organisations want to run a network their way and still connect to outside networks
- Solution... AS
 - Organise routers into **Autonomous Systems (AS)**
 - Routing can then be done hierarchically

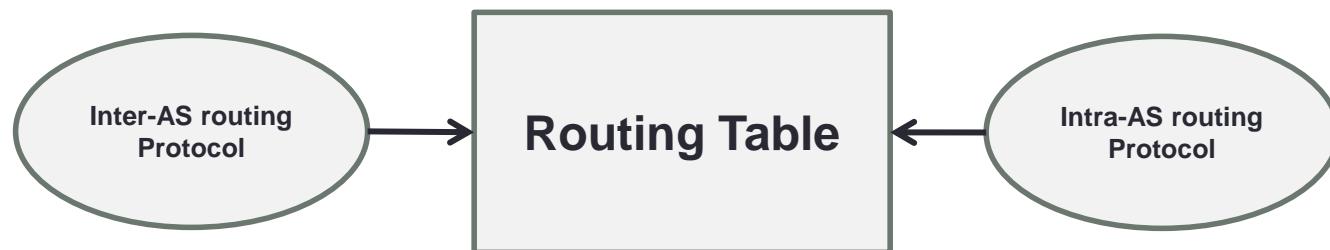


Hierarchical Routing 2

- Autonomous System (AS)
 - AS = group of routers under same administrative control
 - e.g. an ISP or a very large enterprise
 - All routers **within** an AS run same routing algorithm
 - **Intra**-AS routing Protocol *(intra = within)*
 - Determines optimal routing paths for source-destination pairs **within** the AS
- Connecting to other Autonomous System (AS)
 - **Inter**-AS routing protocol is used *(inter = between)*
 - Does two tasks
 1. Gets reachability info from neighbouring AS
 2. Propagates the reachability info to all internal routers in the AS
 - All AS in Internet run same Inter-AS routing protocol (BGP4)
 - **Gateway Routers** forward packets to destinations outside the AS

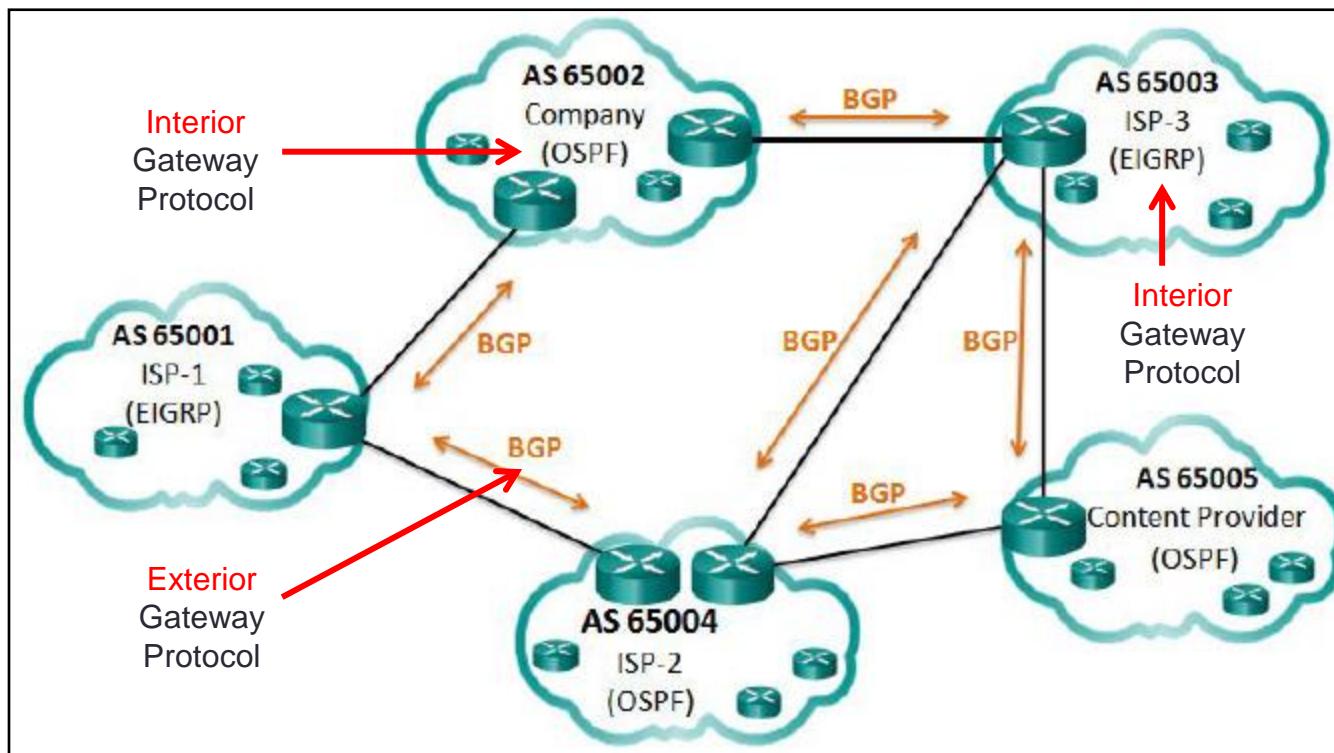
Hierarchical Routing 3

- A very important point
 - Each router within an AS gets routing information from an intra-AS routing protocol **and** an inter-AS routing protocol
 - Intra-AS routing protocol: OSPF, EIGRP (... also called known as **IGPs**)
 - Inter-AS routing protocol: BGP (... also called an **EGP**)
 - Each router uses the information from both intra-AS and inter-AS protocols to configure its routing table.



Hierarchical Routing 4

- IGP (Interior Gateway Protocol) vs. EGP (Exterior Gateway Protocol)



Hierarchical Routing 5

- IGP (Interior Gateway Protocol)
 - Examples: RIP, EIGRP and OSPF.
 - IGPs exchange routing information **within** a company network or an autonomous system (AS).
 - IGPs use a **specific metric**, such as OSPF's cost, to determine the best paths to destination networks.
 - IGPs are used to route traffic within the same organization and administered by a single organization.
 -

Hierarchical Routing 6

- EGP (Exterior Gateway Protocol)
 - Example: Border Gateway Protocol (BGP).
 - BGP is used to exchange routing information **between** autonomous systems.
 - Every AS is assigned a unique 16-bit or 32-bit AS number that uniquely identifies AS on the Internet.
 - BGP **does not use a single metric** like IGPs. BGP routers exchange several path attributes including a list of AS numbers (hop by hop) required to reach a destination network.

Hierarchical Routing 7

- EGP (Exterior Gateway Protocol) e.g BGP ...continued
 - BGP updates are encapsulated over TCP on port 179. BGP inherits the connection-oriented properties of TCP, this ensures that BGP updates are transmitted reliably.
 - BGP is used to route between networks administered by two different organizations.
 - BGP is used by an AS to advertise its networks to the rest of the Internet (and in some cases, networks that it learned about from other AS).

Hierarchical Routing 8

- Summary
 - Defining Autonomous Systems....
 - Allows for hierarchical routing
 - Solves the problems of scale and administrative authority
 - Scale solution
 - All routers within an AS run same intra-AS routing protocol.
 - So an intra-AS router needs only know about routes within its own AS
 - Does not need to know about topological structure of other AS
 - Does not need to store info about other AS topologies
 - Administrative authority solution
 - An organization can run whatever intra-AS protocol it likes
 - An organization can decide its own selective route advertising policy to implement customer/provider relationships
 - .

Reference

James Kurose and Keith W. Ross (2013)

Computer Networking: A Top-Down Approach, 6th Edition



Chapter 7: Network Evolution



Connecting Networks

Cisco | Networking Academy®
Mind Wide Open™



Chapter 7 – Videos in the On-Line Course

- **7.1 Internet of Things**
 - 7.1.1.3 Challenges to Connecting Things (Video) (1:14)
 - 7.1.2.1 The Network Connectivity Pillar (Video) (2:34)
 - 7.1.2.4 Data Analytics Pillar (Video) (3:35)
 - 7.1.2.6 Application Enablement Platform Pillar (Video) (5:38)
- **You need to watch the below videos. Good Summary of All**
- 7.2 Cloud and Virtualization
 - **7.2.1.1 Video Tutorial - Cloud and Virtualization (5 mins)**
- 7.3 Network Programming
 - **7.3.1.1 Video Tutorial - Network Programming, SDN, and Controllers (5 mins)**



Chapter 7 - Sections & Objectives

- 7.1 Internet of Things
 - Explain the value of the Internet of Things.
- 7.2 Cloud and Virtualization
 - Explain why cloud computing and virtualization are necessary for evolving networks.
- 7.3 Network Programming
 - Explain why **network programmability** is necessary for evolving networks.

7.1 Internet of Things

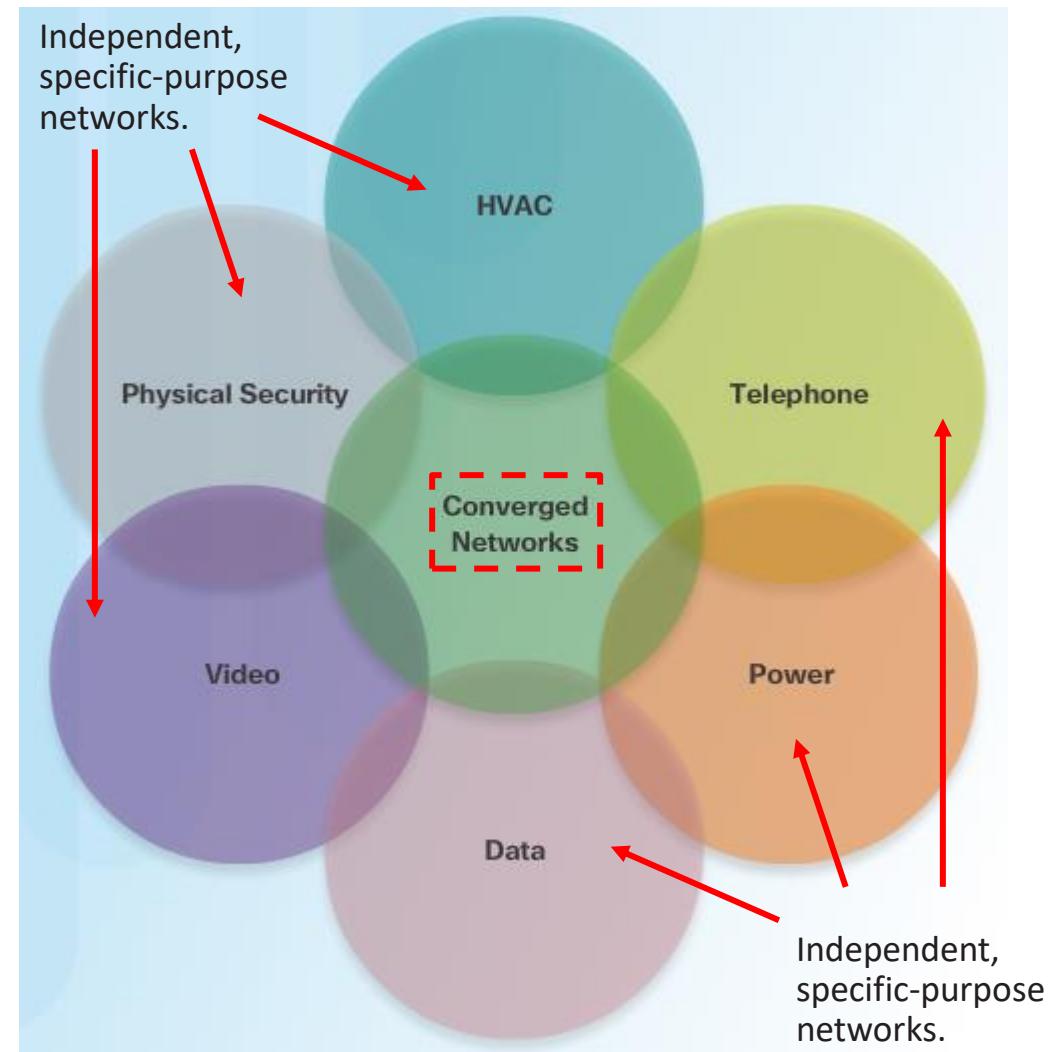




Internet of Things

Internet of Things - Elements

- Cisco estimates that 50 billion **things** will be connected to the Internet by 2020.
- Independent, specific-purpose networks exist in buildings to control heating, ventilation, and air conditioning (HVAC), telephone, security, and lighting.
- Such dissimilar networks are **converging** to share the same network infrastructure
- The converged network uses IoT technologies to increase the power of the network
- The IoT connects smart objects to the Internet





Internet of Things IoT Elements

- The challenge for IoT is to **securely** integrate millions of new things from multiple vendors into existing networks.
- The **Cisco IoT System** provides an infrastructure designed to manage large scale systems of different endpoints and platforms, and the **huge amount of data** that they create.





Internet of Things IoT Pillars - Cisco

- **Network Connectivity** identifies devices that can be used to provide IoT connectivity to many diverse industries and applications.
- **Fog Computing** An IoT network model for a distributed computing infrastructure closer to the network edge. Enables edge devices to run applications locally and make immediate decisions.
- **Security** offers scalable cybersecurity solutions, enabling an organization to quickly and effectively discover, contain, and remediate an attack to minimize damage.
- **Data Analytics** consists of distributed network infrastructure components and IoT-specific, application programming interfaces (APIs).
- **Management and Automation** products can be customized for specific industries to provide enhanced security and control and support.
- **Application and Enablement** provides the infrastructure for application hosting and application mobility between cloud and Fog computing.



Note: Fog Computing

"The fog extends the cloud to be closer to the things that produce and act on IoT data".
See reference below.

http://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf

Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are



Network Evolution - How did we get here?

- Previously **computing**, **storage** and **networking** were intentionally kept separate for **security** reasons
 - Physically separate
 - Management and operational monitoring separate.
- **Computing**, **storage** and **networking** brought together by a demand for inexpensive computing power
- Management and operations brought together



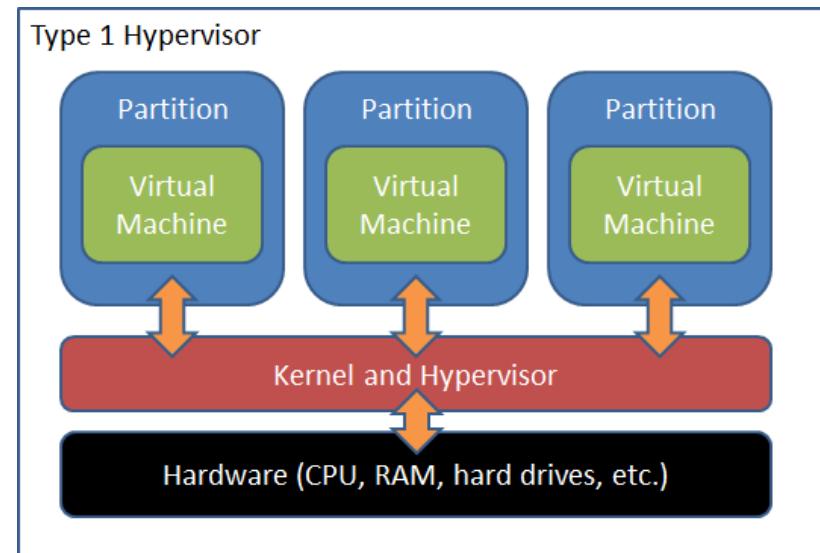
Network Evolution - How did we get here?

- Data centers were originally designed to separate traditional computing elements;
 - Servers
 - Storage
 - Networking connection
- Specific and dedicated functionality based on computing power.
 - Small servers or DBs servicing desktops locally.
- Servers eventually migrated to allow for sharing amongst enterprise users.



Network Evolution - How did we get here?

- Virtualization
 - A **host** operating system could execute multiple **client** operating systems.
 - Software known as a **hypervisor** creates a virtual environment to synthesize a real computing environment.
 - Virtual NIC
 - BIOS
 - Sound adapter
 - Video adapter





Network Evolution - How did we get here?

- Virtualization
 - The client program acted as a large file.
 - The file treated like any other file on a hard disk.
 - Copied, moved and run at another location.
 - The guest OS could be paused without knowing it, entering into a suspended state.
 - The OS could now be viewed as an **ubiquitous computing** and **storage** platform.



Network Evolution - How did we get here?

- Virtualization
 - With **increases in memory, computing power and storage** servers became capable of executing different operating systems simultaneously in a virtual environment.
 - Single-host virtualisation could move to data centre environment .
 - Control and execution of hundreds/thousands of virtual machines from a single console.
 - Single dedicated bare machines not needed
 - Elastic computing - scaling up/down computing resource requirements as needed by the enterprises

7.2 Cloud and Virtualization





Cloud

Cloud Computing

- Cloud computing involves large numbers of computers connected through a network that can be **physically located anywhere**.
- Providers rely heavily on **virtualization** to deliver their Cloud computing services.
- Cloud computing can **reduce operational costs** by using resources more efficiently.
- Organizations can treat computing and storage expenses more as a **utility**.

Treat as a '**utility**' => 'buy' computing just as you would buy electricity or gas.



Cloud

Cloud Computing

- The three main cloud computing services defined by the NIST are:
 - **Software as a Service (SaaS)**: Applications delivered over the web to the end users. Examples?
 - **Platform as a Service (PaaS)**: Development tools and services used to deliver the applications.
 - **Infrastructure as a Service (IaaS)**: Hardware and software for servers, operating systems ,storage, network equipment access, virtual network services.

NIST = National Institute for Standards and Technology, US Dept. of Commerce



Cloud

Cloud Computing

- Cloud service providers now also offer **Information Technology as a Service (ITaaS)** - an extension of the model that provides IT support for each of the three cloud computing services.
- **(ITaaS)** allows business customers to extend the capability of IT without requiring investment in new infrastructure, training new personnel, or licensing new software.
- The services are available on demand and delivered economically to any device anywhere in the world without compromising security or function.



Cloud

Cloud Computing

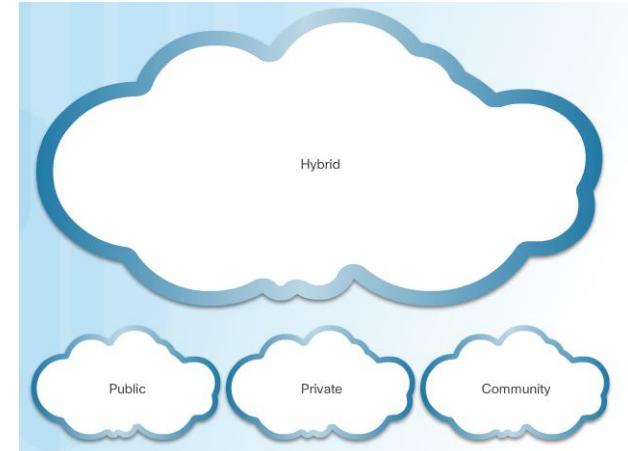
- The four primary **cloud models** are **Public, Private, Hybrid & Community**.

- **Public clouds**

- Made available to the **general population**
 - Uses the Internet to provide services.
 - **Free or pay-per-use model**

- **Private clouds**

- Intended for a **specific organization or entity** e.g. government
 - Organisation can use
 - Own private network, but **expensive** to build and maintain
 - Or managed by an outside organization with strict access **security**.





Cloud

Cloud Computing

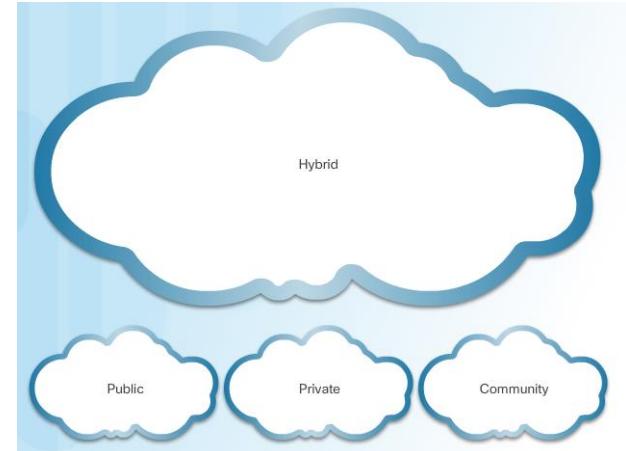
- The four primary **cloud models** are **Public, Private, Hybrid & Community**.

- **Hybrid clouds:**

- A hybrid cloud is made up of **two or more** cloud model (...part public & part custom)
- Connected using a single architecture
- Access to various services is based on user access rights.

- **Community clouds (Custom clouds)**

- A community cloud is created for exclusive use by a **specific community or industry**
- e.g. healthcare organizations – with special authentication and confidentiality requirements.





Cloud

Data Center vs. Cloud Computing

■ Data Centre

- Usually a facility for data storage and processing run by company's own IT department
- Expensive to build and maintain – only large organizations can afford them. (Google, Facebook, etc.)
- May also be a **leased**, off-site facility – smaller organizations
 - Lease server and storage from larger cloud based data center
 - Reduces overall cost of ownership
- Data Centers make cloud computing possible.

■ Cloud Computing

- Usually an off-site service giving on-demand access to a shared pool of computing resources.
- The resources are configurable by company's own IT department.
- The resources can be quickly provisioned and rolled out with less management and configuration effort overall.



Cloud and Virtualization

Cloud and Virtualization

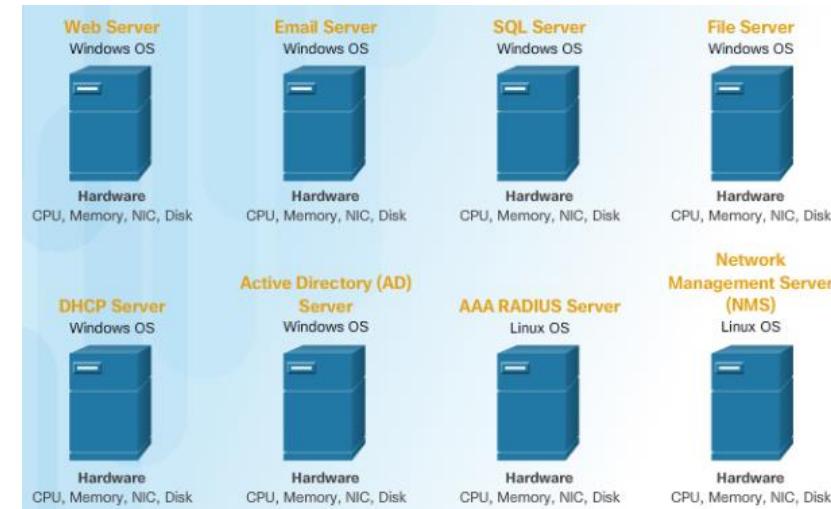
- The terms “**Cloud computing**” and “**virtualization**” have different meanings.
- **Cloud computing separates the application from the hardware.**
- **Virtualization separates the OS from the hardware.**
 - **Virtualization** is the foundation of Cloud computing. Cloud not really possible without it.
- Cloud providers allow customers to dynamically provision just the resources they need at a given time.
- This allows customer to scale their computing requirements up or down according to business demand.
- Amazon’s Elastic Compute 2 (EC2) service allows customers to create virtualized instances of servers on demand as needed.



Cloud and Virtualization

Virtualization

- Previously enterprise servers consisted of a server operating system (OS), such as Windows Server or Linux Server, **installed on specific hardware**.
- **All** of a server's RAM, processing power, and hard drive space were **dedicated to the service provided** (e.g., Web, email, etc.)
- **Single point of failure**
 - Component fails, server fails, service not available
- **Underuse**
 - Servers sat idle for long intervals
- **Energy & space waste**
 - More space than service - server sprawl

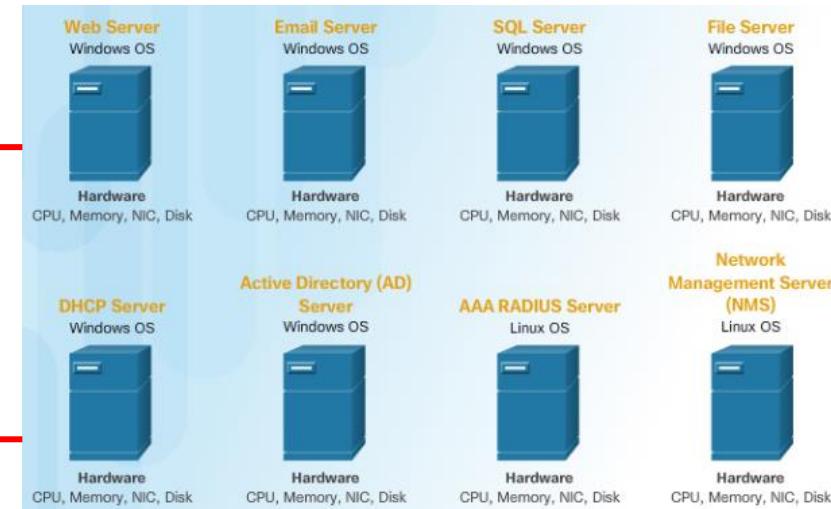
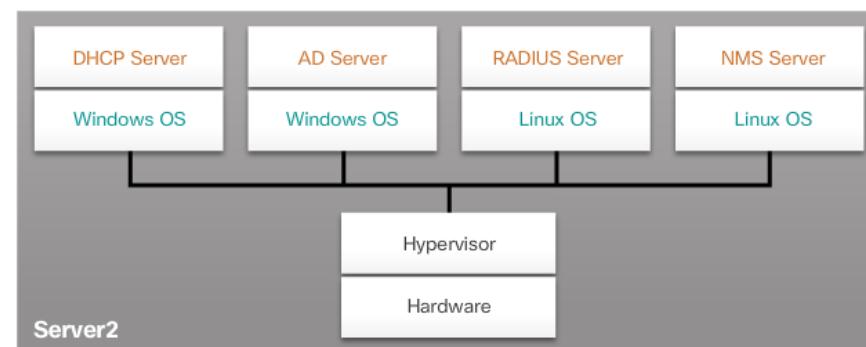
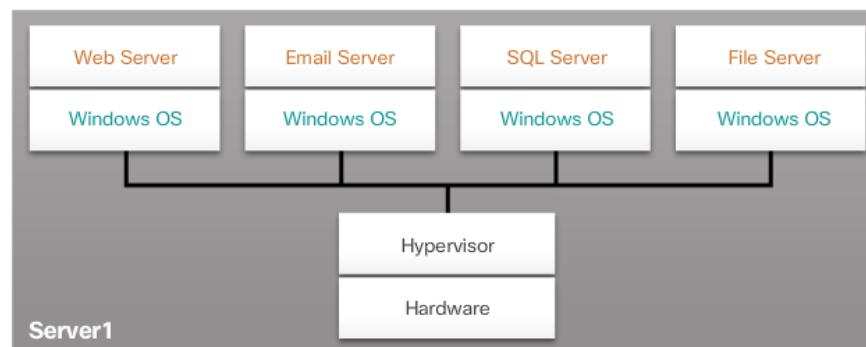




Cloud and Virtualization

Virtualization

- Server virtualization
 - takes advantage of idle resources
 - consolidates number of servers.
 - Multiple OS on a single boxes



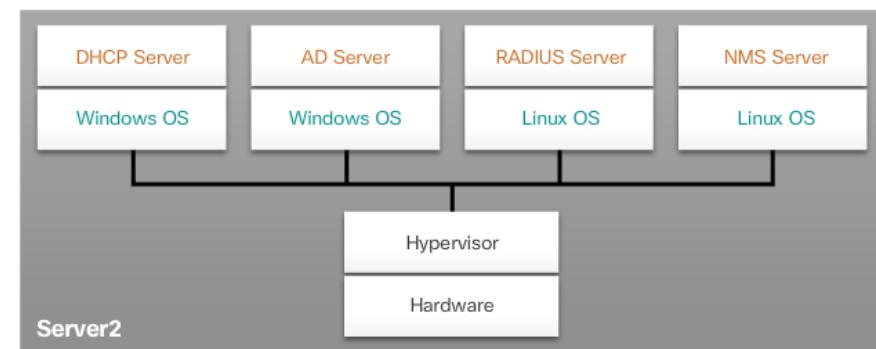
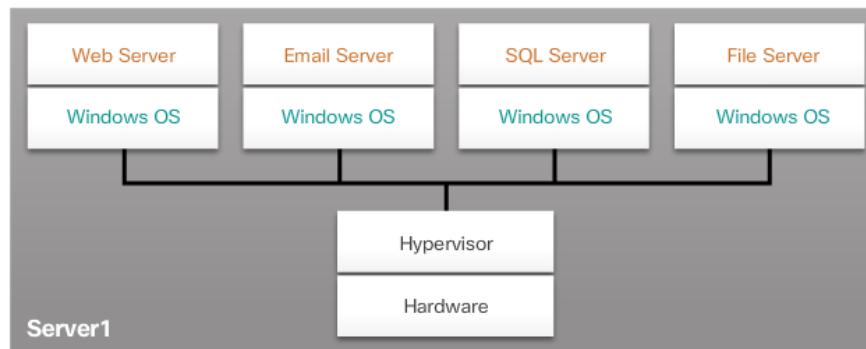
- Eight dedicated servers consolidated to two servers using hypervisors to support multiple virtual instances of the OS.



Cloud and Virtualization

Virtualization

- Virtualization separates the OS from the hardware allowing multiple operating systems to exist on a single hardware platform.
- The **hypervisor** adds an abstraction layer on top of the real physical hardware used to create virtual machines which have access to all the hardware of the physical machine such as CPUs, memory, disk controllers, and NICs.
- Summary of virtualization advantages include:
 - Less equipment is required
 - Less energy is consumed
 - Less space is required
 - Easier prototyping
 - Faster server provisioning
 - Increased server uptime
 - Improved disaster recovery
 - Legacy support





Cloud and Virtualization

Virtualization

- Advantages of Virtualization in detail
 - Major advantage = overall cost reduction
 - Less equipment is required
 - Virtualization enables server **consolidation**, which requires fewer physical servers, fewer networking devices, and less supporting infrastructure.
 - It also means **lower maintenance costs**.
 - Less energy is consumed
 - Consolidating servers lowers the monthly power and cooling costs.
 - Reduced consumption helps enterprises to achieve a smaller carbon footprint.
 - Less space is required
 - Server consolidation with virtualization reduces the overall **footprint** of the data center.
 - Fewer servers, network devices, and racks reduce the amount of required .



Cloud and Virtualization

Virtualization

- Advantages of Virtualization in detail
 - Easier prototyping
 - Self-contained labs, operating on isolated networks, can be **rapidly created for testing and prototyping network deployments.**
 - If a mistake is made, an administrator can revert to a previous version.
 - The testing environments can be online, but **isolated** from end users.
 - When testing is completed, the servers and systems can be deployed.
 - Faster server provisioning
 - Creating a virtual server is far faster than provisioning a physical server.
 - Increased server uptime
 - Most server virtualization platforms now offer **advanced redundant fault tolerance** features, such as live migration, storage migration, high availability, and distributed resource scheduling.
 - Support the ability to **move a virtual machine** from one server to another.



Cloud and Virtualization

Virtualization

- Advantages of Virtualization in detail
 - Improved disaster recovery
 - Virtualization offers advanced business continuity solutions.
 - It provides **hardware abstraction** capability so that the recovery site no longer needs to have hardware that is identical to the hardware in the production environment.
 - Most enterprise server virtualization platforms also have software that can help test and automate the failover before a disaster does happen.
 - Legacy Support
 - Virtualization can extend the life of OSs and applications providing more time for organizations to migrate to newer solutions.

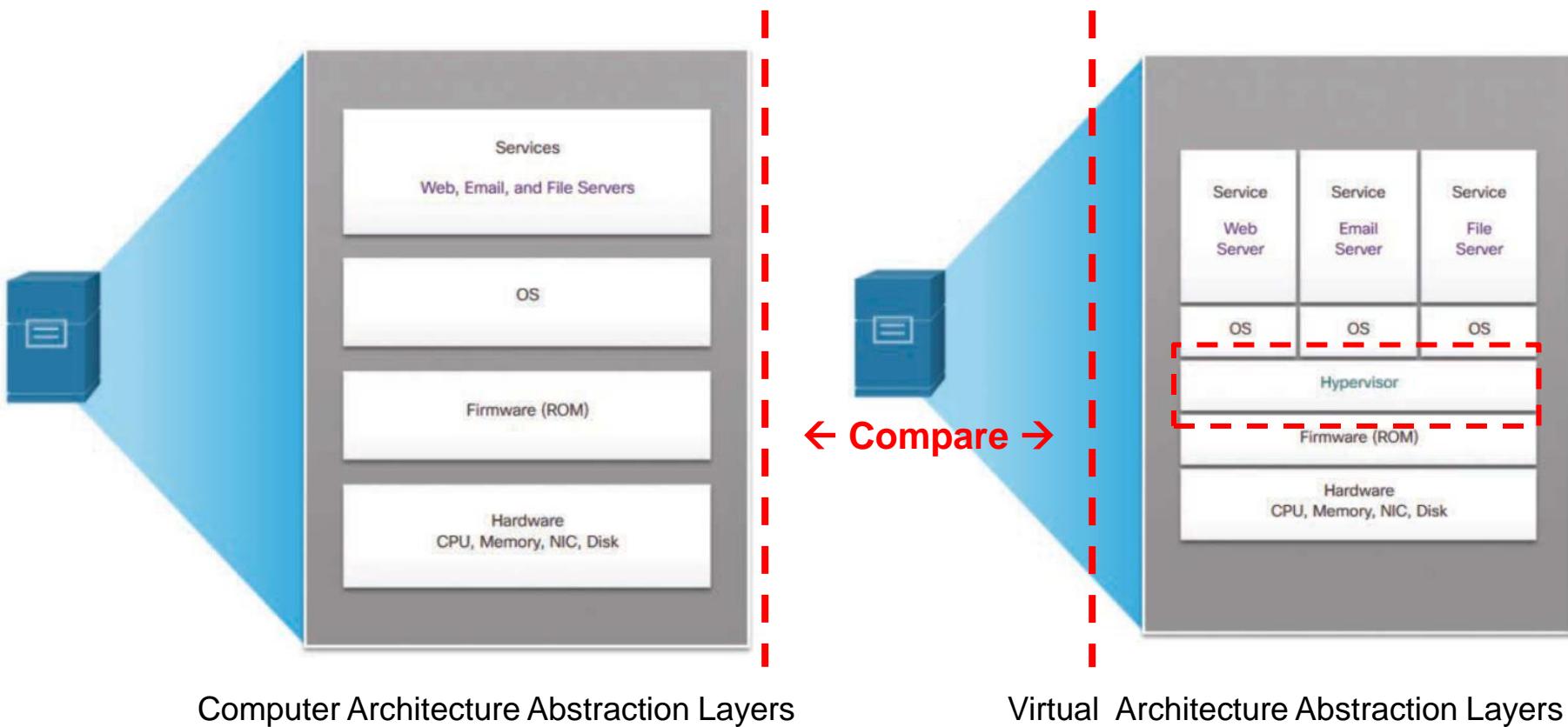


Cloud and Virtualization

Virtualization

■ Abstraction Layers

- Computer system architecture abstraction layers
- Virtualization...Hypervisor installed between the firmware and the OS
- Hypervisor supports multiple instances of OSs





Cloud and Virtualization

Virtual Network Infrastructure

- There are two approaches to installing a Hypervisor:
 - Type 1 “**Bare Metal**” approach in which the hypervisor is installed directly on the hardware.

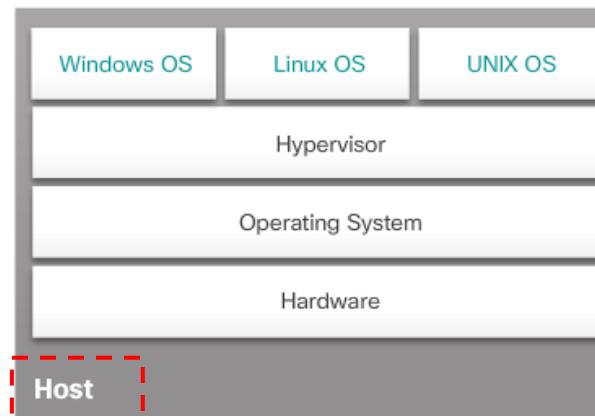
Bare Metal
- KVM
- Red Hat RHEV



KVM = Kernel-based Virtual Machine
RHEV = Red Hat Enterprise Virtualization

- Type 2 “**Hosted**” approach in which the hypervisor is installed on top of an existing operating system.

Hosted
- Virtual Box
- VM Workstation





Cloud and Virtualization

Virtual Network Infrastructure

■ Network Virtualization

- Server virtualization hides server resources (number and identity of physical servers, processors, and OSs) from server users.
- This can create problems if the data center is using traditional network architectures.
 - E.g. VLANs used by VMs must be assigned to the same switch port as the physical server running the hypervisor.
 - VMs can be moved. The network administrator must be able to add, drop, and change network resources and profiles. This process is hard to do with traditional network switches.
- Another problem is that traffic flows are different to the normal client/server model.
 - Data center has a lot traffic **between** virtual servers (**East-West** traffic).
 - The flows change in location and intensity over time. A flexible approach to network resource management is needed.



Cloud and Virtualization

Virtual Network Infrastructure

■ Network Virtualization (continued)

- Current network infrastructure can react to changing requirements to manage traffic flows using QoS and security-level configurations for flows.
- However, reconfiguration can be time consuming in large enterprises with multivendor equipment each time a new VM is enabled.
- The network infrastructure can benefit from virtualization.
- SDN Software-defined networking (SDN) can be used to virtualize the network.
- SDN moves the control plane from each network device to a central SDN controller.
- The SDN controller defines the data flows that occur in the SDN data plane.

7.3 Network Programming (Network Programmability)

(SDN Software-Defined
Networking)





Network Programming

Software-Defined Networking (SDN) *

- A network device contains the following **planes**: *
 - **Control plane**
 - Typically regarded as the **brains** of a device and is used to make **forwarding decisions**.
 - The control plane contains **Layer 2** and **Layer 3** route **forwarding mechanisms**, such as routing protocol neighbor tables and topology tables, IPv4 and IPv6 routing tables, STP, and the ARP table.
 - Information sent to the control plane is processed by the CPU.
 - **Data plane**
 - Also called the **forwarding plane**, this plane is typically the **switch fabric** connecting the various network ports on a device.
 - The data plane of each device is used to forward traffic flows.
 - Routers and switches use information from the **control plane** to **forward incoming traffic** out the appropriate egress (exit) interface.
 - Information in the data plane is typically processed by a special data plane processor, such as a digital signal processor (DSP), without the CPU getting involved.

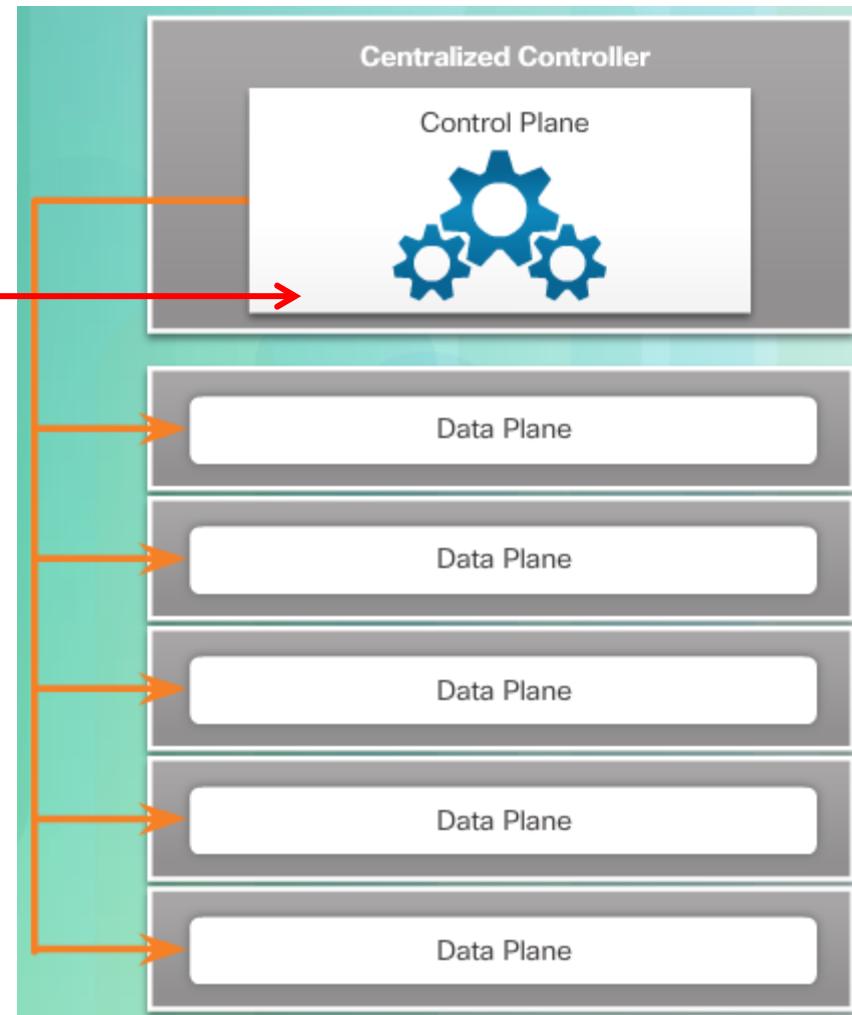


Network Programming

Software-Defined Networking *

- SDN virtualizes the network, removing the control plane function from each device and performing it on a **centralized controller**.

- The centralized controller communicates control plane functions to each device.
- Each device can now focus on forwarding data while the centralized controller manages data flow, increases security, and provides other services.





Network Programming

Software-Defined Networking

- Technology developed by VMware allows a host OS to support more than one client OS. Most of the current virtualisation technology is based on this.
- Major Virtualisation Architectures
 - **Software Defined Networking (SDN)** - A network architecture that virtualizes the network.
 - **Cisco Application Centric Infrastructure (ACI)** - A purpose-built hardware solution for integrating Cloud computing and data center management.



