



Module 7

Quality of Service

ITNET04

WAN Connectivity



Module Objectives

Module Title: Quality of Service

Module Objectives:

- Explain the purpose and characteristics of QoS.
- Explain how networking devices implement QoS

Module References:

- CCNAv7 ENSA– Module 9

7.1 QoS Overview

Different Types of Traffic

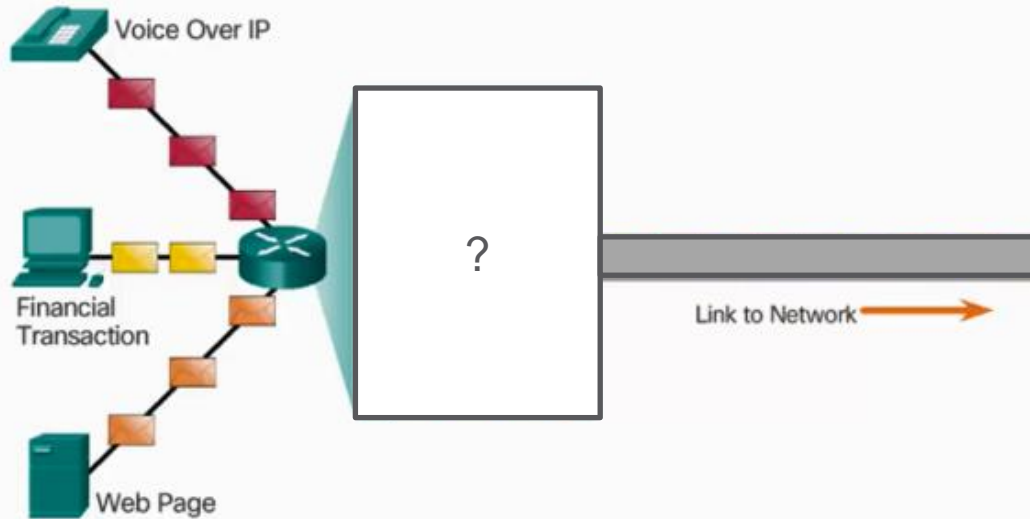
In a typical school network, what types of network traffic would you normally expect to find?

If you were the network administrator, which of these traffic would you consider important?

Network Transmission Quality

The Purpose of QoS

QoS – What is it and why is it needed?

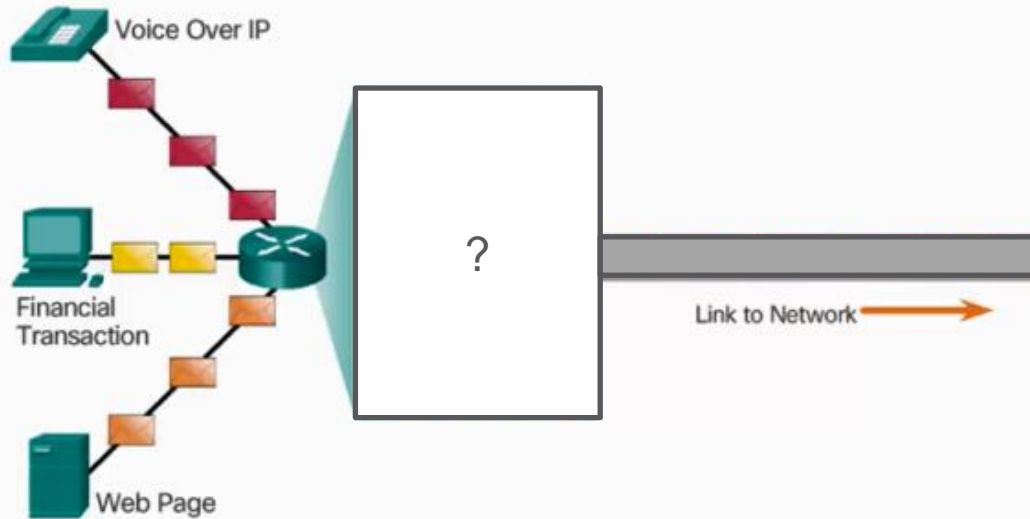


- Congestion occurs when multiple communication lines aggregate onto a single device, and then much of that data is placed on fewer outbound interfaces or onto a slower interface.
- When the volume of traffic is greater than what can be transported across the network, devices queue the packets in memory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

Network Transmission Quality

The Purpose of QoS

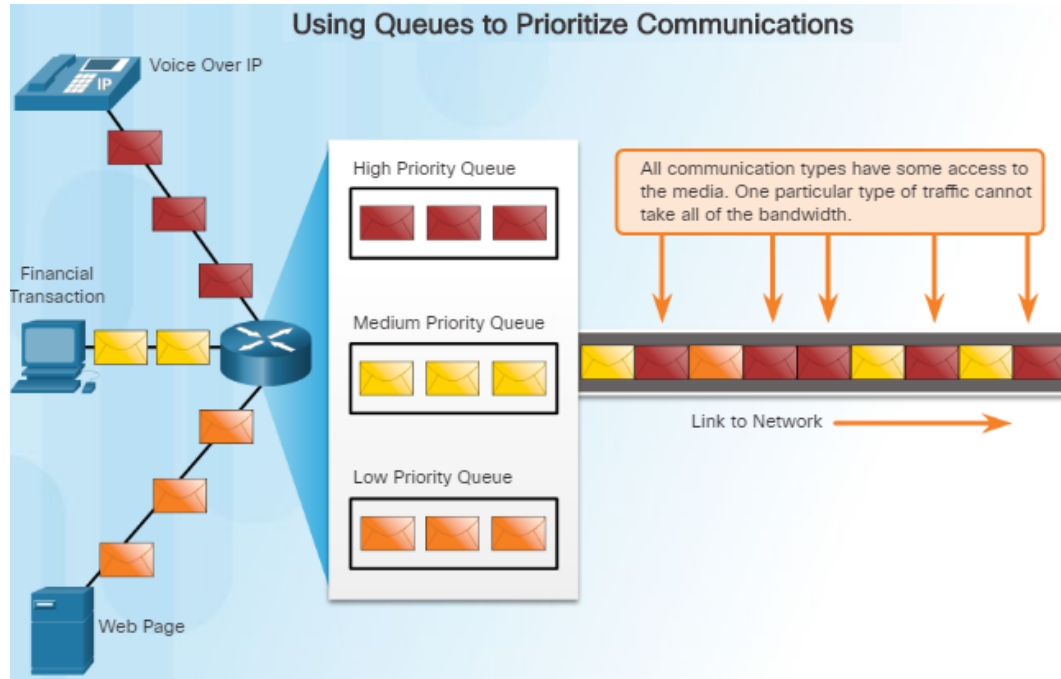
QoS – What is it and why is it needed?



- QoS or Quality of Service, allows the network administrator to prioritize certain types of traffic over others.
- Example:
 - Video traffic and voice traffic require greater resources, such as bandwidth, from the network than other types of traffic.
 - Financial transactions are time sensitive and require minimal transmission delay
 - An FTP transfer or web traffic (HTTP) may tolerate some delay in transmission without significantly impacting user experience.
- A QoS technique that can help manage these different traffic is to classify data into multiple queues

Network Transmission Quality

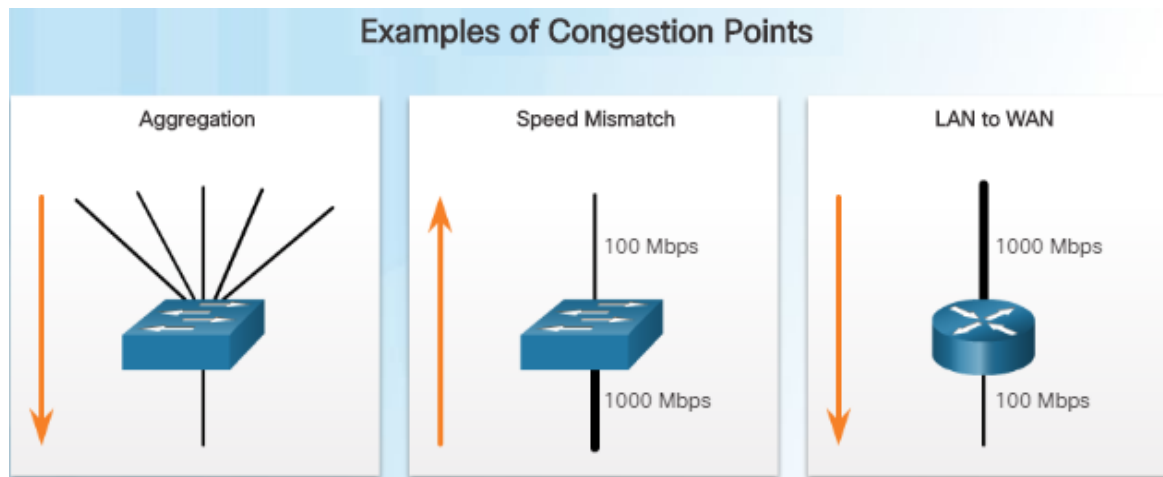
Prioritizing Traffic



- Packets are buffered at the router and three priority queues are established:
 - High Priority Queue
 - Medium Priority Queue
 - Low Priority Queue
- Packets from each queue are allocated resources based on their priority
- QoS is an ever increasing requirement of networks today due to new applications which create higher expectations for quality delivery.
- Note that a device should implement QoS only when it is experiencing congestion.

Bandwidth, Congestion, Delay, and Jitter

- Network bandwidth is measured in the number of bits that can be transmitted in one second (bps).
- Network congestion causes delay. An interface experiences congestion when it is presented with more traffic than it can handle.



Bandwidth, Congestion, Delay, and Jitter

- Delay or latency refers to the time it takes for a packet to travel from the source to the destination.
 - Fixed delay – delays that all packets experience regardless of network conditions

Delay	Description
Code Delay	Time to compress data at source before transmitting to the first internetworking device
Packetization Delay	Time to encapsulate a packet with all necessary headers
Serialization Delay	Time to transmit a frame onto the network media
De-jitter Delay	Time to buffer a flow of packets then send them out in evenly spaced intervals

- Variable delay – delays that are introduced depending on network conditions at a given time

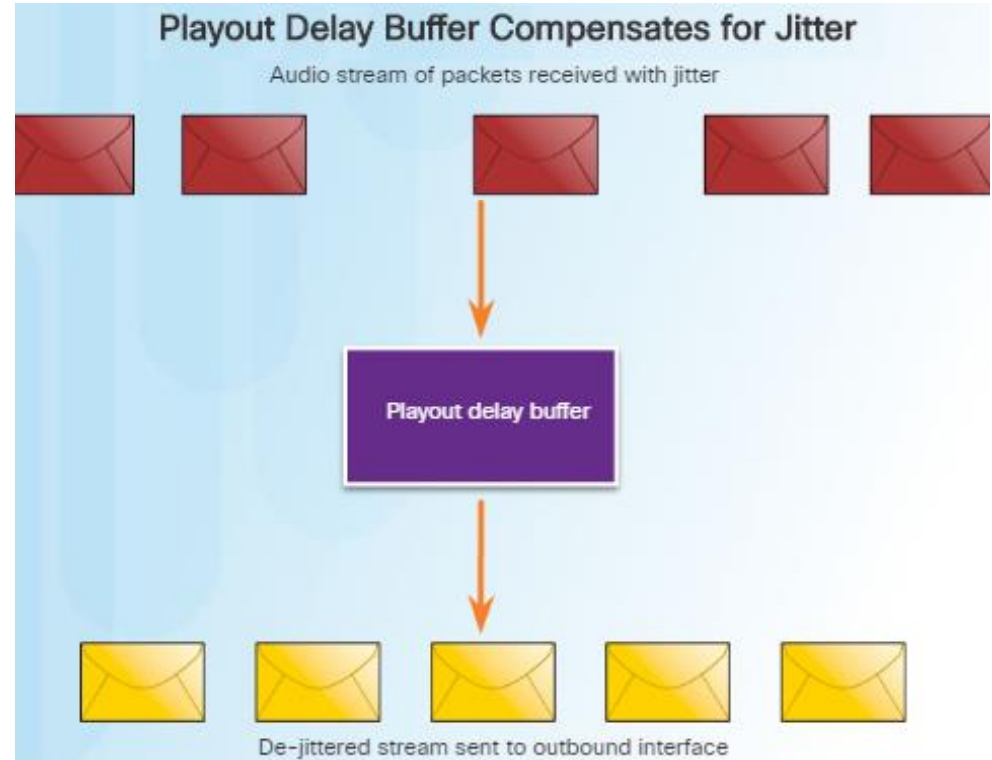
Delay	Description
Queuing Delay	Time a packet waits to be transmitted on the link
Propagation Delay	Time for a packet to travel between source and destination

- Jitter is the variation in delay of received packets.

Network Transmission Quality

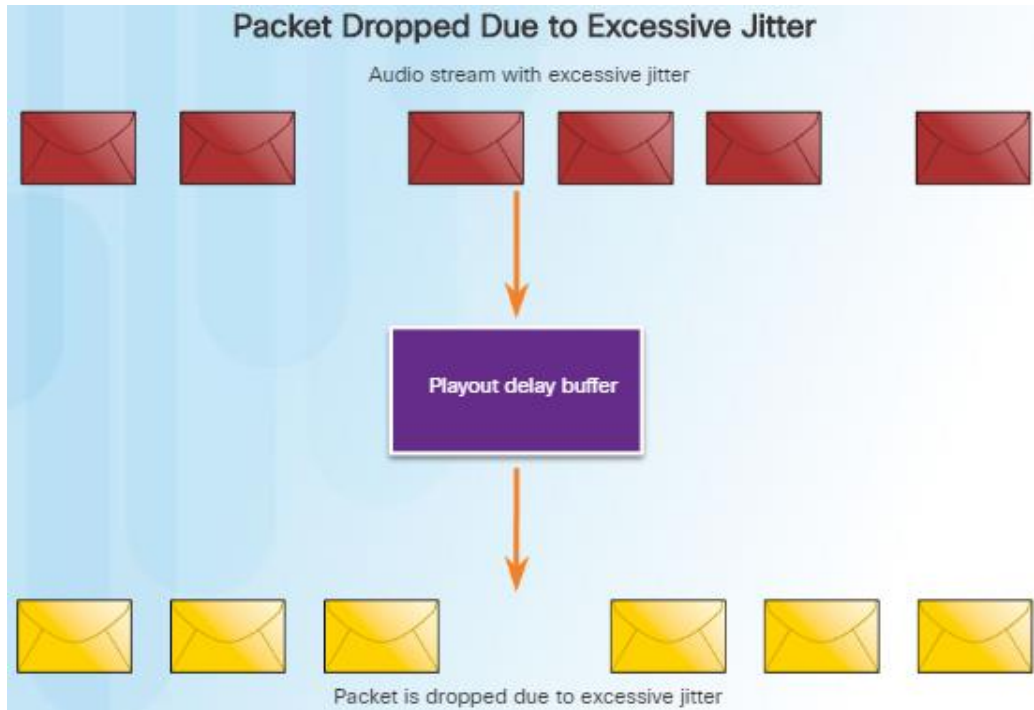
Packet Loss

- Without any QoS mechanisms in place, packets are processed in the order in which they are received and can be dropped when congestion occurs.
- Example: A router receives a digital audio stream for VoIP.
 - Because VoIP is time-sensitive, router must compensate for the jitter that is encountered.
 - Playout delay buffer performs this function by buffering these packets and then transmitting them in a steady stream.
 - The digital packets are later converted back to an analog audio stream.



Network Transmission Quality

Packet Loss (Cont.)



- If the jitter is too large that it causes packets to be received out of the range of the buffer, the out-of-range packets are discarded
 - For minimal losses, the digital signal processor (DSP) can interpolate what it thinks the audio should be and no problem is audible to the user.
 - When jitter exceeds what the DSP can handle, audio problems are heard.
- In a properly designed network, voice packet loss should be zero
- Network engineers use QoS mechanisms to classify voice packets for zero packet loss.

Traffic Characteristics

Network Traffic Trends

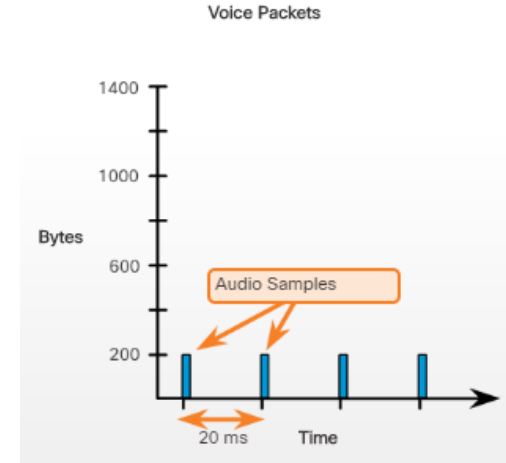


- In the year 2000s, the predominant types of IP traffic are voice, data and video.
 - Voice traffic has a predictable bandwidth need and known packet arrival times.
 - Data traffic is not real-time and has an unpredictable bandwidth need.
 - Video traffic is greedy in bandwidth
- According to the Cisco Visual Networking Index (VNI), video traffic represented 67% of all traffic in 2014. By 2019, video will represent 80% of all traffic.
- The type of demands that voice, video, and data traffic place on the network are very different.

Traffic Characteristics

Voice

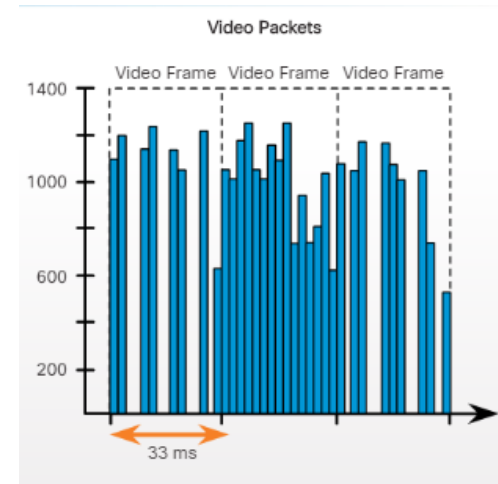
- Characteristics:
 - Predictable and smooth.
 - Very sensitive to delay and dropped packets;
 - Not required to retransmit voice if packets are lost.
 - Can tolerate a certain amount of latency, jitter, and loss without any noticeable effects.
- One-way Requirements:
 - Latency ≤ 150 ms.
 - Jitter ≤ 30 ms.
 - Voice packet loss $\leq 1\%$.
 - Bandwidth = 30 to 128 kbps
 - Packets must receive a higher priority than other types of traffic.



Traffic Characteristics

Video

- Characteristics:
 - Greedy - has a high volume of data per packet
 - Bursty – number and size of video packets sent varies per unit of time
 - Less resilient to loss and drop sensitive, delay sensitive
 - With insufficient bandwidth, video quality typically degrades (blurry picture or unsynchronized audio)
- One way requirements:
 - Latency $\leq 200 - 400$ ms
 - Jitter $\leq 30 - 50$ ms
 - Loss $\leq 0.1 - 1\%$
 - Bandwidth = 384 Kb/s to 20+ Mb/s



Traffic Characteristics

Data

- Applications may use TCP or UDP, hence characteristics and requirements vary depending on application
 - Data applications that have no tolerance for data loss, such as email and web pages, use TCP to ensure packets will be resent in the event they are lost.
 - Some TCP applications can be very greedy, consuming a large portion of network capacity (e.g. FTP)
- Relatively insensitive to drops and delays, but a network administrator still needs to consider the quality of the user experience.
- Traffic prioritization is determined based on 2 factors:

		Is the application interactive?	
		Yes	No
Is it mission critical?	Yes	Prioritize for lowest delay among data traffic (1-2 sec response time)	Delay can vary greatly as long as minimum bandwidth is supplied
	No	Application could benefit from lower delay	Provide any leftover bandwidth after all other traffic needs are met

7.2 QoS Mechanisms

Selecting an Appropriate QoS Policy Model

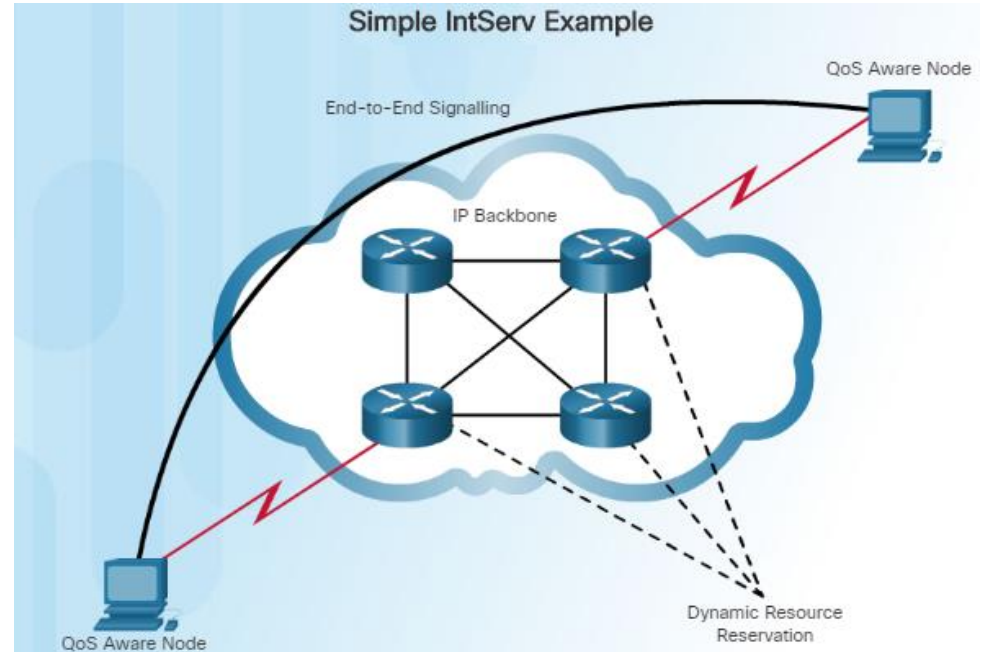
- How can QoS be implemented in a network? The three models for implementing QoS are these:
 - Best-effort model
 - Integrated services (IntServ)
 - Differentiated Services (DiffServ)
- The table in the figure to the left summarizes these three models.
- QoS is implemented in a network using either or both of these:
 - IntServ – provides the highest guarantee of QoS, but is resource-intensive
 - DiffServ – less resource intensive and more scalable

Best-Effort

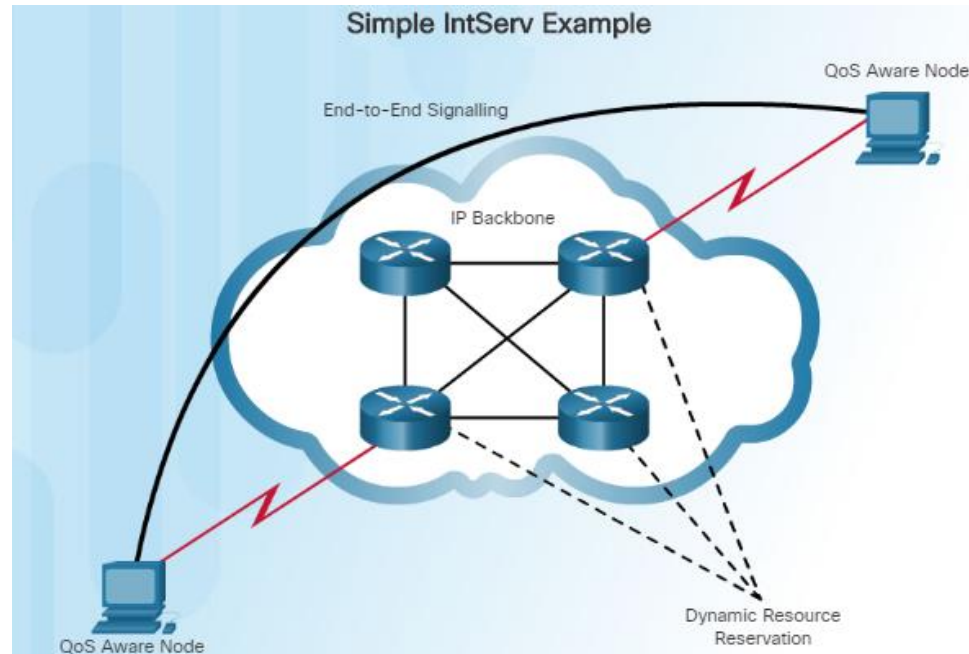
- The basic design of the Internet - treats all network packets the same way and provides no guarantees
- Basically no QoS - the network cannot tell the difference between packets.
- Pros:
 - Most scalable and is limited only by bandwidth
 - No special QoS mechanisms needed
 - Easiest and quickest model to deploy
- Cons
 - No guarantee of delivery – Packets arrive in any order and may not arrive at all
 - No preferential treatment of packets hence critical data is handled in the same way as non-essential data

Integrated Services (IntServ)

- Provides a way to deliver end-to-end QoS that real-time applications require by explicitly managing network resources to provide QoS to specific user packet streams.
- Development of the model in 1994 was motivated by the needs of real-time applications, such as remote video, multimedia conferencing, visualization, and virtual reality
- Uses a connection-oriented approach inherited from telephony network design.