Network Programming Software-Defined Networking

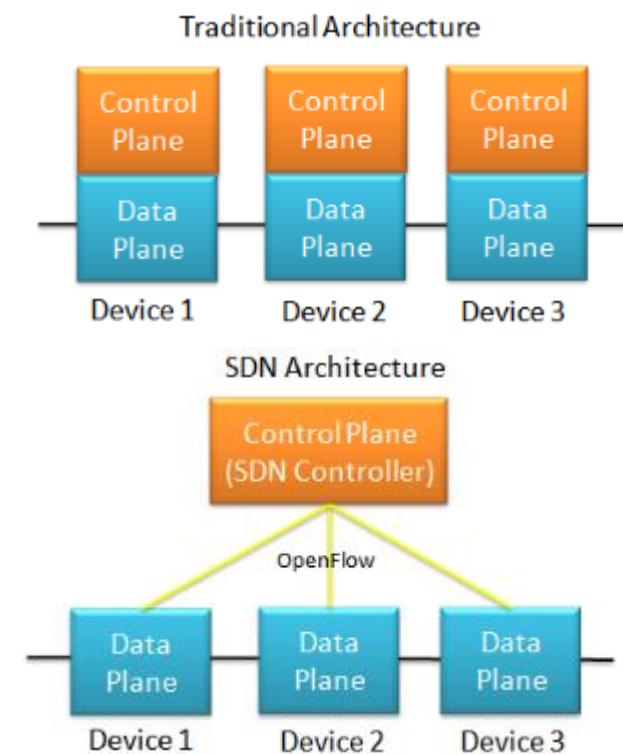
- Network virtualization techniques
 - OpenFlow
 - Developed at Stanford University to manage traffic between routers, switches, wireless access points, and a controller.
 - The OpenFlow protocol is a basic element in building SDN solutions.
 - OpenStack
 - A **virtualization** and **orchestration** platform for building **scalable Cloud environments** and providing an IaaS solution.
 - **Orchestration** in networking is the process of **automating** the provisioning of network components such as servers, storage, switches, routers, and applications.



Network Programming

Software-Defined Networking

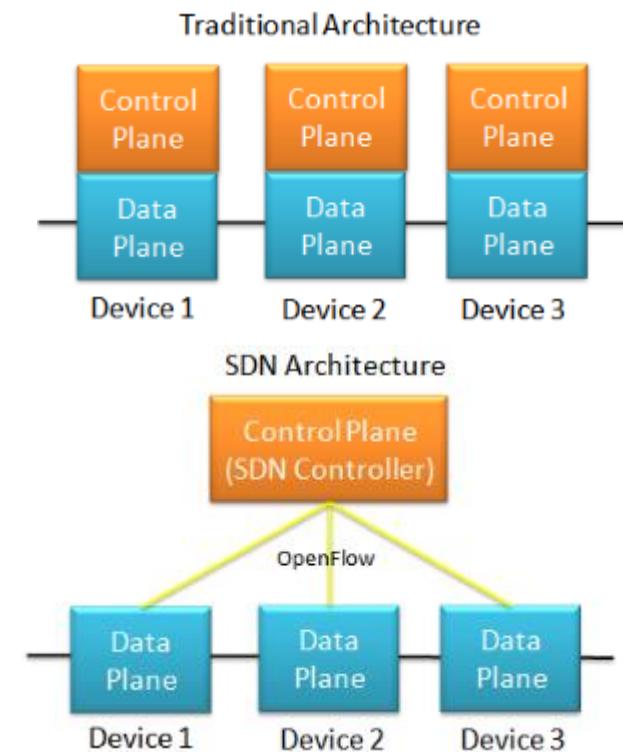
- **Traditional Router or Switch Architecture ***
 - Control plane and data plane functions are in the **same device**.
 - Routing decisions and packet forwarding are the responsibility of the device operating system
- **SDN Architecture ***
 - Controller-based SDN
 - Move control plane from each network device to a “*central network intelligence*” & policy-making entity called the **SDN controller**.
 - An architecture developed to virtualize the network.
 - Virtualizes the control plane.





Network Programming Software-Defined Networking

- The SDN controller is a **logical entity** that enables network administrators to manage and dictate **how the data plane** of virtual switches and routers should **handle network traffic**.
- It orchestrates, mediates, and facilitates communication between applications and network elements



<https://www.opennetworking.org/sdn-resources/sdn-definition>



Network Programming

Software-Defined Networking *

- The SDN controller defines the **data flows** that occur in the SDN Data Plane.
- A **flow** is a sequence of packets traversing a network that share a set of header field values.
 - e.g. a flow could consist of all packets with the same source and destination IP addresses, or all packets with the same VLAN identifier.
- Each flow through the network must first get **permission** from the SDN controller, which verifies that the communication is permissible according to the **network policy**.
- If the controller allows a flow, it computes a route for the flow to take, and adds an entry for that flow in each of the switches along the path.

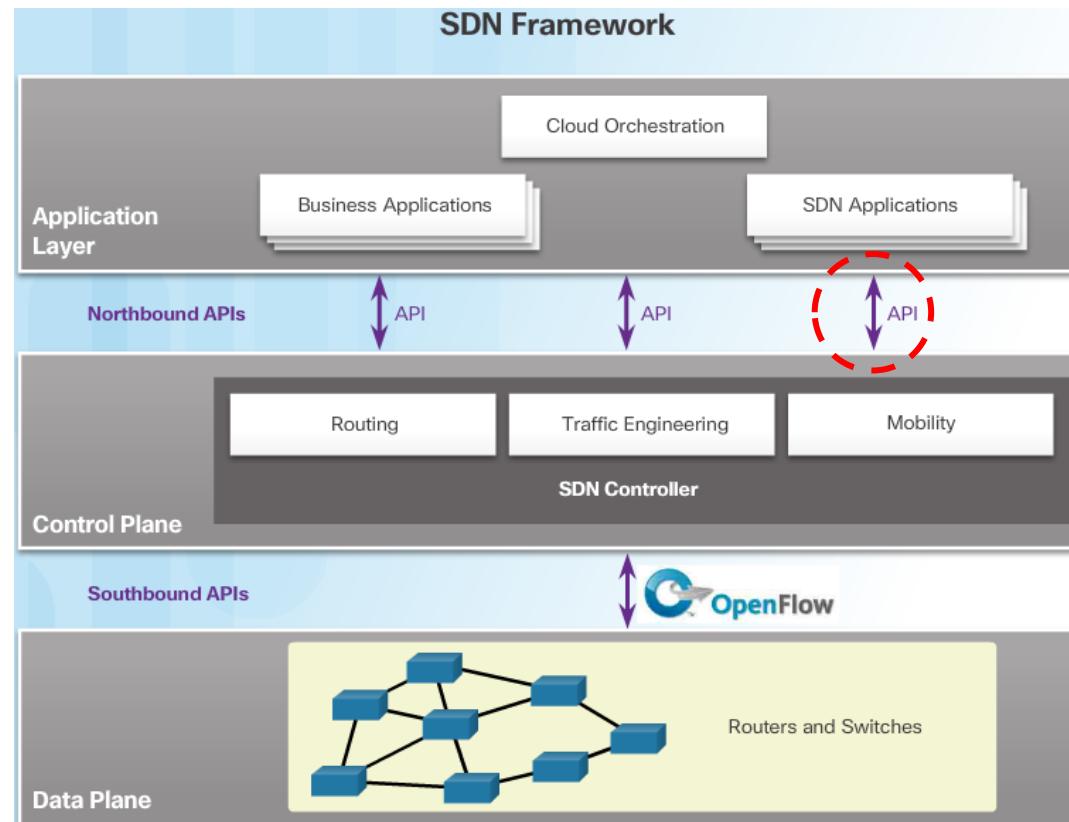
Note: Network Policy = a set of rules for the behaviour of network devices.

See <https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-network-policy.html>



Network Programming Software-Defined Networking

- The SDN framework uses northbound APIs to communicate with upstream applications and southbound APIs to define the behaviour of downstream routers and switches.

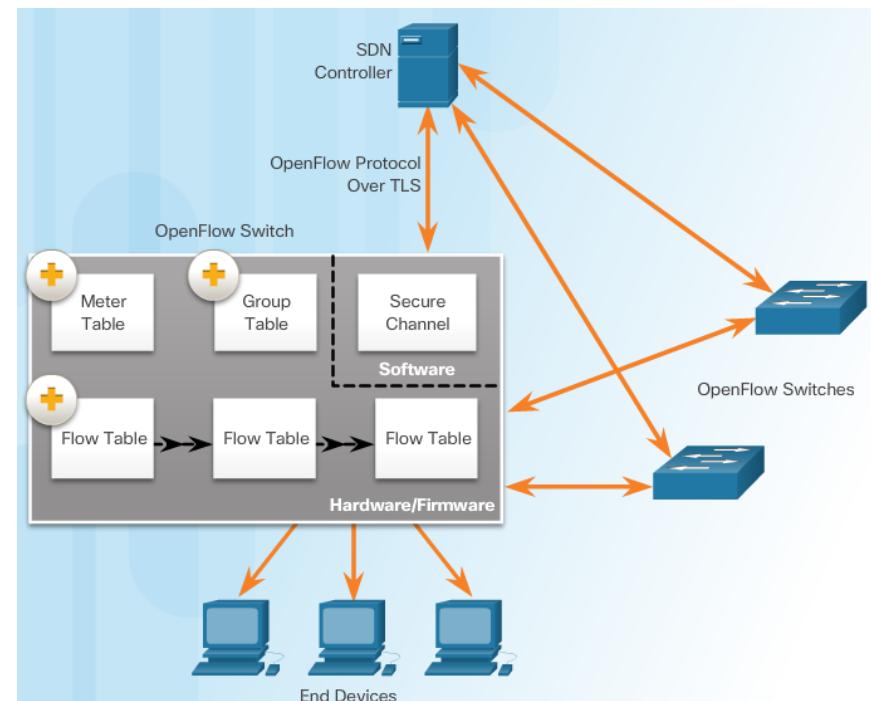


**APIs =>
Network
Programming**



Network Programming Controllers *

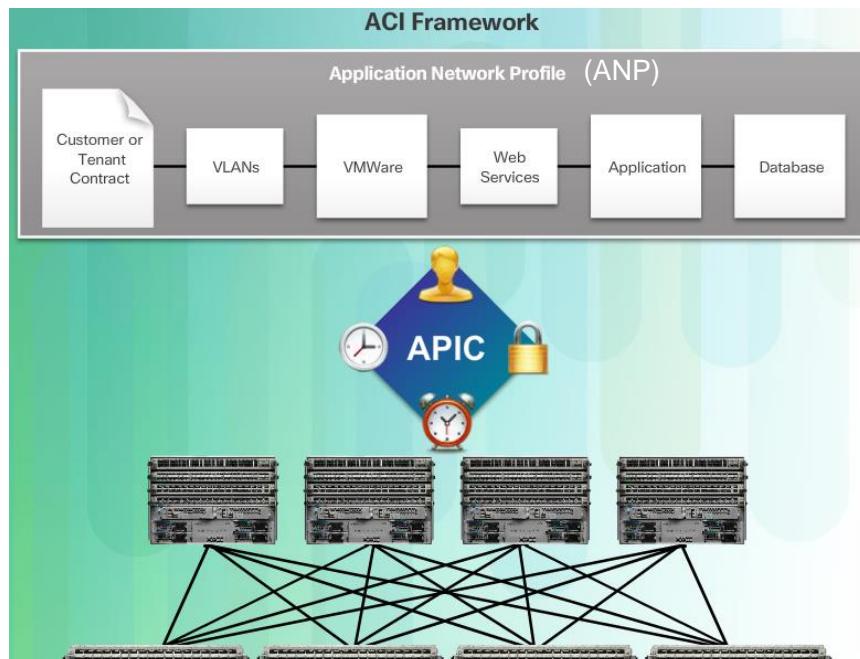
- The SDN controller defines the data flows that occur in the SDN Data Plane.
- Using the OpenFlow protocol, the controller populates a series of tables implemented in hardware or firmware
- The following tables manage the flows of packets through the switch:
 - **Flow table** - This table matches incoming packets to a particular flow and specifies the functions that are to be performed on the packets. There may be multiple flow tables that operate in a pipeline fashion.
 - **Group table** - A flow table may direct a flow to a Group Table, which may trigger a variety of actions that affect one or more flows.
 - **Meter table** - The table triggers a variety of performance-related actions on a flow.





Network Programming Controllers

- Cisco developed the Application Centric Infrastructure (ACI) to automate the network, accelerate application deployments, and align IT infrastructures to better meet business requirements.
- These are the three core components of the ACI architecture:
 - **Application Network Profile (ANP)** - a collection of end-point groups (EPG), their connections, and the policies that define those connections
 - **Application Policy Infrastructure Controller (APIC)** - a centralized software controller that manages downstream switches. It translates application policies into network programming.
 - **Cisco Nexus 9000 Series switches** - provide an application-aware switching fabric and work with an APIC to manage the virtual and physical network infrastructure.

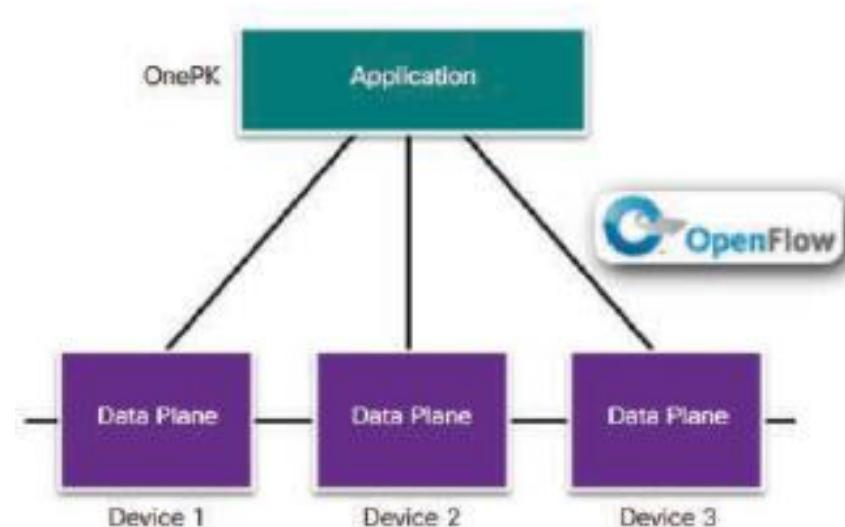


The Cisco **APIC - Enterprise Module (APIC-EM)** extends ACI aimed at enterprise and campus deployments.



Network Programming Controllers

- There are three basic types of SDN:
 - **Device-based SDN** - Devices are **programmable by applications** running on the device itself or on a server in the network. Cisco OnePK is an example of a device-based SDN.



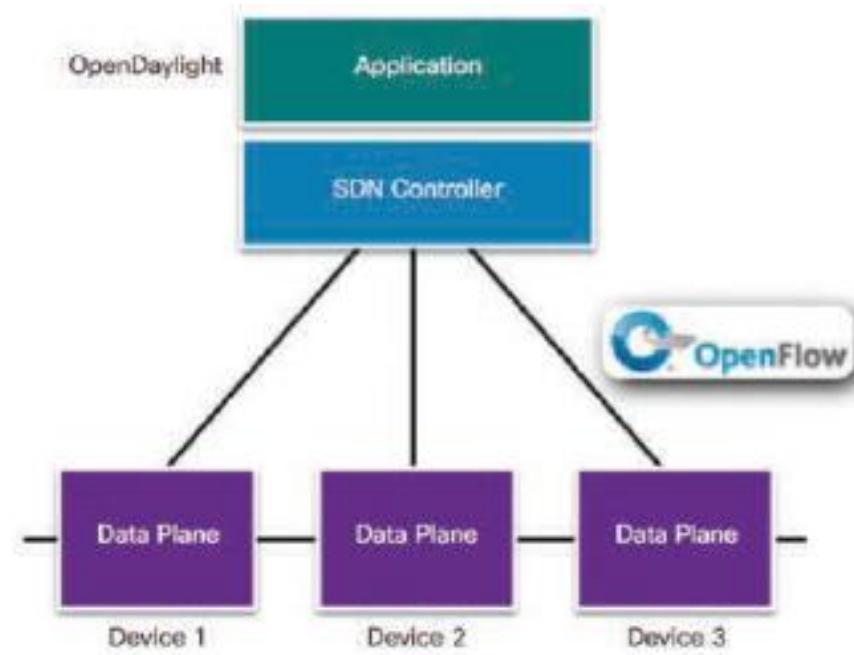


Network Programming Controllers

- There are three basic types of SDN:

- **Controller-based SDN -**

Centralized controller that has knowledge of all devices in the network. The applications can interface with the controller responsible for managing devices and manipulating traffic flows throughout the network. The Cisco Open SDN Controller is a commercial distribution of OpenDaylight.

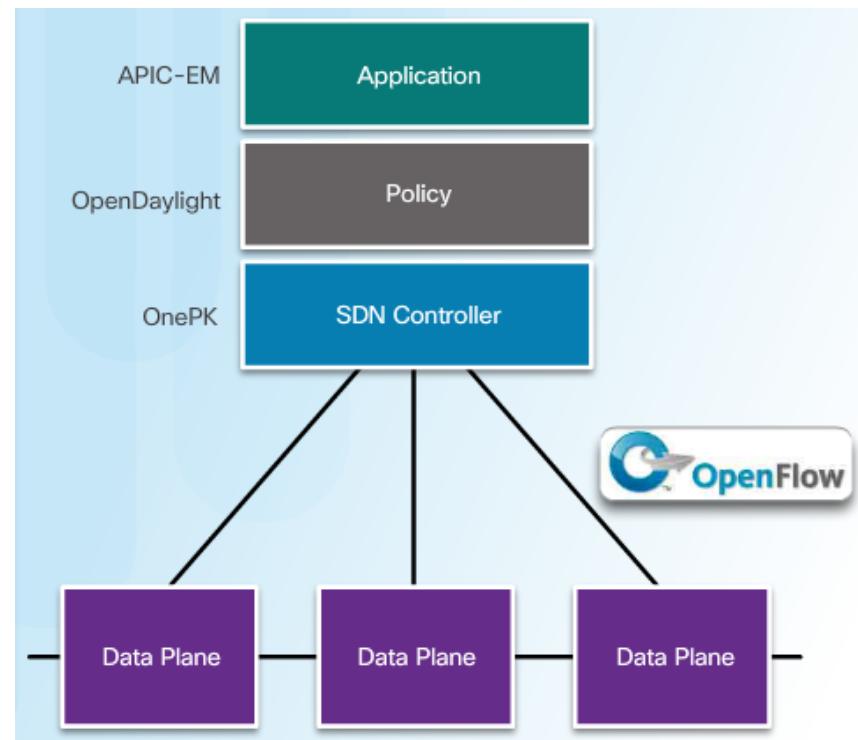


Note: OpenDaylight = an open source SDN controller.
See <https://www.opendaylight.org>



Network Programming Controllers

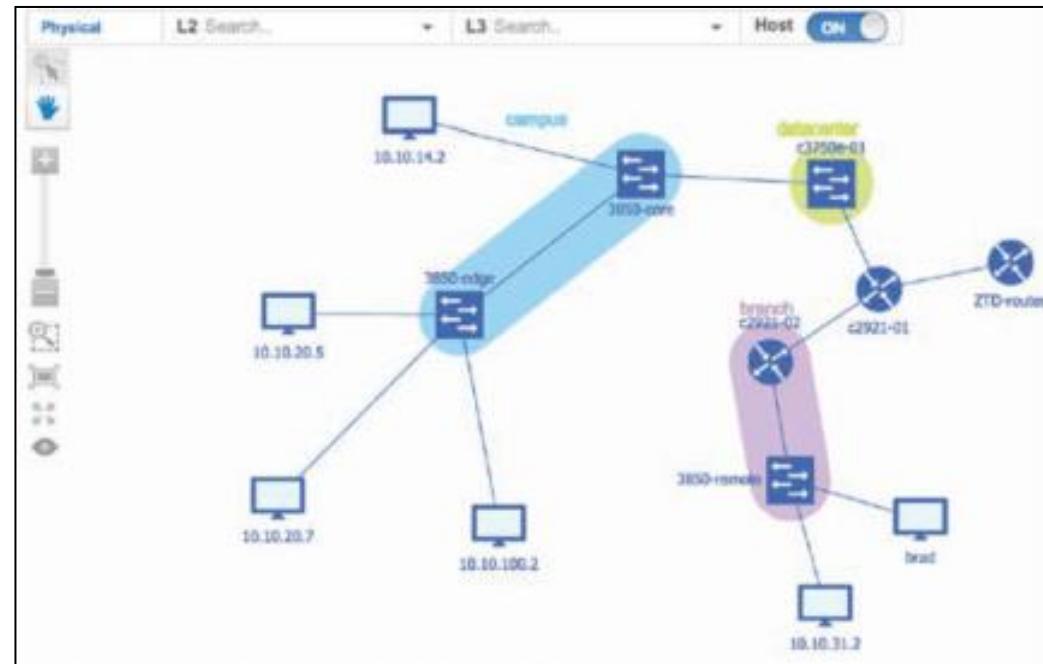
- There are three basic types of SDN:
 - **Policy-based SDN** - Includes an additional Policy layer that operates at a higher level of abstraction. No programming skills are required.
 - **Cisco APIC-EM** is an example of this type of SDN.





Network Programming Controllers

- Cisco APIC-EM provides the following features:
 - **Discovery** - populates controller's device & host inventory database
 - **Device Inventory** - collects detailed info from devices in the network
 - **Host Inventory** - collects detailed info from hosts in the network
 - **Topology** - supports a graphical view of the network (topology view)



APIC-EM Network Topology View



Network Programming Controllers

- **Policy** - ability to view and control policies across the entire network including QoS.
- **Policy Analysis** - ability to trace application specific paths between end devices to quickly identify ACLs in use and problem areas including *ACL Analysis* and *ACL Path Trace*
 - **ACL Analysis** - examines ACLs on devices, searching for redundant, conflicting, or shadowed entries (incorrect ACL entries)

The screenshot shows the 'Policy Analysis' section of the Cisco Network Programming Controller. The left sidebar has a 'Policy Analysis' tab selected. The main area displays a summary of conflicts:

Category	Count
shadowed	1
redundant	7
correlated	1

Below this, a table lists 12 ACL entries. The first three entries are highlighted in red, indicating they are shadowed. The last three entries are highlighted in yellow, indicating they are redundant. The remaining six entries are green. The table columns include:

Line	Action	Protocol	Source IP	Destination IP	Port	Description
1	DENY	TCP	host 192.168.1.10	any	eq WWW	
2	PERMIT	TCP	any	host 161.120.33.40	eq WWW	
3	DENY	TCP	host 140.193.37.10	any	eq WWW	
4	DENY	TCP	host 140.193.37.10	any	eq WWW	
5	DENY	TCP	host 140.193.37.10	any	eq FTP	
6	PERMIT	TCP	host 140.193.37.0/24	any	eq FTP	
7	PERMIT	TCP	host 140.193.37.0/24	host 161.120.33.40	eq FTP	
8	DENY	TCP	host 140.193.37.0/24	host 161.120.33.40	eq WWW	
9	DENY	TCP	any	any	eq FTP	
10	DENY	TCP	any	any	eq 458	
11	DENY	UDP	any	any	eq 458	
12	PERMIT	IP	any	any		

On the right, three conflict categories are shown:

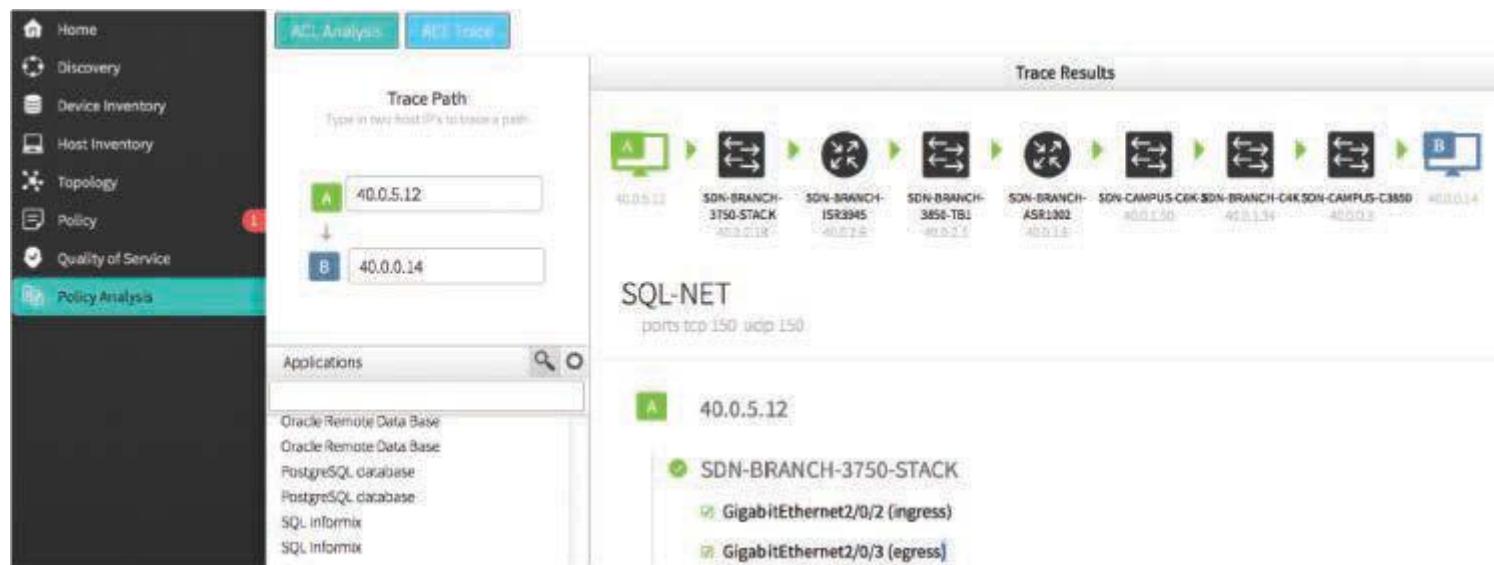
- Line 2 shadows [line 8]**
 - PERMIT TCP any host 161.120.33.40 eq WWW
 - DENY TCP 140.193.37.0/24 host 161.120.33.40 eq WWW
- Line 2 correlated lines 1**
 - PERMIT TCP any host 161.120.33.40 eq WWW
 - DENY TCP host 140.193.37.20 any eq WWW
- Line 2 redundant [lines 3]**
 - PERMIT TCP any host 161.120.33.40 eq WWW
 - PERMIT TCP host 161.120.33.41 host 161.120.33.40 eq WWW

Sample ACL Analysis



Network Programming Controllers

- **ACL Path Trace** - examines specific ACLs on the path between two end nodes, displaying any potential issues.



Sample ACL Path Trace



Network Programming Controllers

■ Cisco APIC-EM :

- Play with the APIC-EM at Cisco DevNet
- You will need to create an account
- You can then login with your NetAcad credentials and try some hands-on Network Programming for free at link below ...interesting video course Python + Cisco APIC-EM sandbox.

<https://developer.cisco.com/video/net-prog-basics/>

7.4 Chapter Summary





Chapter Summary

Summary

- The six pillars of IoT are:
 - Network Connectivity
 - Fog Computing
 - Security
 - Data Analytics
 - Management and Automation
 - Application Enablement Platform
- Cloud computing services include:
 - Software as a Service (SaaS)
 - Platform as a Service (PaaS)
 - Infrastructure as a Service (IaaS)
 - IT as a Service (ITaaS)
- Cloud models include:
 - Public clouds
 - Private clouds
 - Hybrid clouds
 - Community clouds



Chapter Summary

Summary

- Type 1 hypervisors are installed directly on the hardware.
Type 2 hypervisors are installed on top of any existing OS.
- SDN is a network architecture that has been developed to virtualize the network. The SDN controller defines the data flows that occur in the SDN data plane.
- The three types of SDN are:
 - Device-based SDN
 - Controller-based SDN
 - Policy-based SDN
- Policy-based SDN, such as Cisco's APIC-EM, provides a simple mechanism to control and manage policies across the entire network.
- The ability to manage policies is one of the most important features of the APIC-EM controller.



Reminder

Lab on Friday

- The lab work from now on will be 'gearing up' towards the Skills Based Assessment (SBA) on Friday 27/11/20.
- You will get a chance in Friday's Lab to do a set of activities based on the previous labs to help you revise most of the following:
 - Configuring OSPF
 - Configuring PPP and Authentication (CHAP)
 - Configuring VPNs and GRE Tunnels
 - Configuring SNMP
 - Configuring BGP
 - Configuring Standard and Extended ACLs
 - etc...
- It is important that you complete all the labs including the remaining labs to iron out anything that may be unclear about the material to date.







Chapter 8: Network Troubleshooting



Connecting Networks

Cisco | Networking Academy®
Mind Wide Open™



Chapter 8 - Sections & Objectives

- 8.1 Troubleshooting Methodology
 - Explain troubleshooting approaches for various network problems.
- 8.2 Troubleshooting Scenarios
 - Troubleshoot end-to-end connectivity in a small to medium-sized business network, using a systematic approach.

8.1 Troubleshooting Methodology

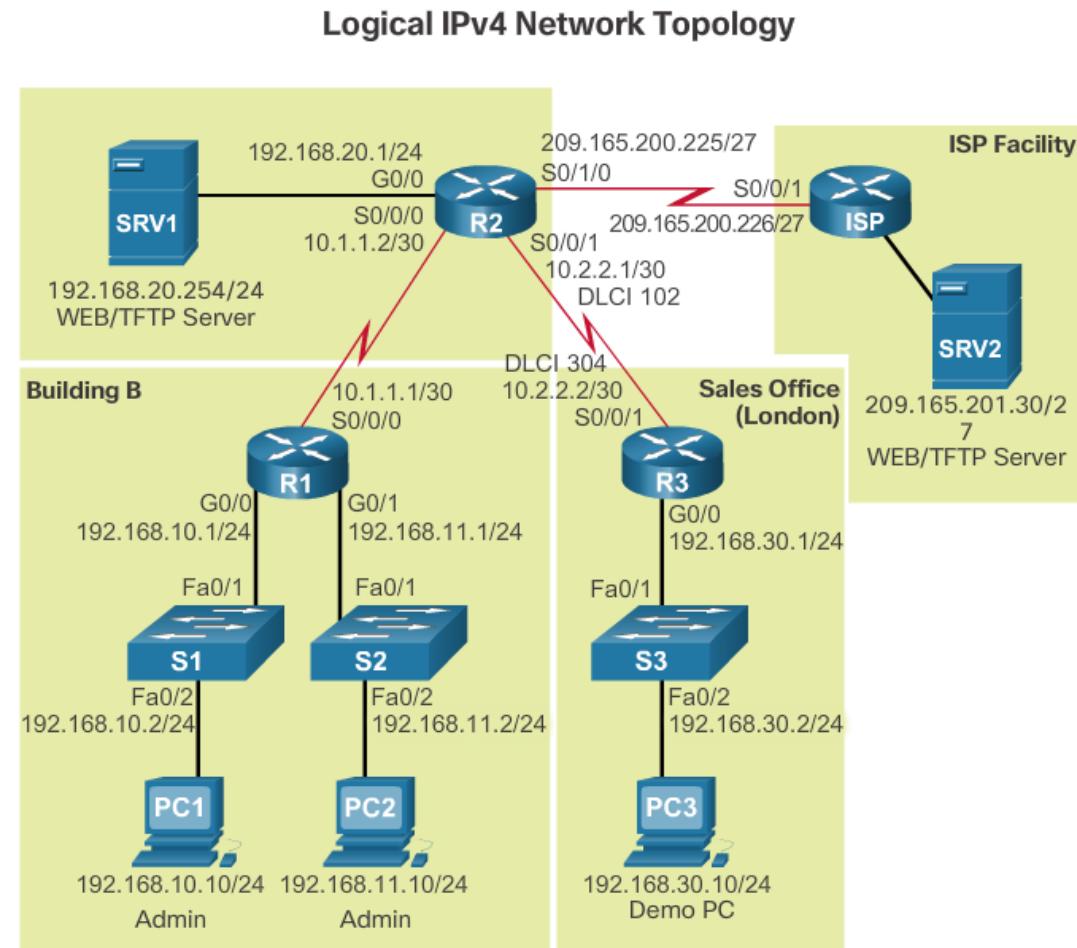




Troubleshooting Methodology

Network Documentation

- Documentation is critical to being able to monitor and troubleshoot a network.
- Documentation includes:
 - Configuration files, including network configuration files and end-system configuration files
 - Physical and logical topology diagrams
 - **Baseline** performance levels





Troubleshooting Methodology

Network Documentation

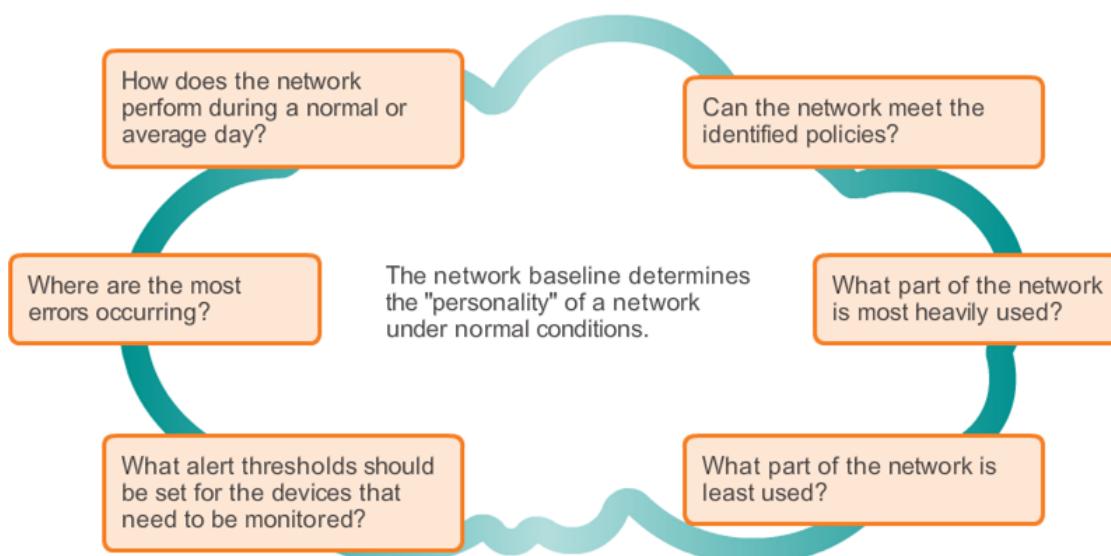
- Common Cisco IOS commands used for data collection.
- Manual collection of data should be reserved for smaller networks or limited to mission-critical network devices.
- Sophisticated network management software is typically used to create a **baseline** for large and complex networks.

Command	Description
<code>show version</code>	Shows uptime, version information for device software and hardware.
<code>show ip interface[brief]</code> <code>show ipv6 interface[brief]</code>	Shows all the configuration options that are set on an interface. Use the brief keyword to only show up/down status of IP interfaces and the IP address is of each interface.
<code>show interfaces</code> [<code>interface_type</code> <code>interface_num</code>]	Shows detailed output for each interface. To show detailed output for only a single interface, include the interface type and number in the command (e.g. gigabitethernet 0/0).
<code>show ip route</code> <code>show ipv6 route</code>	Shows the contents of the routing table.
<code>show arp</code> <code>show ipv6 neighbors</code>	Shows the contents of the ARP table (IPv4) and the neighbor table (IPv6).
<code>show running-config</code>	Shows current configuration.
<code>show port</code>	Shows the status of ports on a switch.
<code>show vlan</code>	Shows the status of VLANs on a switch
<code>show tech-support</code>	This command is useful for collecting a large amount of information about the device for troubleshooting purposes. It executes multiple <code>show</code> commands which can be provided to technical support representatives when reporting a problem.
<code>show ip cache flow</code>	Displays a summary of the NetFlow accounting statistics.



Network Documentation

Establishing a Network Baseline



Questions that a Network Baseline answers

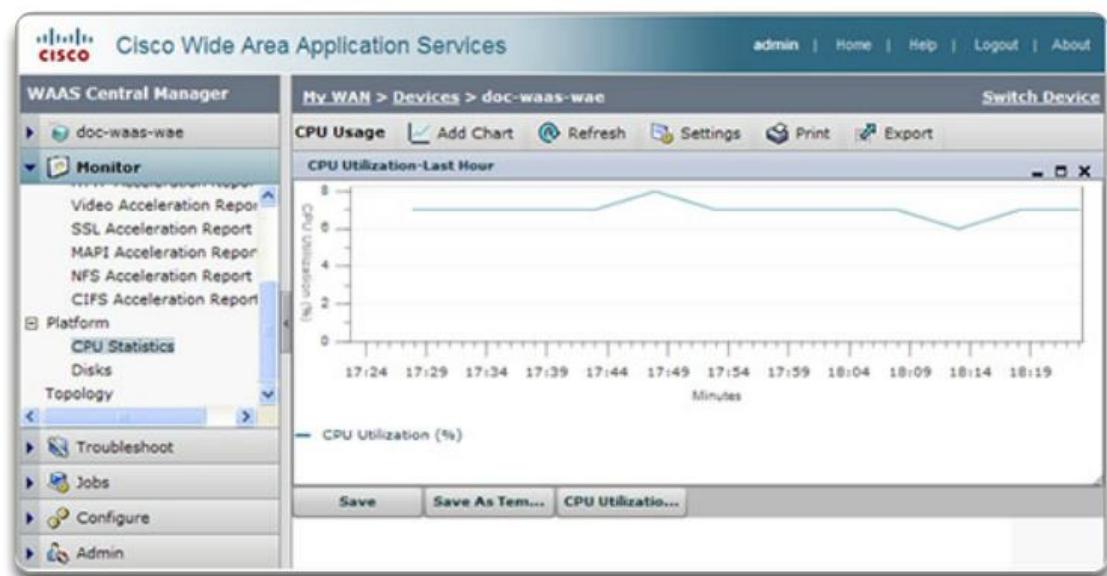
- The purpose of network monitoring is to watch network performance in comparison to a predetermined baseline.
- The baseline is used to establish normal network or system performance.
- Allows admins to determine the difference between behaviour.
- Determines if current network design is sufficient.



Network Documentation

Establishing a Network Baseline (cont.)

- **Step 1.** Determine what types of data to collect.
Start simply and fine-tune.
- **Step 2.** Identify devices and ports of interest.
Servers, key users, critical operations.
- **Step 3.** Determine the baseline duration.
Minimum of 7 days recommended.