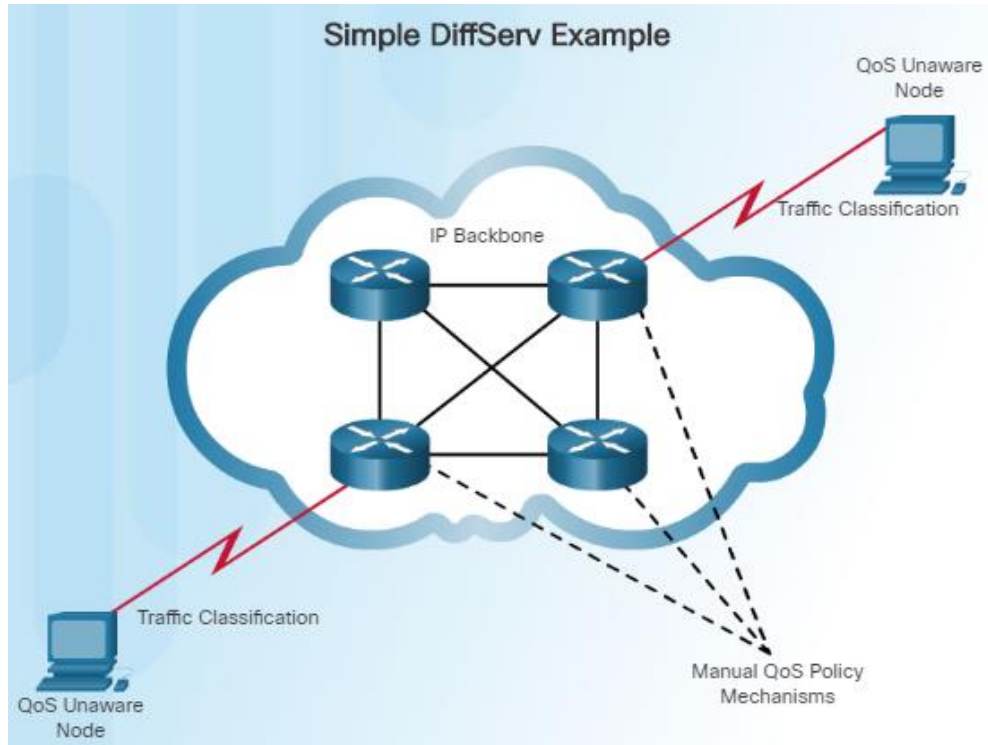


Integrated Services (con't)



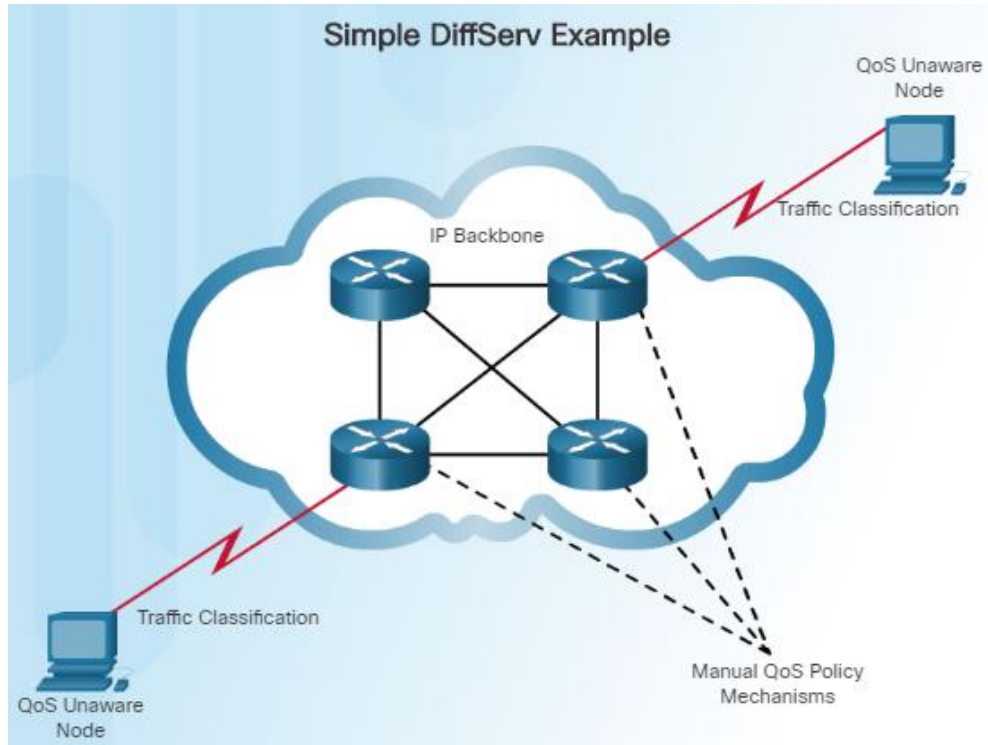
- Uses resource reservation and admission-control to establish and maintain QoS.
 - Step 1: The application informs the network of its traffic profile and requests a particular kind of service that can encompass its bandwidth and delay requirements.
 - Step 2: IntServ uses the Resource Reservation Protocol (RSVP) to signal the QoS needs of an application's traffic along devices in the end-to-end path through the network.
 - Step 3: If the network devices along the path can reserve the necessary bandwidth, the originating application can begin transmitting – otherwise, no data is sent.
- Provides the highest guarantee of QoS, but is resource-intensive

Differentiated Services (DiffServ)



- The differentiated services (DiffServ) QoS model:
 - Specifies a simple and scalable mechanism for classifying and managing network traffic.
 - Provides QoS guarantees on modern IP networks.
 - Can provide low-latency guaranteed service to critical network traffic such as voice or video.
- Not an end-to-end QoS strategy because it cannot enforce end-to-end guarantees. However, it is a more scalable approach to implementing QoS.

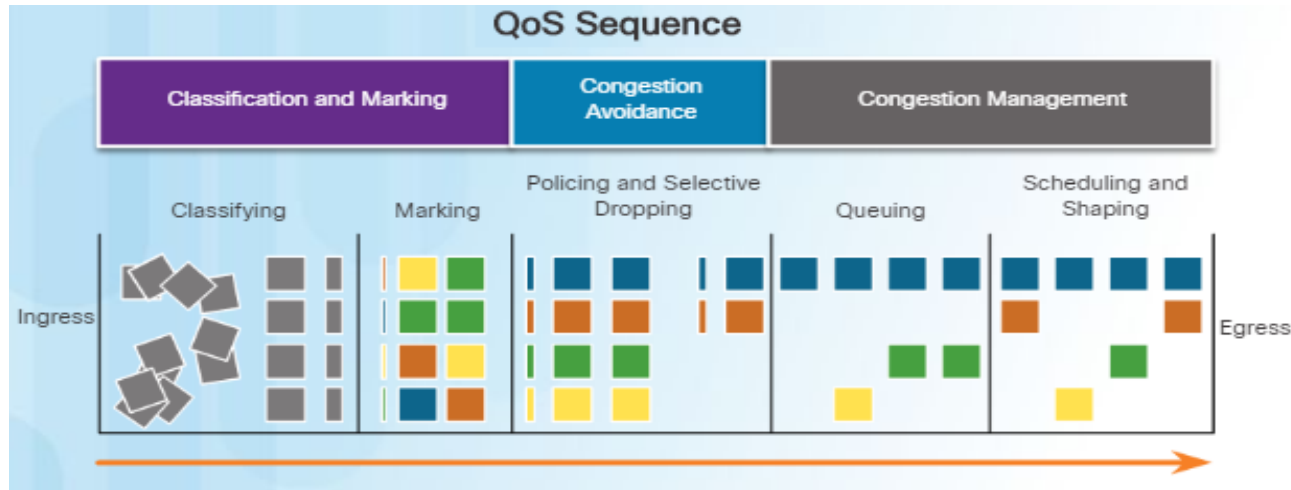
Differentiated Services (Cont.)



- DiffServ divides network traffic into classes based on business requirements. Each class can then be assigned a different level of service.
- DiffServ enforces and applies QoS mechanisms on a hop-by-hop basis uniformly applying global meaning to each traffic class to provide both flexibility and scalability.
- Overcomes the limitations of both the best-effort and IntServ models by providing an “almost guaranteed” QoS while still being cost-effective and scalable.

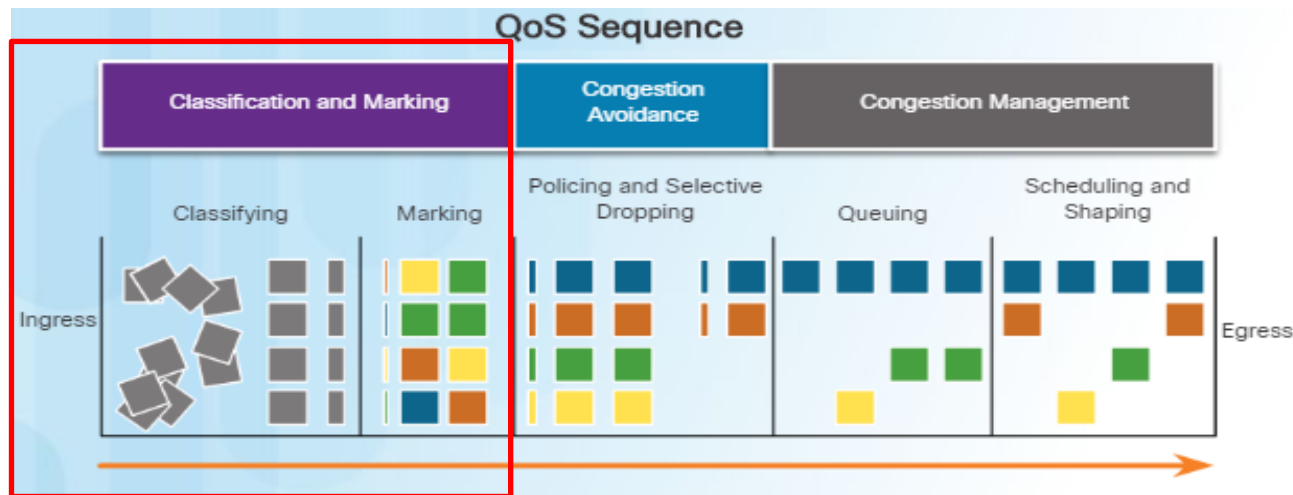
QoS Tools

- QoS implementation tools can be categorized into three main categories:
 - Classification and marking tools – Session traffic is classified into different priority groupings and packets are marked.
 - Congestion avoidance tools – Traffic classes are allotted network resources and some traffic may be selectively dropped, delayed or remarked to avoid congestion.
 - Congestion management tools – During congestion, traffic is queued to await the availability of those resources; tools include class based weighted fair queuing, and low latency queuing.



Classification and Marking

- Classification and marking allows identification of packet types and determines the class of traffic to which packets or frames belong so that a QoS policy can be applied
 - Layer 2 and 3 - methods include using interfaces, ACLs, and class maps.
 - Layers 4 to 7 - using Network Based Application Recognition (NBAR).
- Marking adds a value to the packet header and devices that receive the packet look at this field to see if it matches a defined policy.



Classification and Marking Technologies

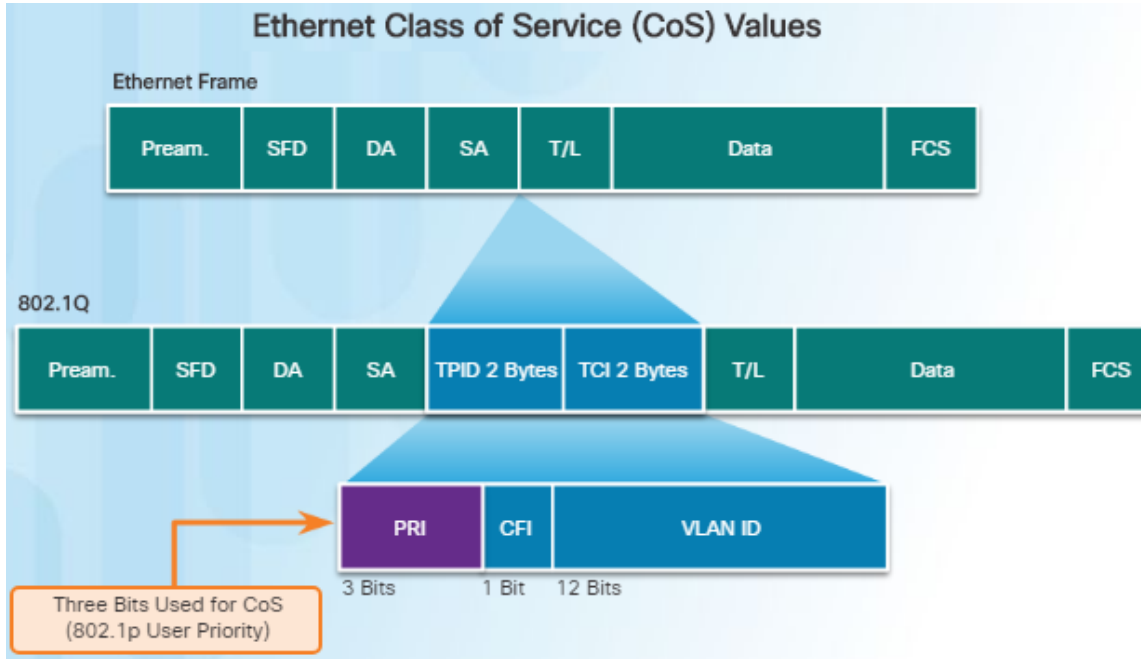
- Marking may be performed at Layer 2 or 3 using various technologies and works by utilizing specific fields in frame / packet headers

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	3
IPv4 and IPv6	3	Differentiated Services Code Point (DSCP)	6

- When deciding whether to mark at Layer 2 or Layer 3, the following points should be considered:
 - Layer 2 marking of frames can be performed for non-IP traffic.
 - Layer 2 marking of frames is the only QoS option available for switches that are not “IP aware”.
 - Layer 3 marking will carry the QoS information end-to-end.

QoS Implementation Techniques

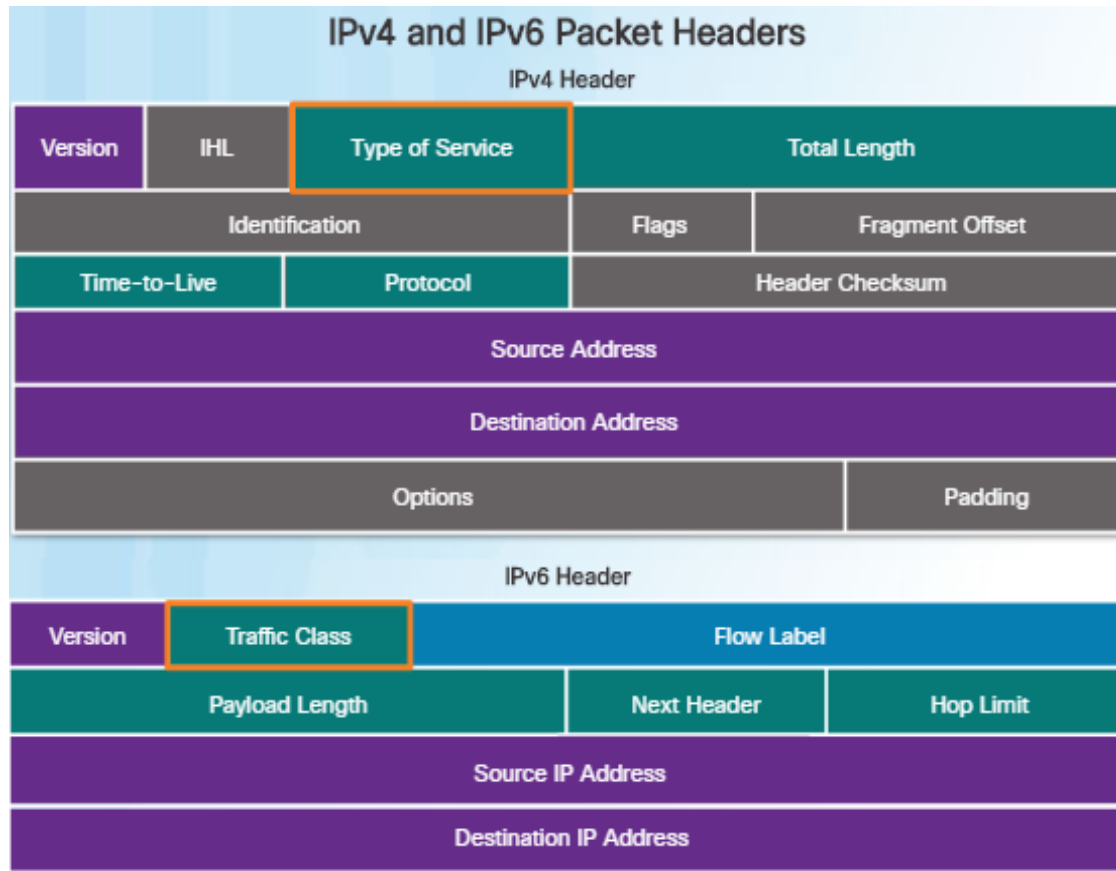
Marking at Layer 2



- 802.1Q is the IEEE standard that supports VLAN tagging at Layer 2 on Ethernet networks.
- IEEE 802.1p is the QoS prioritization scheme included with 802.1q.
- The standard uses the first three bits in the Tag Control Information (TCI) field and identifies the Class of Service (CoS) markings.
- These three bits allow eight levels of priority (0-7).

Marking at Layer 3

- IPv4 and IPv6 specify an 8-bit field in their headers to carry the packet marking assigned by the QoS classification tools.
 - IPv4 – Type of Service (ToS) field
 - IPv6 – Traffic Class field
- Offers a maximum of 64 possible classes of service.
- RFC 2474 renames the ToS and traffic class fields as the Differentiated services (DS) field
- Differentiated Service Code Point (DSCP) is a marking technique that uses the IP DS field to encode a 6-bit packet classification code



Marking at Layer 3 (Cont.)

The 64 DSCP values are organized into three categories:

- Best-Effort (BE)
 - Default for all IP packets. DSCP value is 0 (000000)
 - Packets classified into this category are normally handled using best effort delivery
- Expedited Forwarding (EF)
 - The DSCP value is 46 (101110)
 - Packets classified into this category are those that require low delay, low loss and low jitter.
 - Normally should only be used to mark voice packets.
- Assured Forwarding (AF)
 - Used to provide priority values and varying levels of reliability to different data applications by controlling queueing and drop preference
 - Allows an operator to provide assurance of delivery as long as the traffic does not exceed some subscribed rate

Marking at Layer 3 (Cont.)

- The 64 DSCP values are organized into 3 categories:
 - Assured Forwarding (AF)
 - The 1st to 3rd bit indicates queueing class - Class 4 is the best priority queue and Class 1 is the worst queue.
 - The 4th and 5th bits designate the drop preference.
 - The 6th most significant bit is set to zero.

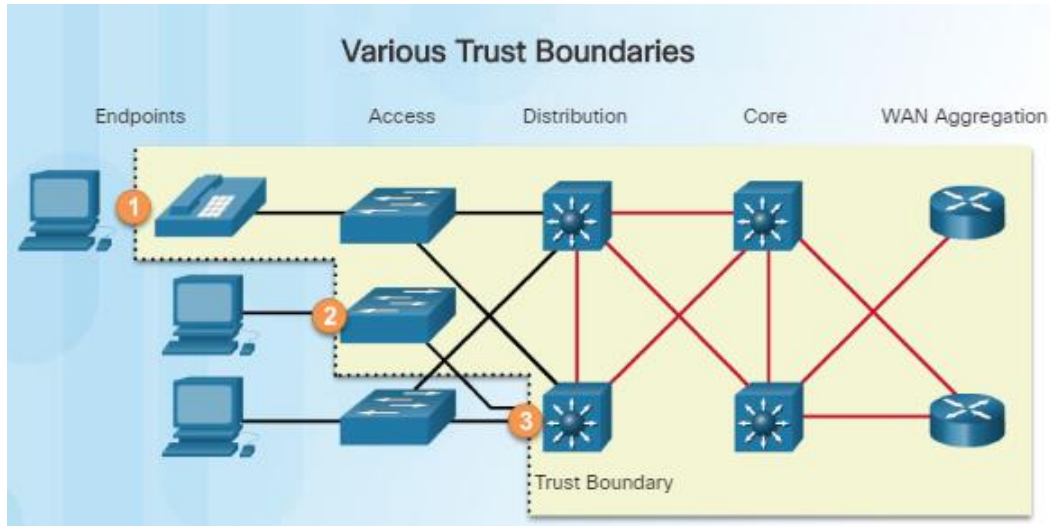


	Dropping	Low	Mid	High
Class 4		AF41 (34)	AF42 (36)	AF43 (38)
Class 3		AF31 (26)	AF32 (28)	AF33 (30)
Class 2		AF21 (18)	AF22 (20)	AF23 (22)
Class 1		AF11 (10)	AF12 (12)	AF13 (14)

Best priority ↑
↓ Worst priority

QoS Implementation Techniques

Trust Boundaries



- The trust boundary is the starting point at which the network trusts (does not override) the markings placed by devices on network traffic
- Best practice is to classify and mark traffic as close to its source as possible.
- Common devices where the trust boundary is placed.
 - Endpoints with the capability and intelligence to mark application traffic to the appropriate Layer 2 CoS or Layer 3 DSCP values. Ex: IP phones, wireless AP, and videoconferencing systems.
 - Access layer switches
 - Distribution switches and routers.
- Re-marking of traffic is typically necessary at the trust boundary.

QoS Implementation Techniques

Avoiding Packet Loss

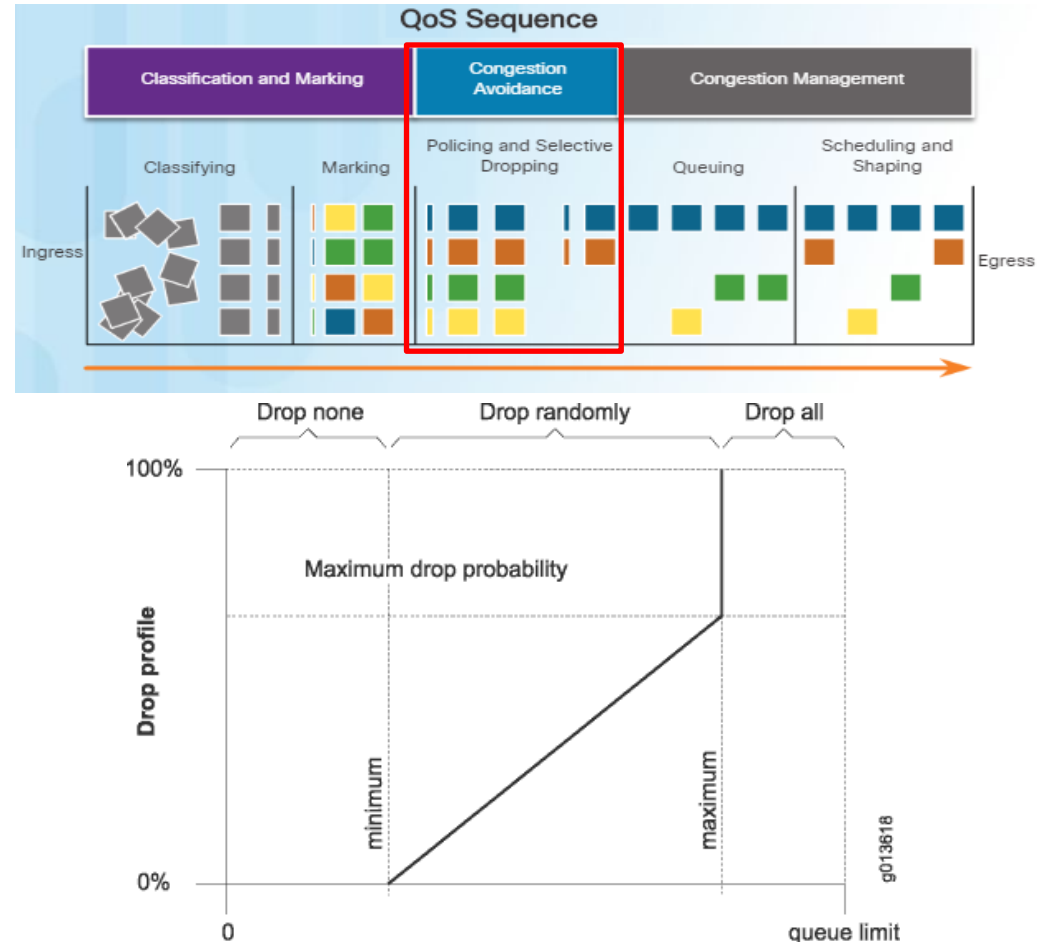


- Packet loss is usually the result of congestion on an interface.
- Most TCP applications experience slowdown because TCP automatically adjusts to network congestion.
 - Some applications do not use TCP and cannot handle drops (fragile flows).
- The following approaches can prevent drops in sensitive applications:
 - Increase link capacity to ease or prevent congestion.
 - Prevent congestion by dropping lower-priority packets before congestion occurs – weighted random early detection (WRED).
 - Guarantee enough bandwidth and increase buffer space to accommodate bursts of traffic from fragile flows – queueing algorithms

QoS Implementation Techniques

Congestion Avoidance

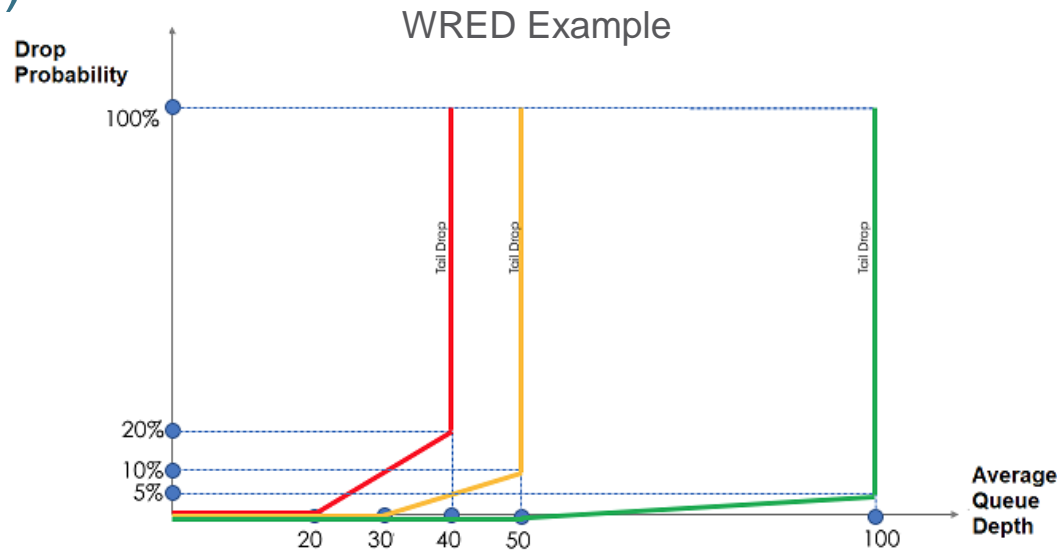
- Congestion avoidance tools monitor network traffic loads to anticipate and avoid congestion at common network bottlenecks before congestion becomes a problem.
- Congestion avoidance is achieved through monitoring the average depth of the queue and dropping packets to manage queue depth.
- Example:
 - As the queue fills up to the maximum threshold, an increasing percentage of packets are dropped.
 - When the maximum threshold is passed, all packets are dropped.