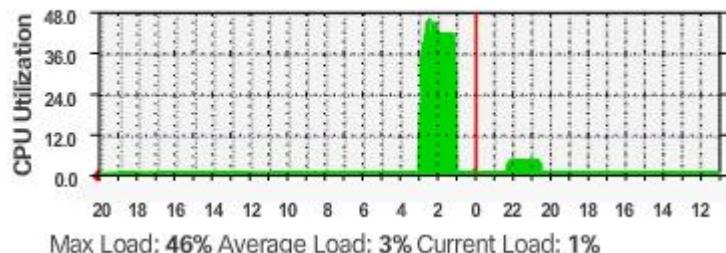




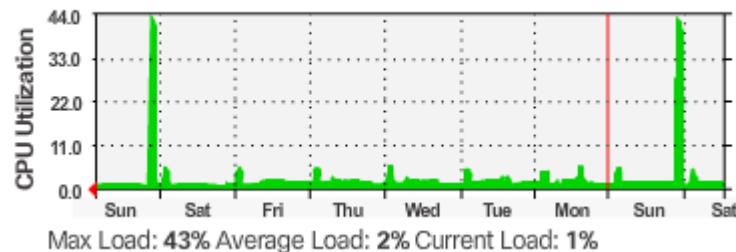
Network Documentation

Establishing a Network Baseline

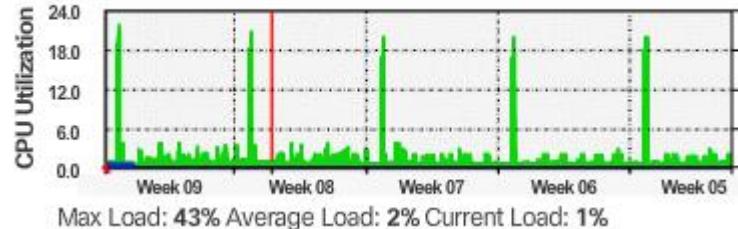
Daily Graph (5 minute Average)



Weekly Graph (2 Hour Average)

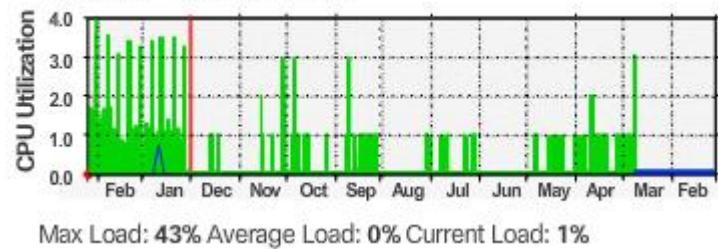


Monthly Graph (30 Minute Average)



<https://www.hea.net/>

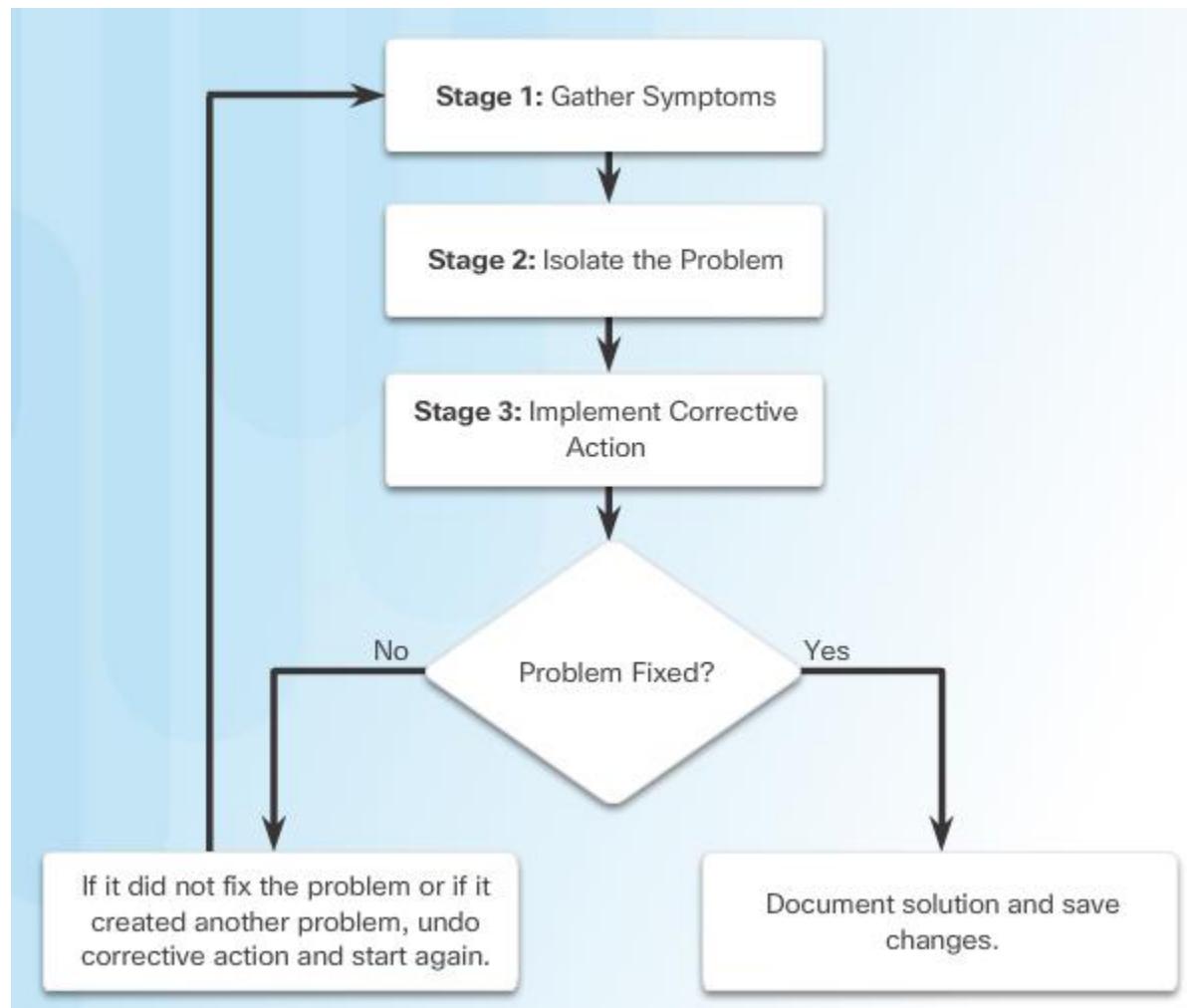
Yearly Graph (1 day Average)





Troubleshooting Methodology

Troubleshooting Process





Troubleshooting Methodology

Troubleshooting Process

- Common Cisco IOS commands used to gather the symptoms of a network problem.

Command	Description
<code>ping {host ip-address}</code>	Sends an echo request packet to an address, then waits for a reply. The <code>host</code> or <code>ip-address</code> variable is the IP alias or IP address of the target system.
<code>traceroute {destination}</code>	Identifies the path a packet takes through the networks. The <code>destination</code> variable is the hostname or IP address of the target system.
<code>telnet {host ip-address}</code>	Connects to an IP address using the Telnet application.
<code>ssh -l userid ip-address</code>	Connects to an IP address using SSH.
<code>show ip interface brief</code> <code>show ipv6 interface brief</code>	Displays a summary of the status of all interfaces on a device.
<code>show ip route</code> <code>show ipv6 route</code>	Displays the current IPv4 and IPv6 routing tables, which contains the routes to all known network destinations.
<code>show running-config</code>	Displays contents of currently running configuration file.
<code>[no] debug ?</code>	Displays a list of options for enabling or disabling debugging events.
<code>show protocols</code>	Displays the configured protocols and shows the global and interface-specific status of any configured Layer 3 protocol.



Troubleshooting Methodology

Troubleshooting Process

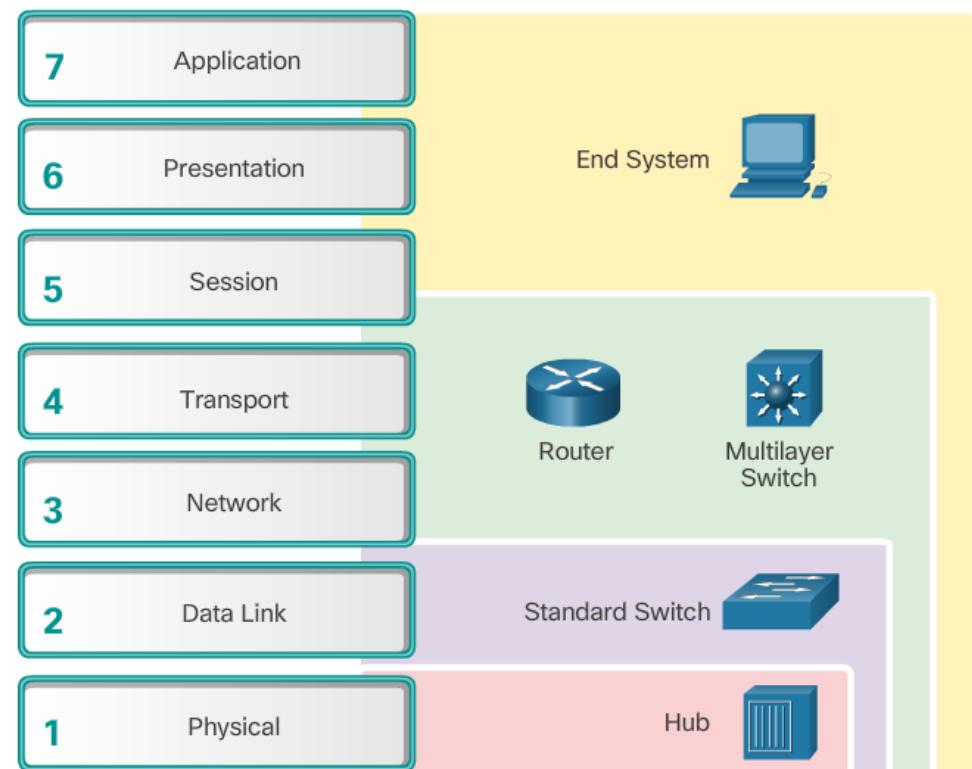
- Common Cisco IOS commands used to gather the symptoms of a network problem.

Command	Description
<code>ping {host ip-address}</code>	Sends an echo request packet to an address, then waits for a reply. The <code>host</code> or <code>ip-address</code> variable is the IP alias or IP address of the target system.
<code>traceroute {destination}</code>	Identifies the path a packet takes through the networks. The <code>destination</code> variable is the hostname or IP address of the target system.
<code>telnet {host ip-address}</code>	Connects to an IP address using the Telnet application.
<code>ssh -l userid ip-address</code>	Connects to an IP address using SSH.
<code>show ip interface brief</code> <code>show ipv6 interface brief</code>	Displays a summary of the status of all interfaces on a device.
<code>show ip route</code> <code>show ipv6 route</code>	Displays the current IPv4 and IPv6 routing tables, which contains the routes to all known network destinations.
<code>show running-config</code>	Displays contents of currently running configuration file.
<code>[no] debug ?</code>	Displays a list of options for enabling or disabling debugging events.
<code>show protocols</code>	Displays the configured protocols and shows the global and interface-specific status of any configured Layer 3 protocol.



Troubleshooting Methodology Isolating the Issue Using Layered Models

- After gathering symptoms, the network administrator compares the characteristics of the problem to the logical layers of the network to isolate and solve the issue.

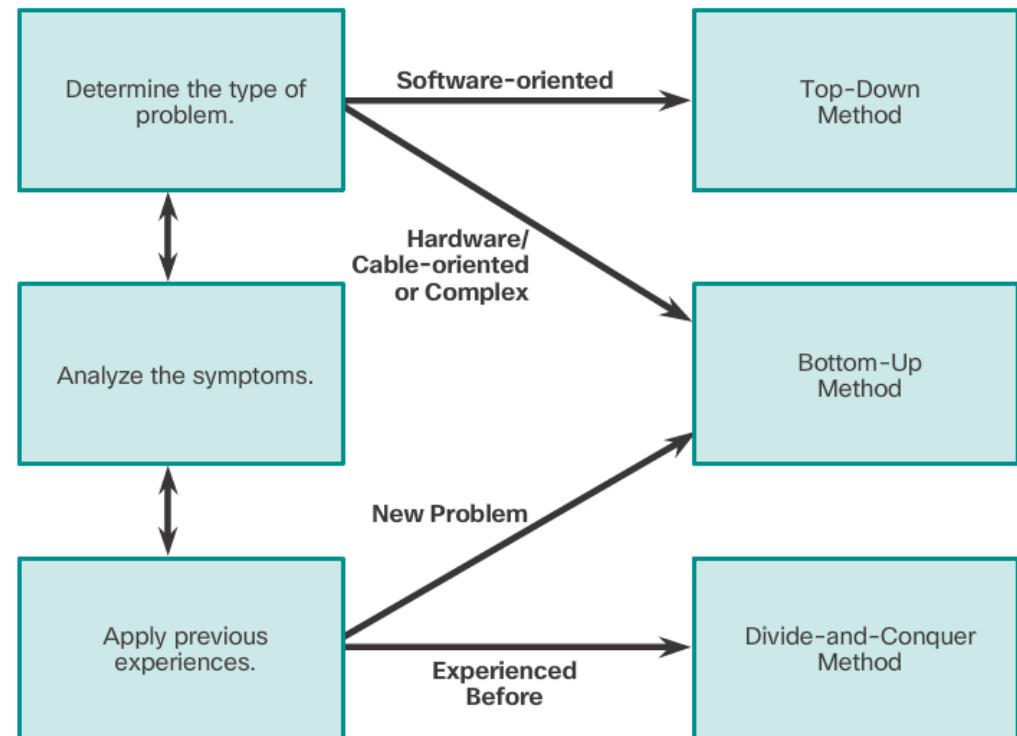




Troubleshooting Methodology

Isolating the Issue Using Layered Models

- Using the layered models, there are three primary methods for troubleshooting networks:
 - Bottom-up
 - Top-down
 - Divide-and-conquer



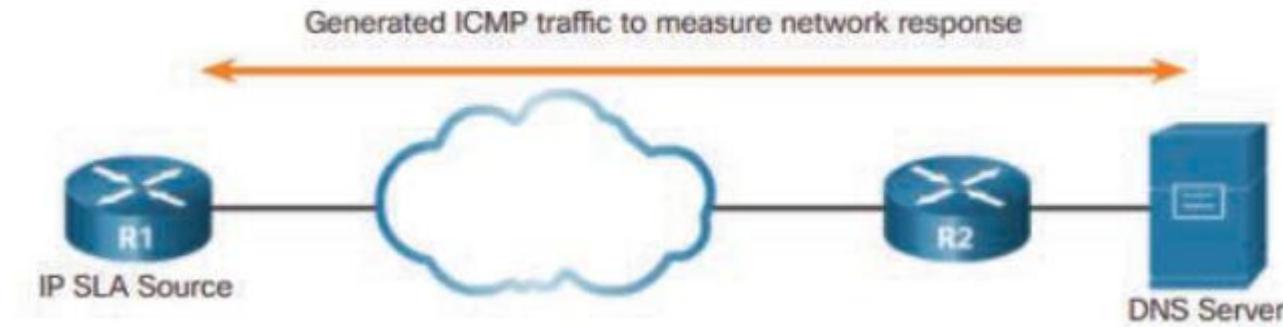
8.2 Troubleshooting Scenarios





Troubleshooting Scenarios Using IP SLA

- Cisco IP Service Level Agreements (SLA) generate traffic to measure network performance.



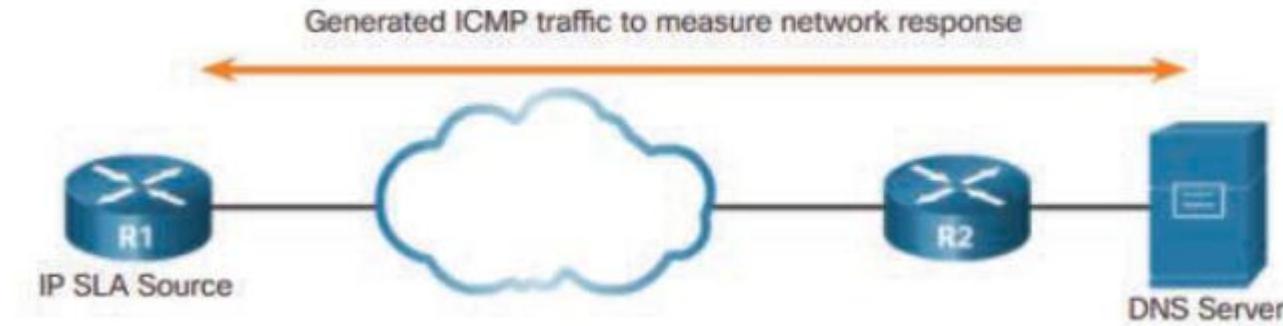
R1 is the IP SLA source. It monitors the connection to the DNS server by periodically sending ICMP requests to the server.

- Cisco IP SLA is a feature available in Cisco IOS software
 - Can be used to generate traffic and report on it **in real time** to monitor performance



Troubleshooting Scenarios Using IP SLA

- Cisco IP Service Level Agreements (SLA) generate traffic to measure network performance.



R1 is the IP SLA source. It monitors the connection to the DNS server by periodically sending ICMP requests to the server.

- Additional benefits include:

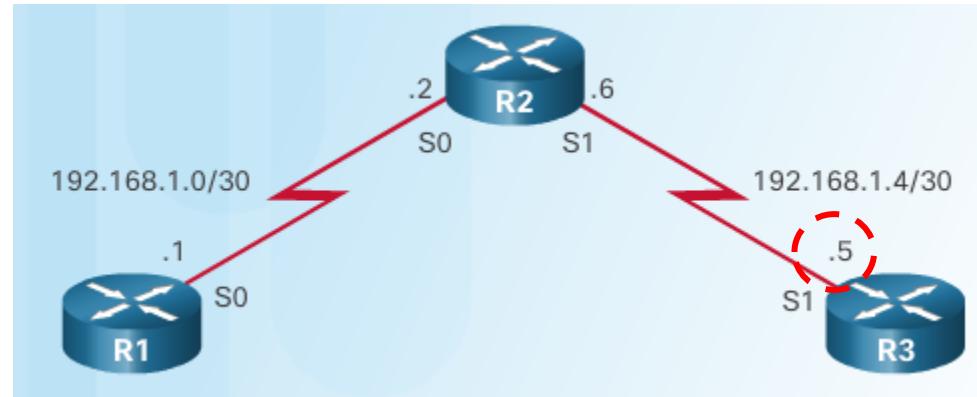
- SLA monitoring, measurement, and verification
- Measure the jitter, latency, or packet loss in the network
- IP service network health assessment
- Edge-to-edge network availability

Note: IP SLA information can be displayed using CLI commands or through **SNMP**



Troubleshooting Scenarios Using IP SLA

IP SLA ICMP Echo Configuration



Instead of using **ping** manually, we can use the IP SLA ICMP echo operation to test the availability of network devices.

```
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# ip sla 1
R1(config-ip-sla)# icmp-echo 192.168.1.5
R1(config-ip-sla-echo)# frequency 30
R1(config-ip-sla-echo)# exit
R1(config)# ip sla schedule 1 start-time now life forever
R1(config)# end
R1#
```

Set IP SLA operation with an operation number of 1

Monitor this destination address.

IP SLA rate set to 30-second intervals

start immediately (now) and continue until manually canceled (forever).



Troubleshooting Scenarios Using IP SLA

Verifying IP SLA Configuration

```
R1# show ip sla configuration
IP-SLAs Infrastructure Engine-III
Entry number: 1
Owner:
Tag:
Operation timeout (milliseconds): 5000
Type of operation to perform: icmp-echo
Target address/Source address: 192.168.1.5/0.0.0.0
Type Of Service parameter: 0x0
Request size (ARR data portion): 28
Verify data: No
Vrf Name:
Schedule:
  Operation frequency (seconds): 30 (not considered if randomly scheduled)
  Next Scheduled Start Time: Start Time already passed
  Group Scheduled : FALSE
  Randomly Scheduled : FALSE
  Life (seconds): Forever
  Entry Ageout (seconds): never
  Recurring (Starting Everyday): FALSE
  Status of entry (SNMP RowStatus): Active
Threshold (milliseconds): 5000
Distribution Statistics:
  Number of statistic hours kept: 2
  Number of statistic distribution buckets kept: 1
  Statistic distribution interval (milliseconds): 20
Enhanced History:
History Statistics:
  Number of history Lives kept: 0
  Number of history Buckets kept: 15
  History Filter Type: None
```

```
R1# show ip sla statistics
IPSLAs Latest Operation Statistics
```

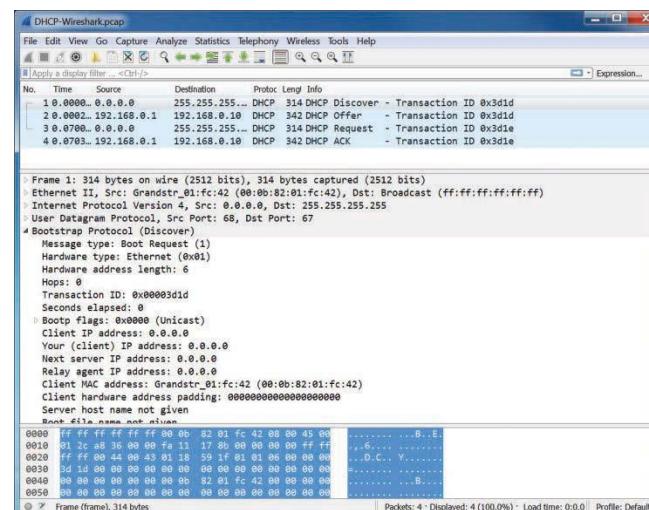
```
IPSLA operation id: 1
  Latest RTT: 12 milliseconds
  Latest operation start time: 00:12:31 UTC Wed Jan 27 2016
  Latest operation return code: OK
  Number of successes: 57
  Number of failures: 0
  Operation time to live: Forever
```



Troubleshooting Scenarios

Troubleshooting Tools

- Common software troubleshooting tools include:
 - Network Management System Tools** include device-level monitoring, configuration, and fault-management tools. These tools can be used to investigate and correct network problems.
 - Knowledge Bases** from device vendors, combined with Internet search engines like Google, are used by network administrators to access a vast pool of experience-based information.
 - Tools & Resources** at <http://www.cisco.com> provide information on Cisco-related hardware and software.
 - Baselining Tools** can draw network diagrams, help keep network software and hardware documentation up-to-date, and help to cost-effectively measure baseline network bandwidth use.
 - Protocol Analyzers** are useful to investigate packet content while flowing through the network, e.g Wireshark.





Troubleshooting Scenarios

Troubleshooting Tools

- Common hardware troubleshooting tools include:
 - **Digital Multimeters** are test instruments that are used to directly measure electrical values of voltage, current, and resistance.
 - **Cable Testers** are specialized, handheld devices designed for testing the various types of data communication cabling. These devices send signals along the cable and wait for them to be reflected. The time between sending the signal and receiving it back is converted into a distance measurement.
 - **Cable Analyzers** are multifunctional handheld devices that are used to test and certify copper and fiber cables for different services and standards.
 - **Portable Network Analyzers** can be plugged in anywhere in the network and used for troubleshooting.
 - **Network Analysis Module** can capture and decode packets and track response times to pinpoint an application problem to a particular network or server.



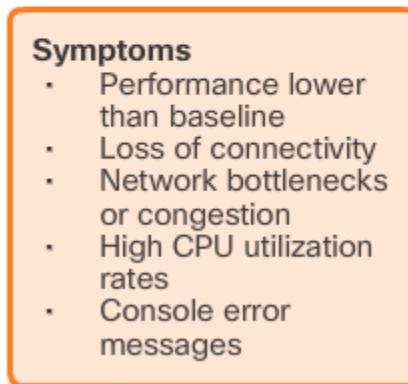


Troubleshooting Scenarios

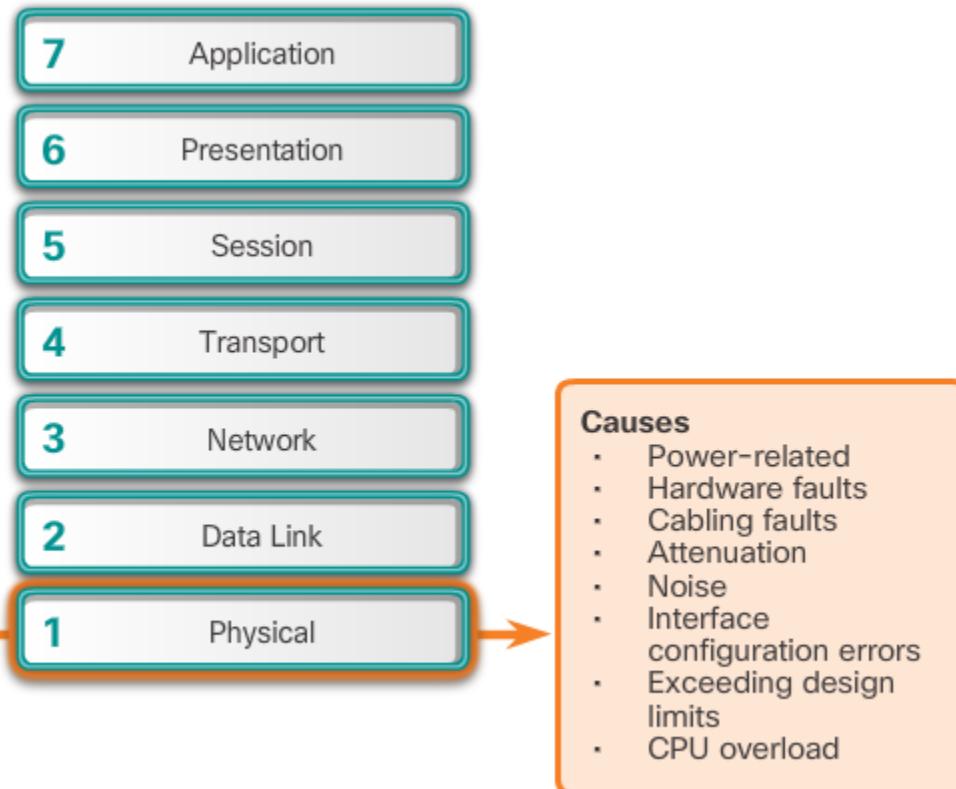
Symptoms and Causes of Network Troubleshooting

Note: A layered approach helps isolate, understand and solve network problems.

There are characteristic physical layer, data link layer, network layer, transport layer, and application layer symptoms and problems that the network administrator should be aware of.



Physical Layer Troubleshooting



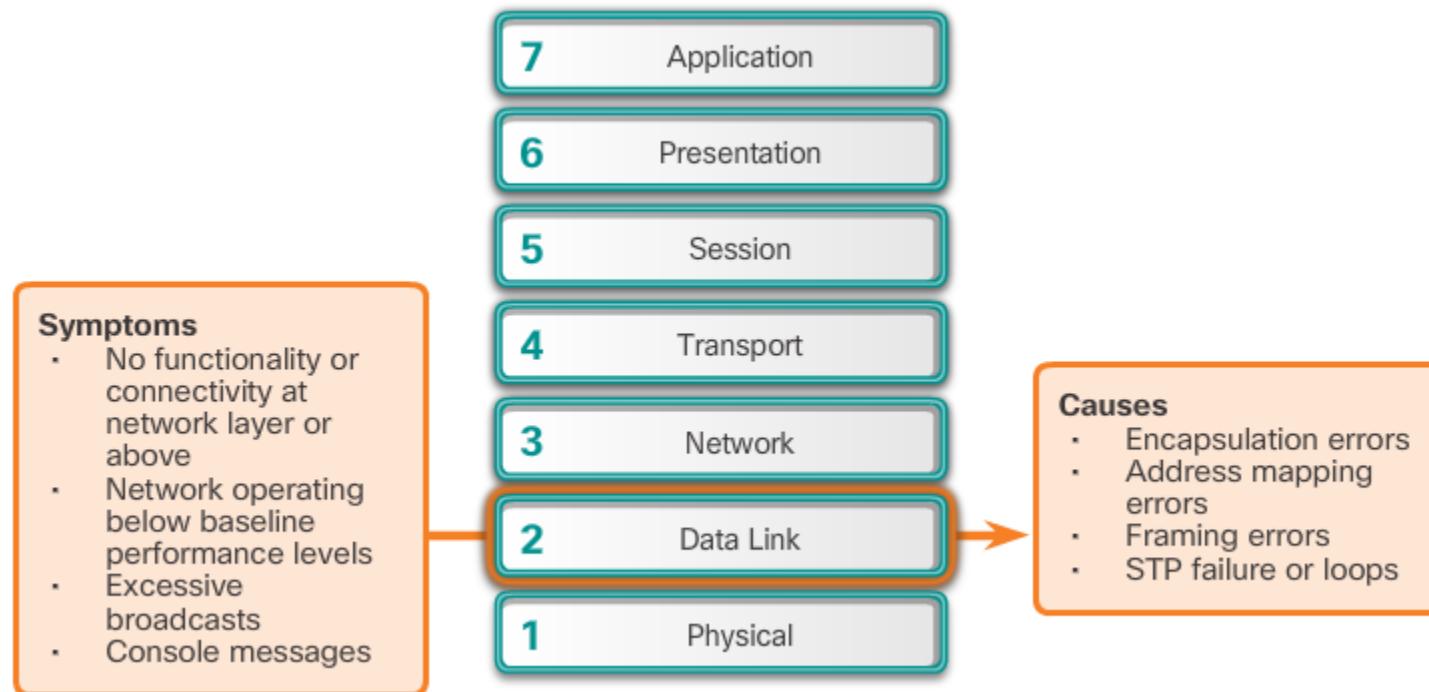
Physical Layer Symptoms and Causes



Troubleshooting Scenarios

Symptoms and Causes of Network Troubleshooting

Data Link Layer Troubleshooting



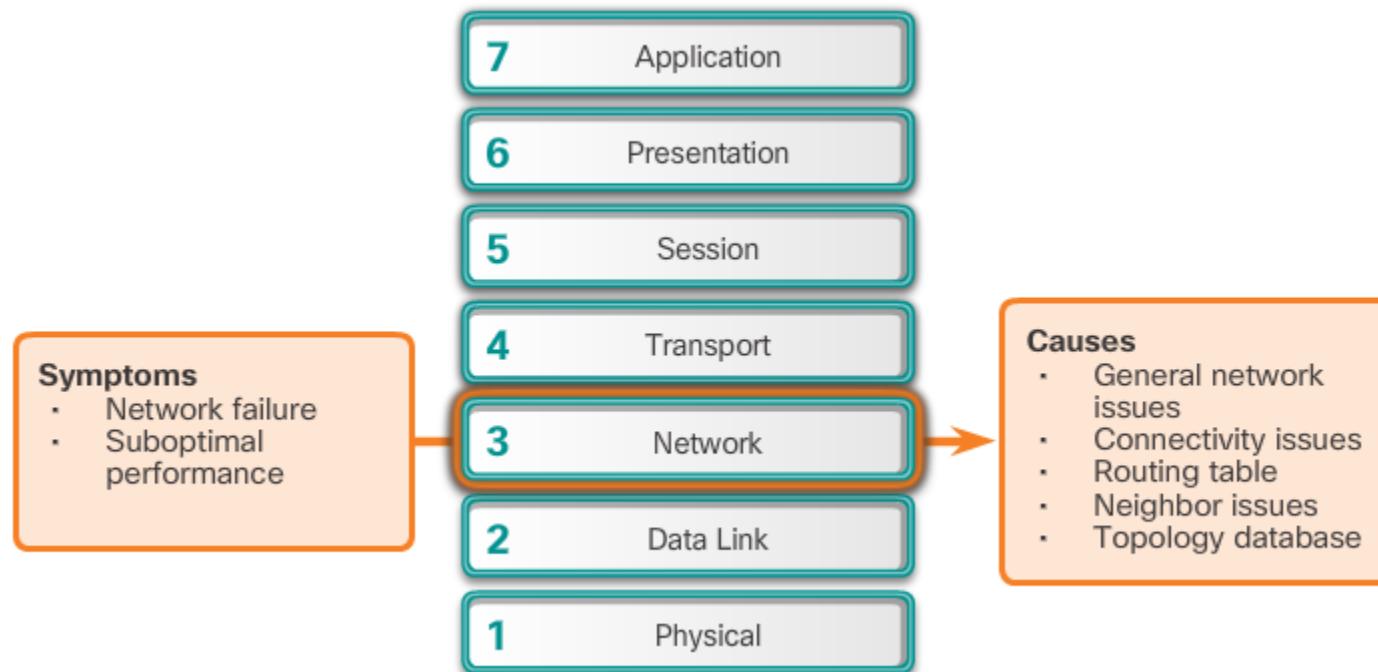
Data Link Layer Symptoms and Causes



Troubleshooting Scenarios

Symptoms and Causes of Network Troubleshooting

Network Layer Troubleshooting



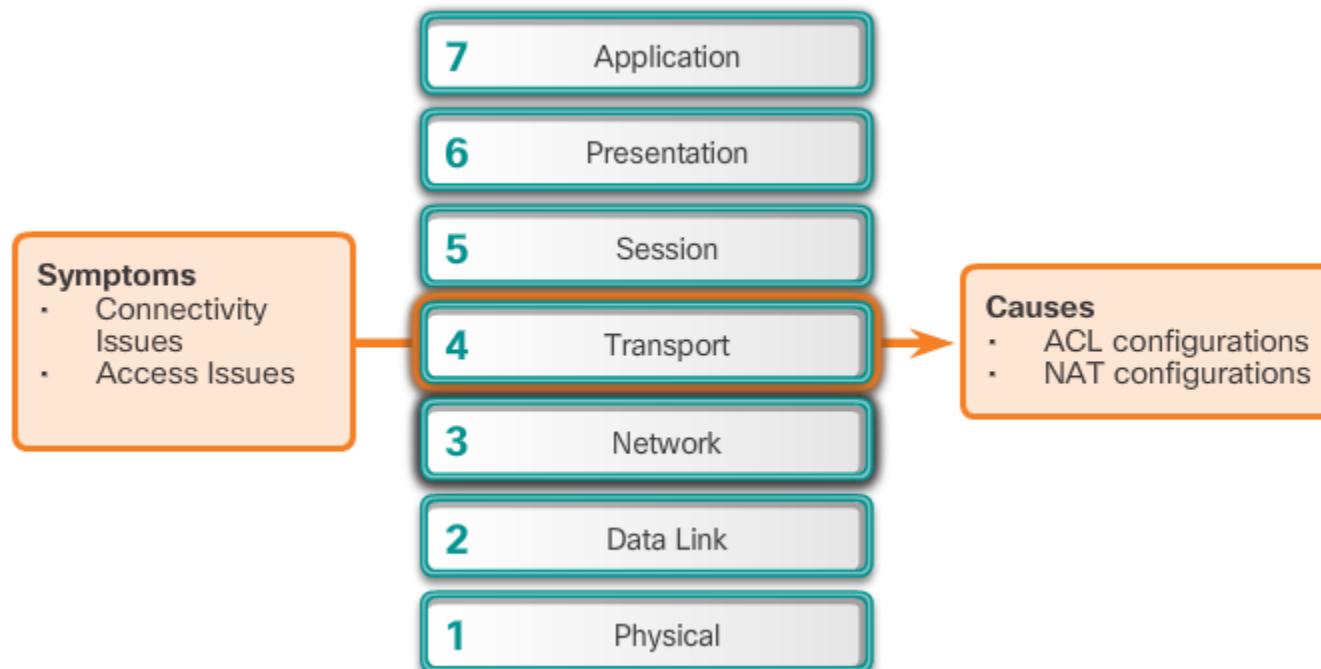
Network Layer Symptoms and Causes



Troubleshooting Scenarios

Symptoms and Causes of Network Troubleshooting

Transport Layer Troubleshooting



Network Layer Symptoms and Causes



Troubleshooting Scenarios

Symptoms and Causes of Network Troubleshooting

Application Layer Troubleshooting

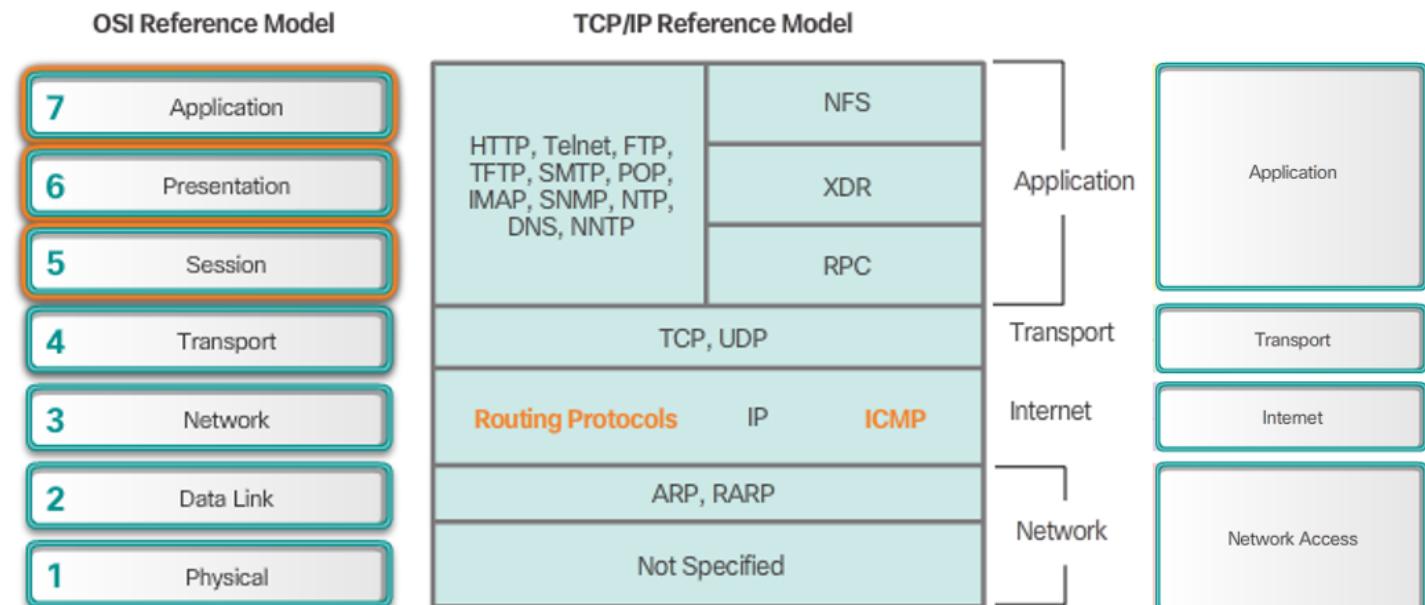
Most of the application layer protocols provide user services.

The types of symptoms and causes depend upon the actual application itself.



Application Layer

Assuming physical, data link, network, and transport layers working...

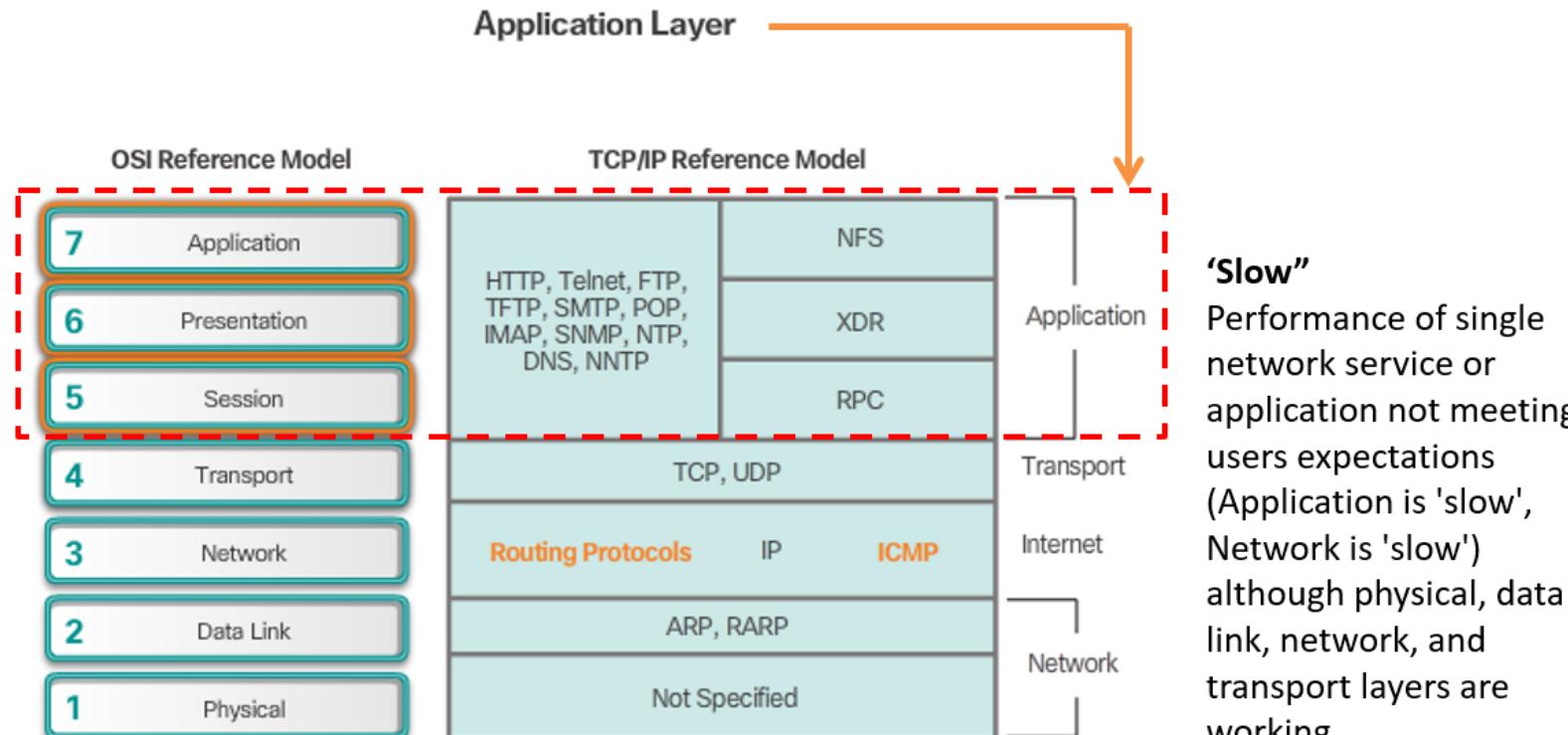




Troubleshooting Scenarios

Symptoms and Causes of Network Troubleshooting

Application Layer Troubleshooting

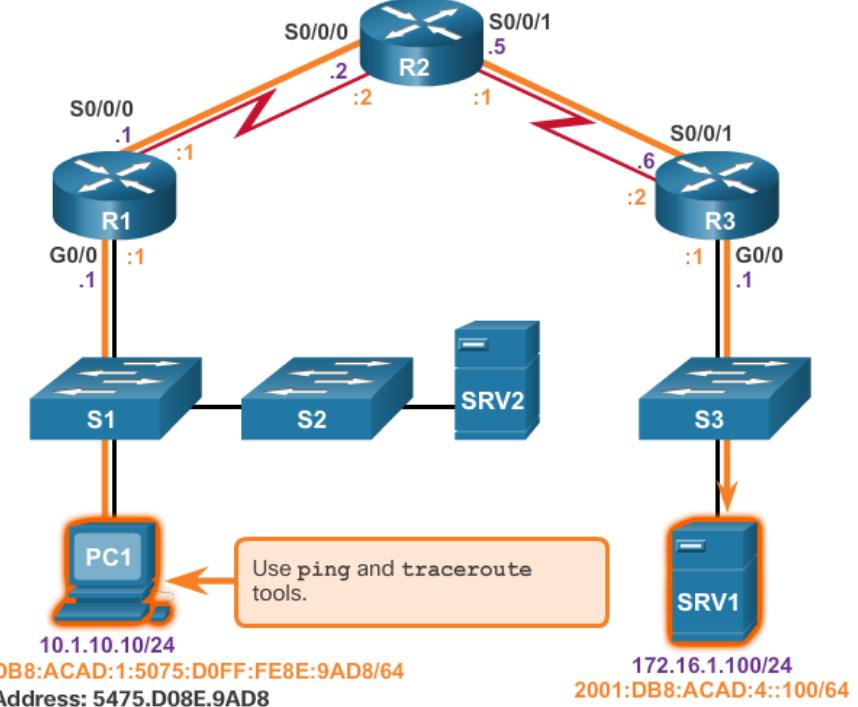




Troubleshooting Scenarios

Troubleshooting IP Connectivity

- Common bottom-up troubleshooting steps for **end-to-end** connectivity:
 - **Step 1.** Check physical connectivity
 - **Step 2.** Check for duplex mismatches.
 - **Step 3.** Check data link and network layer addressing.
 - **Step 4.** Verify that the default gateway is correct.
 - **Step 5.** Ensure that devices are determining the correct path from the source to the destination.
 - **Step 6.** Verify the transport layer is functioning properly.
 - **Step 7.** Verify that there are no ACLs blocking traffic.
 - **Step 8.** Ensure that DNS settings are correct.