QoS Implementation Techniques

Congestion Avoidance (Cont.)

- The Cisco IOS offers weighted random early detection (WRED) as a possible congestion avoidance solution for TCP traffic.
 - Allows for preferential treatment of which packets will get dropped by setting individual thresholds for different traffic classes.
 - Provides buffer management and allows TCP traffic to decrease, or throttle back, before buffers are exhausted.
 - Helps avoid tail drops and maximizes network use and TCP-application performance.
- There is no congestion avoidance for UDP traffic – such as voice traffic.

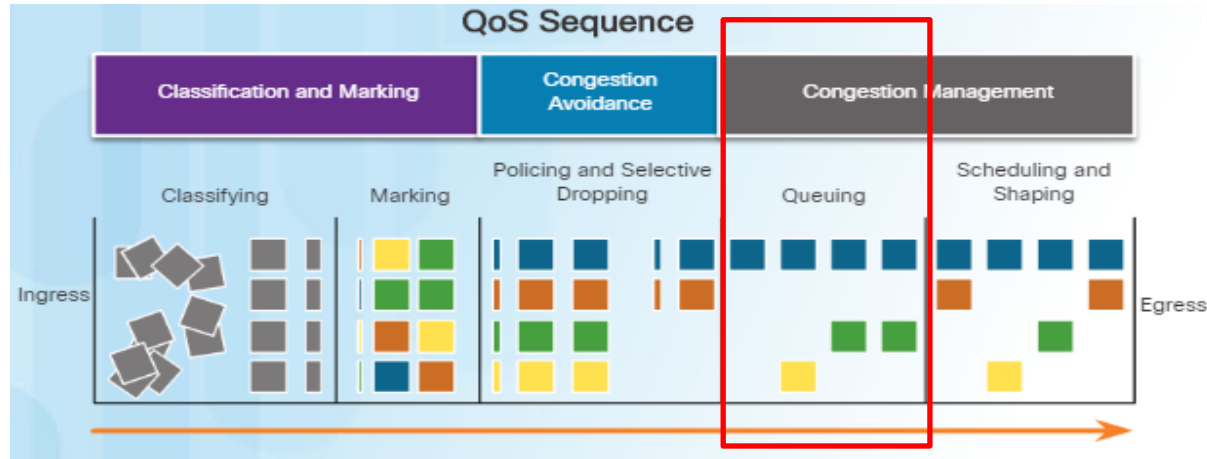


Dropping	Low	Mid	High
Class 4	AF41	AF42	AF43
Min	50	30	20
Max	100	50	40
Drop %	5%	10%	20%

QoS Implementation Techniques

Congestion Management

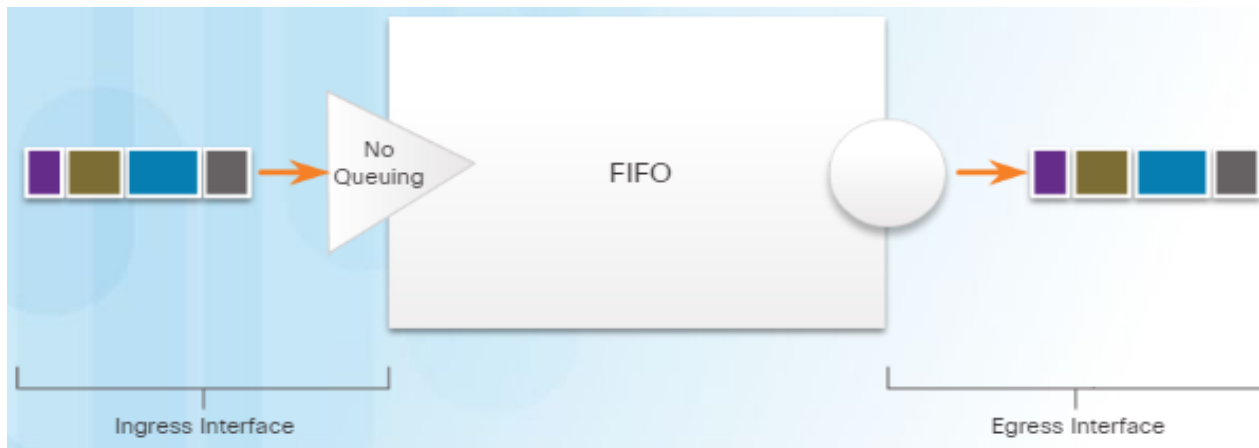
- If QoS is used in a network, the QoS policy implemented by the network administrator becomes active when congestion occurs on the link.
- Queuing is a congestion management tool that can buffer, prioritize, and if required, reorder packets before being transmitted to the destination.



- Some common queuing algorithms:
 - First-In, First-Out (FIFO)
 - Weighted Fair Queuing (WFQ)
 - Class-Based Weighted Fair Queuing (CBWFQ)
 - Low Latency Queuing (LLQ)

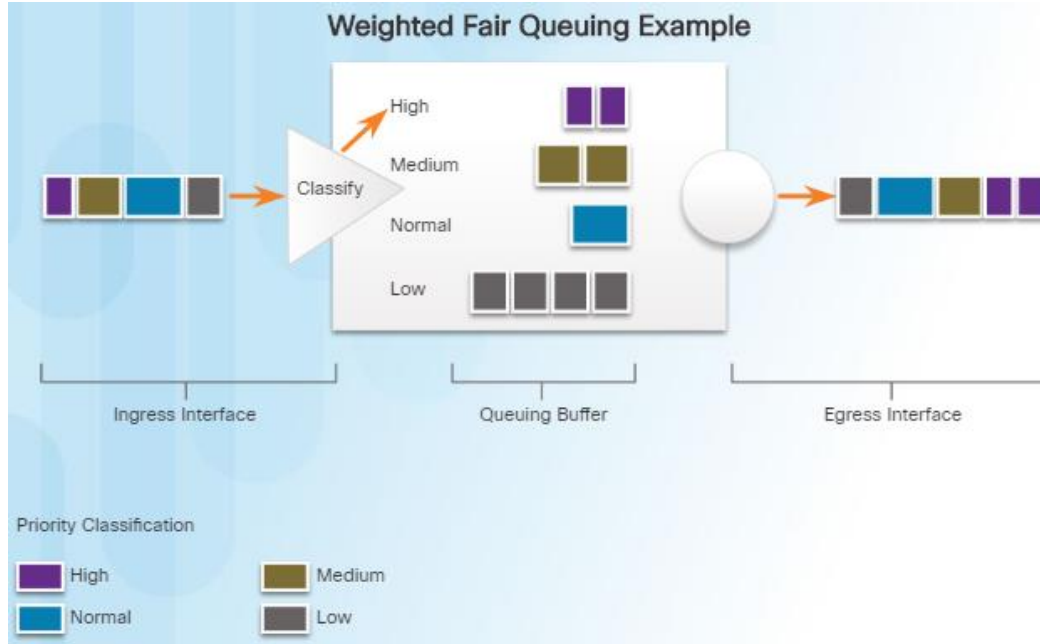
First In First Out (FIFO)

- Involves buffering and forwarding of packets in the order of arrival (a.k.a. first-come, first-served)
- No concept of priority or classes of traffic → Single queue, equal treatment of all packets.
- Important or time-sensitive traffic can be dropped when congestion occurs on the
- Used on serial interfaces at E1 (2.048 Mbps) speed and below by default if no other strategy used.
- Effective for large links that have little delay and minimal congestion



Queuing Algorithms

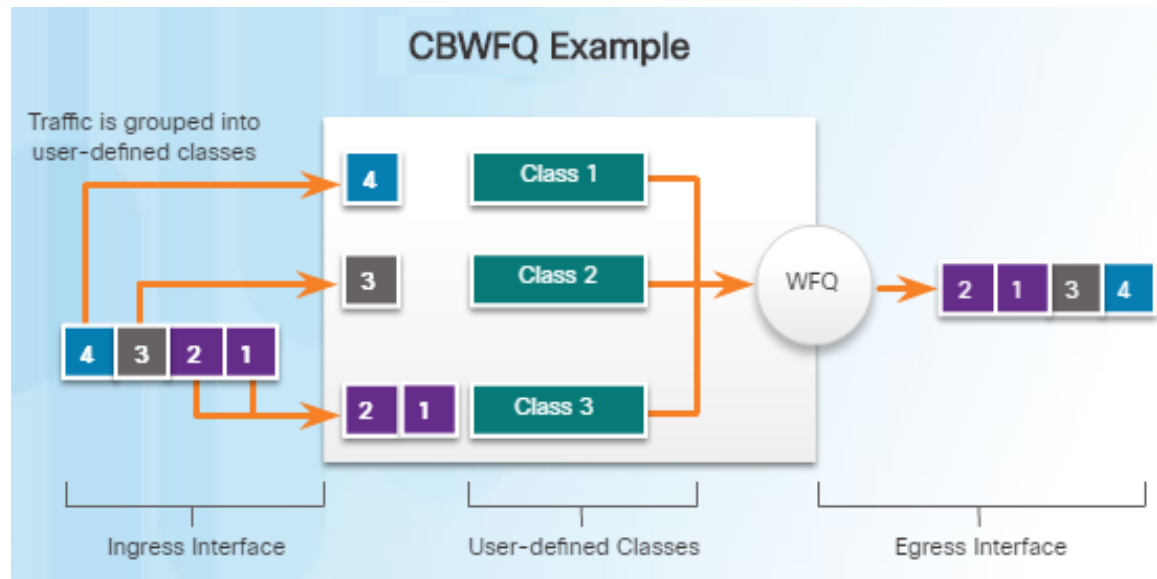
Weighted Fair Queuing (WFQ)



- Automated scheduling method that provides fair bandwidth allocation to all network traffic.
- Traffic is classified into conversations or flows based on packet header addressing, including source/destination IP addresses, MAC addresses, port numbers, protocols, and type of service (ToS) values.
- Applies priority, or weights per flow of traffic then determines how much bandwidth each flow is allowed relative to other flows.
- Schedules interactive traffic to the front of a queue to reduce response time. It then shares the remaining bandwidth among high-bandwidth flows.

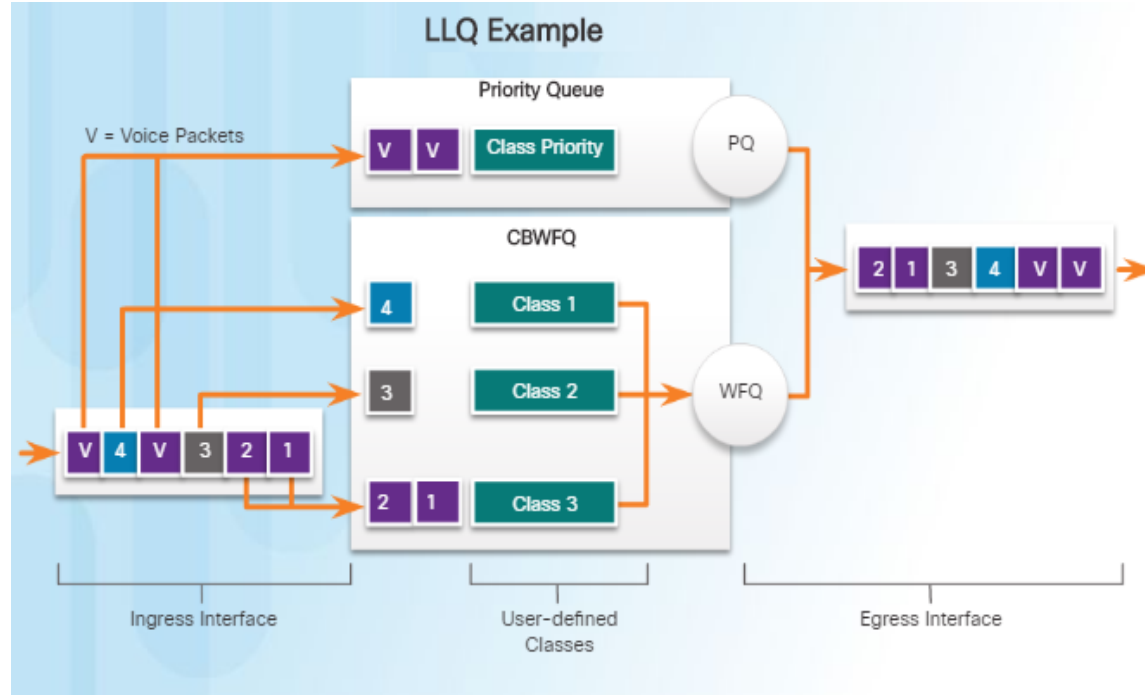
Class-Based Weighted Fair Queuing (CBWFQ)

- Extends the standard WFQ functionality to provide support for user-defined traffic classes.
- User can define traffic classes based on match criteria including protocols, ACLs, and input interfaces, then assign characteristics
 - To characterize a class, bandwidth, weight, and maximum packet limit is assigned.
 - A FIFO queue is reserved for each class, and traffic belonging to a class is directed to the queue.
 - The bandwidth assigned to a class is the guaranteed bandwidth delivered to the class during congestion.