Troubleshooting Scenarios

Troubleshooting IP Connectivity

- Common bottom-up troubleshooting steps for **end-to-end** connectivity:
 - **Step 1.** Check physical connectivity at the point where network communication stops. Faulty cable, interface, misconfigured/faulty hardware?
 - **Step 2.** Check for duplex mismatches. Does duplex mode match between both ends of Ethernet link?
 - **Step 3.** Check data link and network layer addressing on local network. IPv4 ARP tables, IPv6 neighbor tables, MAC address tables, VLAN assignments?
 - **Step 4.** Verify that the default gateway is correct. No access beyond local network otherwise.
 - **Step 5.** Ensure that devices are determining the correct path from the source to the destination. Is routing information correct?
 - **Step 6.** Verify the transport layer is functioning properly. Can use Telnet to test transport layer connections, but use SSH for remote config & management.
 - **Step 7.** Verify that there are no ACLs blocking traffic.
 - **Step 8.** Ensure that DNS settings are correct. DNS server accessible?



Troubleshooting Scenarios

Troubleshooting IP Connectivity

- **ping and traceroute**

- **ping**

- Uses ICMP Layer 3 protocol that is a part of the TCP/IP suite
- Uses the ICMP echo request and ICMP echo reply packets.
- Host at a specified address receives the ICMP echo request, responds with an ICMP echo reply packet.
- Ping can be used to verify end-to-end connectivity for both IPv4 and IPv6.

```
PC1> ping 172.16.1.100

Pinging 172.16.1.100 with 32 bytes of data:
Reply from 172.16.1.100: bytes=32 time=8ms TTL=254
Reply from 172.16.1.100: bytes=32 time=1ms TTL=254
Reply from 172.16.1.100: bytes=32 time=1ms TTL=254
Reply from 172.16.1.100: bytes=32 time=1ms TTL=254

Ping statistics for 172.16.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round-trip times in milliseconds:
    Minimum = 1ms, Maximum = 8ms, Average = 2ms
```



Troubleshooting Scenarios

Troubleshooting IP Connectivity

- **ping and traceroute**

- **traceroute (or tracert in Windows OS)**

- Generates a list of hops, router IP addresses, and the final destination IP address that are successfully reached along the path.
- List provides important verification and troubleshooting information.
- If the data reaches the destination, the trace lists the interface on every router in the path.
- If the data fails at some hop along the way, the address of the last router that responded to the trace is known.
- This address is an indication of where the problem or security restrictions reside.

```
C:\Windows\system32> tracert 172.16.1.100

Tracing route to 172.16.1.100 over a maximum of 30 hops

 1  1 ms    <1 ms    <1 ms      10.1.10.1
 2  2 ms    2 ms     1 ms      192.168.1.2
 3  2 ms    2 ms     1 ms      192.168.1.6
 4  2 ms    2 ms     1 ms      172.16.1.100

Trace complete.
```



8.3 Chapter Summary



Cisco | Networking Academy®
Mind Wide Open™



Chapter Summary

Summary

- For network administrators to be able to monitor and troubleshoot a network, they must have a complete set of accurate and current network documentation, including configuration files, physical and logical topology diagrams, and a baseline performance level.
- The three major stages to troubleshooting problems are gather symptoms, isolate the problem, then correct the problem.
- The OSI model or the TCP/IP model can be applied to a network problem. A network administrator can use the bottom-up method, the top-down method, or the divide-and-conquer method.
- Common software tools that can help with troubleshooting include network management system tools, knowledge bases, baselining tools, host-based protocol analyzers, and Cisco IOS EPC. (embedded packet capture)
- Hardware troubleshooting tools include a NAM, digital multimeters, cable testers, cable analyzers, and portable network analyzers. Cisco IOS log information can also be used to identify potential problems.
- There are characteristic physical layer, data link layer, network layer, transport layer, and application layer symptoms and problems of which the network administrator should be aware. The administrator may need to pay particular attention to physical connectivity, default gateways, MAC address tables, NAT, and routing information.



Reminder

Lab on Friday

- The lab work from now on will be ‘gearing up’ towards the Skills Based Assessment (SBA)
- You will get a chance in Friday’s Lab to do a set of activities to help you revise most of the following:
 - ~~Configuring OSPF~~ – done last Friday 13/11/20
 - ~~Configuring PPP and Authentication (PAP and CHAP)~~ – done last Friday 13/11/20
 - ~~Configuring VPNs and GRE Tunnels~~ – done last Friday 13/11/20
 - Configuring SNMP
 - Configuring BGP
 - Configuring Standard and Extended ACLs
 - etc...
- You should ensure you have mastered the above skills.





Chapter 8 Network Trouble Shooting

Here are all the Layered Model Diagrams in the one place with the Symptoms and Cause of Network Problems included.

D. Carroll, School of Computer Science, DIT Kevin Street.

8.1.3 Isolating the Issue Using Layered Models

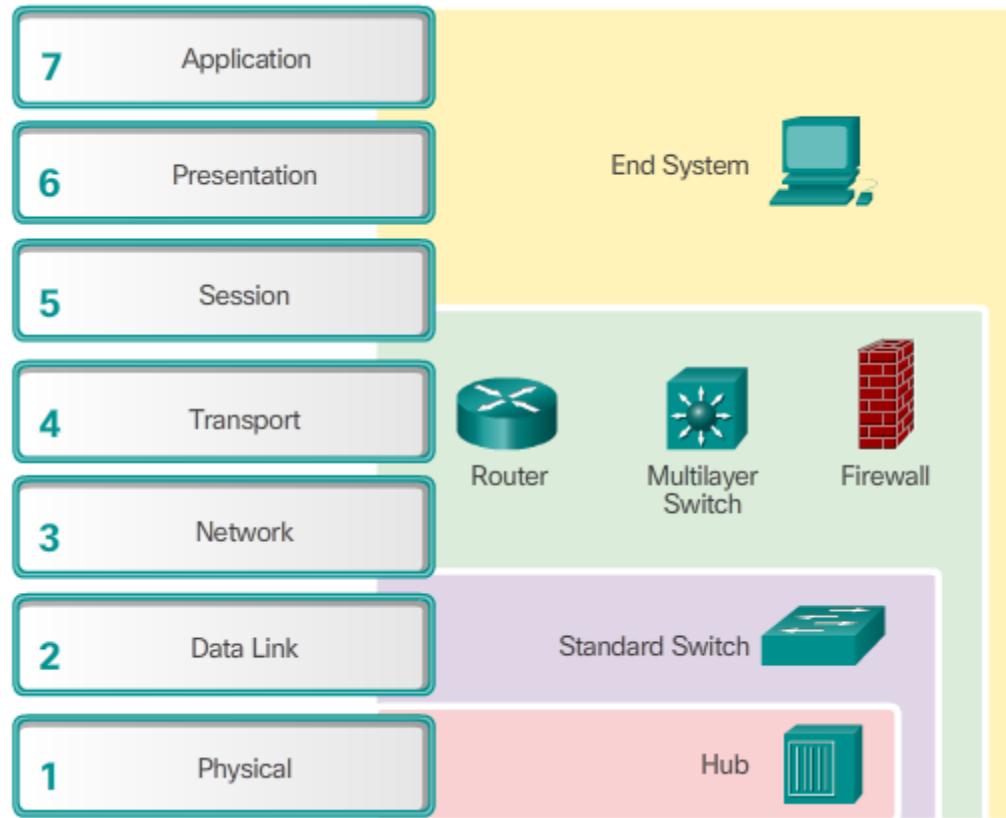
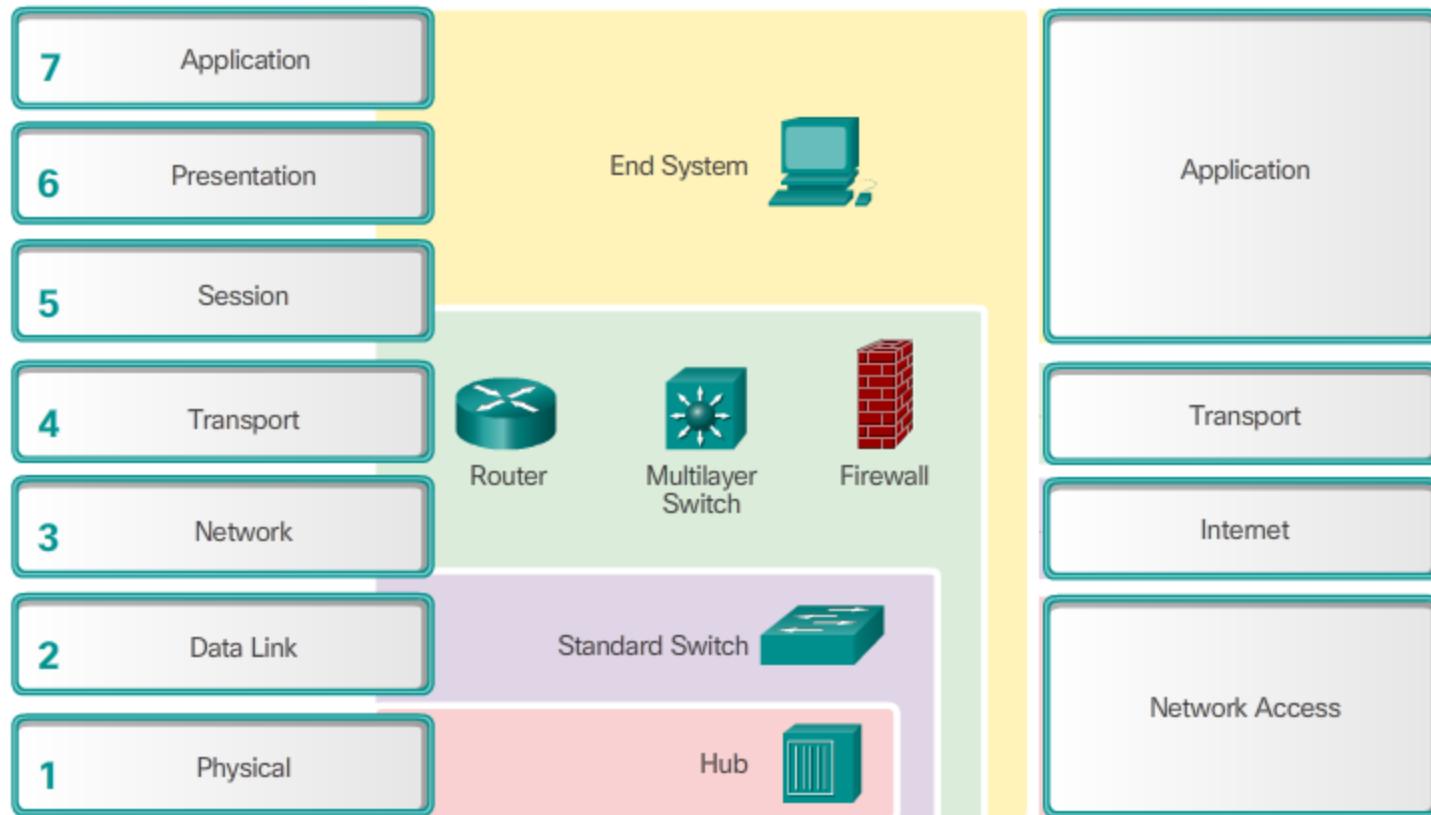


Fig 8-7 (Modified) OSI Reference Model

8.1.3 Isolating the Issue Using Layered Models



8.1.3 Isolating the Issue Using Layered Models

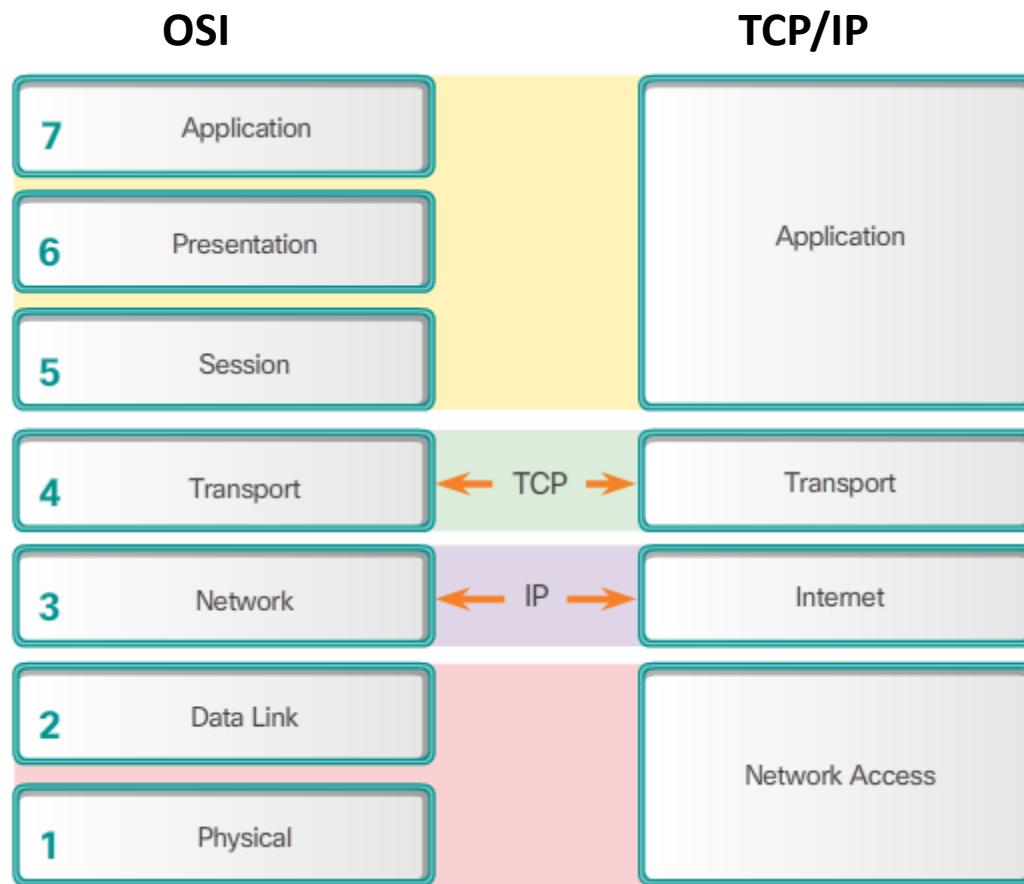
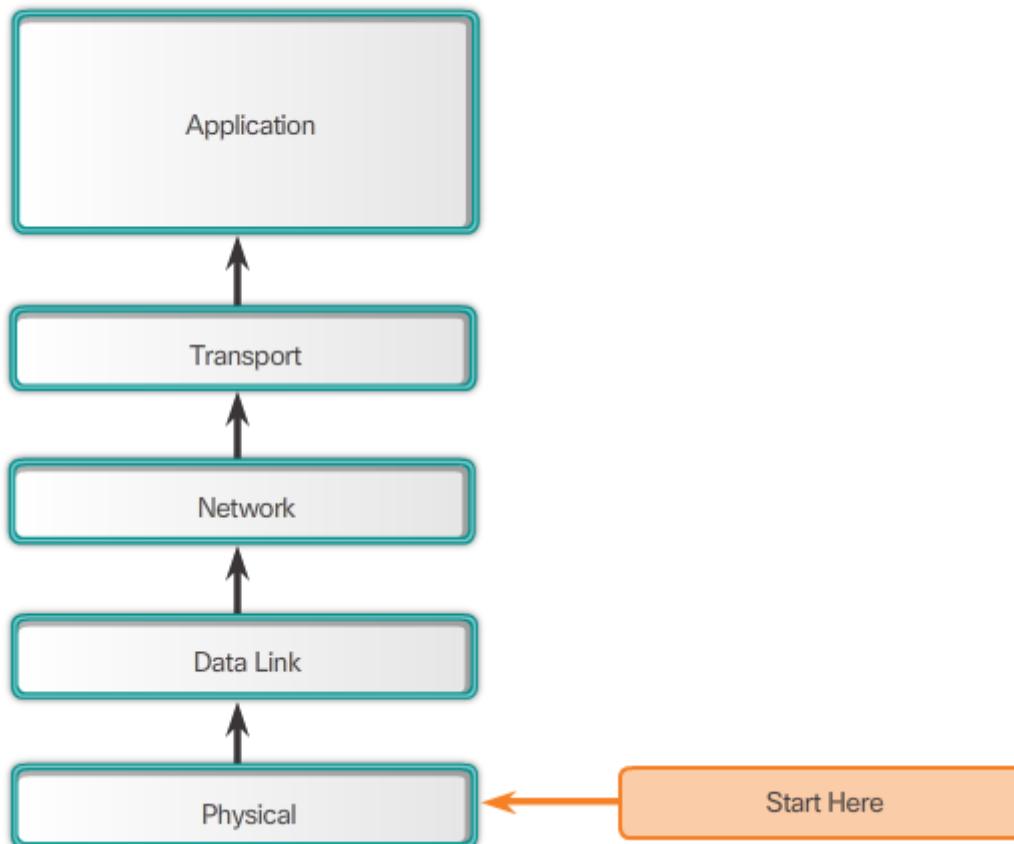


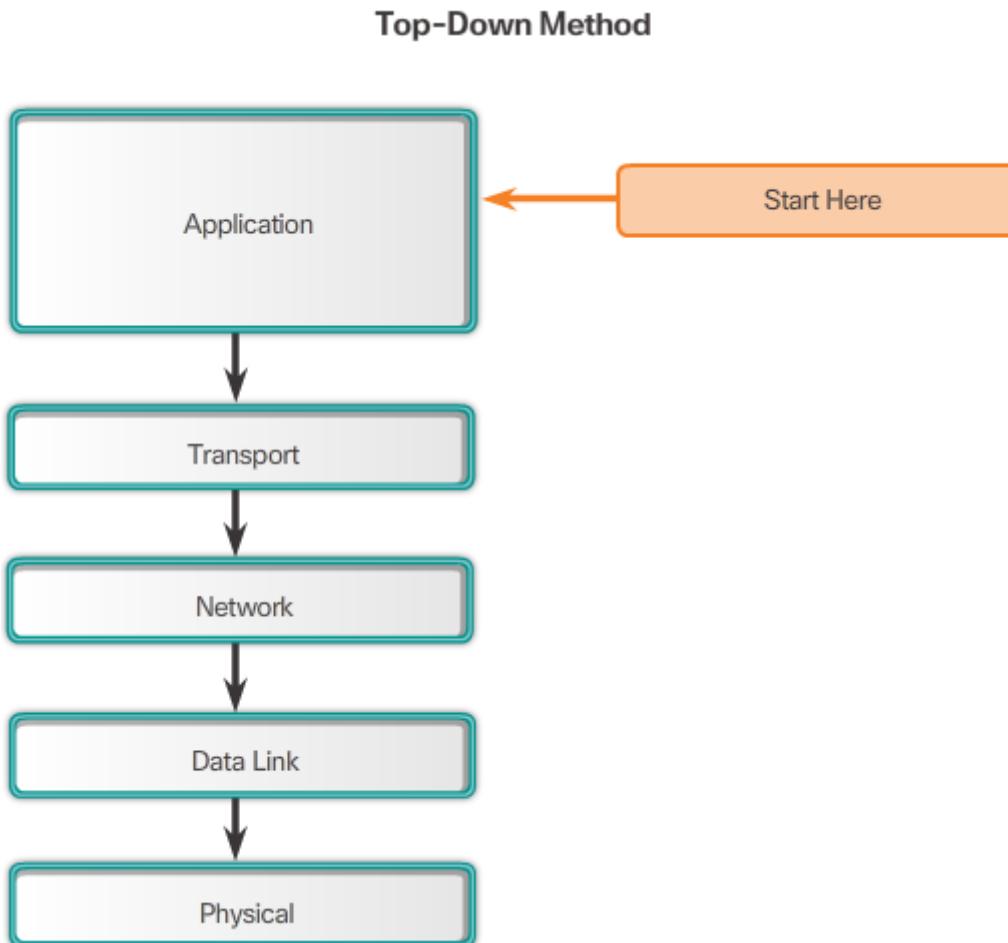
Fig 8-8 Comparing OSI Model and TCP/IP Model

8.1.3 Isolating the Issue Using Layered Models

Bottom-Up Method

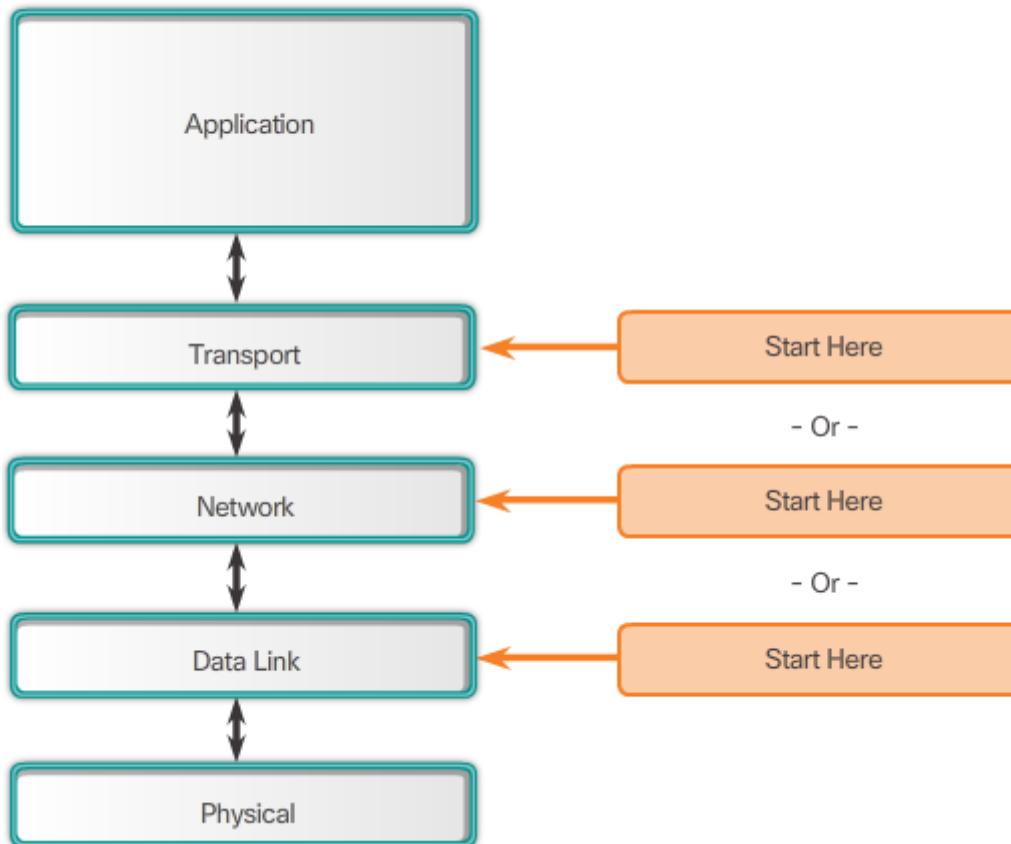


8.1.3 Isolating the Issue Using Layered Models



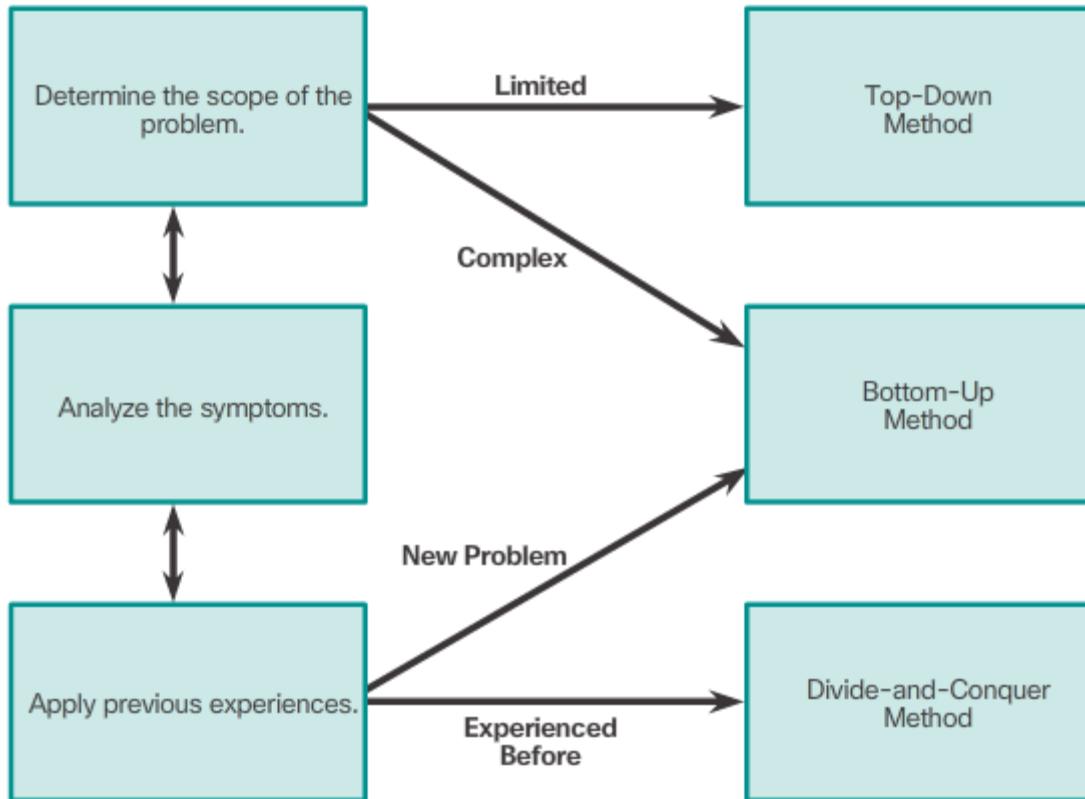
8.1.3 Isolating the Issue Using Layered Models

Divide-And-Conquer Method



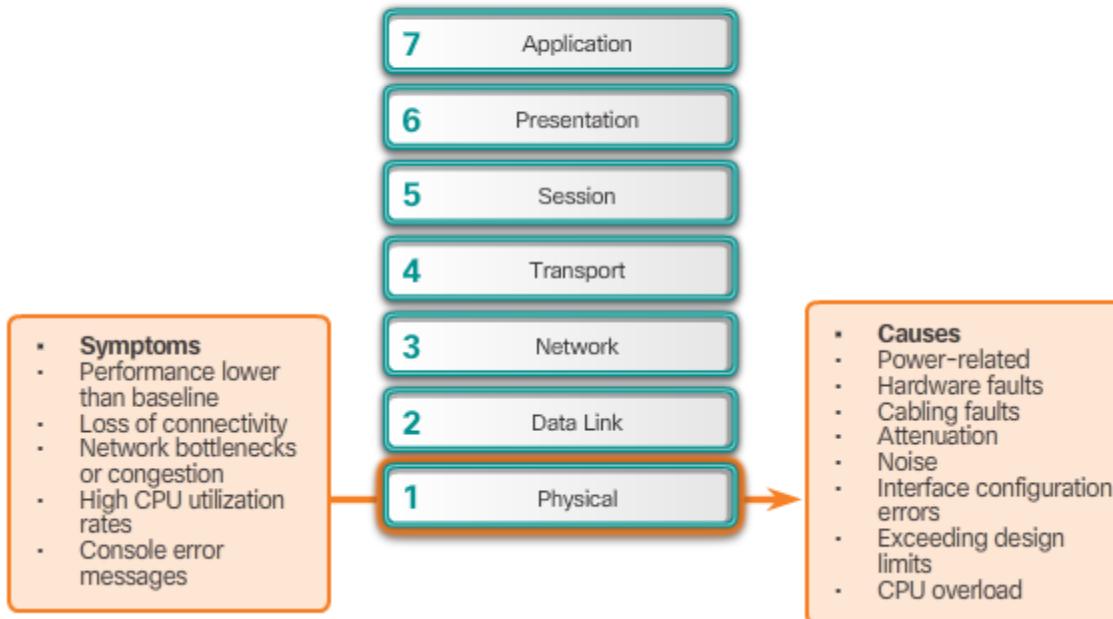
8.1.3 Isolating the Issue Using Layered Models

Guidelines for Selecting a Troubleshooting Method



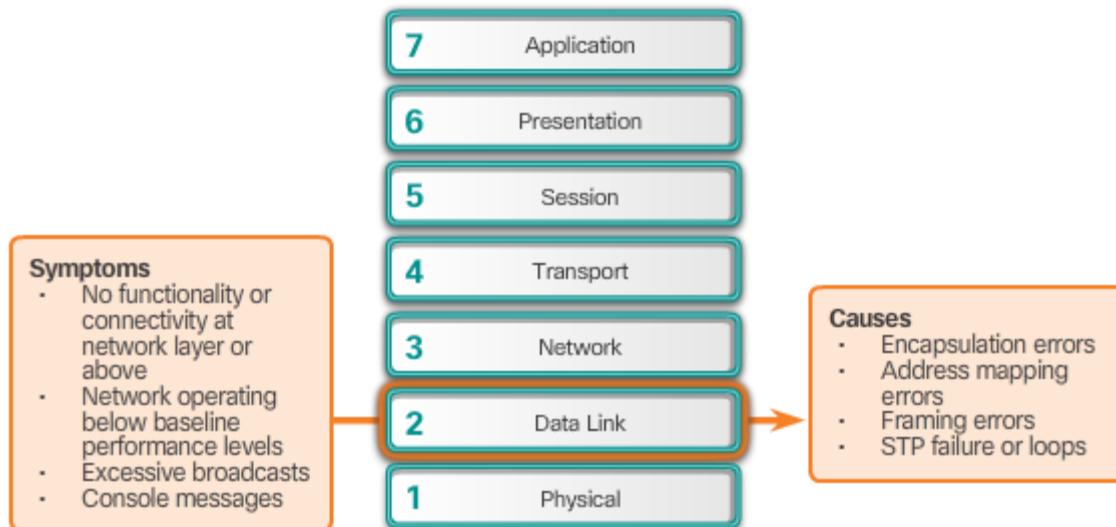
8.2.3 Symptoms and Causes of Network Troubleshooting

Physical Layer Symptoms and Causes



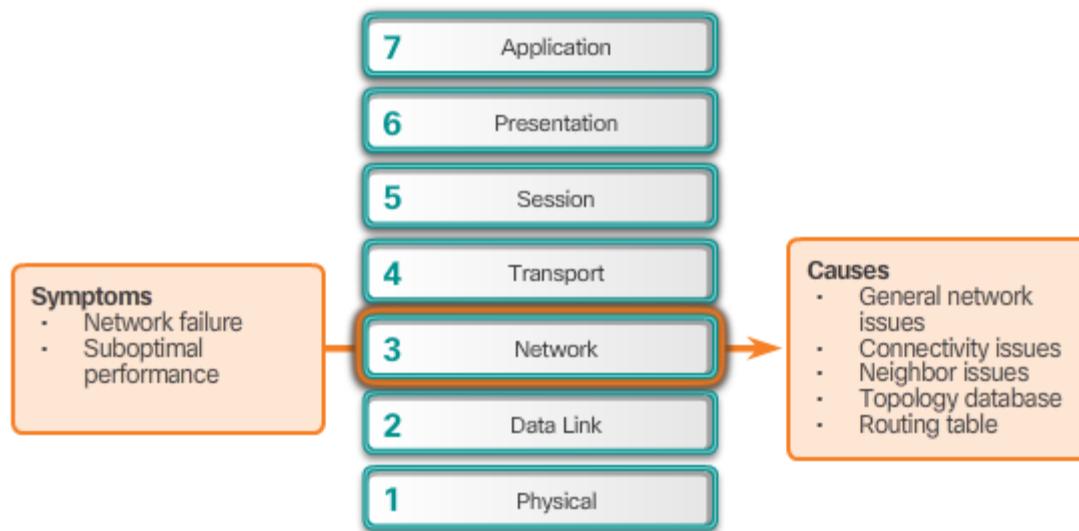
8.2.3 Symptoms and Causes of Network Troubleshooting

Data Link Layer Symptoms and Causes



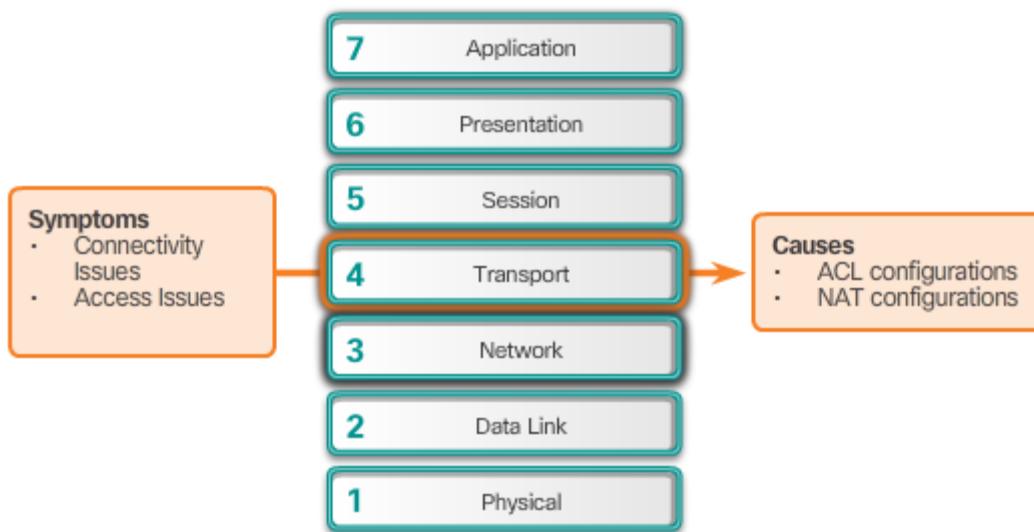
8.2.3 Symptoms and Causes of Network Troubleshooting

Network Layer Symptoms and Causes



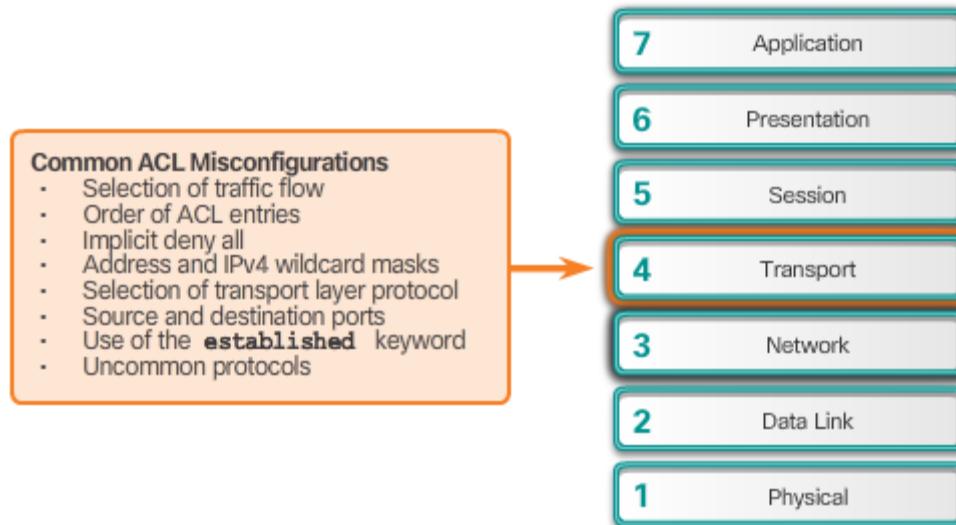
8.2.3 Symptoms and Causes of Network Troubleshooting

Transport Layer Symptoms and Causes



8.2.3 Symptoms and Causes of Network Troubleshooting

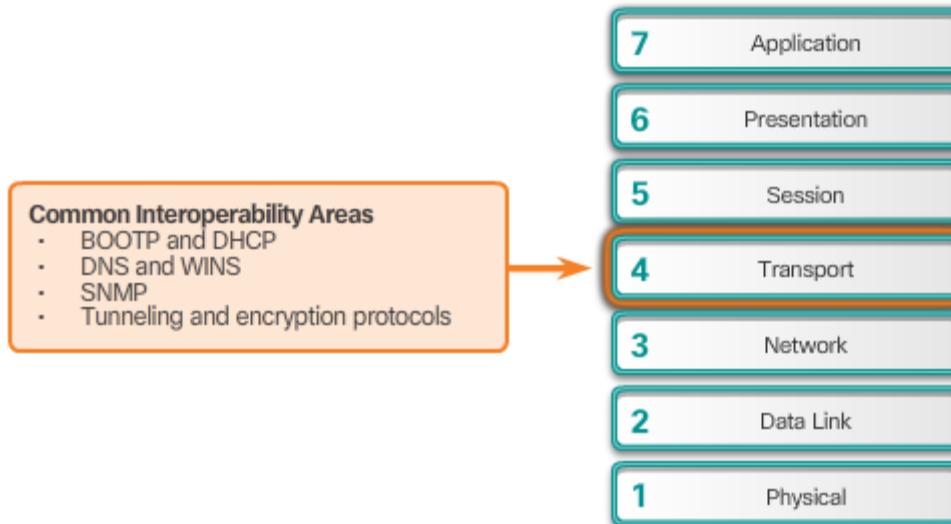
Common ACL Misconfigurations



Transport Layer: ACL- Problems

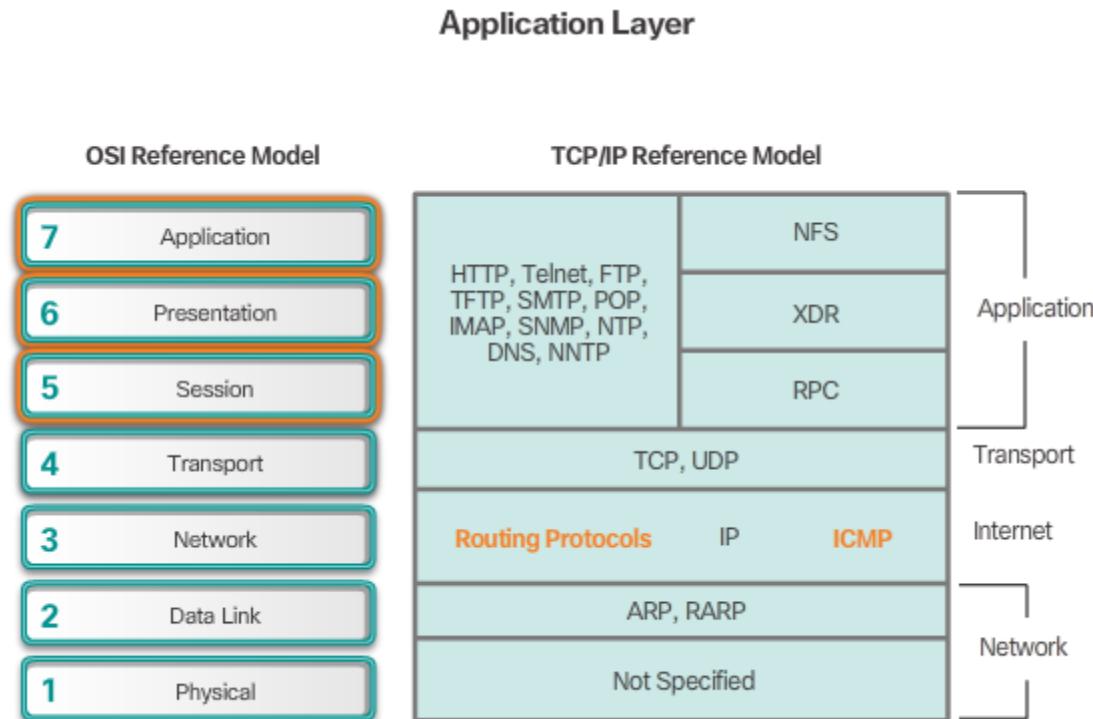
8.2.3 Symptoms and Causes of Network Troubleshooting

Common Interoperability Areas with NAT



Transport Layer: NAT for IPv4- Problems

8.2.3 Symptoms and Causes of Network Troubleshooting



8.2.3 Symptoms and Causes of Network Troubleshooting

Most of the application layer protocols provide user services.

The types of symptoms and causes depend upon the actual application itself.

Symptoms

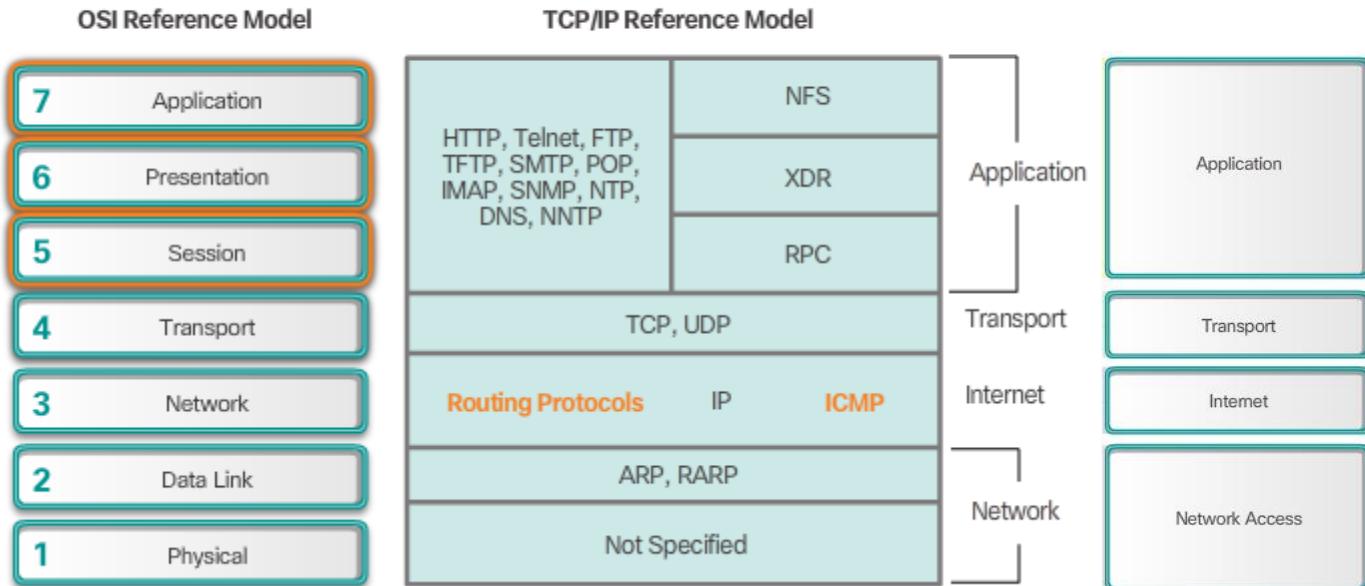
- * Applications can't provide data
- * Application data transfer 'low'
- * Application nwk svcs requests slow

Cause

- * Could be anything at Application Layer ...Application settings etc.