Queuing Algorithms

Low Latency Queuing (LLQ)

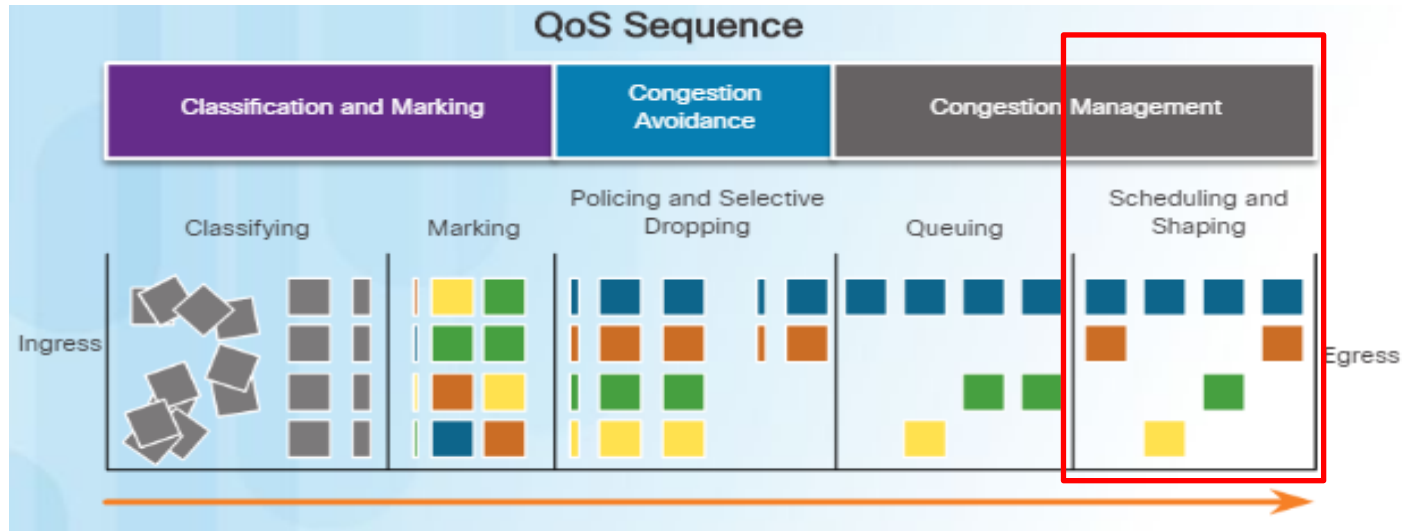


- Brings strict priority queuing (PQ) to CBWFQ to reduce jitter for time-sensitive data
- Strict PQ allows delay-sensitive data to be sent before packets in other queues.
- If CBWFQ only, all packets are serviced fairly based on weight → can cause issue for voice traffic that is delay intolerant
- With LLQ, delay-sensitive data is sent first, giving preferential treatment before packets in other queues are treated.

QoS Implementation Techniques

Congestion Management

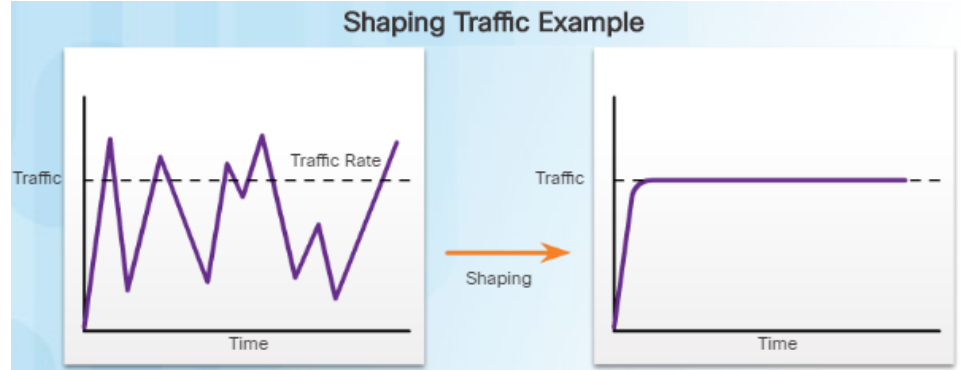
- Traffic shaping and policing are two mechanisms provided by the Cisco IOS QoS software to additionally prevent and manage congestion.
- Packets are queued and forwarded out the egress interface based on their defined QoS shaping and policing policy.



QoS Implementation Techniques

Shaping and Policing

- Traffic shaping retains excess packets in a queue and then schedules the excess for later transmission over increments of time.
 - The result of traffic shaping is a smoothed packet output rate as shown in the figure.
 - Shaping requires sufficient memory.
 - Used on outbound traffic.
- Policing is commonly implemented by service providers to enforce a contracted customer information rate (CIR).
 - Either drops or remarks excess traffic.
 - Often applied to inbound traffic.





Questions?

What Did You Learn In This Module?

- Quality of Service (QoS) is implemented to alleviate the effects of network congestion.
Without QoS:
 - Packets are processed in the order in which they are received
 - Time-sensitive will be dropped with the same frequency as data that is not time-sensitive
- Queuing packets causes delay
 - Fixed delays are: code delay, packetization delay, serialization delay, de-jitter delay.
 - Variable delays are: queuing delay, propagation delay
- Jitter is the variation in the delay of received packets.
- Voice traffic is smooth and benign, but it is sensitive to drops and delays. It can tolerate a certain amount of latency, jitter, and loss without any noticeable effects.
- Video traffic is bursty, greedy, drop sensitive, and delay sensitive.
- Data traffic often use TCP applications which can retransmit data and, therefore, are not sensitive to drops and delays.

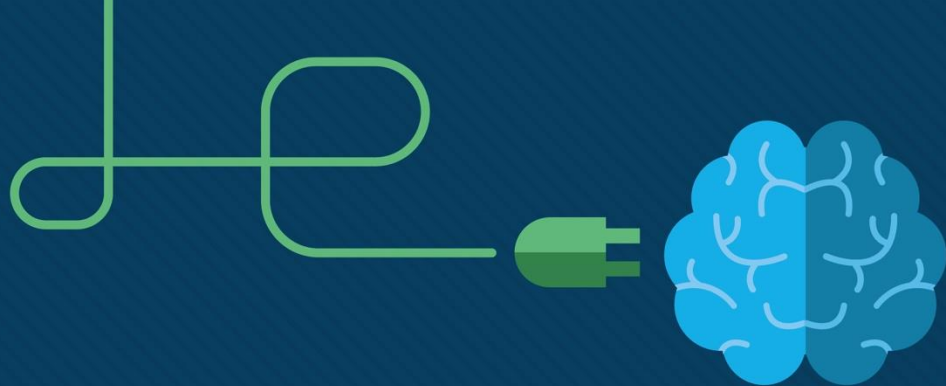
What Did You Learn In This Module?

- . Models for implementing QoS
 - Best effort treats all network packets the same way and provides no guarantees
 - IntServ architecture model uses a connection-oriented approach by implementing resource reservation and admission-control
 - DiffServ QoS model divides network traffic into classes based on business requirements. Each class can then be assigned a different level of service
- Queuing is a congestion management tool that can buffer, prioritize, and, if required, reorder packets before being transmitted to the destination.
 - FIFO queuing buffers and forwards packets in the order of their arrival.
 - WFQ provides fair bandwidth allocation by applying priority, or weights, to identified traffic and classifies it into conversations or flows.
 - CBWFQ, is similar to WFQ but uses traffic classes based on match criteria including protocols, access control lists (ACLs), and input interface
 - LLQ feature brings strict priority queuing (PQ) to CBWFQ.

What Did You Learn In This Module?

- Classification determines the class of traffic to which packets or frames belong. Traffic may be classified using interfaces, ACLs, class maps and Network Based Application Recognition (NBAR).
- Congestion management includes queuing and scheduling methods where excess traffic is buffered or queued (and sometimes dropped) while it waits to be sent out an egress interface.
- Congestion avoidance tools help to monitor network traffic loads to anticipate and avoid congestion at common network and internetwork bottlenecks before congestion becomes a problem.





Module 8

Network Troubleshooting

ITNET04

WAN Connectivity



Module Objectives

Module Title: Network Troubleshooting

Module Objectives:

- Explain how network documentation is essential in aiding troubleshooting
- Explain troubleshooting approaches for various network problems.
- Troubleshoot end-to-end connectivity in a small to medium-sized business network, using a systematic approach.

Module References:

- CCNAv7 ENSA– Module 12

8.1 Troubleshooting Methodology

Documenting the Network

- To efficiently diagnose and correct network problems, a network engineer needs to know:
 - How the network has been designed.
 - The network's expected performance.
- This information is captured in the network documentation. Network administrators must have a complete set of accurate and current network documentation which includes:
 - Configuration details, including network device and end-system configuration
 - Topology diagrams keep track of the location, function, and status of devices on the network.
 - Baseline performance levels

Network Documentation

Infrastructure Device Documentation

- Infrastructure device documentation focuses on the details (IP settings, connections, platform information, location) of routers, switches, access points, firewalls, etc

Router Device Documentation

Device	Model	Description	Location	IOS		License	
Central	ISR 4321	Central Edge Router	Building A Rm: 137	Cisco IOS XE Software, Version 16.09.04 flash:isr4300-universalk9_ias.16.09.04.SPA.bin		ipbasek9 securityk9	
Interface	Description		IPv4 Address		IPv6 Address	MAC Address	Routing
G0/0/0	Connects to SVR-1		10.0.0.1/30		2001:db8:acad:1::1/64	a03d.6fe1.e180	OSPF
G0/0/1	Connects to Branch-1		10.1.1.1/30		2001:db8:acad:a001::1/64	a03d.6fe1.e181	OSPFv3
G0/1/0	Connects to ISP		209.165.200.226/30		2001:db8:feed:1::2/64	a03d.6fc3.a132	Default
S0/1/1	Connects to Branch-2		10.1.1.2/24		2001:db8:acad:2::1/64	n/a	OSPFv3

Switch Device Documentation

Device	Model	Description	Mgt. IP Address		IOS		VTP	
S1	Cisco Catalyst WS-C2960-24TC-L	Branch-1 LAN1 switch	192.168.77.2/24		IOS: 15.0(2)SE7 Image: C2960-LANBASEK9-M		Domain: CCNA Mode: Server	
Port	Description		Access	VLAN	Trunk	EtherChannel	Native	Enabled
Fa0/1	Port Channel 1 trunk to S2 Fa0/1		-	-	Yes	Port-Channel 1	99	Yes
Fa0/2	Port Channel 1 trunk to S2 Fa0/2		-	-	Yes	Port-Channel 1	99	Yes
Fa0/3	*** Not in use ***		Yes	999	-	-		Shut
Fa0/4	*** Not in use ***		Yes	999	-	-		Shut
Fa0/5	Access port to user		Yes	10	-	-		Yes

End System Documentation

- End-system documentation focuses on the IP configuration and services of end-system devices such as servers, network management consoles, and user workstations.