Application Layer

Assuming physical, data link, network, and transport layers working...



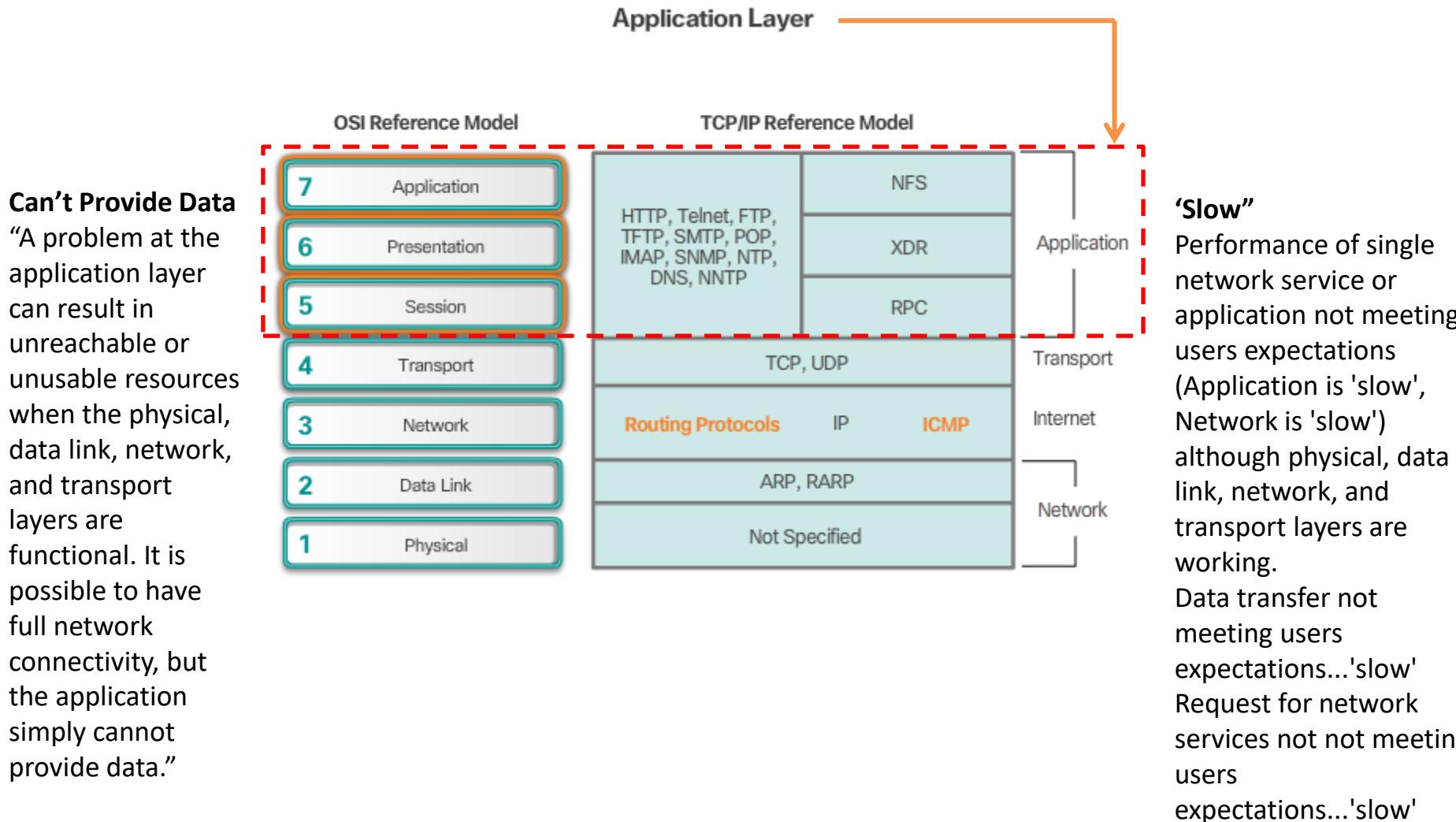
8.2.3 Symptoms and Causes of Network Troubleshooting

Most of the application layer protocols provide user services.

The types of symptoms and causes depend upon the actual application itself.

Problem at Application layer can result in...

- Applications can't provide Data... physical, data link, network, and transport layers working
- Application is 'slow' ... physical, data link, network, and transport layers working



9.2.2 Symptoms and Causes of Network Troubleshooting

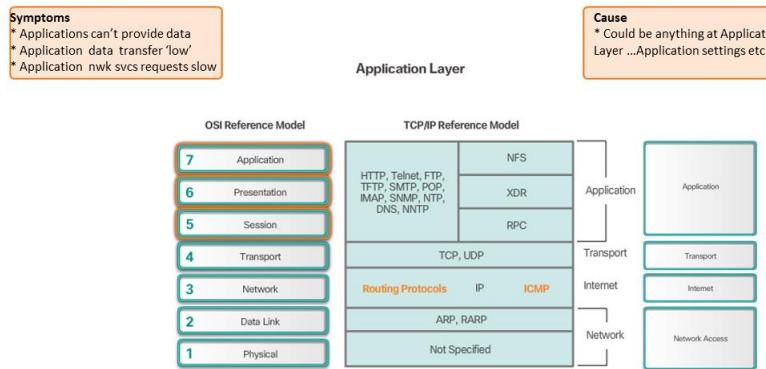


Fig 8-32, p. 397, (modified)

Common ACL Misconfigurations

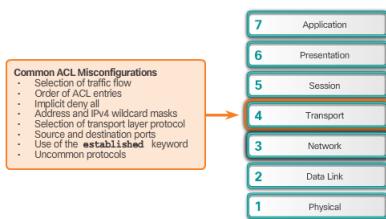


Fig 8-30, p. 394

Common Interoperability Areas with NAT

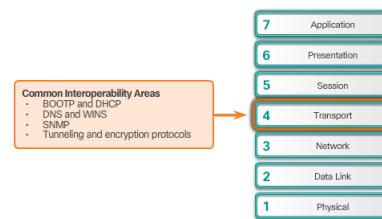


Fig 8-31, p. 396

Physical Layer Symptoms and Causes

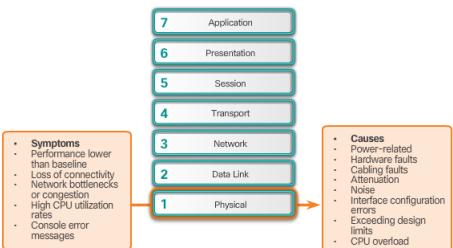


Fig 8-26, p. 388

Data Link Layer Symptoms and Causes

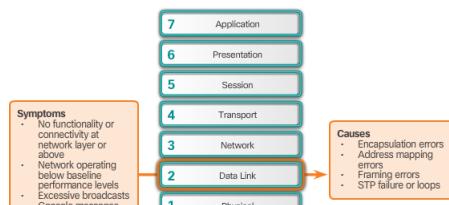


Fig 8-27, p. 390

Network Layer Symptoms and Causes

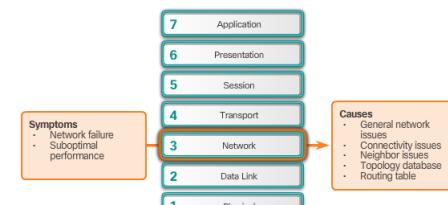


Fig 8-28, p. 392

Transport Layer Symptoms and Causes

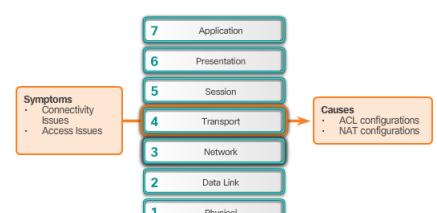


Fig 8-29, p. 394



WAN Technology– Revision 1



Connecting Networks

Cisco | Networking Academy®
Mind Wide Open™



Chapter 1 - Sections & Objectives

- 1.1 WAN Technologies Overview
 - Explain WAN access technologies available to small to medium-sized business networks.
- 1.2 Selecting a WAN Technology
 - Select WAN access technologies to satisfy business requirements.
- Contextual Examples
 - Choosing a WAN Link connection
 - Using VPNs to support WAN infrastructure



1.1 WAN Technologies Overview



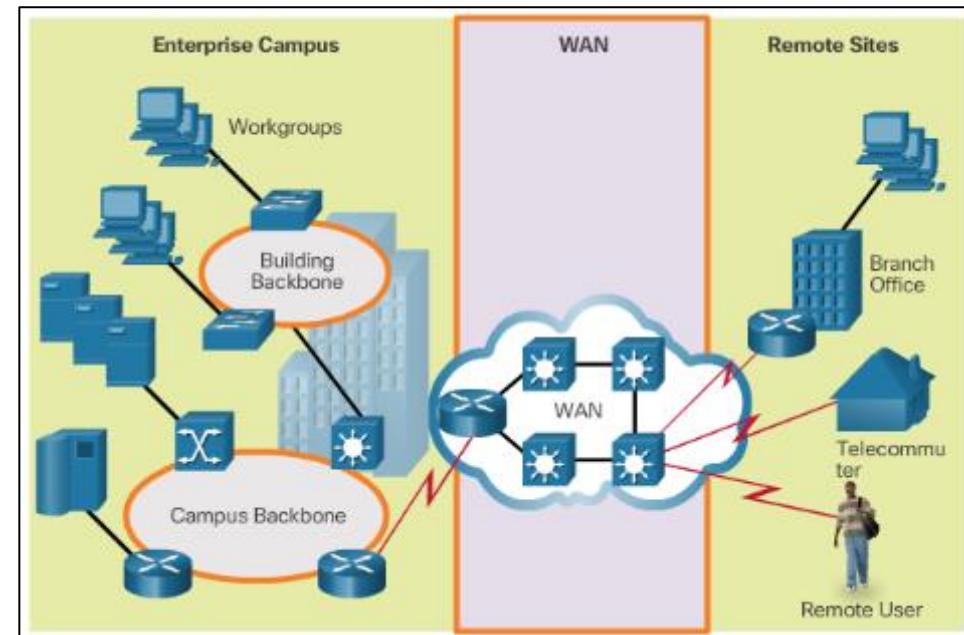
Cisco | Networking Academy®
Mind Wide Open™



WAN Technologies Overview

Purpose of WANs *

- WANs connect LANs
- WANs are used to **connect remote geographically separate sites to the enterprise network.**
 - e.g. connect remote branch offices to main enterprise network.
 - Support business communications requirements
- WANs connect home users to the Internet.
- Enterprise networks are using security and privacy solutions over the Internet to connect remote sites and users.





WAN Technologies Overview

Purpose of WANs *

- Supporting business communications requirements *
- As an organization expands it needs to **communicate and share data between geographically separate sites.**
- A **WAN interconnects local LANs to remote LANs** in branch sites and telecommuter sites.
- A WAN allows an organization to **share business information** with customers, business partners and employees that are **geographically dispersed** including teleworkers and those traveling on company business.



WAN Technologies Overview

Purpose of WANs *

- Common WAN topologies (advantages/disadvantages):: *

- Point-to-Point**

- Point-to-point circuit between two endpoints
- Usually dedicated leased-line (T1/E1)
- Expensive

- Hub-and-Spoke**

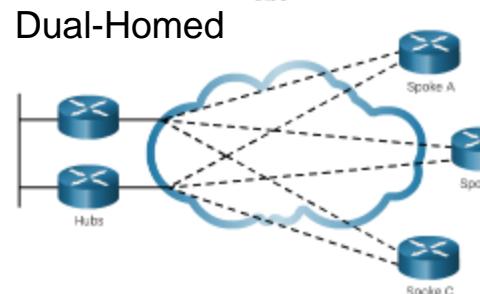
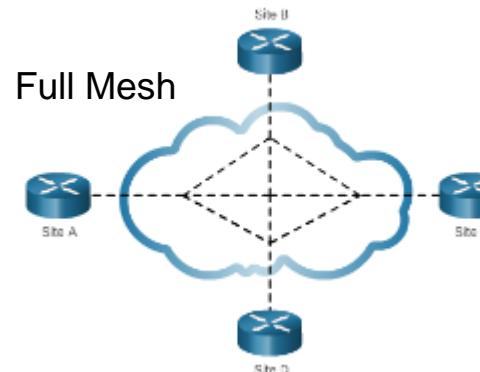
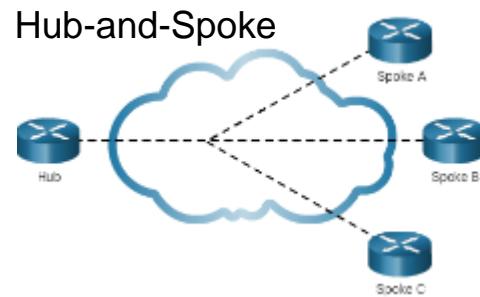
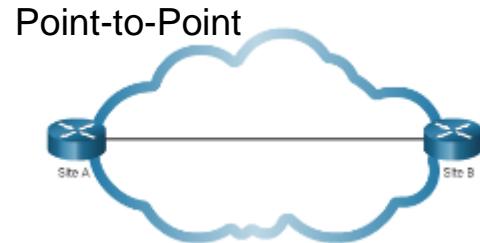
- A single-homed, point-to-multipoint topology
- Allows connection between multiple sites
- All spoke circuits share a single interface to the hub via virtual interfaces. All traffic goes through the hub
- Hub could be **single point of failure**

- Full Mesh**

- Each router has a connection to every other router; requires a **large number of virtual interfaces**
- Full mesh requires **a lot of maintenance** to configure virtual interfaces

- Dual-homed**

- Provides **redundancy** for a single-homed, hub-and-spoke topology by providing a second hub to connect to spoke routers
- Dual homed are more **expensive** and more **complex**.

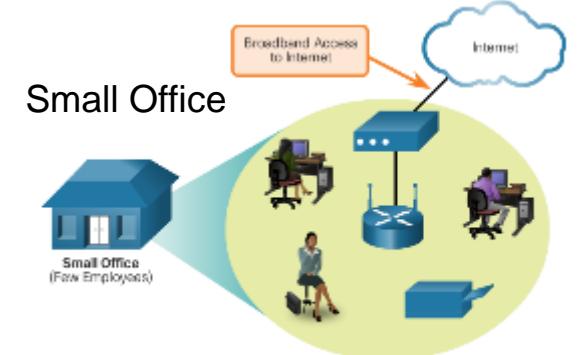




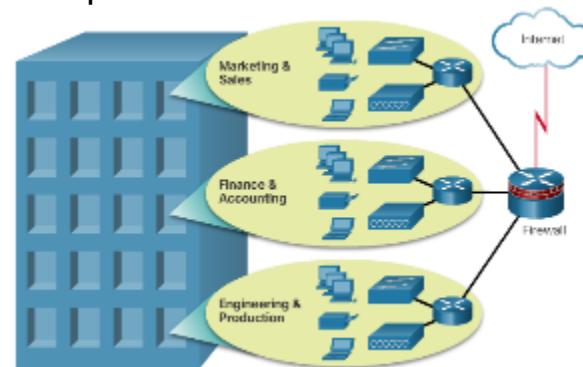
WAN Technologies Overview

Purpose of WANs

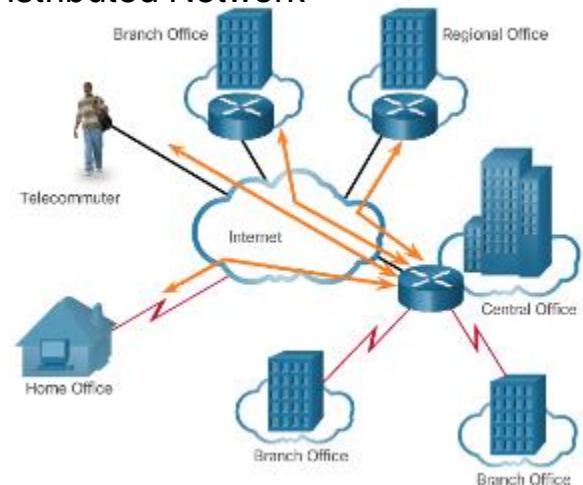
- As businesses grow, the topologies and WAN strategies change:
 - Small Office** – These businesses typically consist of one LAN at one location that connects to the Internet through a broadband technology.
 - Campus Network** – A small- to medium-sized business with one location and multiple LANs uses specialized equipment and technologies to connect to the Internet.
 - Branch Networks** – As the business grows, it adds more branch offices, each with its own campus network. WAN contracts to connect the remote networks are negotiated.
 - Distributed Network** – A multinational business has a network distributed across the globe. These businesses have complex WAN strategies to securely connect to regional offices, branch offices, partners, and telecommuters.



Campus Network



Distributed Network

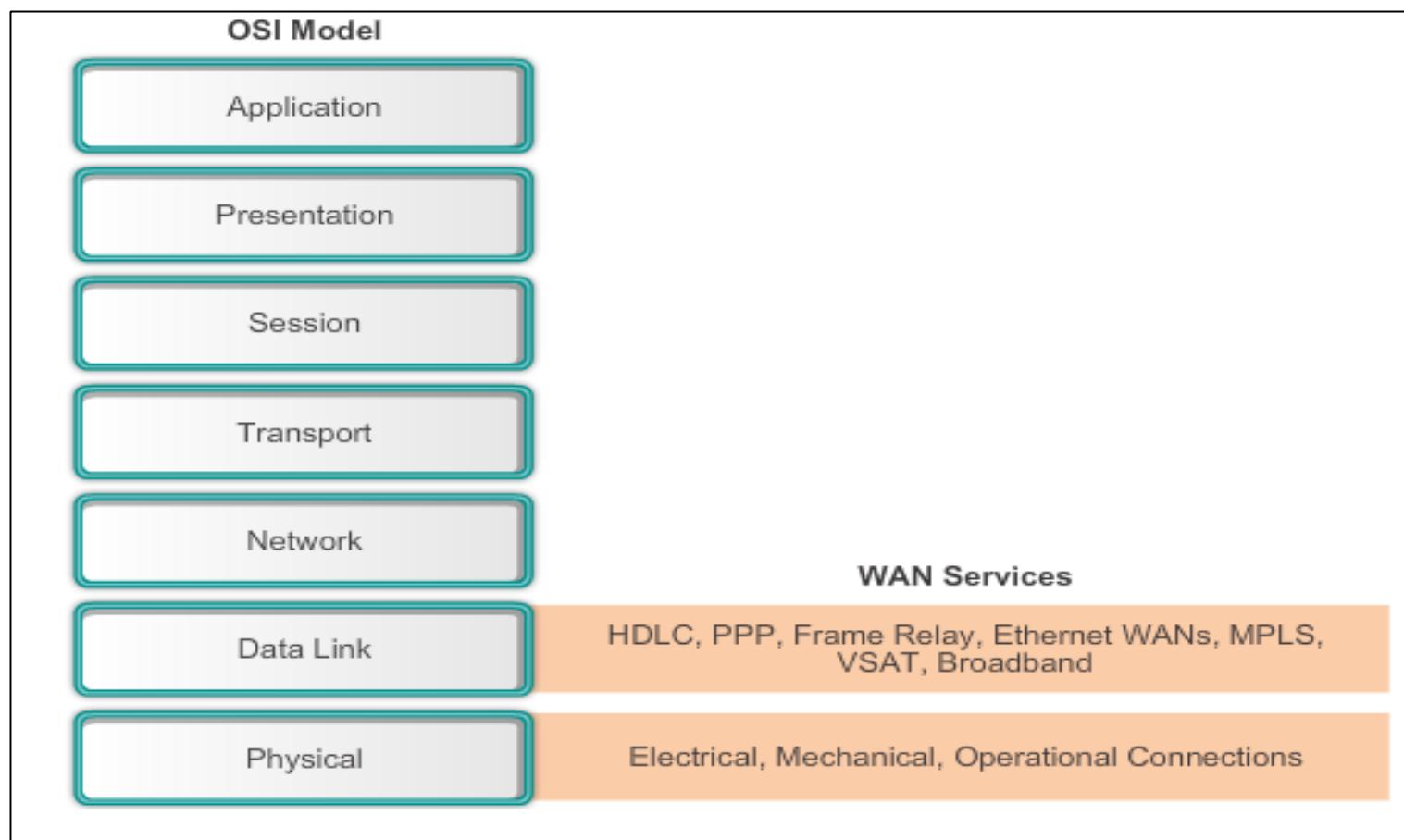




WAN Operations

WANs in the OSI Model

WAN access standards typically describe both **physical** layer delivery methods and **data link** layer requirements, including physical addressing, flow control, and encapsulation.





WAN Operations

WANs in the OSI Model

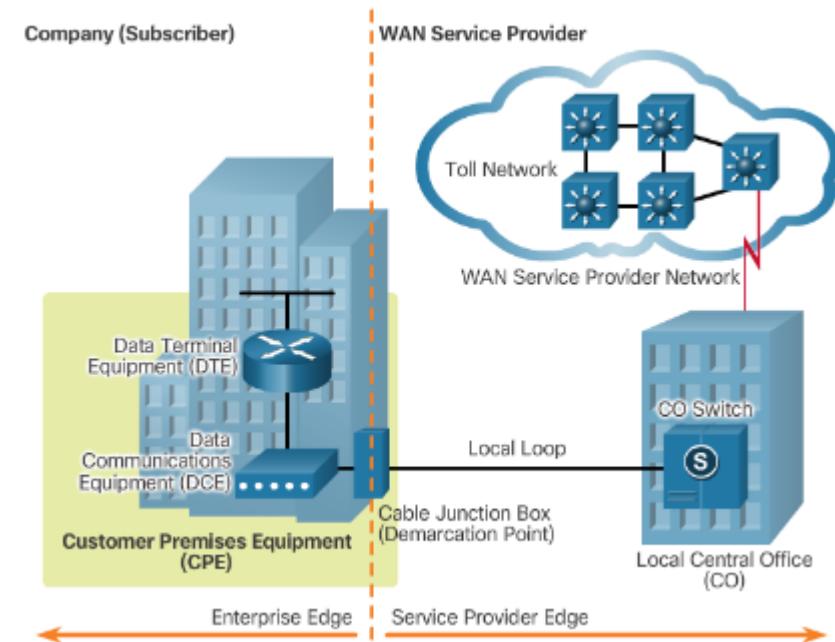
- Layer 1 protocols describe how to provide electrical, mechanical, operational, and functional connections to the services of a communications service provider.
- Layer 2 protocols define how data is **encapsulated** for transmission toward a remote location, and the mechanisms for transferring the resulting frames.
- A variety of different technologies are used, such as the **Point-to-Point Protocol (PPP)**, **Frame Relay**, and **ATM**. Some of these protocols use the same basic framing or a subset of the **High-Level Data Link Control (HDLC)** mechanism.
- Most WAN links are point-to-point. For this reason, the address field in the Layer 2 frame is usually not used (unlike Ethernet).



WAN Technologies Overview

WAN Operations

- WAN operations focus primarily on the physical layer (OSI Layer 1) and the data link layer (OSI Layer 2).
 - Layer 1 protocols describe how to provide electrical, mechanical, operational, and functional connections
 - Layer 2 protocols define how data is encapsulated
- WAN Terms include:
 - **Customer Premises Equipment (CPE)** – owned by the business or leased from the service provider.
 - **Data Communications Equipment (DCE)** – provides an interface to connect subscribers to a communication link on the WAN cloud.
 - **Data Terminal Equipment (DTE)** – connects to the local loop through the DCE.
 - **Demarcation Point** – separates customer equipment from service provider equipment and is the place where the responsibility for the connection changes from the user to the service provider.
 - **Local Loop** – cable that connects the CPE to the CO of the service provider (last mile).
 - **Central Office (CO)** – local service provider facility or building that connects the CPE to the provider network.
 - **Toll network** – all the cabling and equipment inside the WAN provider network.

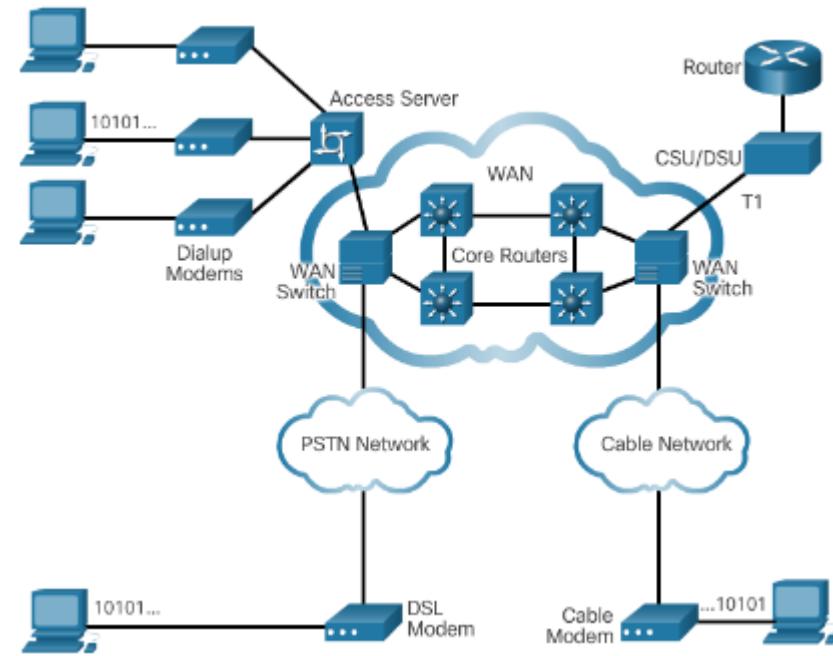




WAN Technologies Overview

WAN Operations

- WAN devices include:
 - **Dialup modem** – legacy WAN technology that converts digital signals into voice frequencies to be transmitted over the analog lines of the public telephone network.
 - **Access server** – legacy WAN technology that coordinates dial-in and dial-out user communications.
 - **Broadband modem** – used with high-speed DSL or cable Internet service
 - **CSU/DSU** – used to convert digital, leased-line signals into frames that the LAN can interpret and vice versa.
 - **WAN switch** – multiport internetworking device used in service provider networks
 - **Router** – provides internetworking and WAN access interface ports to connect to the service provider network
 - **Core router/Multilayer switch** – resides within the backbone of the WAN, supports multiple interfaces, and forwards IP packets at full line speed



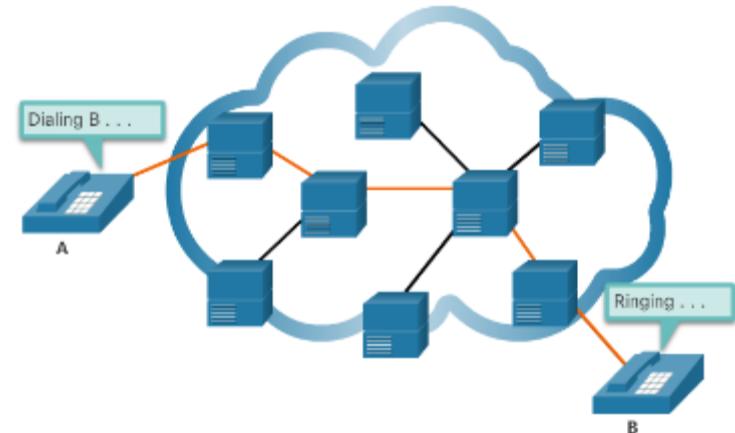


WAN Technologies Overview

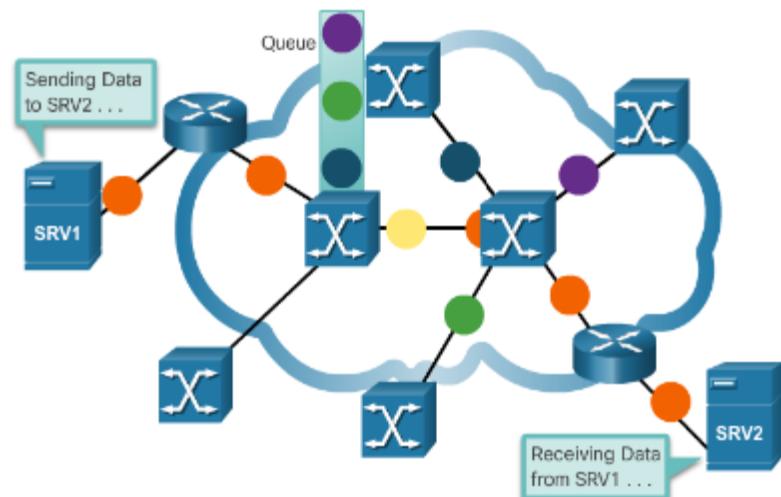
WAN Operations

- WANs can operate as circuit-switched or packet-switched networks:
 - **Circuit-switched Networks** – establish a **dedicated circuit** between source and destination before the users may communicate, such as making a telephone call
 - **Packet-Switched Networks** – **split traffic into packets** that are routed over a shared network and do not require a dedicated circuit between source and destination

Circuit-Switched



Packet-Switched



1.2 Selecting a WAN Technology



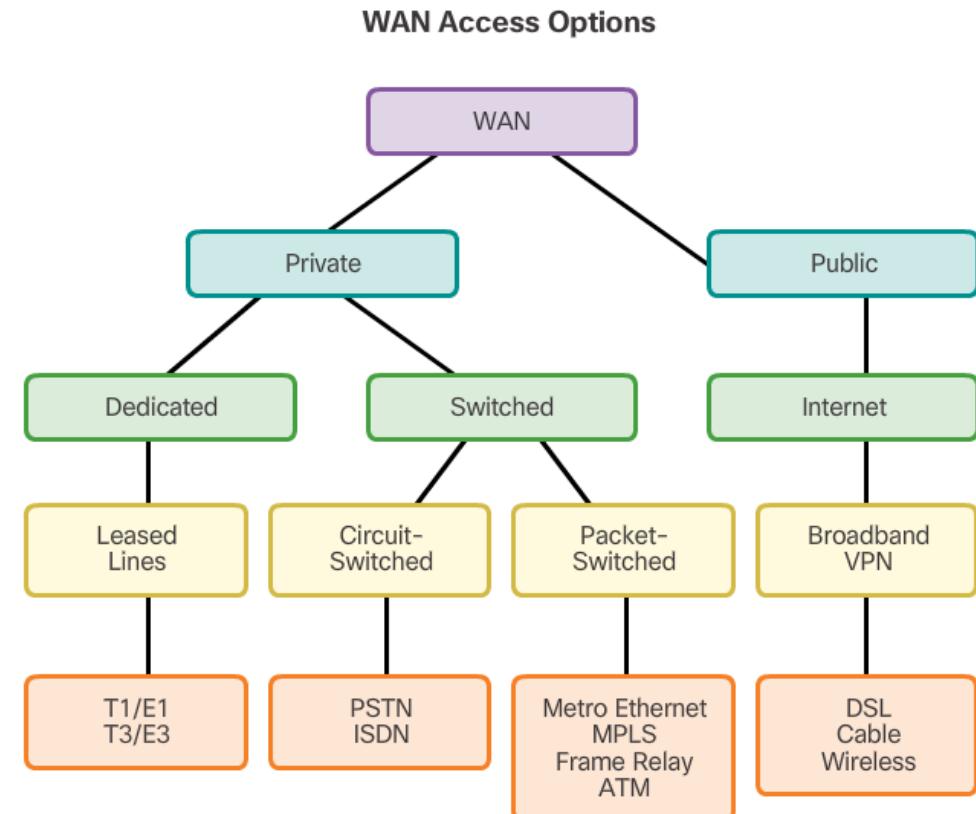


Selecting a WAN Technology

WAN Services

Two ways that a business can get WAN access:

- Private WAN Infrastructure
 - The business negotiates for dedicated or switched WAN access with a service provider.
- Public WAN Infrastructure
 - WAN access is achieved through the Internet using broadband connections.
VPNs secure the connections.

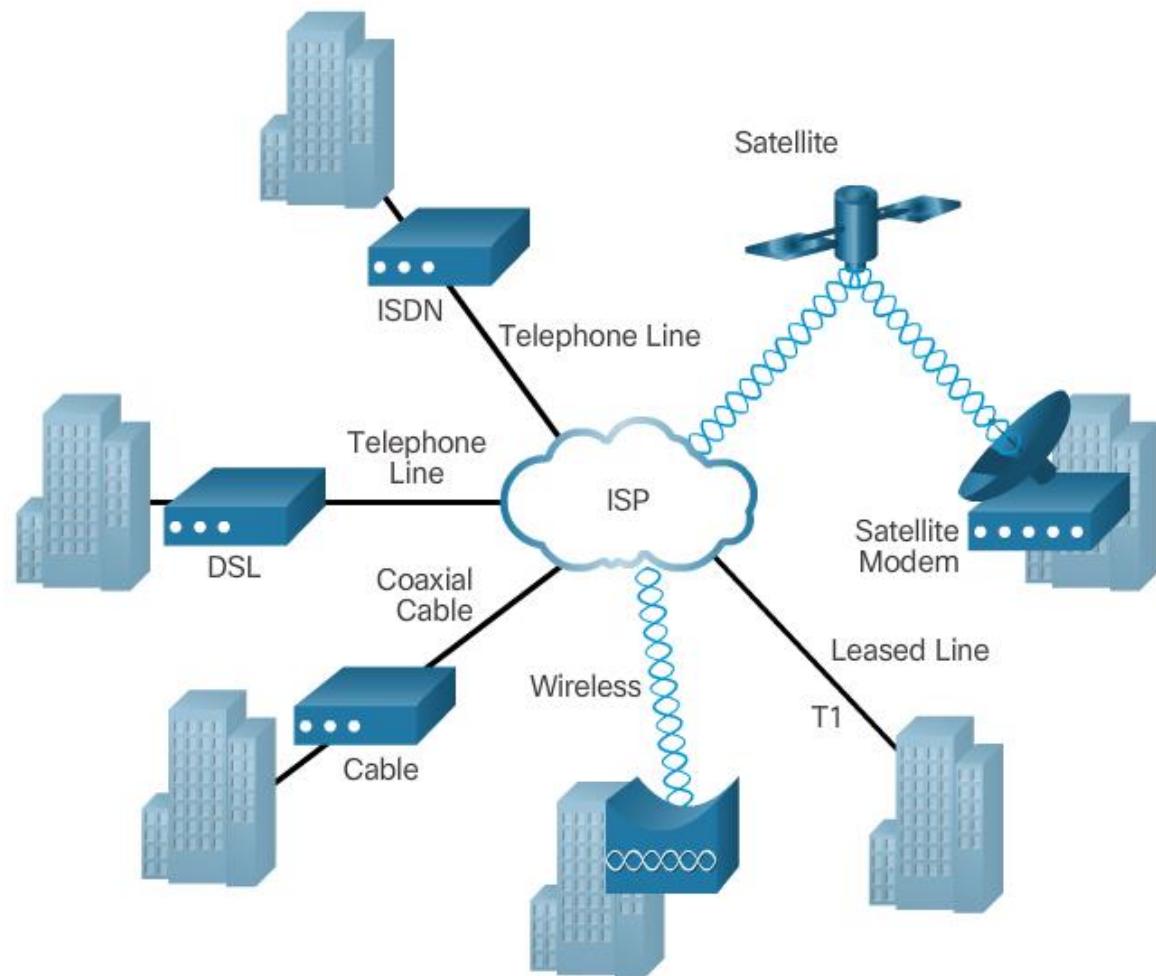




Selecting a WAN Technology

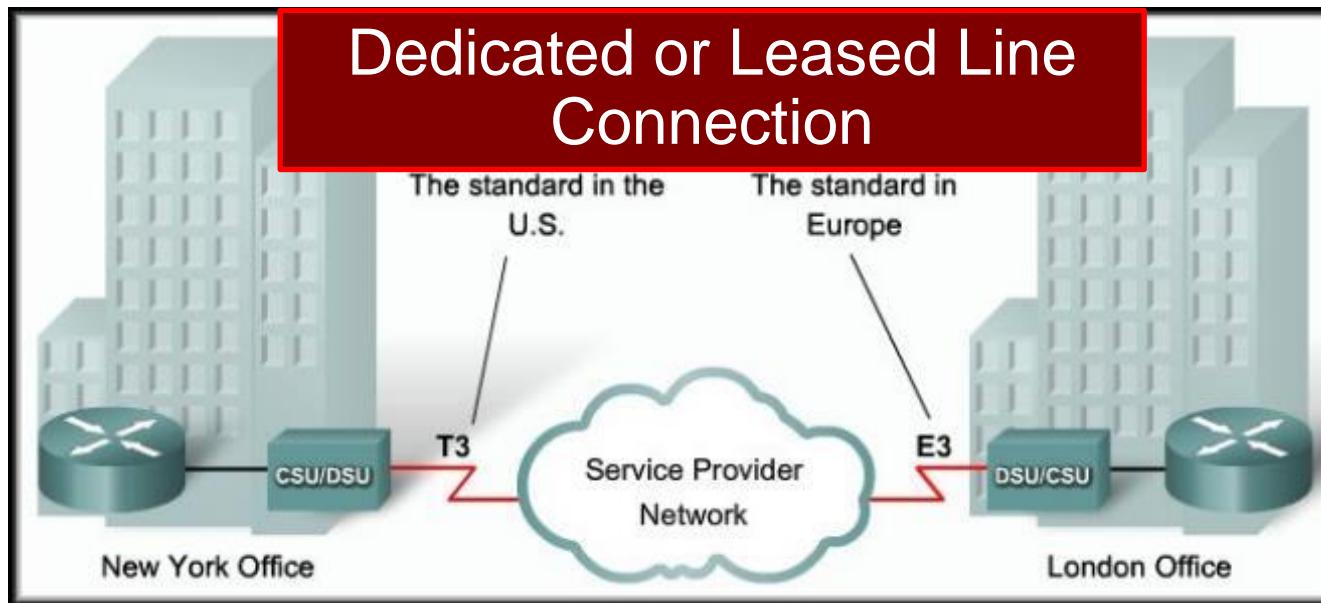
WAN Services (cont.)

This topology illustrates some of these WAN access technologies.





Leased Lines



- When **permanent dedicated connections** are required, **a point-to-point** link is used to provide a pre-established WAN communications path from the customer premises through the provider network to a remote destination.
- A point-to-point link is used to provide a pre-established WAN communications path from the customer premises through the provider network to a remote destination.
- Point-to-point links are usually more expensive than **shared** services such as Frame Relay.
- The Layer 2 protocol is usually HDLC or PPP.

Source: D. Clarke 2017



Private WAN Infrastructures

Leased Lines

Advantages:

- **Simplicity** - Point-to-point communication links require minimal expertise to install and maintain.
- **Quality** - Point-to-point communication links usually offer high service quality, if they have adequate bandwidth. The dedicated capacity removes latency or jitter between the endpoints.
- **Availability** - Constant availability is essential for some applications, such as e-commerce. Point-to-point communication links provide permanent, dedicated capacity which is required for VoIP or Video over IP.

Disadvantages:

- **Cost** - Point-to-point links are generally the most expensive type of WAN access. The cost of leased line solutions can become significant when they are used to connect many sites over increasing distances. In addition, each endpoint requires an interface on the router, which increases equipment costs.
- **Limited flexibility** - WAN traffic is often variable, and leased lines have a fixed capacity, so that the bandwidth of the line seldom matches the need exactly. Any change to the leased line generally requires a site visit by ISP personnel to adjust capacity.

Source: D. Clarke 2017



Private WAN Infrastructures Leased Lines

Some Interesting Links:

<https://business.bt.com/products/broadband/bt-leased-lines/>

<https://www.submarinecablemap.com/>

<http://www.aquacomms.com/>

Source: D. Clarke 2017



Selecting a WAN Technology

Private WAN Infrastructures

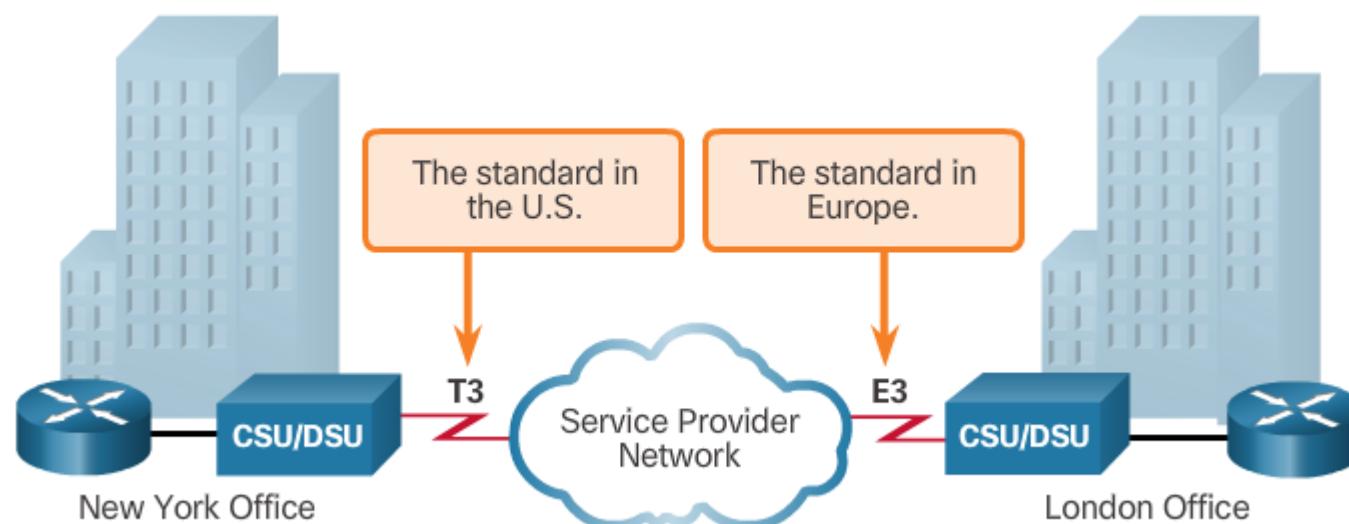
Dialup

Advantages:

- Simplicity
- Quality
- Availability

Disadvantages:

- Cost
- Limited flexibility



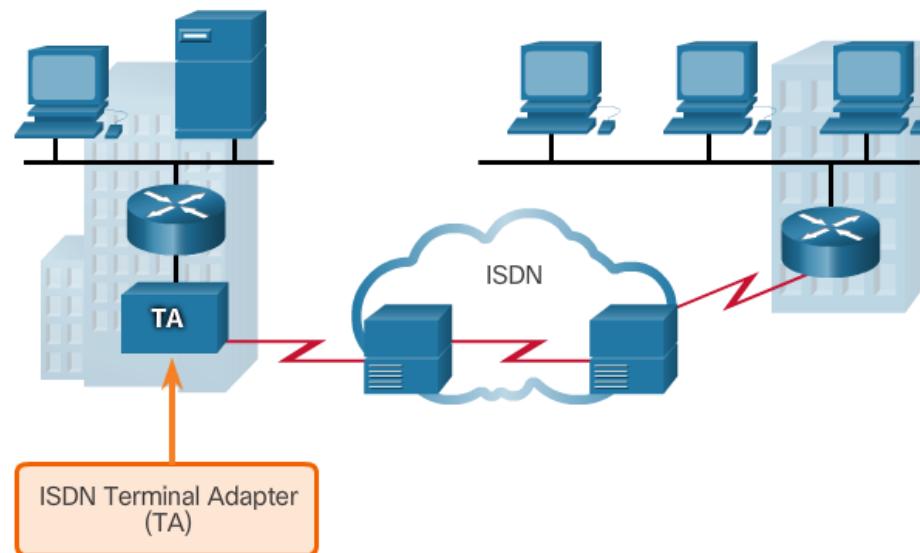


Selecting a WAN Technology

Private WAN Infrastructures (Cont.)

ISDN

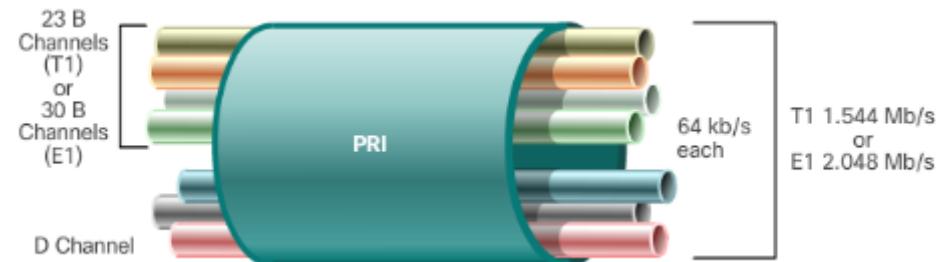
Sample ISDN Topology



ISDN BRI



ISDN PRI

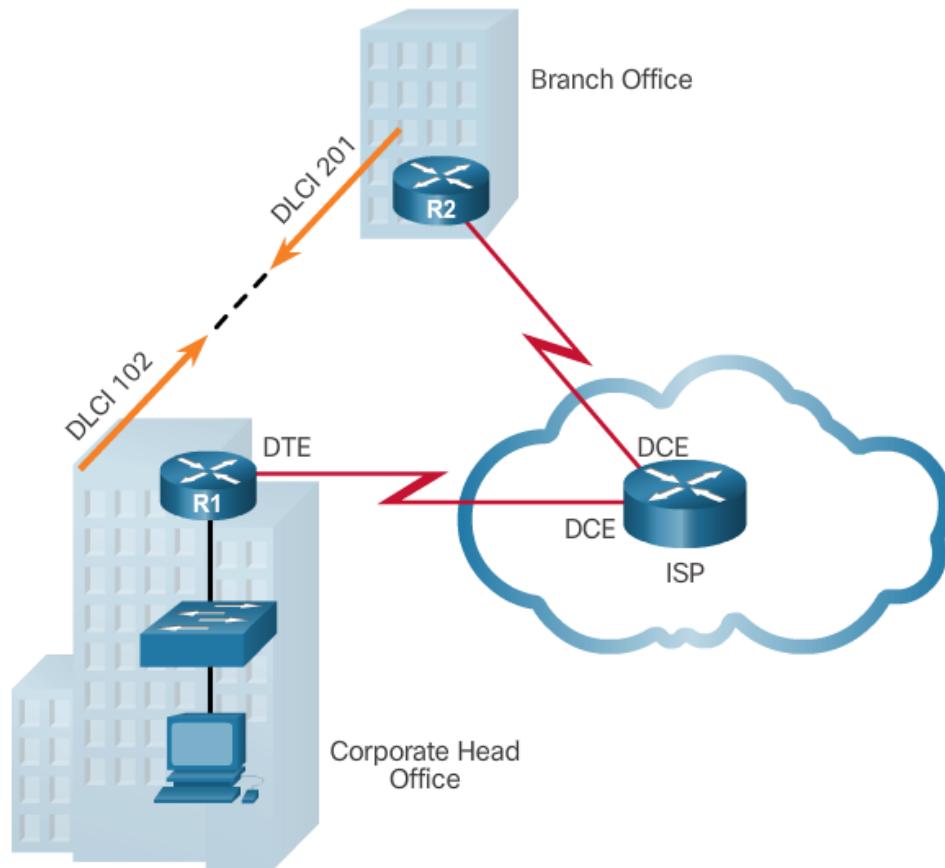




Selecting a WAN Technology

Private WAN Infrastructures (Cont.)

Frame Relay (Obsolete)



- 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.

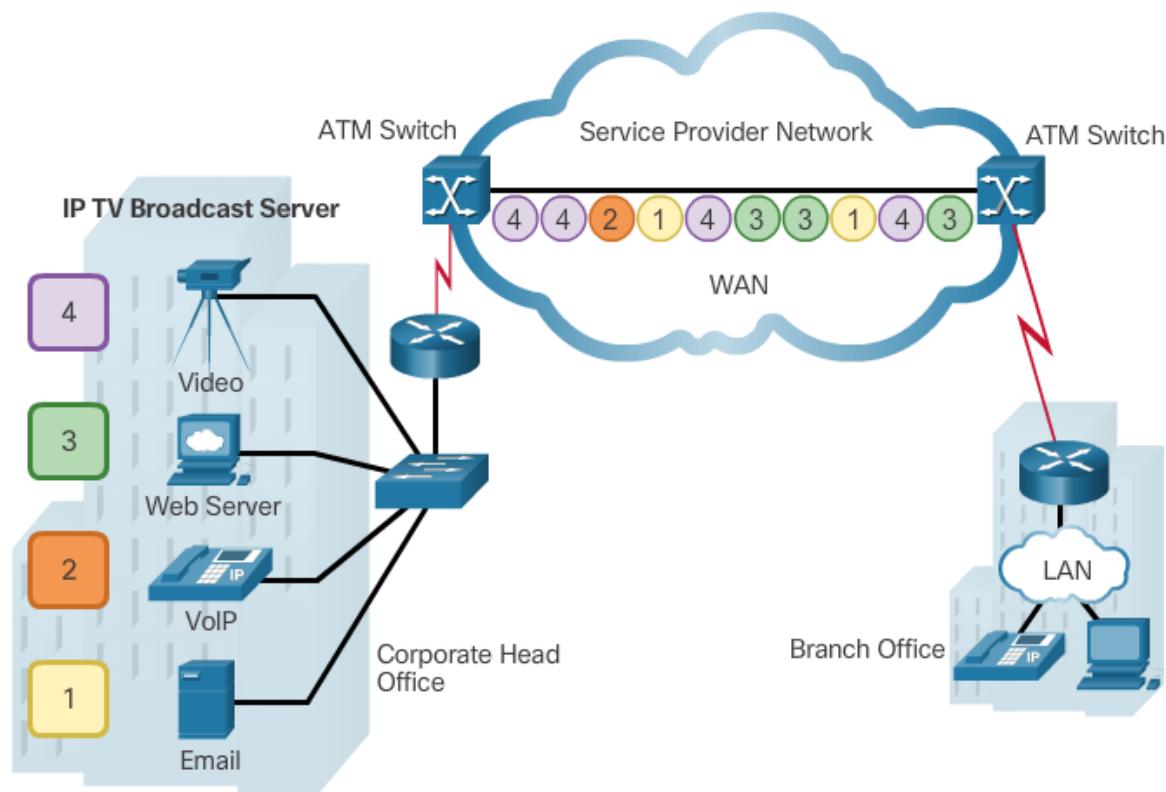


Selecting a WAN Technology

Private WAN Infrastructures (Cont.)

ATM (Obsolete)

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





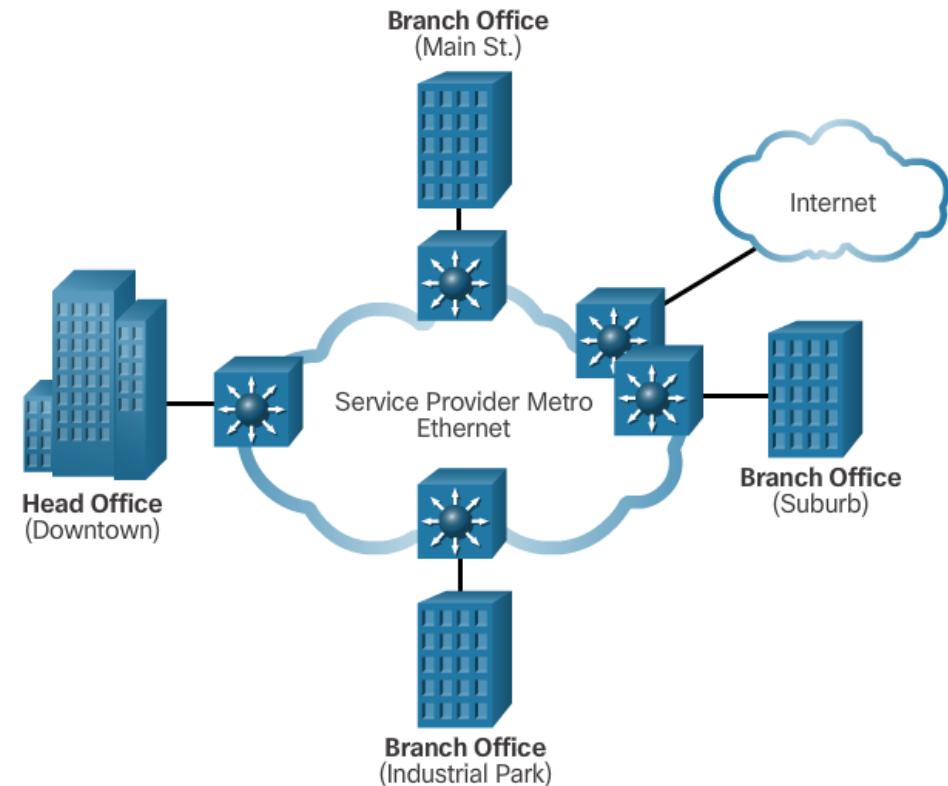
Selecting a WAN Technology

Private WAN Infrastructures (Cont.)

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.

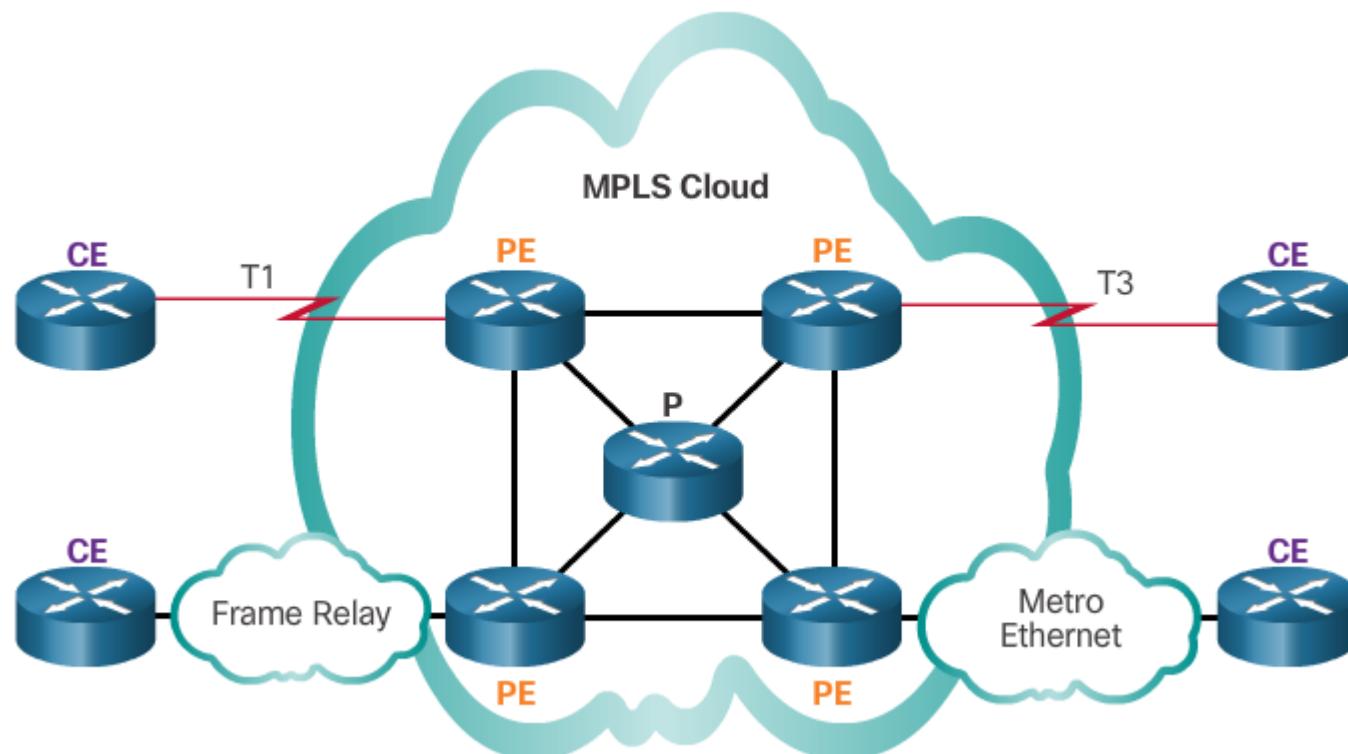


Selecting a WAN Technology

Private WAN Infrastructures (Cont.)

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.



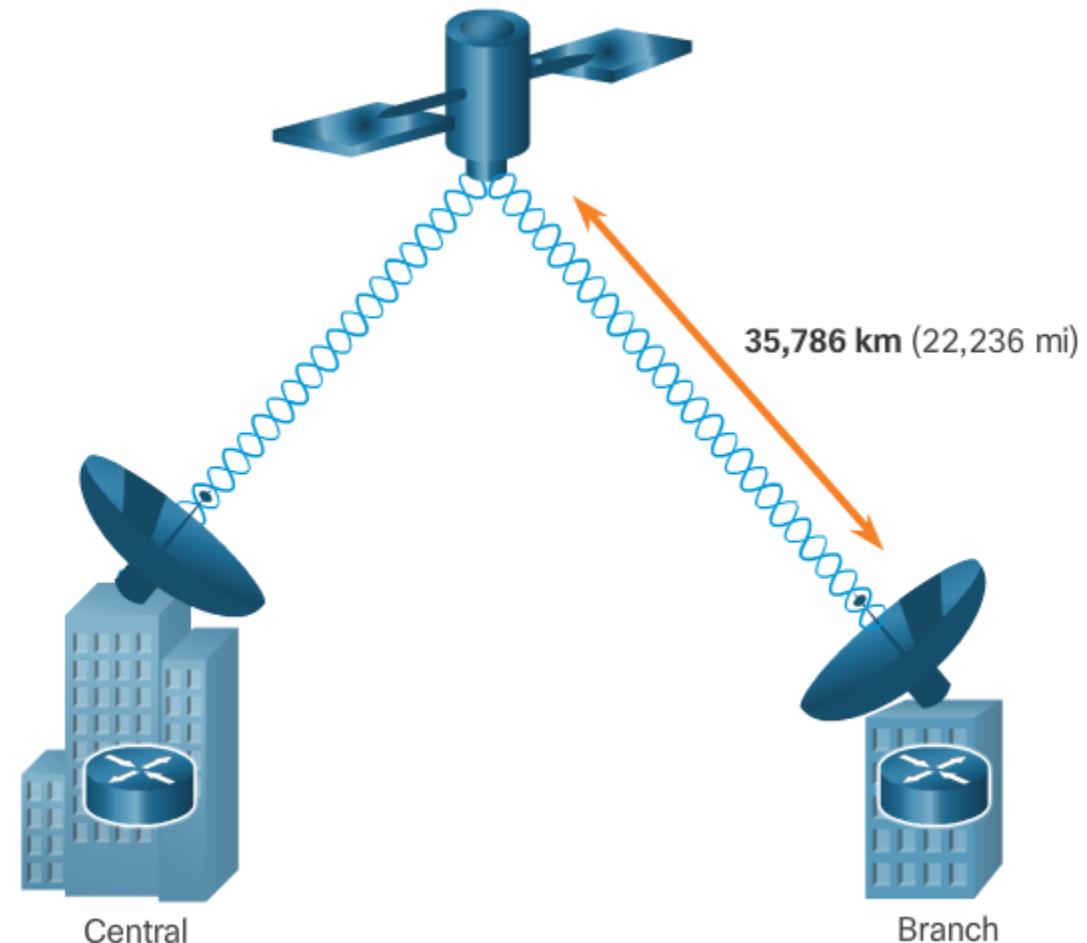


Selecting a WAN Technology

Private WAN Infrastructures (Cont.)

VSAT

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



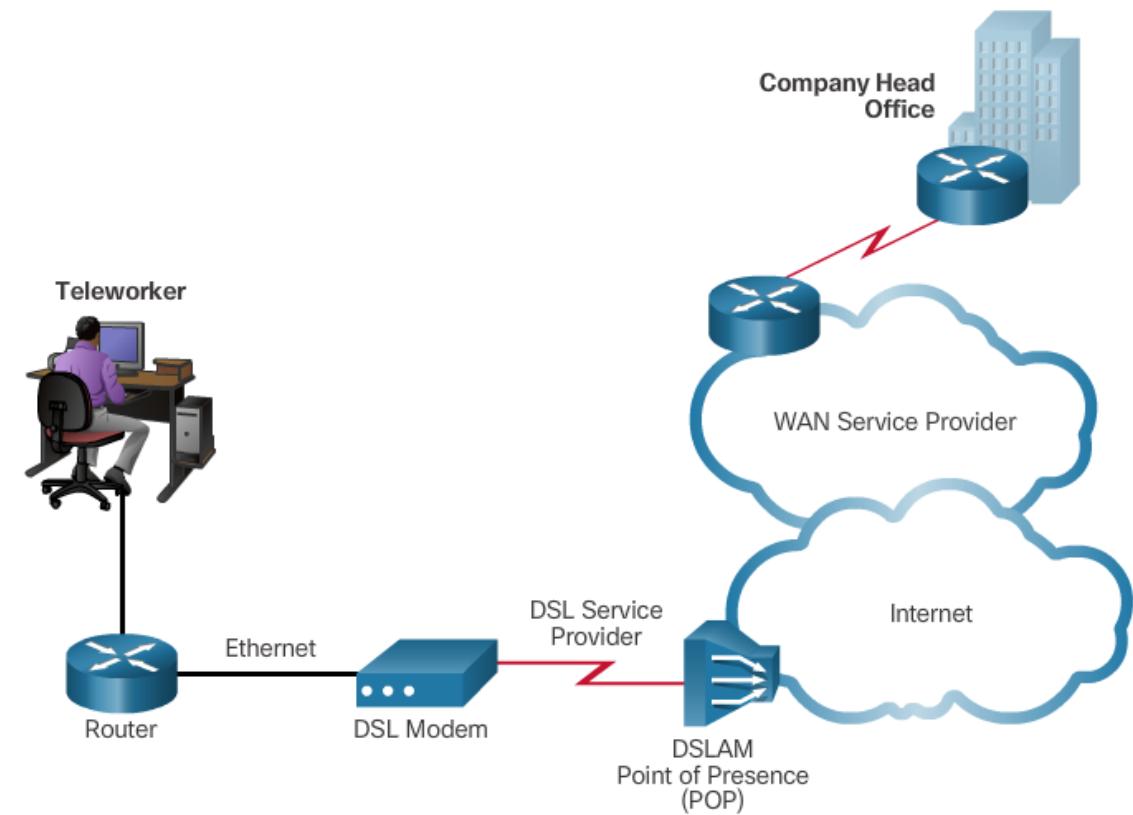


Selecting a WAN Technology

Public 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.



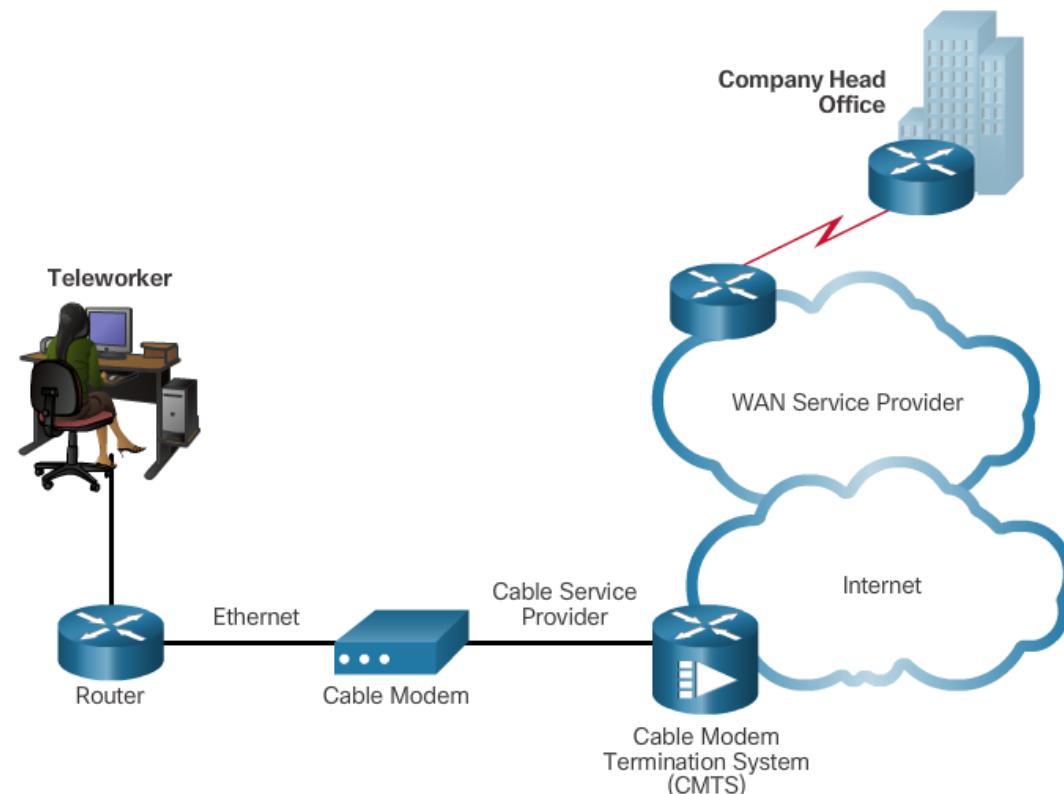


Selecting a WAN Technology

Public WAN Infrastructures (Cont.)

Cable

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





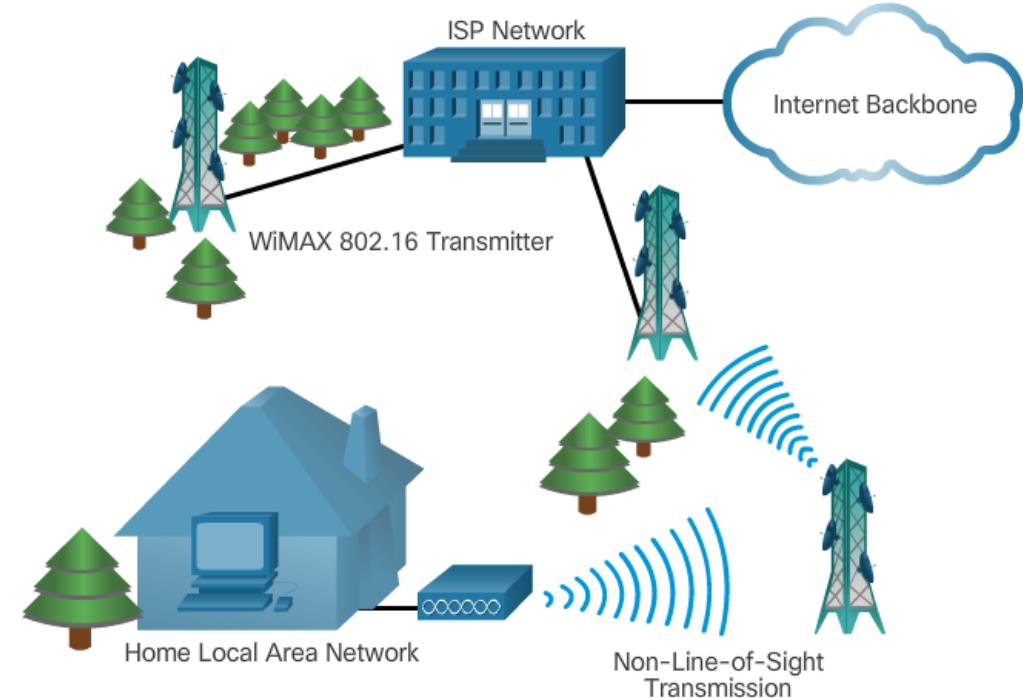
Selecting a WAN Technology

Public WAN Infrastructures (Cont.)

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** - Typically used by rural users where cable and DSL are not available.





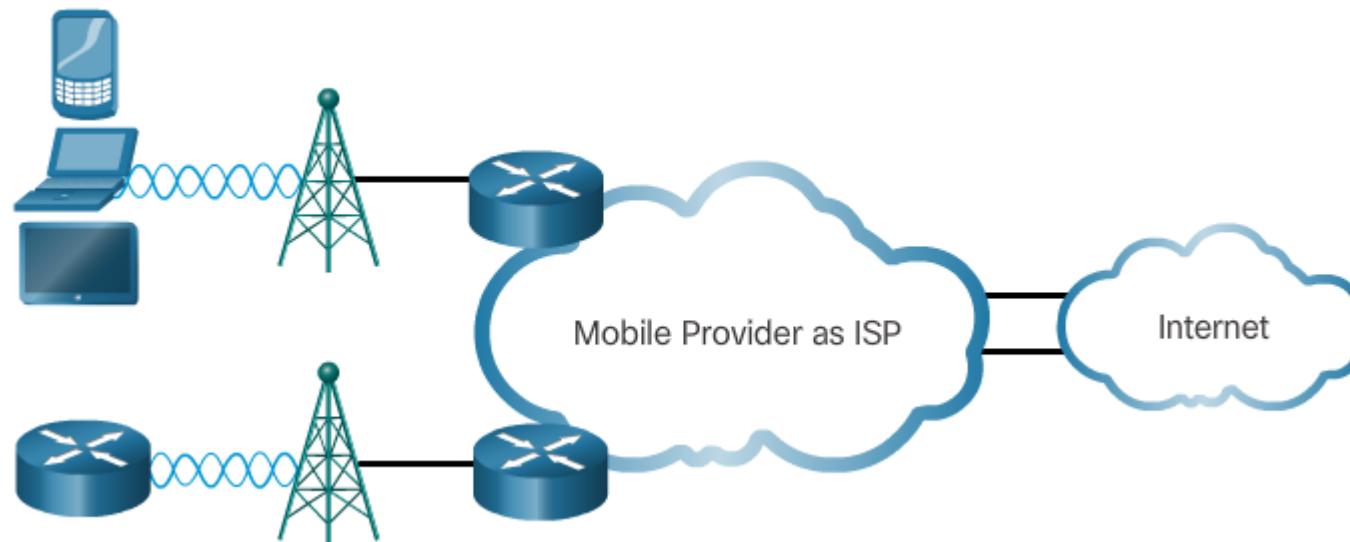
Selecting a WAN Technology

Public WAN Infrastructures (Cont.)

3G/4G

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.

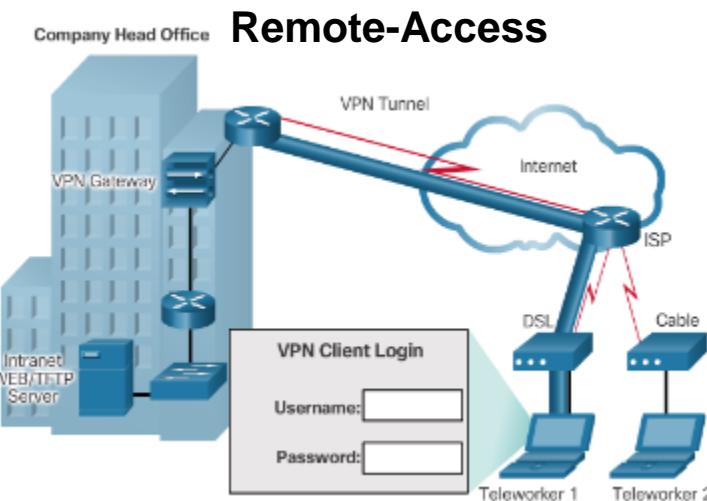
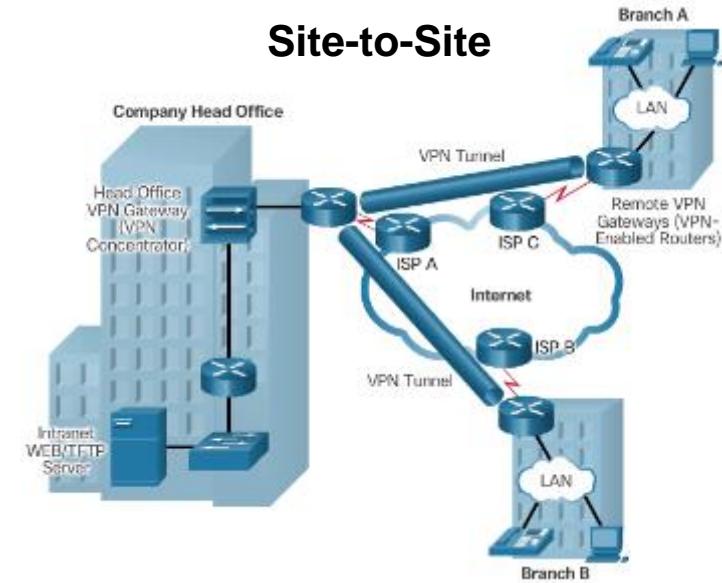




Selecting a WAN Technology

Public WAN Infrastructures (Cont.) *

- A VPN is a private network created via **tunneling** over a public network, such as the Internet.
 - VPNs establish a virtual point-to-point connection that enables hosts to send and receive data securely across public networks using dedicated connections and encryption.
 - VPNs provide a secure, reliable, and cost-effective method of interconnecting multiple networks to allow remote access to company resources.



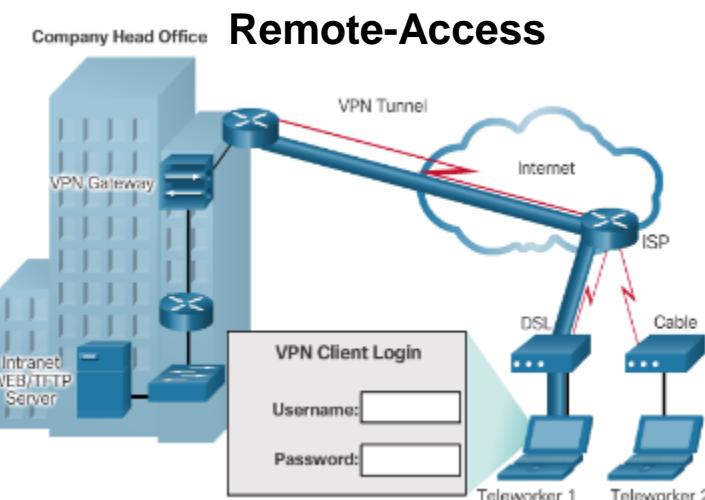
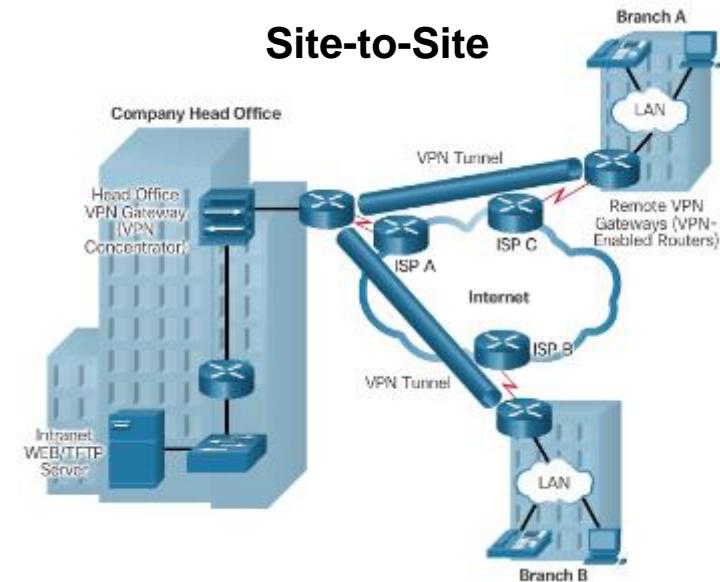
VPN = Virtual Private Network



Selecting a WAN Technology

Public WAN Infrastructures (Cont.)

- Public WANs rely on VPNs for securing data between private networks as it crosses a public network, such as the Internet.
- Benefits:
 - Cost savings
 - Security
 - Scalability
 - Compatibility with broadband technology
- Two types of VPN:
 - Site-to-site VPNs
 - Remote-access VPNs





Selecting a WAN Technology

Selecting WAN Services

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?
- 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?



Choosing a WAN Link Connection *

- What is the purpose of the WAN?
 - Do you want to connect local branches, connect remote branches, connect to business partners?
- What is the geographic scope?
 - Depending on the range, some WAN connection options may be better than others.
- What are the traffic requirements?
 - Traffic type (data only, VoIP, video, large files) determines performance requirements.
- Should the WAN use a private or public infrastructure?
 - A private infrastructure offers the best security, whereas the public Internet offers lowest expense.
- For a private WAN, should it be dedicated or switched?
- For a public WAN, what type of VPN access do you need?
- Which connection options are available locally?
- What is the cost of the available connection options?

Source: D. Clarke 2017



Choosing a WAN Link Connection *

- **Contextual Example:**
- Your company is opening a new branch office and wishes to provide the branch office with Web Conferencing, IP telephony, video on demand, wireless services and TelePresence (Video Conferencing). What questions would you ask to help choose a suitable WAN Link connection to the new branch office?.
- **What is the purpose of the WAN?**
 - Will the business be connecting to a local branch in the same area, or to remote branch, (..one branch now, more branches later)?
 - Will the WAN connect to customers, business partners, or employees or a combination of all three?
 - Will the WAN provide full or limited access the business intranet for authorized users?
- **What is the geographic scope?**
 - Local WAN, regional WAN, or global WAN?
 - One-to-one (single branch), one-to-many branches, or many-to-many (distributed)?
 - (..one branch now, more branches later)?



Choosing a WAN Link Connection *

- **Contextual Example:** (continued)
- Your company is opening a new branch office and wishes to provide the branch office with Web Conferencing, IP telephony, video on demand, wireless services and TelePresence (Video Conferencing). What questions would you ask to help choose a suitable WAN Link connection to the new branch office.
- **What are the traffic requirements?**
 - Traffic type?
 - What type of traffic must be supported (data only, VoIP, video, large files, streaming files).
 - Traffic volume?
 - What volume of traffic type (voice, video, or data) must be supported for each destination?
 - This determines the bandwidth capacity required for the WAN connection to the ISP.
 - Quality of Service?
 - What Quality of Service is required? This may limit the choices. If the traffic is highly sensitive to latency and jitter, eliminate any WAN connection options that cannot provide the required quality.



Choosing a WAN Link Connection *

- **Contextual Example:** (continued)
- Your company is opening a new branch office and wishes to provide the branch office with Web Conferencing, IP telephony, video on demand, wireless services and TelePresence (Video Conferencing). What questions would you ask to help choose a suitable WAN Link connection to the new branch office.
- **What are the traffic requirements? (continued)**
 - Security?
 - What are the security requirements (data integrity, confidentiality, and security)
 - The security requirements are important if the traffic is of a highly confidential nature.
- **Private WAN - should it be dedicated or switched?**
- **Public WAN - what type of VPN access do you need?**
- **Which connection options are available locally?**
- **What is the **cost** of the available connection options?**



Choosing a WAN Link Connection - VPN Access*

- **Contextual Example:** (continued)
- The company intends to use Virtual Private Networks (VPNs) to support secure access by teleworkers, employees, vendors and clients. How would a VPN benefit the company?
 - Cost savings?
 - Security?
 - Scalability?
 - Compatibility with broadband technology?
- Cost savings?
 - Use of VPNs over the public Internet infrastructure to support secure remote access by teleworkers, vendors and clients reduces costs for the company.
 - Remote access via DSL instead of expensive dedicated WAN links reduces connection costs, while increasing remote connection bandwidth.
- Security?
 - VPNs can protect company data from unauthorized access during transmission across the public Internet using advanced encryption and authentication protocols.



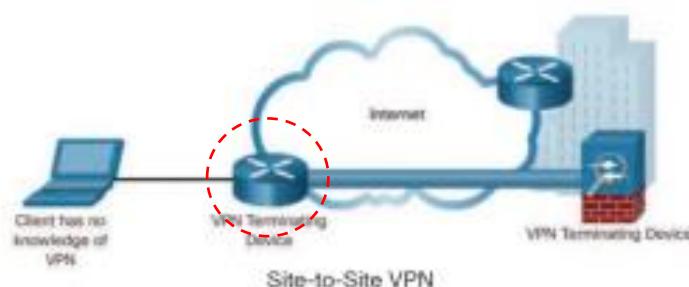
Choosing a WAN Link Connection - VPN Access*

- **Contextual Example:** (continued)
- The company intends to use Virtual Private Networks (VPNs) to support secure access by teleworkers, employees, vendors and clients. How would a VPN benefit the company?
 - Cost savings?
 - Security?
 - Scalability?
 - Compatibility with broadband technology?
- Scalability?
 - VPNs allow the company to use ISP Internet infrastructure and devices for remote connections..
 - New users can be added easily since extra capacity can be provided without adding significant infrastructure..
- Compatibility with broadband technology?
 - VPNs can operate over broadband Internet connections.
 - Mobile workers and teleworkers have high-speed broadband Internet access via DSL and cable.
 - VPNs allow Mobile workers and teleworkers use broadband access to connect remotely to the company network.



Choosing a WAN Link Connection- VPN Access*

- **Contextual Example:** (continued)
- The company has two types of VPN (VPNs) available - Site-toSite VPNs and Remote-Access-VPNs How would they be used to support the company's WAN infrastructure?.

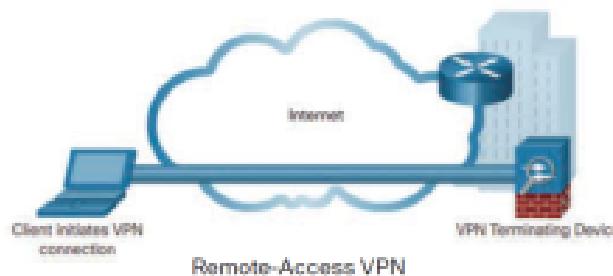


- Site-to-Site VPNs?
 - Site-to-site VPNs connect entire networks to each other such as the company's branch office network at one site to the company's headquarters network at another site.
 - Both sides of the VPN connection are aware of the VPN configuration in advance.
 - The VPN remains static.
 - Internal hosts have no knowledge that a VPN exists.
 - VPN gateway encapsulates and encrypts outbound traffic from a network site.
 - VPN gateway sends the traffic through a VPN tunnel over the Internet to a peer VPN gateway at the target site.
 - Peer VPN gateway strips the headers, decrypts the content, and relays the packet toward the target host inside its private network.



Choosing a WAN Link Connection- VPN Access*

- **Contextual Example:** (continued)
- The company has two types of VPN (VPNs) available - Site-toSite VPNs and Remote-Access-VPNs How would they be used to support the company's WAN infrastructure?



- Remote-Access VPN?
 - Remote-access VPNs securely connect individual teleworker hosts to the company network, usually via an Internet broadband connections.
 - The VPN is dynamic. VPN 'torn' down when communication session ends.
 - VPN Client software installed on teleworker host encapsulates, encrypts, and sends the traffic through a VPN tunnel over the Internet to the destination VPN gateway.
 - VPN gateway strips the headers, decrypts the content, and relays the packet toward the target host inside its private network.



Choosing a WAN Link Connection- VPN Access*

- **Contextual Example:** (continued)
- What design issues should the company consider when planning and implementing its teleworker infrastructure?
 - Security: provide confidentiality, integrity and authentication for data exchanges over the teleworker infrastructure.
 - Cost-effective and easy to manage.
 - Scalability –it should be easy and cost-effective to expand the scale of operation.
 - Should be affordable.
 - Easy to use.
 - Data transfer speed should be appropriate to the requirements.
 - Service should be reliable.