End-System Documentation

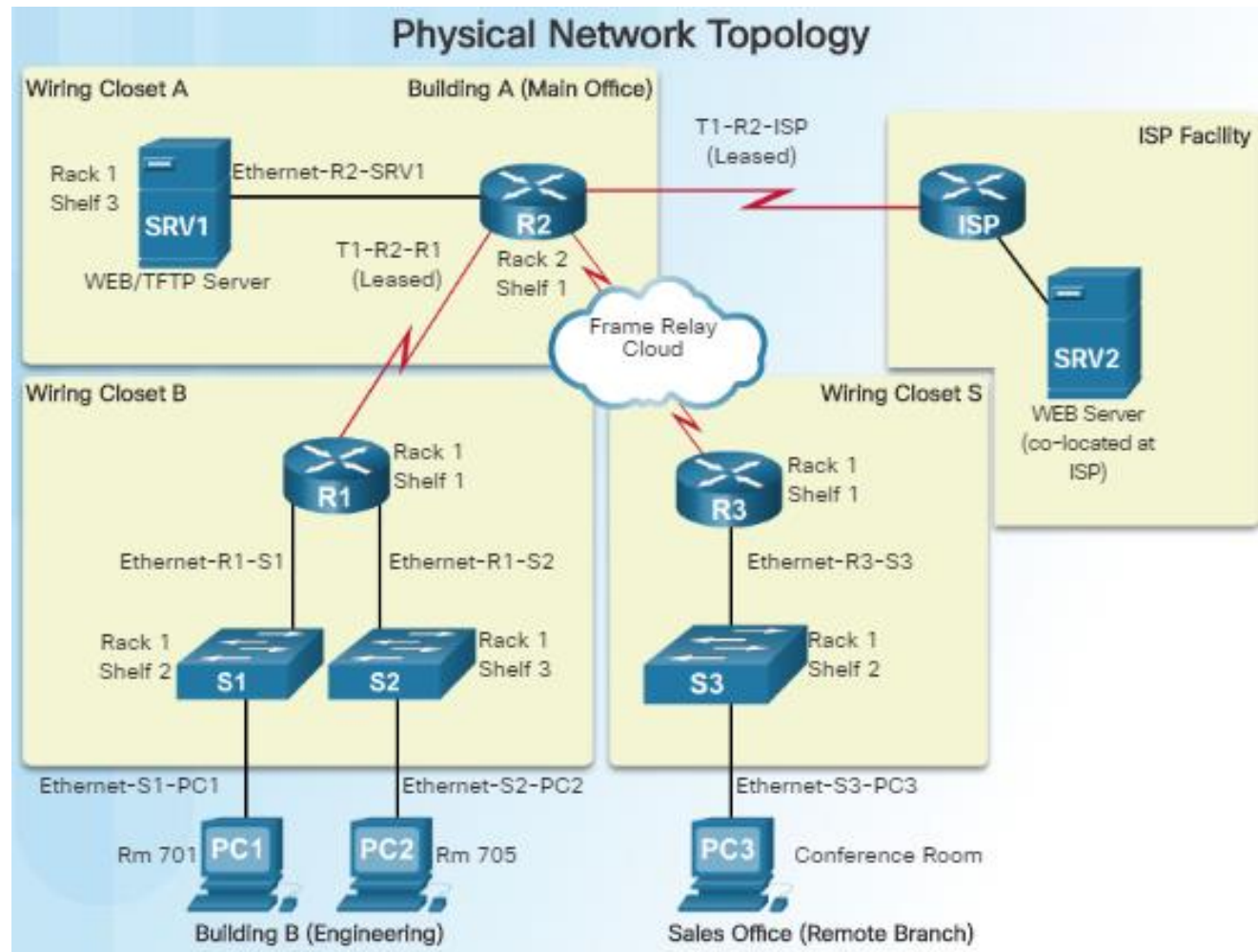
Device	OS	Services	MAC Address	IPv4 / IPv6 Addresses	Default Gateway	DNS
SRV1	MS Server 2016	SMTP, POP3, File services, DHCP	5475.d08e.9ad8	10.0.0.2/30	10.0.0.1	10.0.0.1
				2001:db8:acad:1::2/64	2001:db8:acad:1::1	2001:db8:acad:1::1
SRV2	MS Server 2016	HTTP, HTTPS	5475.d07a.5312	209.165.201.10	209.165.201.1	209.165.201.1
				2001:db8:feed:1::10/64	2001:db8:feed:1::1	2001:db8:feed:1::1
PC1	MS Windows 10	HTTP, HTTPS	5475.d017.3133	192.168.10.10/24	192.168.10.1	192.168.10.1
				2001:db8:acad:1::251/64	2001:db8:acad:1::1	2001:db8:acad:1::1

Network Documentation

Network Topology Diagrams

- Physical Topology network diagrams show the physical layout of the devices connected to the network and typically include:

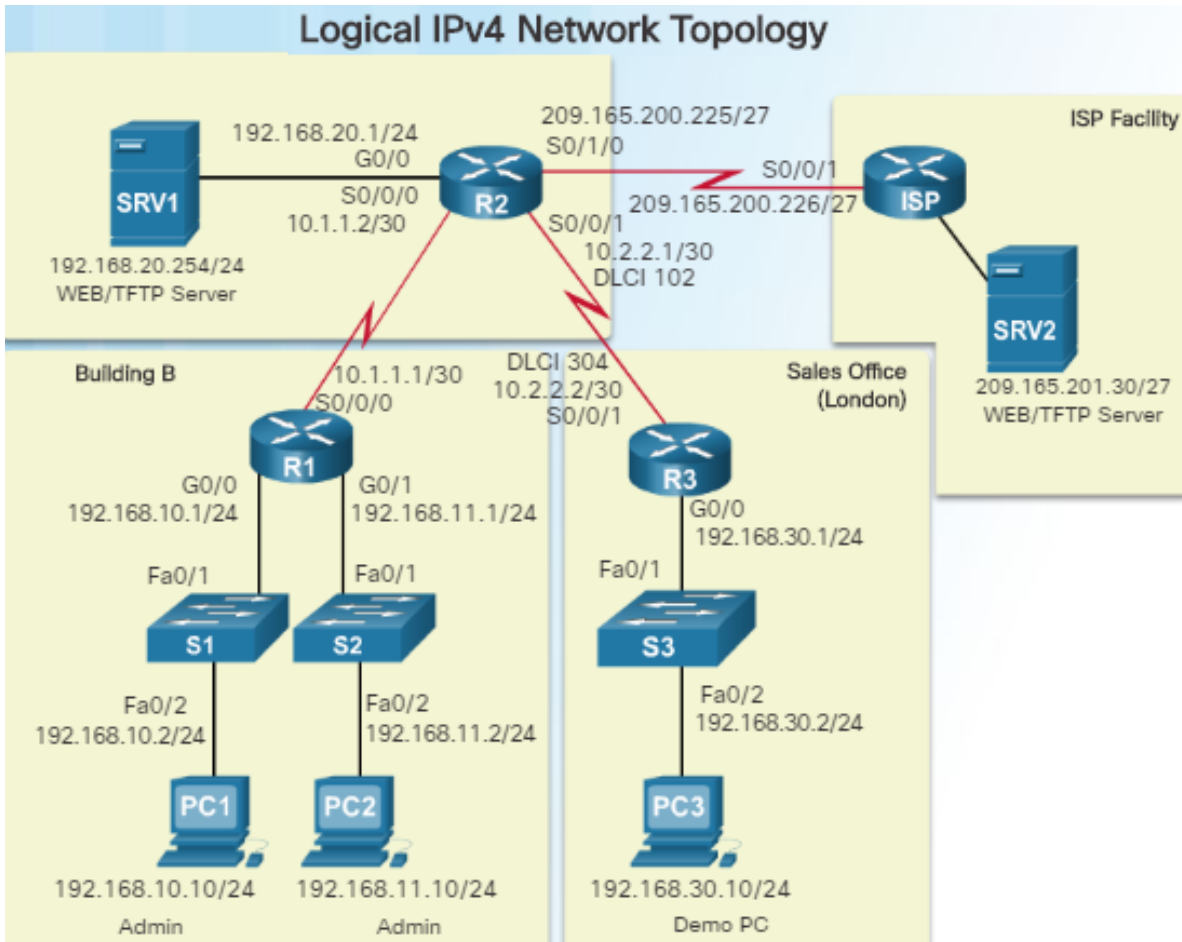
- Device type
- Model and manufacturer
- Operating System version
- Cable type and identifier
- Cable specification
- Connector type
- Cabling endpoints



Network Topology Diagrams (Cont.)

- Logical network topology diagrams illustrate how devices are logically connected to the network and might include:

- Device identifiers
- IP address and prefix lengths
- Interface identifiers
- Connection type
- Frame Relay DLCI for virtual circuits
- Site-to-site VPNs
- Routing protocols and static routes
- WAN technologies used
- Data-link protocols



Establishing a Network Baseline

- The purpose of network monitoring is to watch network performance in comparison to a predetermined baseline.
- A network performance baseline
 - Establishes normal network or system performance
 - Requires collecting performance data from the ports and devices that are essential to operation
 - Allows the network administrator to determine the difference between abnormal behavior and proper network performance
- Analysis after an initial baseline also tends to reveal hidden problems. The collected data can show the true nature of congestion or potential congestion in a network.

A network baseline determines the “personality” of the network under normal conditions

How does a network perform on an average day?

Which part of the network is most heavily used?

What part of the network is least used?

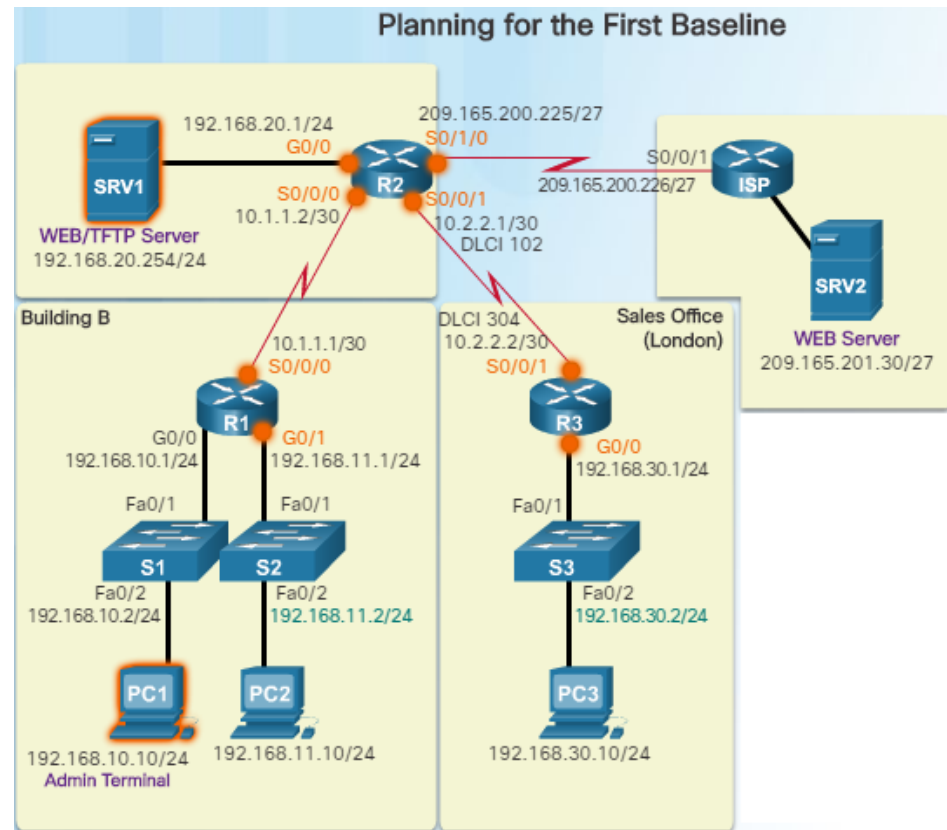
Where are the most errors occurring?

Which devices should be monitored and at what alert threshold?

Can the network meet the identified policies?

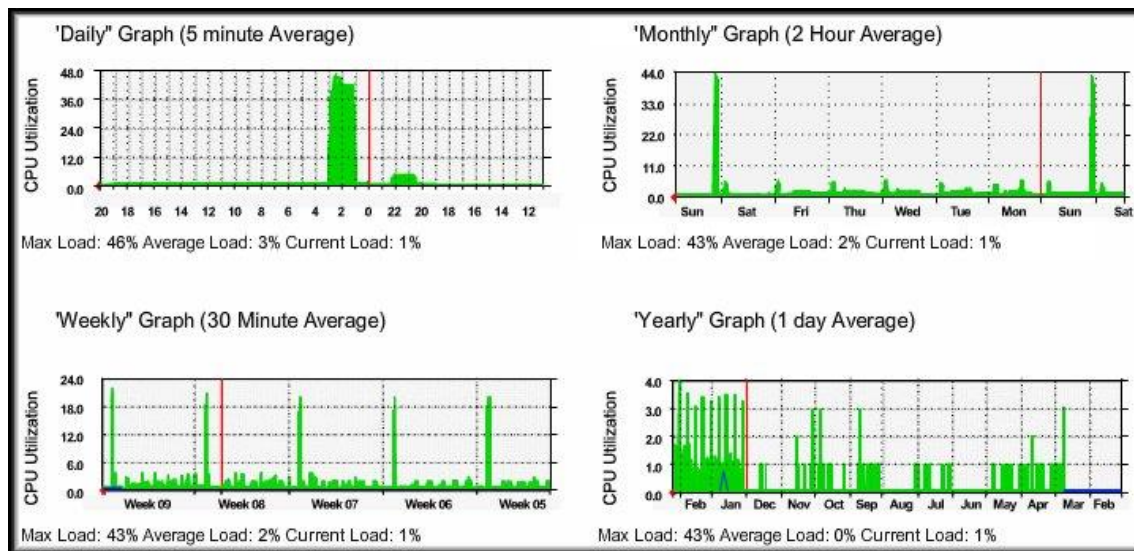
Steps to Establish a Network Baseline

- Step 1: Determine what types of data to collect.
 - Start out with a few variables that represent the defined policy.
 - Capturing too many data points can be overwhelming and make analysis difficult.
 - Start out simply, and fine-tune along the way.
- Step 2: Identify devices and ports of interest.
 - Use the network topology to identify key devices where performance data should be measured.
 - Devices and ports of interest include network device ports that connect to other network devices, servers, and key users.



Steps to Establish a Network Baseline (Cont.)

- Step 3: Determine the baseline duration
 - The length of time and baseline information being gathered must be sufficient for establishing a typical picture of the network.
 - Daily trends of network traffic should be measured.
 - Monitor for trends that occur over a longer period of time such as weekly or monthly.



- Capture data trends and include:
 - Screenshots of CPU utilization trends captured over a daily, weekly, monthly, and yearly period
- Note: Baseline measurements should not be performed during times of unique traffic patterns.