1.3 Summary



Cisco | Networking Academy®
Mind Wide Open™



Chapter Summary

Summary

- WAN access standards operate at Layers 1 and 2 of the OSI model.
- Permanent, dedicated point-to-point connections are provided by using leased lines.
- Private WAN connections include:
 - Dialup
 - ISDN
 - Frame Relay (Obsolete)
 - ATM (Obsolete)
 - Metro Ethernet
 - MPLS
 - VSAT
- Public WAN connections include:
 - DSL
 - Cable
 - Wireless
 - Cellular
- Security over public infrastructure connections can be provided by using remote-access or site-to-site Virtual Private Networks (VPNs).



Reminder

Lab on Friday

- The Skills Based Assessment (SBA) takes place this Friday 27th November 2020.
 - Configuring: OSPF, PPP and Authentication (PAP and CHAP), VPNs and GRE Tunnels, Standard and Extended ACLs
 - etc...

Cisco | Networking Academy®

Mind Wide Open™





WAN Technology – Revision 2



Connecting Networks

Cisco | Networking Academy®
Mind Wide Open™



Chapter 2 - Sections & Objectives

- 2.1 Serial Point-to-Point Overview
 - Configure HDLC encapsulation.
- 2.2 PPP Operation
 - Explain how PPP operates across a point-to-point serial link.
- 2.3 PPP Implementation
 - Configure PPP encapsulation.
- Also LAN Security



2.1 Serial Point-to-Point Overview

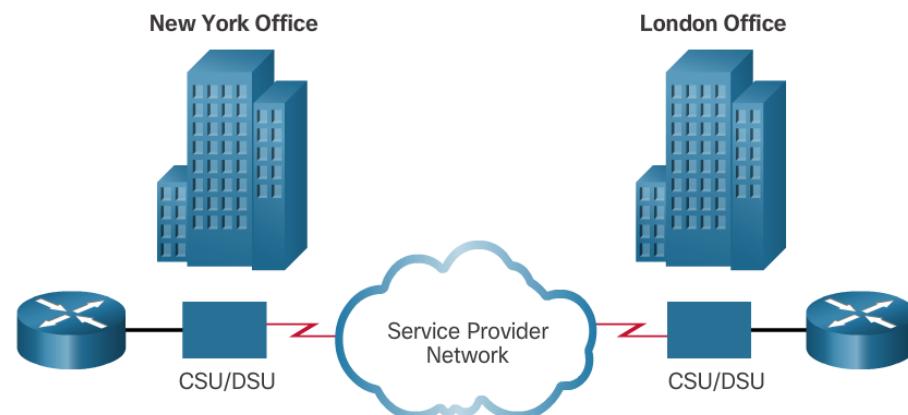


Cisco | Networking Academy®
Mind Wide Open™



Serial Point-to-Point Overview Serial Communications

- Point-to-point connections are used to connect LANs to service provider WANs, and to connect LAN segments within an enterprise network.
- A point-to-point link can connect two geographically distant sites, such as a corporate office in New York and a regional office in London.
- Serial connection bandwidths can be incrementally increased to accommodate the need for faster transmission.





Serial Point-to-Point Overview

HDLC Encapsulation

- On each WAN connection, data is encapsulated into frames before crossing the WAN link.
 - HDLC is the default encapsulation type on point-to-point connections, dedicated links, and circuit-switched connections when the link uses two Cisco devices.
- HDLC defines a Layer 2 framing structure that allows for flow control and error control through the use of acknowledgments.
 - HDLC uses a frame delimiter, or flag, to mark the beginning and the end of each frame
 - Cisco HDLC frames contain a field for identifying the network protocol being encapsulated.

Standard HDLC

Flag	Address	Control	Data	FCS	Flag
------	---------	---------	------	-----	------

Supports only single-protocol environments.

Cisco HDLC

Flag	Address	Control	Protocol	Data	FCS	Flag
------	---------	---------	----------	------	-----	------

Uses a protocol data field to support multiprotocol environments.



Serial Point-to-Point Overview

HDLC Encapsulation

- There are two steps to re-enable HDLC encapsulation:
 - **Step 1.** Enter the interface configuration mode of the serial interface.
 - **Step 2.** Enter the **encapsulation hdlc** command to specify the encapsulation protocol on the interface.
- The **show interfaces serial** command returns one of six possible states:
 - Serial x is up, line protocol is up
 - Serial x is down, line protocol is down
 - Serial x is up, line protocol is down
 - Serial x is up, line protocol is up (looped)
 - Serial x is up, line protocol is down (disabled)
 - Serial x is administratively down, line protocol is down
- The **show controllers** command is another important diagnostic tool when troubleshooting serial lines.
 - The output indicates the state of the interface channels and whether a cable is attached to the interface.

2.2 PPP Operation





PPP Operation

Roles of PPP in WANs *

- PPP provides router-to-router and host-to-router connections via synchronous and asynchronous circuits.
- PPP – roles in WANs
 - Link establishment
 - Assignment and management of IP addresses .
 - Multi Network Protocol support
 - Link configuration and link quality testing
 - Error detection
 - Authentication support (PAP, CHAP)



PPP Operation

Benefits of PPP *

- PPP encapsulation used to connect a Cisco router to a non-Cisco router.
- PPP Advantages
 - The link quality management monitors the quality of the link. If too many errors are detected, PPP takes the link down.
 - PPP supports PAP and CHAP authentication.





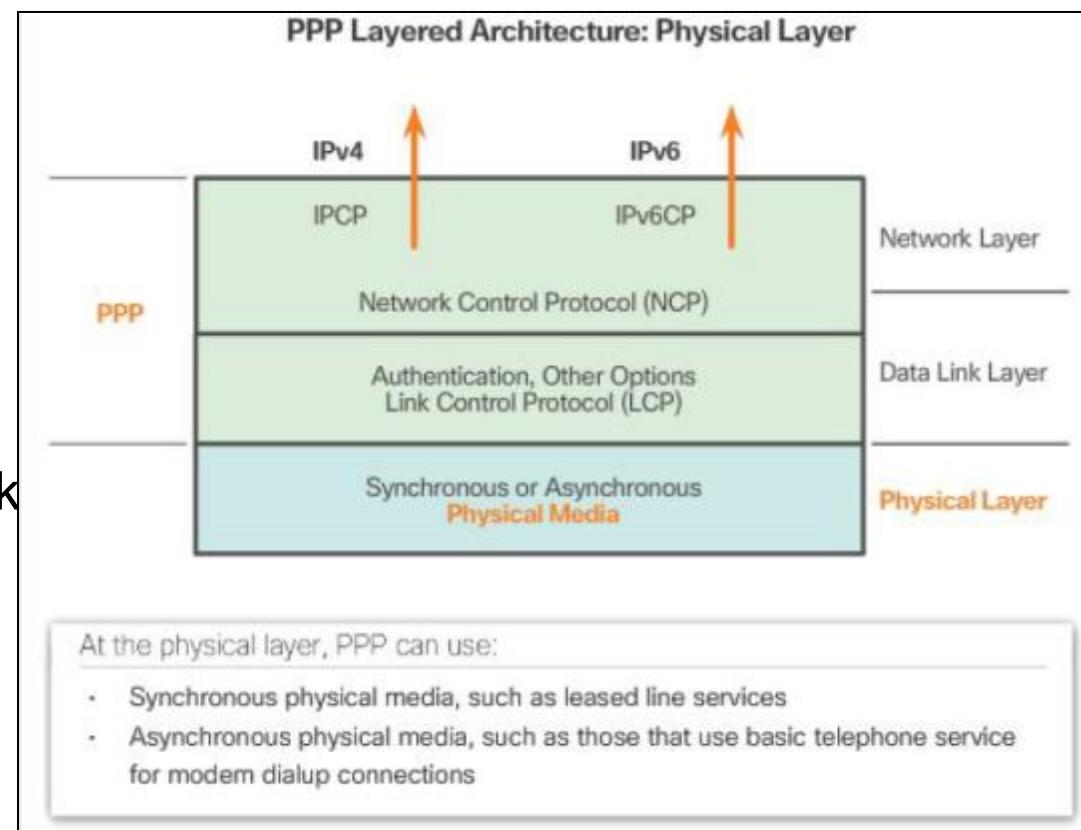
PPP Operation

PPP Layered Architecture *

- PPP uses three layers of the OSI model in its architecture:
 - The **physical layer** is used for the actual point-point connection.
 - The **data link layer** is used to establish and configure the connection.
 - The **network layer** is used to configure different network layer protocols

PPP and OSI share the **same** physical layer.

PPP distributes the functions of **LCP** and **NCP** differently in two protocol sub-layers.





PPP Operation LCP and NCP *

■ PPP Layered Architecture

- PPP and OSI share the same physical layer, but PPP distributes the functions of LCP and NCP differently.
- The only absolute requirement imposed by PPP is a full-duplex circuit, either dedicated or switched, that can operate in an asynchronous or synchronous bit-serial mode.
- Most of the work done by PPP happens at the data link and network layers, by LCP (Link Control Protocol) and NCPs (Network Control Protocols)



PPP Operation LCP and NCP *

Link Control Protocol and Network Control Protocol

R1#sh int s0/0/0
Serial0/0/0 is up, line protocol is up (connected)
Hardware is HD64570
Internet address is 192.168.10.2/30
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, loopback not set, keepalive set (10 sec)
LCP Open
Open: IPCP, CDPCP

LCP and NCP
states

IPCP = an NCP for IPv4

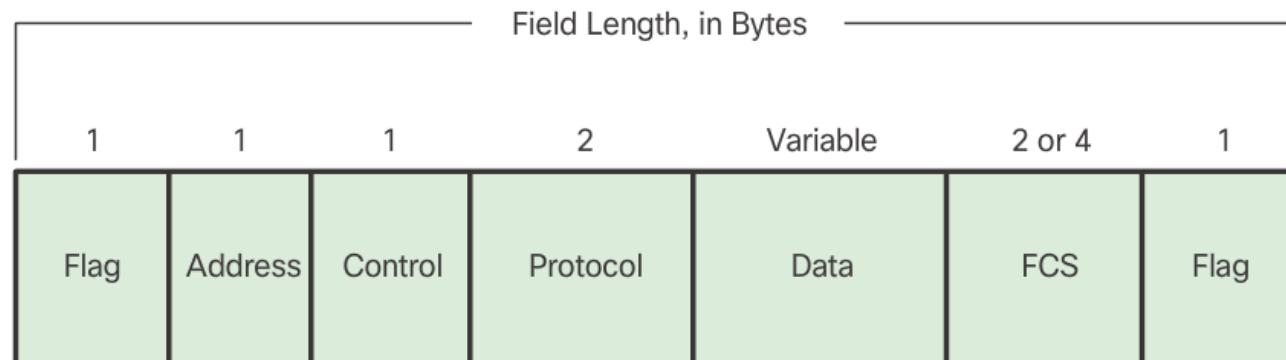


R2#sh int s0/0/0
Serial0/0/0 is up, line protocol is up (connected)
Hardware is HD64570
Internet address is 192.168.10.1/30
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, loopback not set, keepalive set (10 sec)
LCP Open
Open: IPCP, CDPCP



PPP Operation LCP and NCP *

- Link Control Protocol – a protocol sub-layer of PPP
 - LCP sits on top of the physical layer
 - LCP establishes, tests and configures the point-to-point link.
 - LCP also negotiates and sets up control options on the WAN data link, which are handled by the NCPs.
 - After the link is established, PPP also uses LCP to negotiate and agree automatically on encapsulation formats such as authentication, compression, and error detection, multi-link and PPP call back
- A PPP frame consists of six fields:





PPP Operation LCP and NCP *

- Network Control Protocol – a protocol sub-layer of PPP
 - PPP permits multiple network layer protocols to operate on the same communications link.
 - NCP is used to encapsulate and negotiate options for multiple network layer protocols.
 - For every network layer protocol used, PPP uses a separate NCP. (e.g IPCP for IPv4, IPv6CP for IPv6)
 - Each NCP manages the specific needs required by its respective network layer protocols.
 - NCP sits on top of LCP protocol layer



PPP Operation

PPP Sessions *

- There are **four** phases of establishing a PPP session
 - Phase 1: Link establishment and configuration negotiation
 - The originating PPP node sends LCP frames to configure and establish the data link.
 - Phase 2: Link quality determination (optional-phase)
 - The link is tested to determine whether the link quality is sufficient to bring up network layer protocols
 - Phase 3: Network layer protocol configuration negotiation
 - The originating PPP node sends NCP frames to choose and configure the network-layer protocols
 - Phase 4: Link termination negotiation
 - Link remains configured for communications until LCP or NCP frames close the link or until some external event occurs



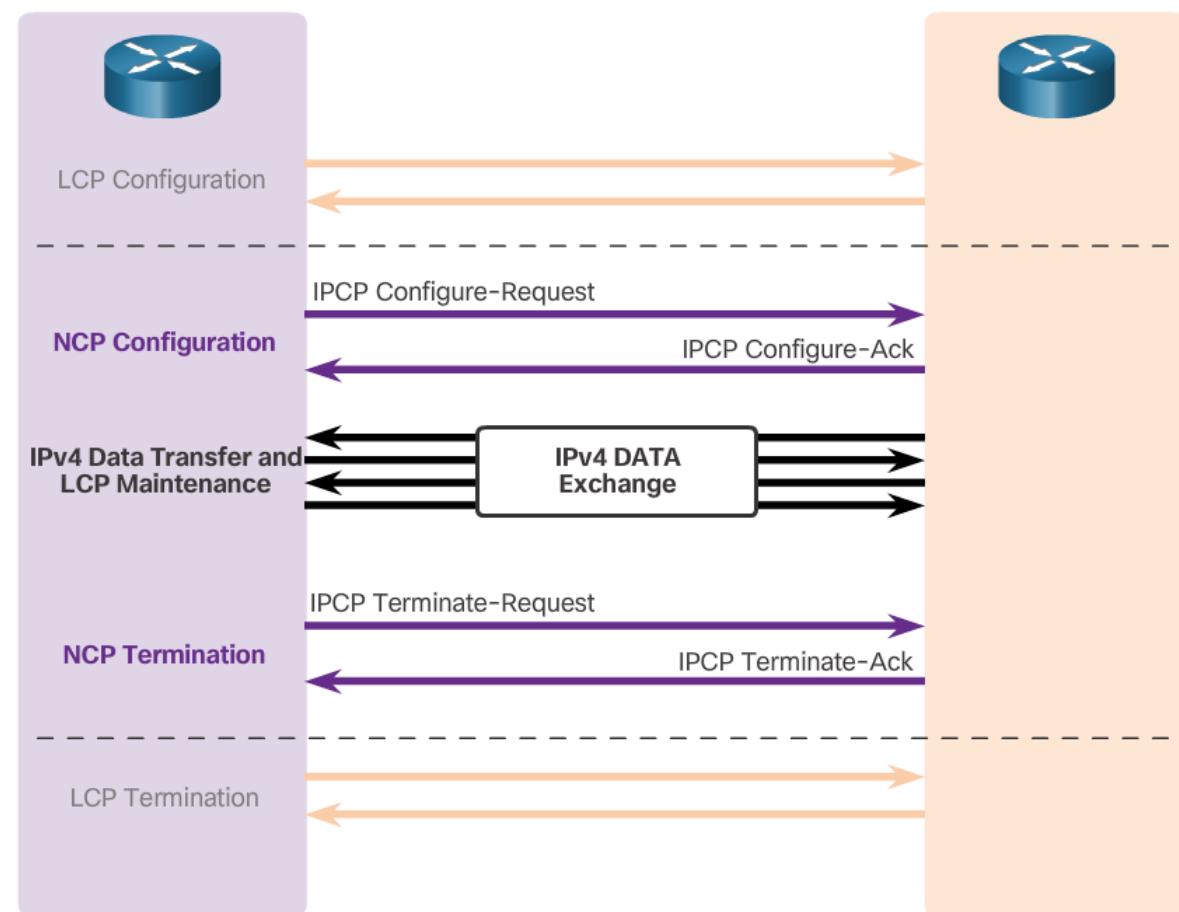
PPP Operation PPP Sessions *

- 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.
 - Link-maintenance frames manage and debug a link.
 - Link-termination frames terminate a link.
- PPP can be configured to support optional functions:
 - Authentication
 - Compression
 - Multilink



PPP Operation PPP Sessions

- After LCP has established the link, the routers exchange IPCP messages
 - Compression
 - IPv4-Address





PPP Operation

PPP Authentication Options (PAP & CHAP) *

- PAP (Password Authentication Protocol)
 - PAP is a very basic two-way process.
 - No encryption (plain text) If accepted, connection allowed..
- CHAP (Challenge Handshake Authentication Protocol)
 - CHAP is more secure, three-way exchange of a shared secret.
 - Authentication is optional
 - Authentication takes place before network layer configuration

2.3 PPP Implementation





PPP Implementation Configure PPP

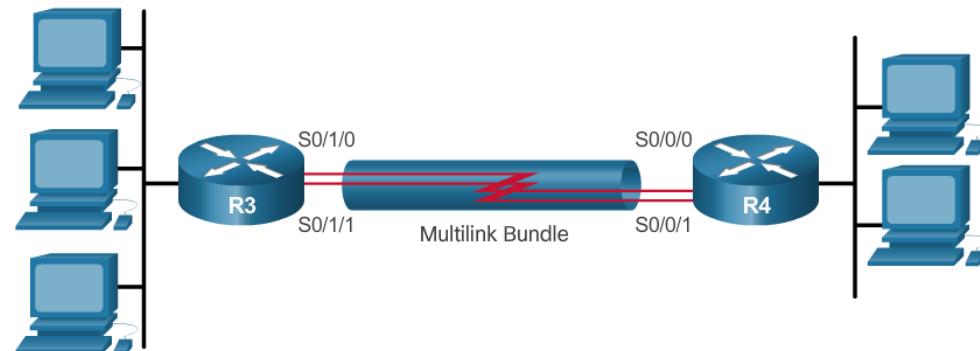
- PPP may include several LCP options:
 - Authentication, Compression, Error detection, PPP Callback, and Multilink
- To set PPP as the encapsulation method used by a serial interface, use the **encapsulation ppp** interface configuration command.
- Point-to-point software compression on serial interfaces can be configured after PPP encapsulation is enabled with the **compress** command.
- The **ppp quality percentage** command ensures that the link meets the quality requirement set; otherwise, the link closes down.



PPP Implementation

Configure PPP

- MPPP allows packets to be fragmented and sends these fragments simultaneously over multiple point-to-point links to the same remote address.
- Configuring MPPP requires two steps:
 - Step 1. Create a multilink bundle.
 - Step 2. Assign interfaces to the multilink bundle.



- Use the **show interfaces serial** command to verify proper configuration of HDLC or PPP encapsulation



PPP Implementation

Configure PPP Authentication *

- RFC 1334, PPP Authentication Protocols, defines two protocols for authentication, PAP and CHAP.
 - PAP is a very basic two-way process. There is no encryption. The username and password are sent in plaintext.
 - CHAP is more secure than PAP. It involves a three-way exchange of a shared secret.
 - To specify the order in which the CHAP or PAP protocols are requested on the interface, use the **ppp authentication** interface configuration command. Use the **no** form of the command to disable this authentication.
 - The PAP username and password that each router sends must match those specified with the **username name password** *password* command of the other router.

2.4 Summary





Chapter Summary

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.
- 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. PPP uses HDLC for encapsulating datagrams. **LCP** is the PPP protocol used to establish, configure, test, and terminate the data link connection. LCP can optionally authenticate a peer using PAP or CHAP. A family of **NCPs** are used by the PPP protocol to simultaneously support multiple network layer protocols. **Multilink PPP** spreads traffic across bundled links by fragmenting packets and simultaneously sending these fragments over multiple links to same remote address, where they are reassembled.
- PPP optionally supports **authentication** using **PAP, CHAP**, or both PAP and CHAP protocols. PAP sends authentication data in plaintext. CHAP uses a 3-way handshake, periodic challenge messaging, and a one-way hash that helps protect against playback attacks.



LAN Security



Cisco | Networking Academy®
Mind Wide Open™



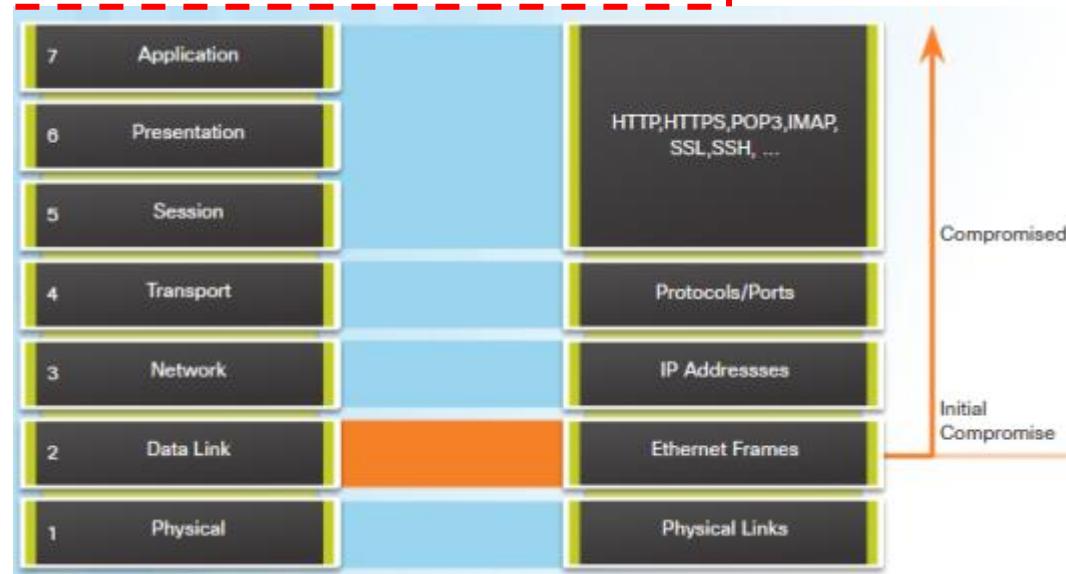
LAN Security

LAN Security Attacks *

- Common attacks against the Layer 2 LAN infrastructure include:

- MAC Address Table Flooding Attacks
- VLAN Attacks
- DHCP Attacks
- CDP Reconnaissance Attacks
- Telnet Attacks

If Layer 2 compromised,
then all layers above
Layer 2 are also affected.





LAN Security

LAN Security Best Practices *

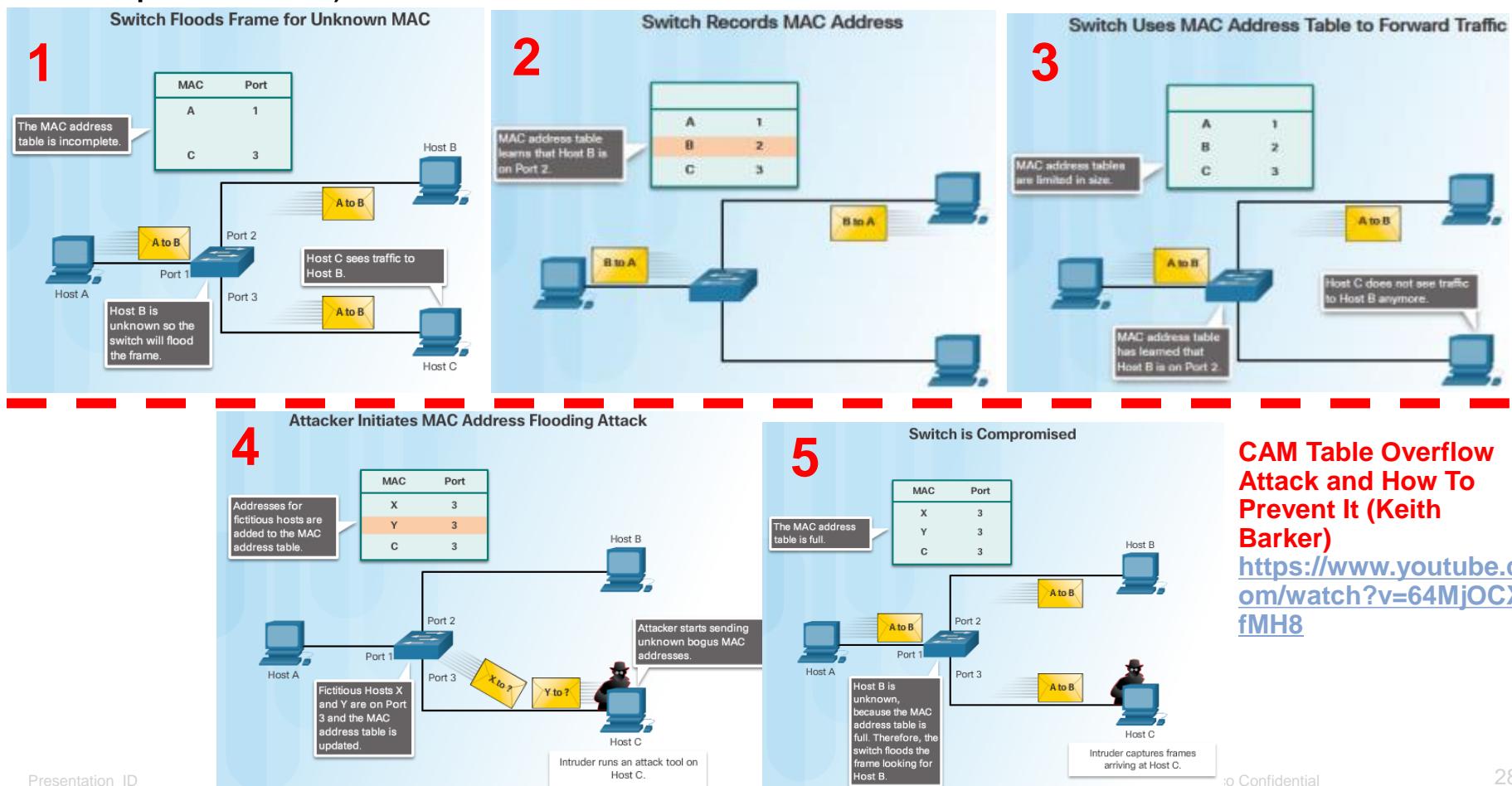
- This topic covers several Layer 2 security solutions:
 - Mitigating MAC address table flooding attacks using port security (fail-open mode)
 - Mitigating VLAN attacks (switch spoofing)
 - Mitigating DHCP attacks using DHCP snooping (spoofing and starvation)
 - Securing administrative access using AAA (local or server based)
 - Securing device access using IEEE 802.1X port authentication
 - 802.1X standard defines a port-based access control and authentication protocol. Restricts unauthorized workstations from connecting to a LAN through publicly accessible switch ports
 - An authentication server authenticates each workstation that is connected to a switch port before making available any services offered by the switch or the LAN.



LAN Security

LAN Security Best Practices *

- This topic covers several Layer 2 security solutions:
 - Mitigating MAC address table flooding attacks using port security (fail-open mode)

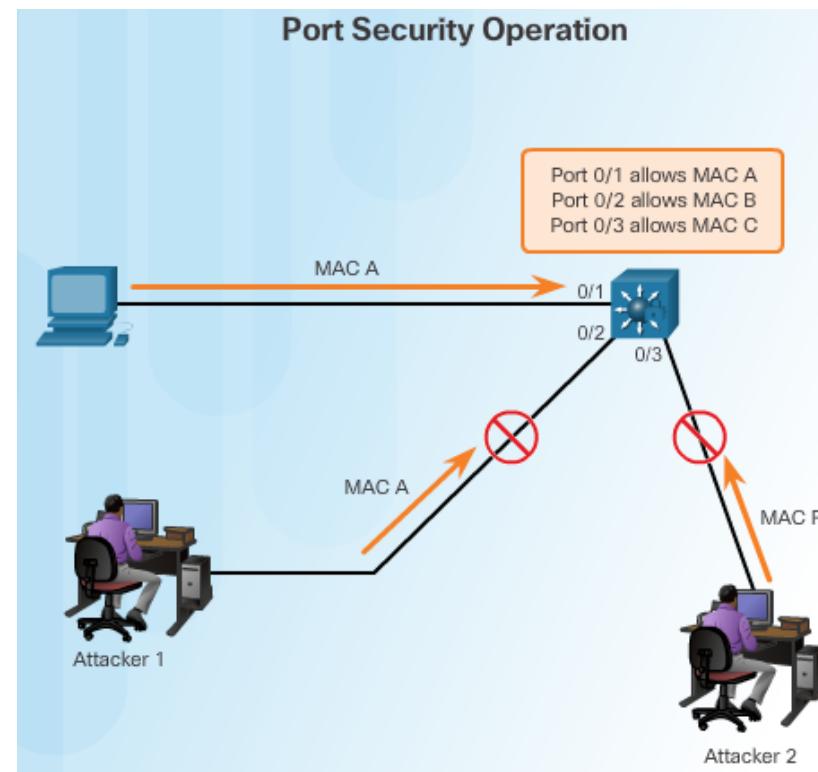




LAN Security

Mitigate MAC Address Attacks *

- Enable port security
- Statically specify MAC addresses for a port
- Limit permitted MAC addresses



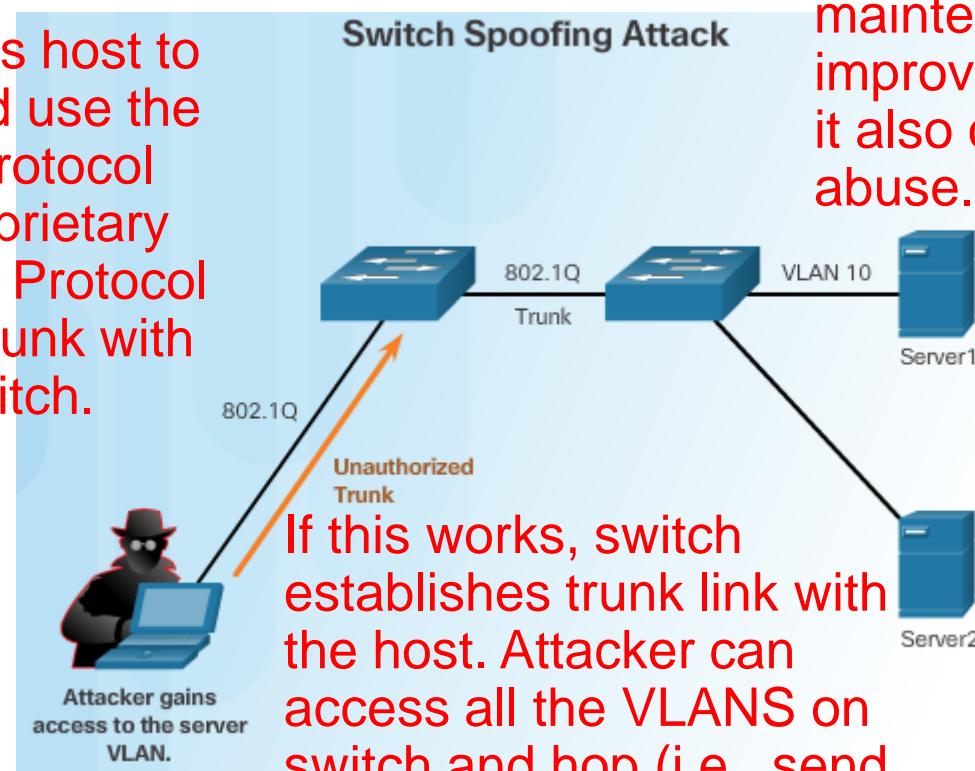


LAN Security

LAN Security Best Practices *

- This topic covers several Layer 2 security solutions:
 - Mitigating VLAN attacks (switch spoofing)

Attacker configures host to spoof a switch and use the 802.1Q trunking protocol and the Cisco-proprietary Dynamic Trunking Protocol (DTP) feature to trunk with the connecting switch.



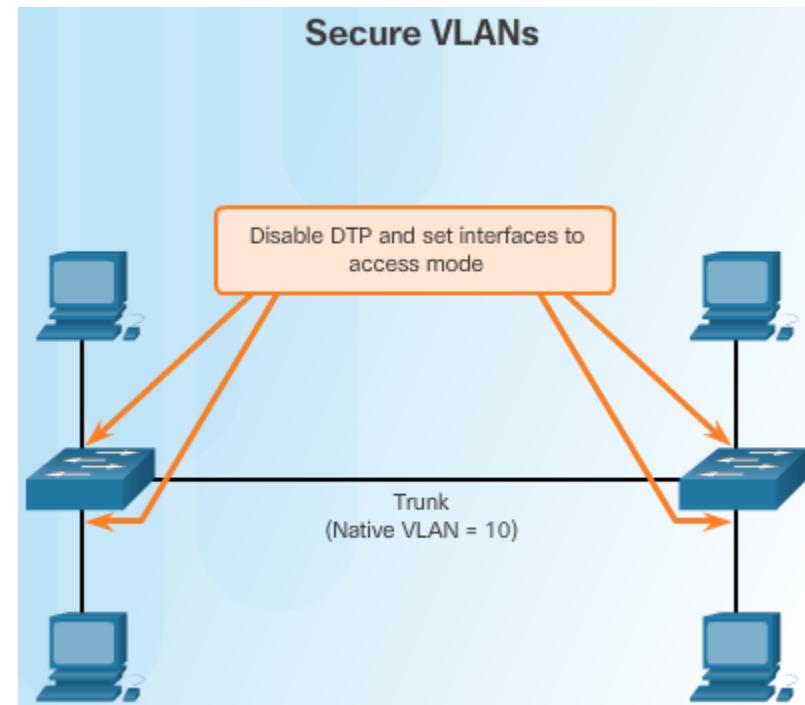
VLAN architecture simplifies network maintenance and improves performance, but it also opens the door to abuse.



LAN Security

Mitigate VLAN Attacks *

- Disable DTP (Auto Trunking)
- Set native VLAN to something other than default VLAN 1
- Disable unused ports. Make them access ports, and assign them to a black hole VLAN.
- Enable port security





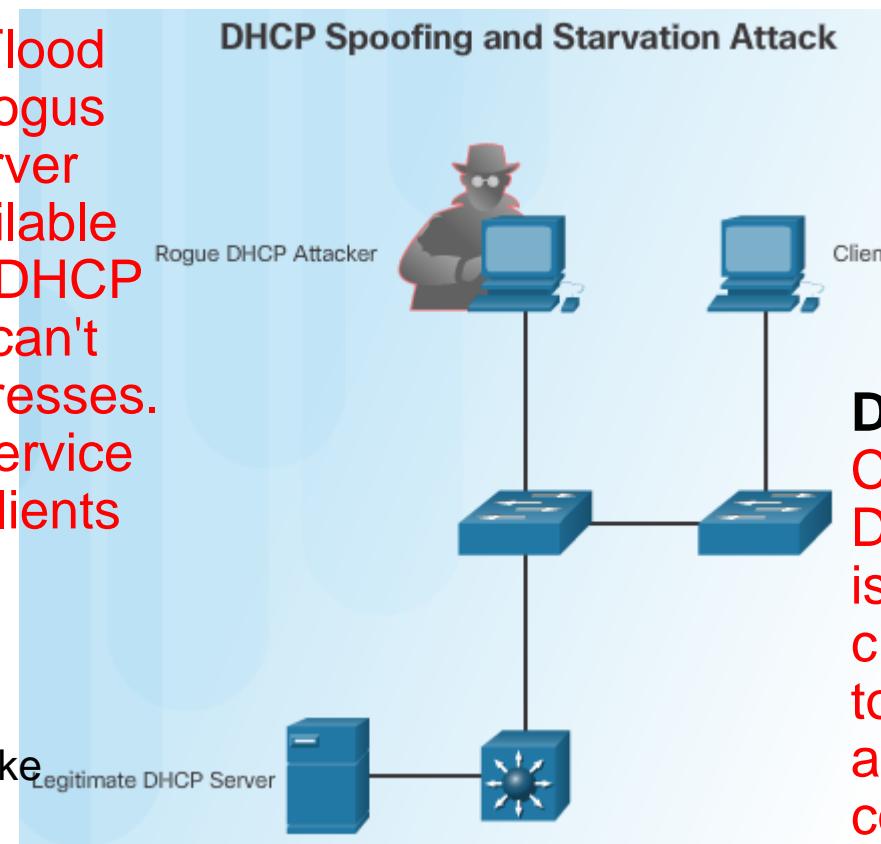
LAN Security

LAN Security Best Practices *

- This topic covers several Layer 2 security solutions:
 - Mitigating DHCP attacks using DHCP snooping (spoofing and starvation)

DHCP starvation. Flood DHCP server with bogus DHCP requests. Server leases all of the available IP addresses in the DHCP server pool. Server can't issue any more addresses. Result is denial-of-service (DoS) attack. New clients cannot get network access.

DHCP starvation is often used before spoofing. Take 'out' legitimate server. Easier to introduce fake DHCP server.



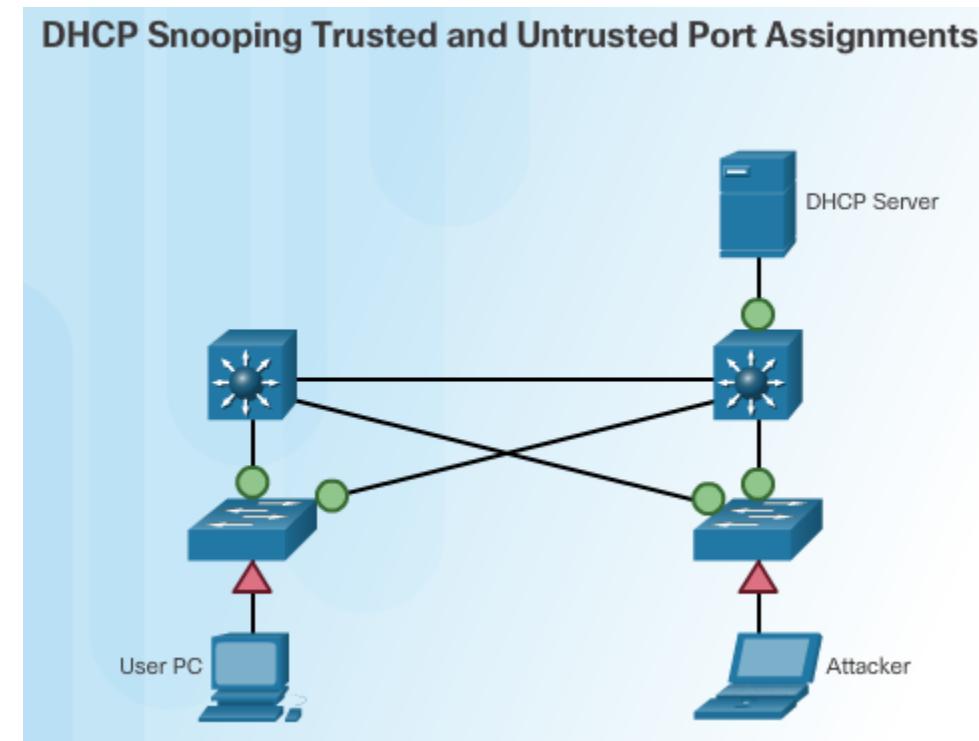
DHCP spoofing. Configures a fake DHCP server. Server issue IP addresses to clients. Forces clients to use false DNS server and computer under control of attacker default gateway.



LAN Security

Mitigate DHCP Attacks *

- Use Port Security
- Use DHCP Snooping
- Compares the DHCP source packet information with that held in a binding DB
 - Switch builds a DHCP binding table that maps a client MAC address, IP address, VLAN and port ID.
 - When DHCP snooping is configured, switch ports are configured as either a trusted port or an untrusted port.
 - A device connected to a trusted port can send any type of DHCP message into the switch.
 - An untrusted port only allows incoming DHCP requests.





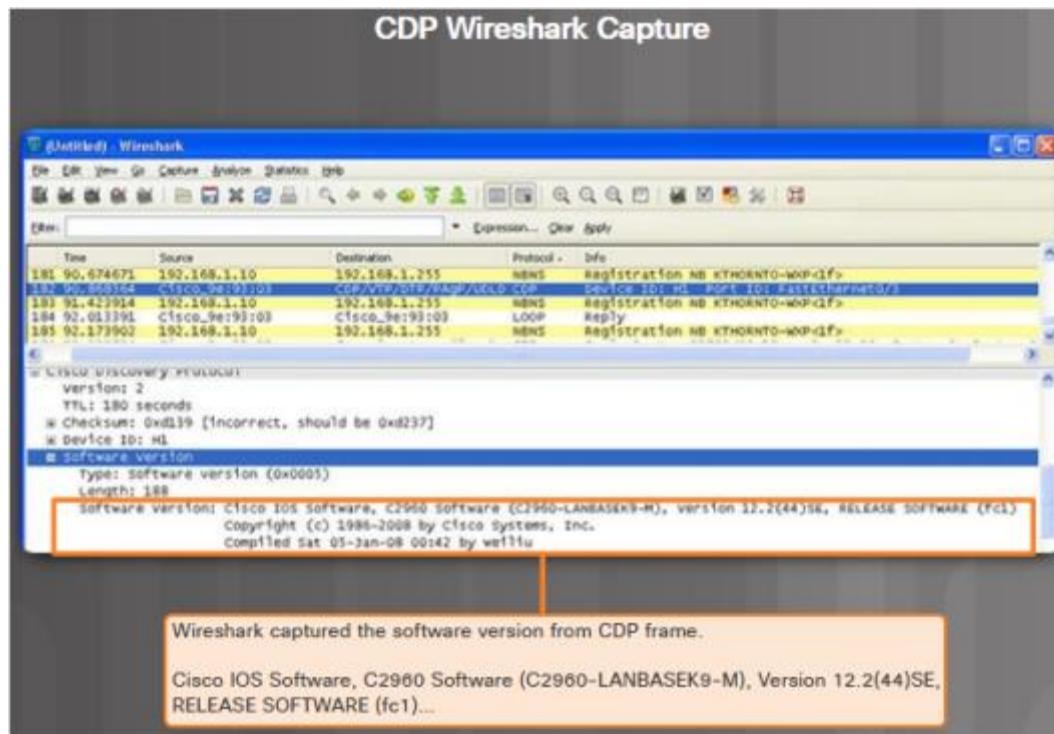
LAN Security

CDP Reconnaissance Attacks *

- Common attacks against the Layer 2 LAN infrastructure include:
 - CDP Reconnaissance Attacks
 - CDP = Cisco Discovery Protocol

CDP: Useful for troubleshooting.

CDP: Useful for attackers
- discover network infrastructure vulnerabilities.



See Wireshark capture...can identify the Cisco IOS software version used by the device.

Attacker can see any security vulnerabilities specific to IOS version..



LAN Security

Mitigate CDP Reconnaissance Attacks *

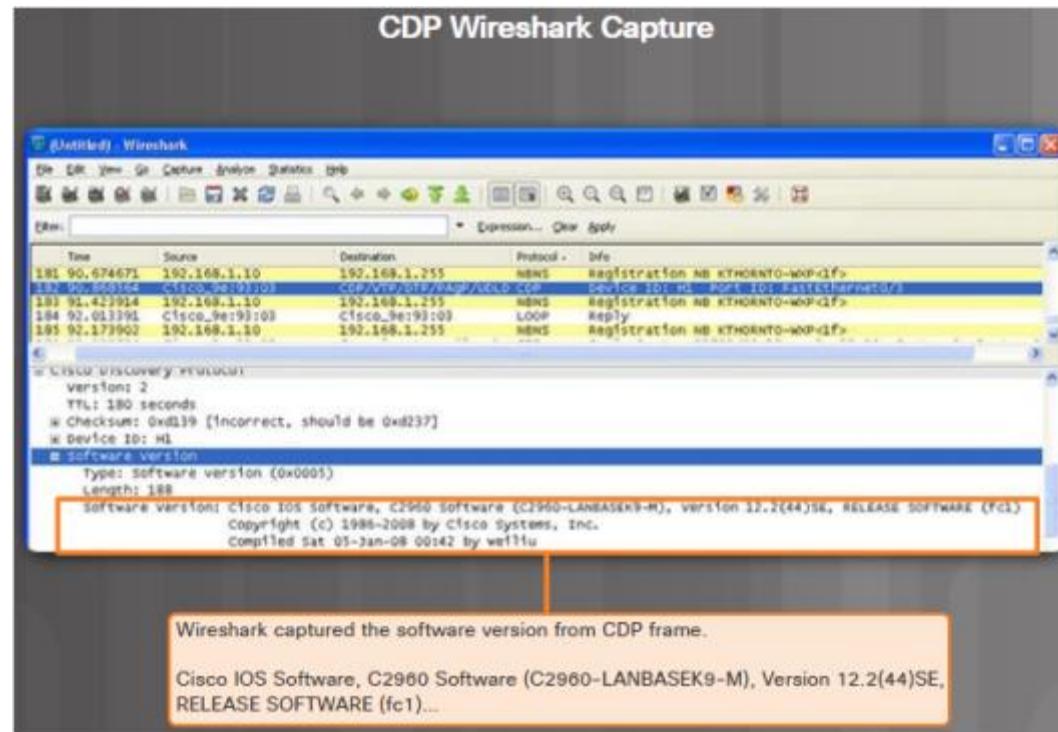
- Limit CDP on devices or ports.
- Disable CDP on edge ports that connect to untrusted devices

CDP globally disable: **no cdp run**

CDP globally enable: **cdp run**

CDP port disable: **no cdp enable** on interface

CDP port disable: **cdp enable** on interface





LAN Security LAN Security Attacks *

- Common attacks against the Layer 2 LAN infrastructure include:
 - Telnet Attacks

Brute Force Password Attack

This screenshot shows a password auditing tool interface. The main window displays a table of user accounts with columns for User Name, Password, Password Age (days), Password Score, Lasted Out, Disabled, Expired, Never Expires, Audit Time, and Method. The 'Method' column indicates that most accounts are being attacked using a dictionary attack (Dictionary) or precomputed hash attack (Precomputed Hash). The bottom pane shows a log of audit results, detailing successful password cracking attempts for users like 'lorge', 'mike', 'jerry', 'kathy', 'laura', 'ben', 'josh', 'and', 'jane', 'theresa', 'william', 'Administrator', 'stake', 'will', 'george', 'thomas', 'DeniseLee', and 'rita'. The log also notes that the auditing session was completed at 05/19/2004 16:44:44.

```

Administrator: a: 0: Fail: 00:00:00:0s: Dictionary
charles: aet: 0: Fail: 00:00:42s: Precomputed Hash
jorge: aaaaaa: 0: Fail: 00:00:29s: Precomputed Hash
mike: cost: 0: Fail: 00:00:30s: Precomputed Hash
laura: crackpot: 0: Fail: 00:00:0s: Dictionary
laura: lorange: 0: Fail: 00:00:57s: Precomputed Hash
ben: benben: 0: Fail: 00:00:57s: Precomputed Hash
josh: aaaa: 0: Fail: 00:00:20s: Dictionary
and: aaaa: 0: Fail: 00:00:39s: Precomputed Hash
kathy: keweenaw: 0: Fail: 00:00:0s: Dictionary
laura: laurajohnny: 0: Fail: 00:00:1s: Dictionary
jane: jrt: 0: Fail: 00:00:39s: Precomputed Hash
theresa: 123: 0: Fail: 00:00:39s: Precomputed Hash
william: emptyt: 0: Fail: 00:00:1s: Dictionary
Administrator: 123456789: 0: Fail: 00:00:0s: Dictionary
Administrator: a: 0: Fail: 00:00:1s: Dictionary
stake: *: 0: Fail: 00:00:0s: Dictionary
will: em: 0: Fail: 00:00:39s: Precomputed Hash
george: rrrrrr: 0: Fail: 00:00:49s: Precomputed Hash
thomas: rrrrrrrr: 0: Fail: 00:00:52s: Precomputed Hash
DeniseLee: aa: 0: Fail: 00:00:42s: Precomputed Hash
rita: aaa: 0: Fail: 00:00:0s: Dictionary

05/19/2004 16:43:35 Cracked password for lorange with Precomputed Hashes.
05/19/2004 16:43:35 Cracked password for mike with Precomputed Hashes.
05/19/2004 16:43:41 Cracked password for theresa with Precomputed Hashes.
05/19/2004 16:43:43 Cracked password for laura with Precomputed Hashes.
05/19/2004 16:43:47 Cracked password for lorraine with Precomputed Hashes.
05/19/2004 16:43:47 Cracked password for DeniseLee with Precomputed Hashes.
05/19/2004 16:44:43 Cracked password for laurajohnny with Precomputed Hashes.
05/19/2004 16:44:43 Cracked password for laura with Precomputed Hashes.
05/19/2004 16:44:44 Auditing session completed.
  
```

Example of Password Auditing Tool.

Two types of Telnet attack

1. Brute Force Password Attack

- 1st Phase: Dictionary attack.
- 2nd Phase: Password auditing tools to create sequential character combinations to guess the password.

2 Telnet DoS Attack

- Continuously request Telnet connections. Makes Telnet service. No admin access to device(s)...
- Can be used with other direct attacks to stop the admin access during a breach.



LAN Security

LAN Security Best Practices *

- There are several strategies to help secure Layer 2 of a network:
 - Always use secure variants of these protocols such as SSH, SCP, SSL, SNMPv3, and SFTP.
 - Always use strong passwords and change them often. (**Users & usability issues?**)
 - Enable CDP on select ports only.
 - Secure Telnet access.
 - Use a dedicated management VLAN where nothing but management traffic resides.
 - Use ACLs to filter unwanted access on vty lines etc.
 - Authenticate and authorize administrative access to the device using AAA with either TACACS+ or RADIUS protocols.

AAA: The Authentication, Authorization, and Accounting framework

TACACS+ : Terminal Access Controller Access Control System (TACACS+) protocol

RADIUS : Remote Authentication Dial-In User Service protocol



LAN Security

LAN Security Best Practices *

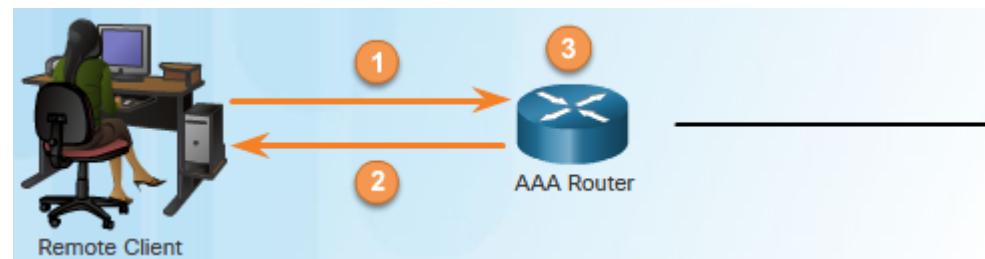
- AAA: The **Authentication**, **Authorization**, and **Accounting** framework. Used to secure administrative access to devices.
- Two common methods of implementing AAA
 - Local AAA Authentication –
 - Local database for authentication - stores usernames and passwords locally in the Cisco router, and users authenticate against the local database. Suitable for small networks.
 - Server-Based AAA Authentication –
 - Server-based AAA authentication - router accesses a **central AAA server** that contains the usernames and password for all users and serves as a central authentication system for all infrastructure devices.



LAN Security

LAN Security Best Practices *

- Local AAA Authentication



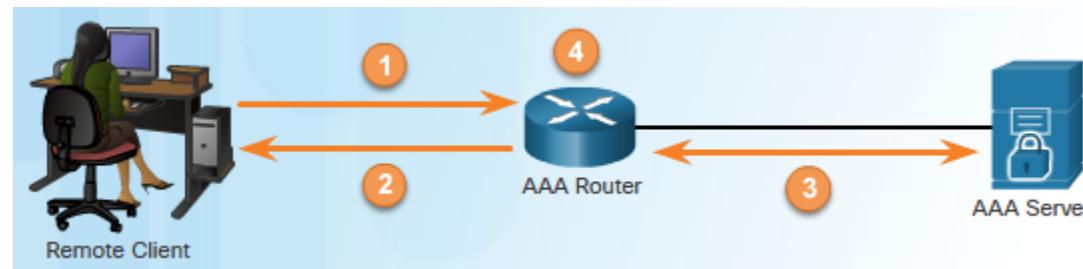
- 1 The client establishes a connection with the router.
- 2 The AAA router prompts the user for a username and password.
- 3 The router authenticates the username and password using the local database. User gets access to network based on the information in the local database.



LAN Security

LAN Security Best Practices *

- Server-Based AAA Authentication



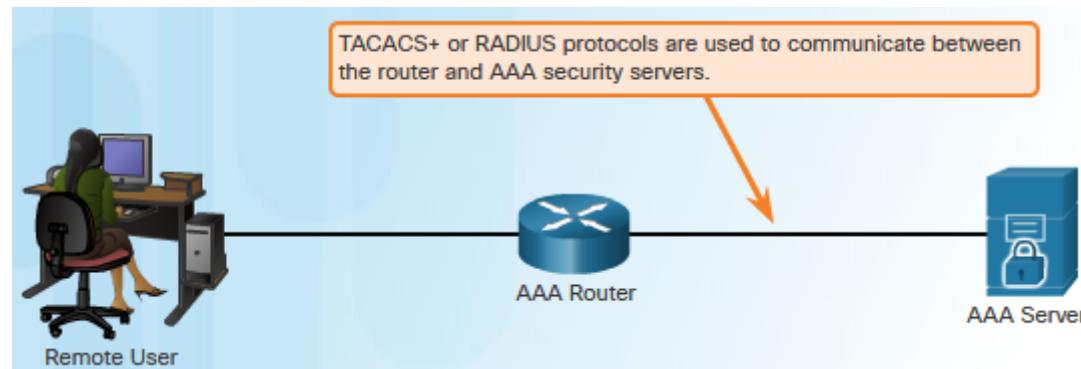
- 1 The client establishes a connection with the router.
- 2 The AAA router prompts the user for a username and password.
- 3 The router authenticates the username and password using a remote AAA server.
- 4 User gets access to network



LAN Security

LAN Security Best Practices *

■ Server-Based AAA Authentication: TACACS+ vs. RADIUS



- TACACS+ : Terminal Access Controller Access Control System (TACACS+) protocol
- RADIUS : Remote Authentication Dial-In User Service protocol

- Both TACACS+ and RADIUS protocols can be used to communicate between a router and AAA servers.
- TACACS+ is more secure. All TACACS+ protocol exchanges are encrypted.
- RADIUS only encrypts the user's password. User names & accounting not encrypted.



Chapter Summary

Summary

- At Layer 2, a number of vulnerabilities exist that require specialized mitigation techniques:
 - **MAC address table flooding attacks** are addressed with port security.
 - **VLAN attacks** are controlled by disabling DTP and following basic guidelines for configuring trunk ports.
 - **DHCP attacks** are addressed with DHCP snooping.
 - **CDP Reconnaissance Attacks** are addressed by limiting the use of CDP on devices or ports.
 - **Telnet Attacks** are addressed by
 - Using strong passwords that are changed often
 - Using SSH instead of Telnet
 - Restricting access on vty lines to admin devices only
 - Using AAA framework to secure admin access to devices.



WAN Technology– Revision 3



Connecting Networks

Cisco | Networking Academy®
Mind Wide Open™



Network Programming

Software-Defined Networking (SDN) *

- A network device contains the following **planes**: *

- **Control plane**

- Typically regarded as the **brains** of a device and is used to make **forwarding decisions**.
 - The control plane contains **Layer 2** and **Layer 3 route forwarding mechanisms**, such as routing protocol neighbor tables and topology tables, IPv4 and IPv6 routing tables, STP, and the ARP table.
 - Information sent to the control plane is processed by the CPU.

- **Data plane**

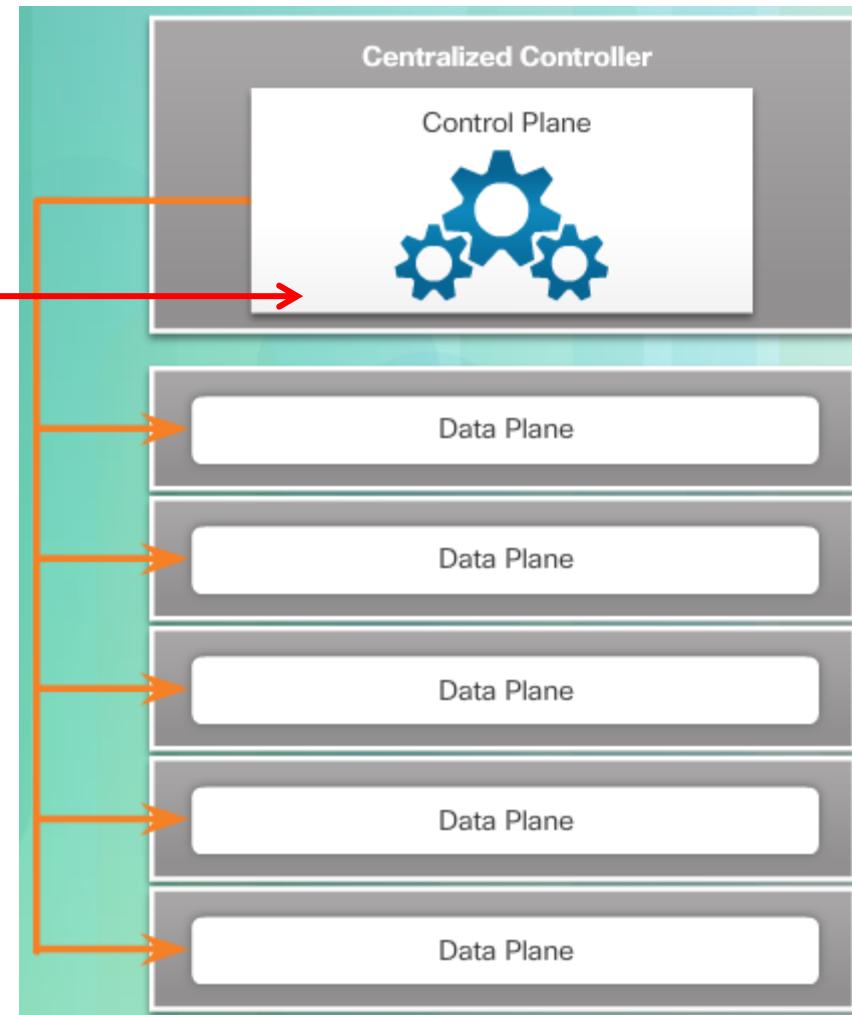
- Also called the **forwarding plane**, this plane is typically the **switch fabric** connecting the various network ports on a device.
 - The data plane of each device is used to forward traffic flows.
 - Routers and switches use information from the **control plane** to **forward incoming traffic** out the appropriate egress (exit) interface.
 - Information in the data plane is typically processed by a special data plane processor, such as a digital signal processor (DSP), without the CPU getting involved.



Network Programming

Software-Defined Networking *

- SDN virtualizes the network, removing the control plane function from each device and performing it on a **centralized controller**. —————
- The centralized controller communicates control plane functions to each device.
- Each device can now focus on forwarding data while the centralized controller manages data flow, increases security, and provides other services.





Network Programming

Software-Defined Networking

- Technology developed by VMware allows a host OS to support more than one client OS. Most of the current virtualisation technology is based on this.
- Major Virtualisation Architectures
 - **Software Defined Networking (SDN)** - A network architecture that virtualizes the network.
 - **Cisco Application Centric Infrastructure (ACI)** - A purpose-built hardware solution for integrating Cloud computing and data center management.



Network Programming

Software-Defined Networking

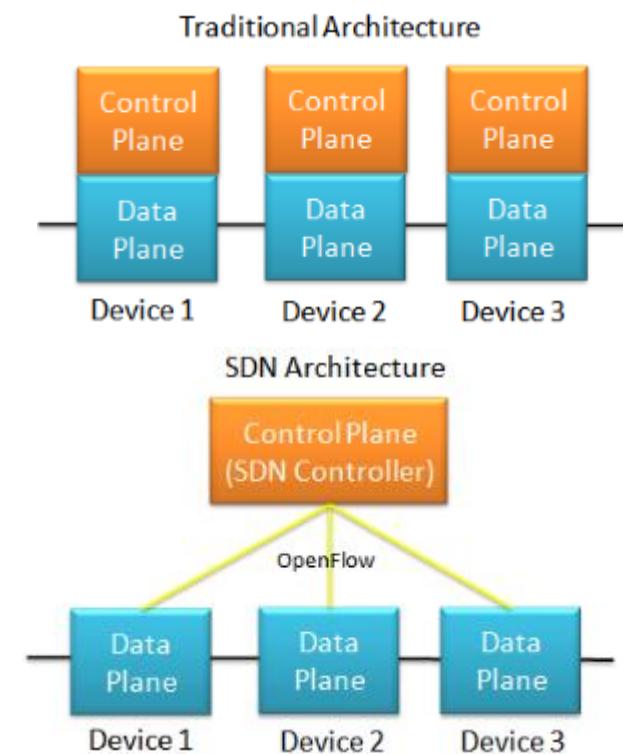
- Network virtualization techniques
 - OpenFlow
 - Developed at Stanford University to manage traffic between routers, switches, wireless access points, and a controller.
 - The OpenFlow protocol is a basic element in building SDN solutions.
 - OpenStack
 - A **virtualization** and **orchestration** platform for building **scalable Cloud environments** and providing an IaaS solution.
 - **Orchestration** in networking is the process of **automating** the provisioning of network components such as servers, storage, switches, routers, and applications.



Network Programming

Software-Defined Networking

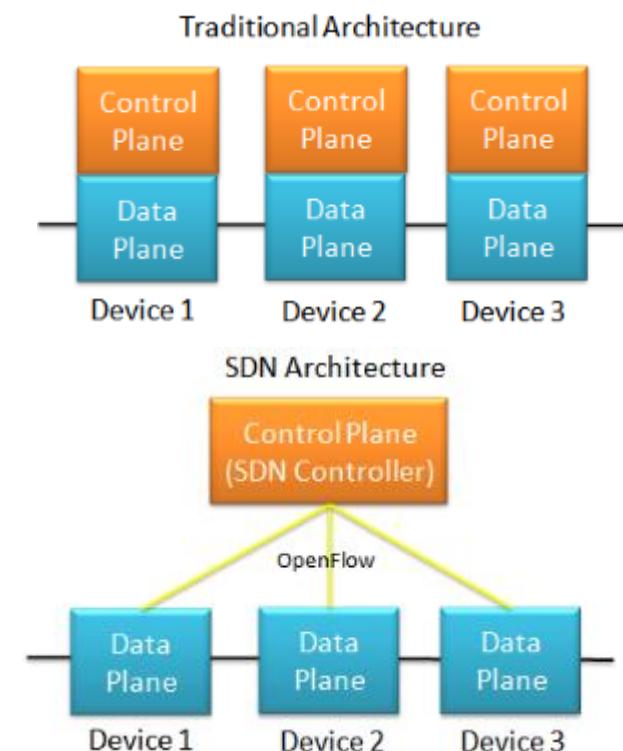
- **Traditional Router or Switch Architecture ***
 - Control plane and data plane functions are in the **same device**.
 - Routing decisions and packet forwarding are the responsibility of the device operating system
- **SDN Architecture ***
 - Controller-based SDN
 - Move control plane from each network device to a “*central network intelligence*” & policy-making entity called the **SDN controller**.
 - An architecture developed to virtualize the network.
 - Virtualizes the control plane.





Network Programming Software-Defined Networking

- The SDN controller is a **logical entity** that enables network administrators to manage and dictate **how the data plane** of virtual switches and routers should **handle network traffic**.
- It orchestrates, mediates, and facilitates communication between applications and network elements



<https://www.opennetworking.org/sdn-resources/sdn-definition>



Network Programming

Software-Defined Networking *

- The SDN controller defines the **data flows** that occur in the SDN Data Plane.
- A **flow** is a sequence of packets traversing a network that share a set of header field values.
 - e.g. a flow could consist of all packets with the same source and destination IP addresses, or all packets with the same VLAN identifier.
- Each flow through the network must first get **permission** from the SDN controller, which verifies that the communication is permissible according to the **network policy**.
- If the controller allows a flow, it computes a route for the flow to take, and adds an entry for that flow in each of the switches along the path.

Note: Network Policy = a set of rules for the behaviour of network devices.

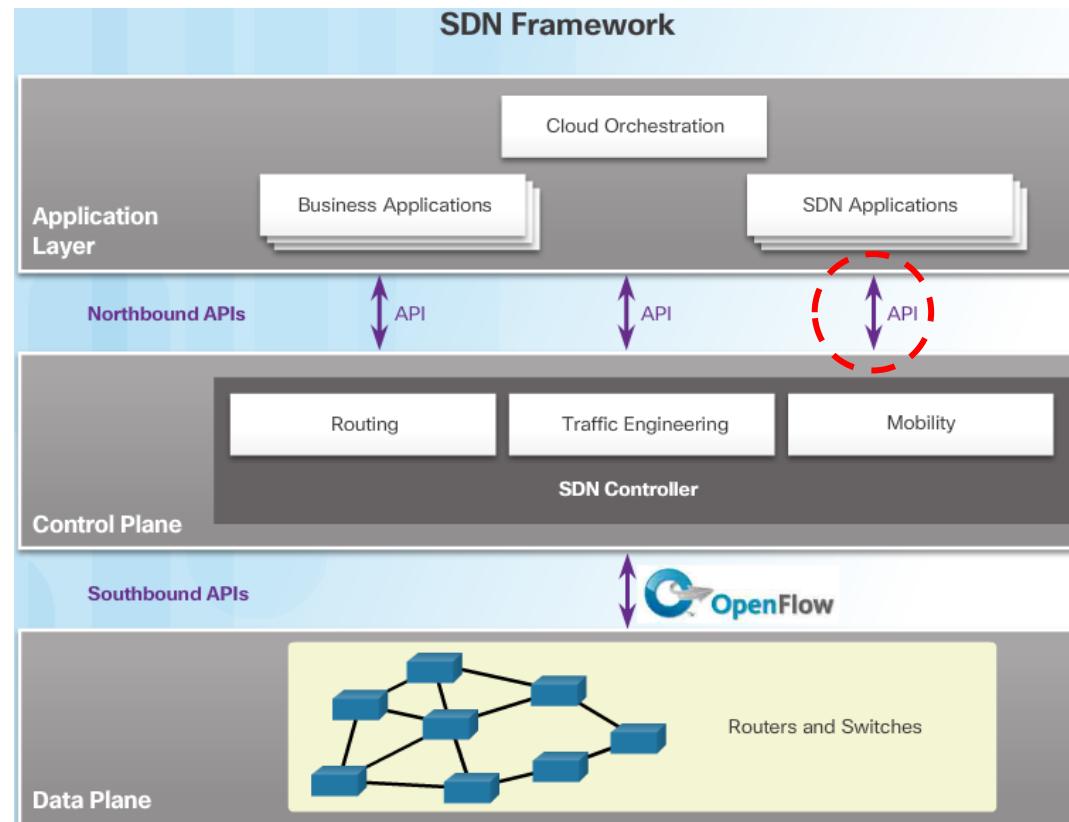
See <https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-network-policy.html>



Network Programming

Software-Defined Networking

- The SDN framework uses northbound APIs to communicate with upstream applications and southbound APIs to define the behaviour of downstream routers and switches.

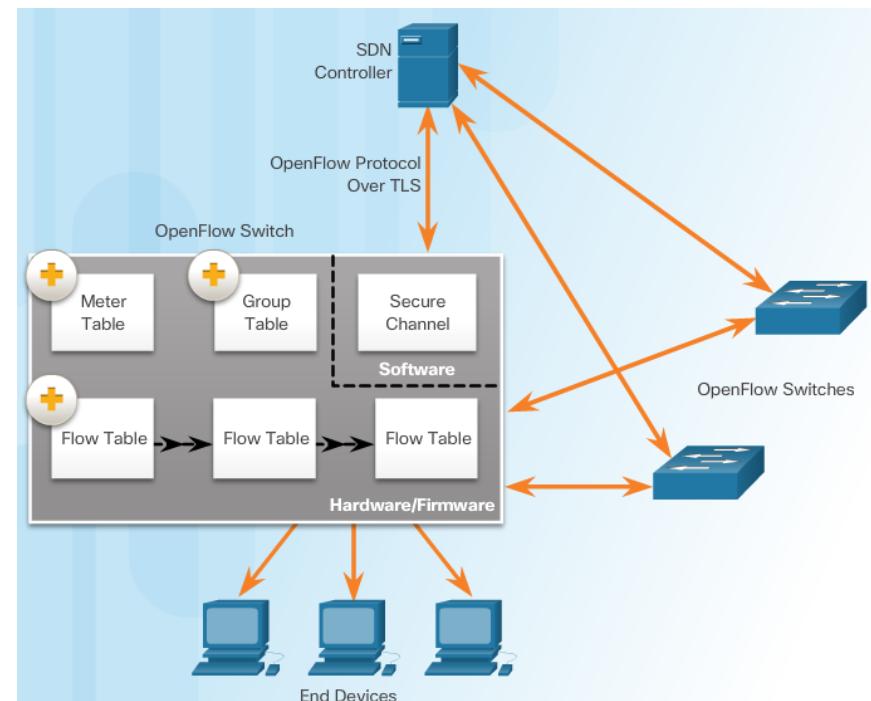


**APIs =>
Network
Programming**



Network Programming Controllers *

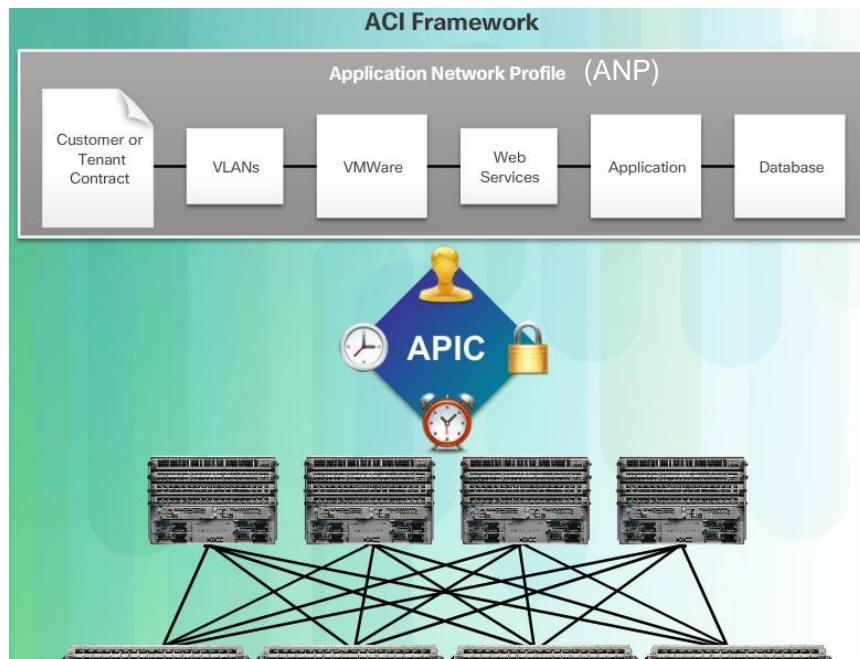
- The SDN controller defines the data flows that occur in the SDN Data Plane.
- Using the OpenFlow protocol, the controller populates a series of tables implemented in hardware or firmware
- The following tables manage the flows of packets through the switch:
 - **Flow table** - This table matches incoming packets to a particular flow and specifies the functions that are to be performed on the packets. There may be multiple flow tables that operate in a pipeline fashion.
 - **Group table** - A flow table may direct a flow to a Group Table, which may trigger a variety of actions that affect one or more flows.
 - **Meter table** - The table triggers a variety of performance-related actions on a flow.





Network Programming Controllers

- Cisco developed the Application Centric Infrastructure (ACI) to automate the network, accelerate application deployments, and align IT infrastructures to better meet business requirements.
- These are the three core components of the ACI architecture:
 - **Application Network Profile (ANP)** - a collection of end-point groups (EPG), their connections, and the policies that define those connections
 - **Application Policy Infrastructure Controller (APIC)** - a centralized software controller that manages downstream switches. It translates application policies into network programming.
 - **Cisco Nexus 9000 Series switches** - provide an application-aware switching fabric and work with an APIC to manage the virtual and physical network infrastructure.

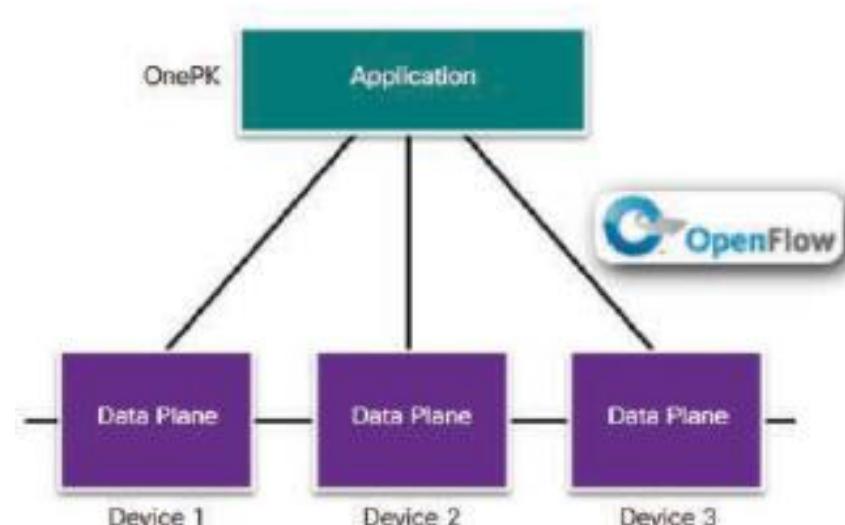


The Cisco **APIC - Enterprise Module (APIC-EM)** extends ACI aimed at enterprise and campus deployments.



Network Programming Controllers

- There are three basic types of SDN:
 - **Device-based SDN** - Devices are **programmable by applications** running on the device itself or on a server in the network. Cisco OnePK is an example of a device-based SDN.



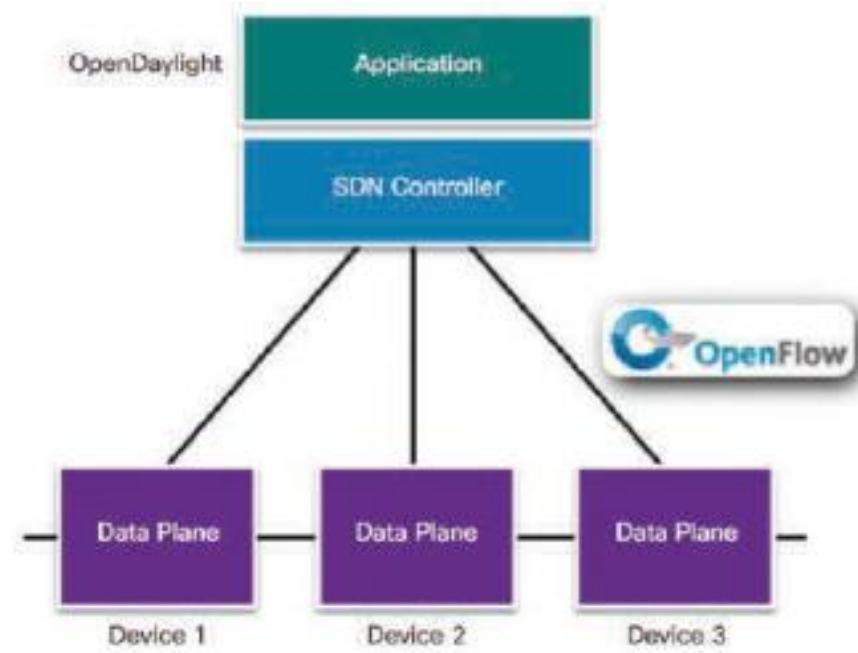


Network Programming Controllers

- There are three basic types of SDN:

- **Controller-based SDN -**

Centralized controller that has knowledge of all devices in the network. The applications can interface with the controller responsible for managing devices and manipulating traffic flows throughout the network. The Cisco Open SDN Controller is a commercial distribution of OpenDaylight.



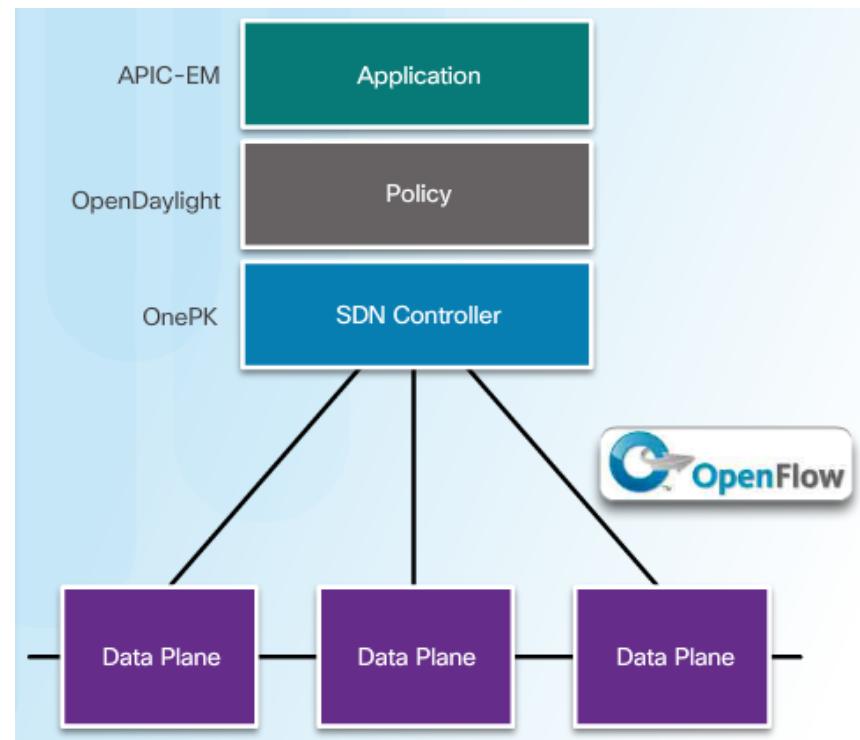
Note: OpenDaylight = an open source SDN controller.

See <https://www.opendaylight.org>



Network Programming Controllers

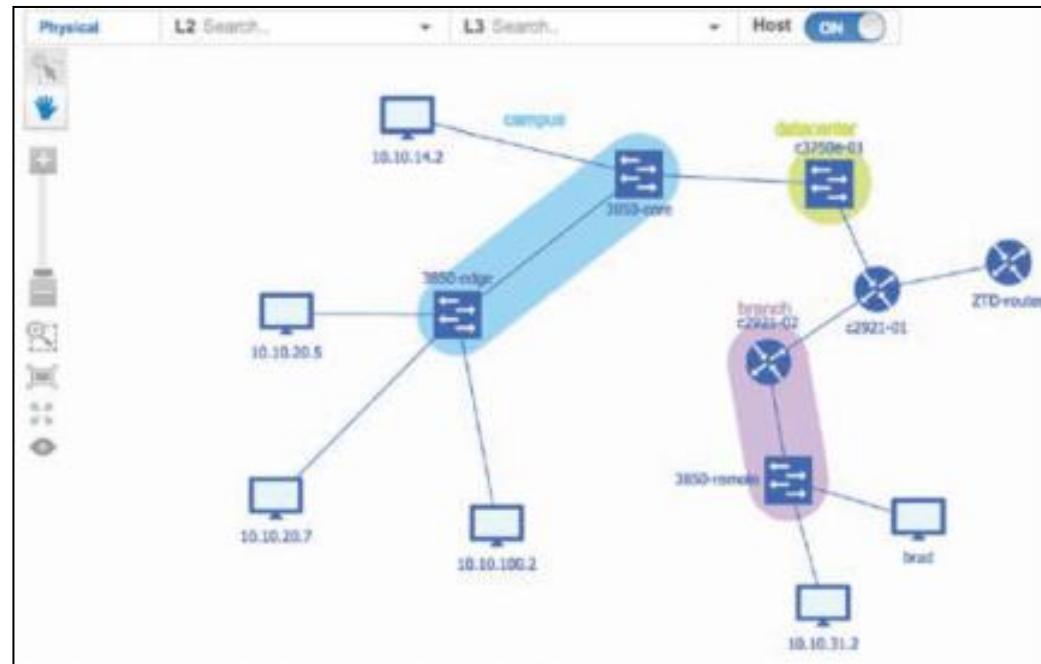
- There are three basic types of SDN:
 - **Policy-based SDN** - Includes an additional Policy layer that operates at a higher level of abstraction. No programming skills are required.
 - **Cisco APIC-EM** is an example of this type of SDN.





Network Programming Controllers

- Cisco APIC-EM provides the following features:
 - **Discovery** - populates controller's device & host inventory database
 - **Device Inventory** - collects detailed info from devices in the network
 - **Host Inventory** - collects detailed info from hosts in the network
 - **Topology** - supports a graphical view of the network (topology view)





Network Programming Controllers

- **Policy** - ability to view and control policies across the entire network including QoS.
- **Policy Analysis** - ability to trace application specific paths between end devices to quickly identify ACLs in use and problem areas including *ACL Analysis* and *ACL Path Trace*
 - **ACL Analysis** - examines ACLs on devices, searching for redundant, conflicting, or shadowed entries (incorrect ACL entries)

The screenshot shows the 'Policy Analysis' section of the Cisco Network Programming Controller. The left sidebar has a 'Policy Analysis' tab selected. The main area displays a summary of conflicts:

Category	Count
shadowed	1
redundant	7
correlated	1

Below this, a list of 12 ACL entries is shown, each with a status icon (green, yellow, red) and a conflict type (e.g., shadowed, redundant, correlated). The entries are:

1. **shadowed**: DENY TCP host 192.168.1.10 any eq WWW
2. **redundant**: PERMIT TCP any host 161.120.33.40 eq WWW
3. **correlated**: DENY TCP host 192.168.1.10 any eq WWW
4. **shadowed**: DENY TCP host 140.192.37.1 host 140.11.25.55 eq WWW
5. **redundant**: DENY TCP 100.6.3.0/24 any eq FTP
6. **correlated**: PERMIT TCP 140.192.37.0/24 any eq FTP
7. **correlated**: PERMIT TCP 140.192.37.0/24 host 161.120.33.40 eq FTP
8. **shadowed**: DENY TCP 192.168.1.10 any eq WWW
9. **redundant**: DENY TCP any any eq FTP
10. **redundant**: DENY TCP any any eq 458
11. **redundant**: DENY UDP any any eq 458
12. **correlated**: PERMIT IP any any

On the right, three conflict types are detailed:

- Line 2 shadows line 8**:
 - 2. PERMIT TCP any host 161.120.33.40 eq WWW
 - 8. DENY TCP 140.192.37.0/24 host 161.120.33.40 eq WWW
- Line 2 correlated lines 1**:
 - 2. PERMIT TCP any host 161.120.33.40 eq WWW
 - 1. DENY TCP host 140.192.37.10 any eq WWW
- Line 2 redundant lines 3**:
 - 2. PERMIT TCP any host 161.120.33.40 eq WWW
 - 3. PERMIT TCP host 161.120.33.41 host 161.120.33.40 eq WWW

Sample ACL Analysis



Network Programming Controllers

- **ACL Path Trace** - examines specific ACLs on the path between two end nodes, displaying any potential issues.

Sample ACL Path Trace



Chapter Summary

Summary

- SDN is a network architecture that has been developed to virtualize the network. The SDN controller defines the data flows that occur in the SDN data plane.
- The three types of SDN are:
 - Device-based SDN
 - Controller-based SDN
 - Policy-based SDN
- Policy-based SDN, such as Cisco's APIC-EM, provides a simple mechanism to control and manage policies across the entire network.
- The ability to manage policies is one of the most important features of the APIC-EM controller.