Network Documentation

Measuring Data

Commands for Data Collection

Command	Description
show version	Shows uptime, version information for device software and hardware.
show ip interface[brief] show ipv6 interface[brief]	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.
show interfaces [interface_type interface_num]	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).
show ip route show ipv6 route	Shows the contents of the routing table.
show arp show ipv6 neighbors	Shows the contents of the ARP table (IPv4) and the neighbor table (IPv6).
show running-config	Shows current configuration.
show port	Shows the status of ports on a switch.
show vlan	Shows the status of VLANs on a switch.
show tech-support	This command is useful for collecting a large amount of information about the device for troubleshooting purposes. It executes multiple show commands which can be provided to technical support representatives when reporting a problem.
show ip cache flow	Displays a summary of the NetFlow accounting statistics.

- When documenting the network, it is necessary to gather information directly from routers and switches.
- **Ping**, **traceroute**, and **telnet** are useful commands to document.
- The figure to the left lists some of the most common Cisco IOS **show** commands used for data collection.
- Manual data collection using **show** commands on individual network devices is very time consuming and is not a scalable solution. This should be reserved for smaller networks or mission critical devices.
- Sophisticated network management software is typically used to baseline large and complex networks.

Network Documentation

Measuring Data

- For documentation, it is necessary to gather information directly from routers and switches.
- **Ping, traceroute, telnet** and **show** are useful commands to document.
- Manual data collection using **show** commands on individual network devices is usually reserved for smaller networks or mission critical devices because it is time consuming.

Command	Description
Show version	Show uptime, hardware info and OS version of device
Show ip interface [brief]	Show status and address configuration on interfaces
Show interface	Show detailed output (protocol, status, statistics, addressing) for an interface
Show ip / ipv6 route	Shows contents of routing table
Show arp / show ipv6 neighbors	Shows ip address to mac address mappings
Show vlan	Shows status of VLANs on a switch
Show port	Shows the status of ports on a switch

General Troubleshooting Approaches

- For network engineers, administrators, and support personnel, troubleshooting is a process that takes the greatest percentage their time.
- Using efficient troubleshooting techniques shortens overall troubleshooting time.
- Two extreme approaches to troubleshooting almost always result in disappointment, delay, or failure.

The *caveman*

- Makes random changes to the network until it miraculously starts working again,
- May not have found and fixed the root cause of the issue

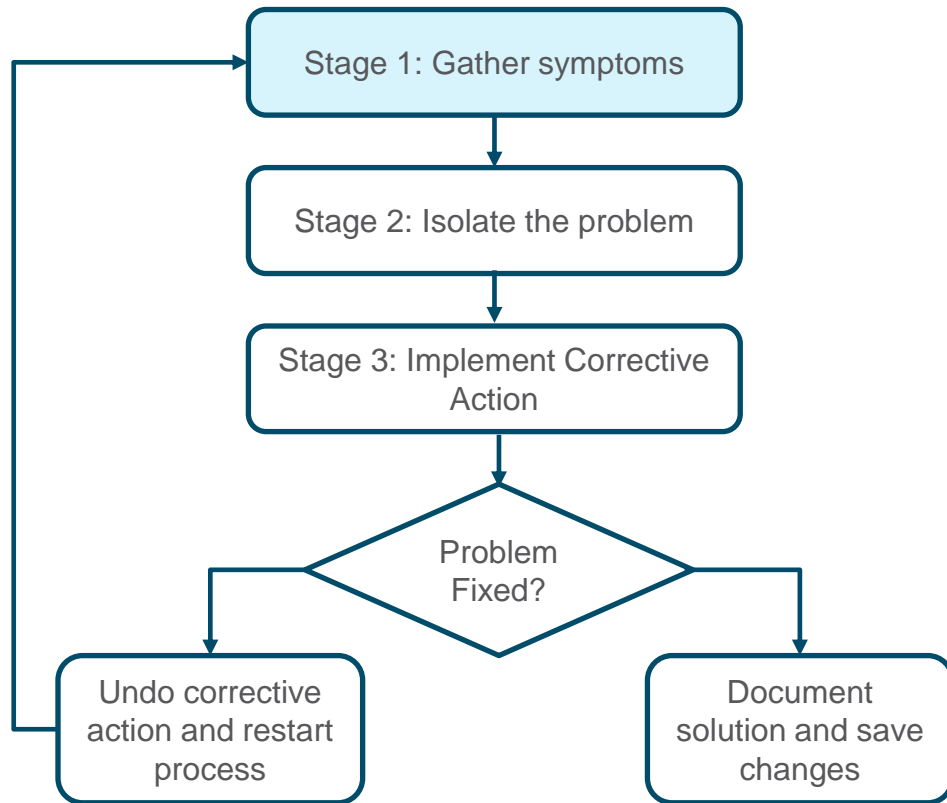


The *rocket scientist*

- Deeply analyzes the situation until the root cause of the problem has been identified
- Takes too long to resolve an issue.

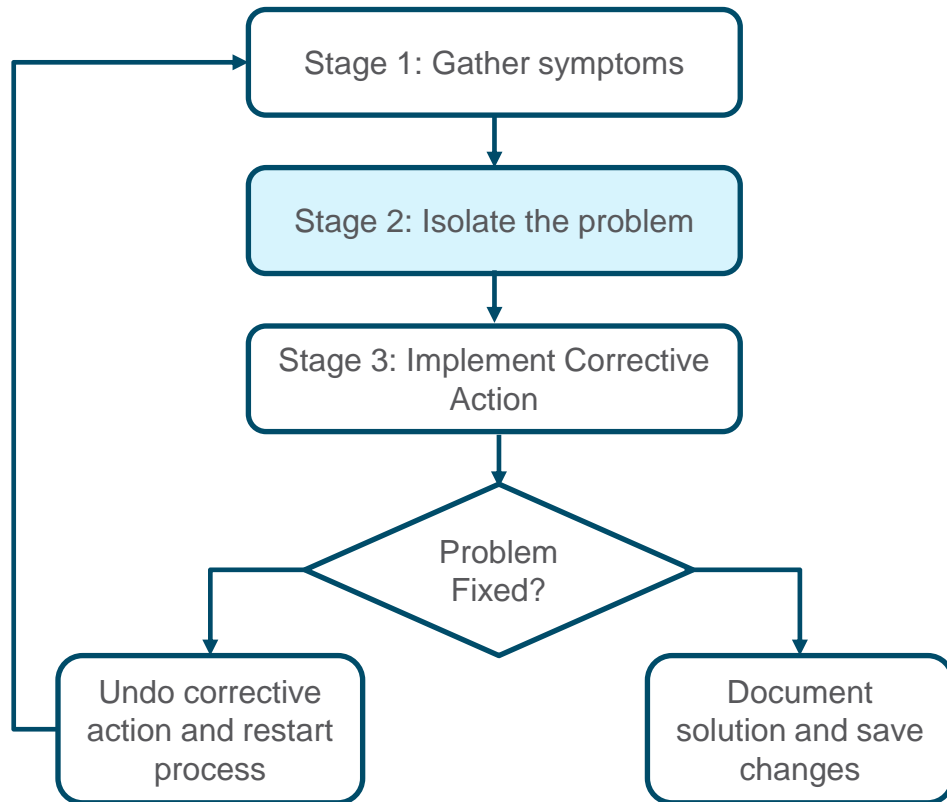
Troubleshooting Procedures

- Use efficient troubleshooting techniques to shorten overall troubleshooting time.
- Stage 1. Gather symptoms –
 - Determines which network components have been affected and how the functionality of the network has changed in comparison to the baseline.
 - Symptoms may come from the network management system, console messages, and user complaints.
 - Question users and investigate the issue in order to localize the problem to a smaller range of possibilities.



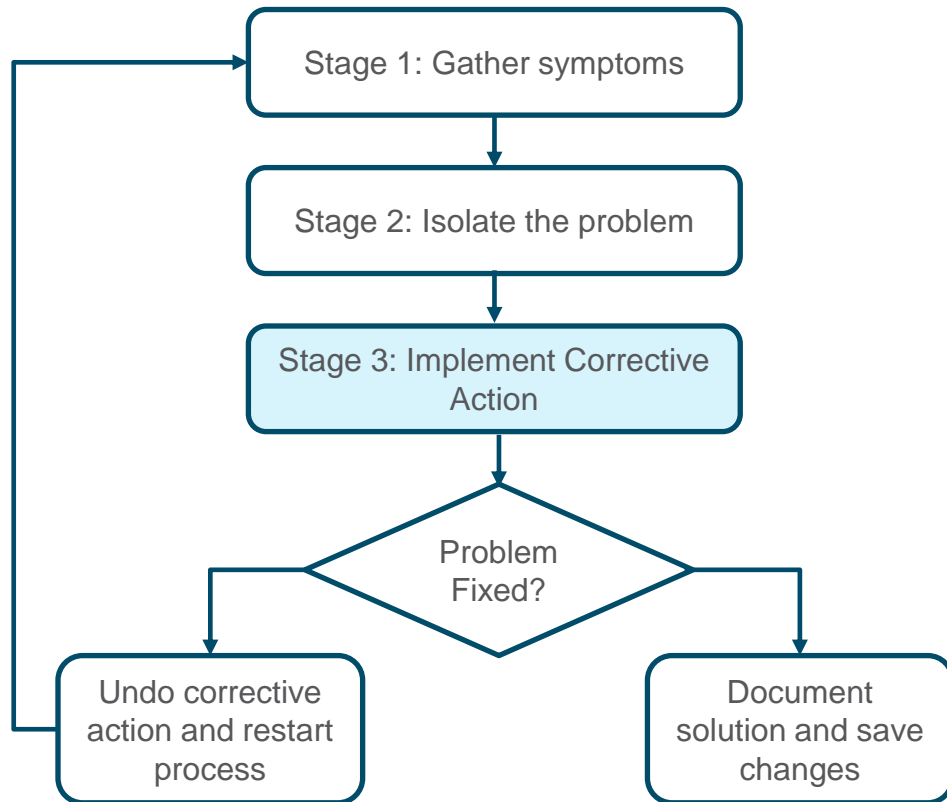
Troubleshooting Procedures

- Use efficient troubleshooting techniques to shorten overall troubleshooting time.
- Stage 2. Isolate the problem –
 - Isolating is the process of eliminating variables until a single problem, or a set of related problems has been identified as the cause.
 - Examine the problems at the logical layer of the network so that the most likely cause can be detected.

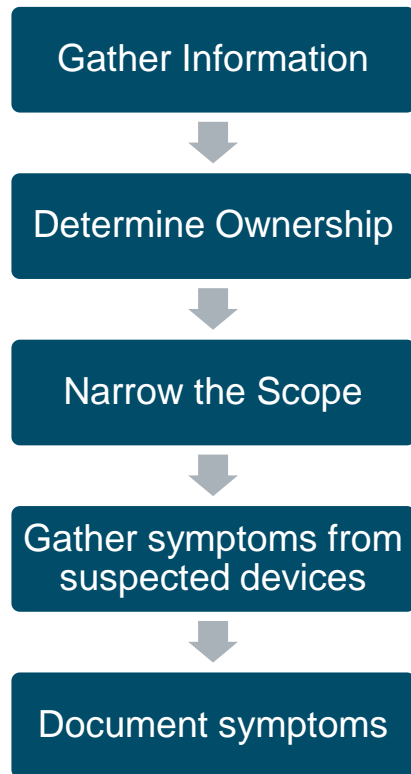


Troubleshooting Procedures

- Use efficient troubleshooting techniques to shorten overall troubleshooting time.
- Stage 3. Implement corrective action –
 - Correct the problem by implementing, testing, and documenting possible solutions.
 - Can the solution be implemented immediately, or does it need to be postponed?
 - The severity of the problem should be weighed against the impact of the solution.

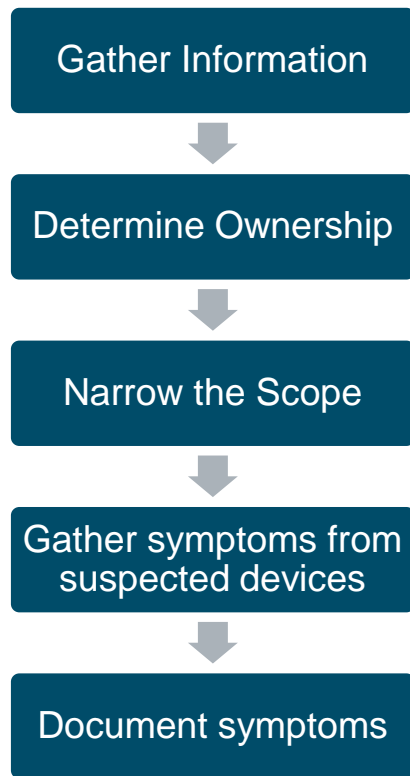


Gathering Symptoms



- It is important to gather facts and evidence that will allow you to progressively eliminate possible causes, and eventually identify the root cause of the issue.
- There are five information gathering steps:
- Step 1. Gather Information
 - Gather information from the trouble ticket, users, or end systems affected by the problem to form a definition of the problem.
- Step 2. Determine ownership
 - If the problem is within the control of the organization, move onto the next stage. If it is outside of the boundary of organizational control, contact an administrator for the external system.


Gathering Symptoms (Cont.)



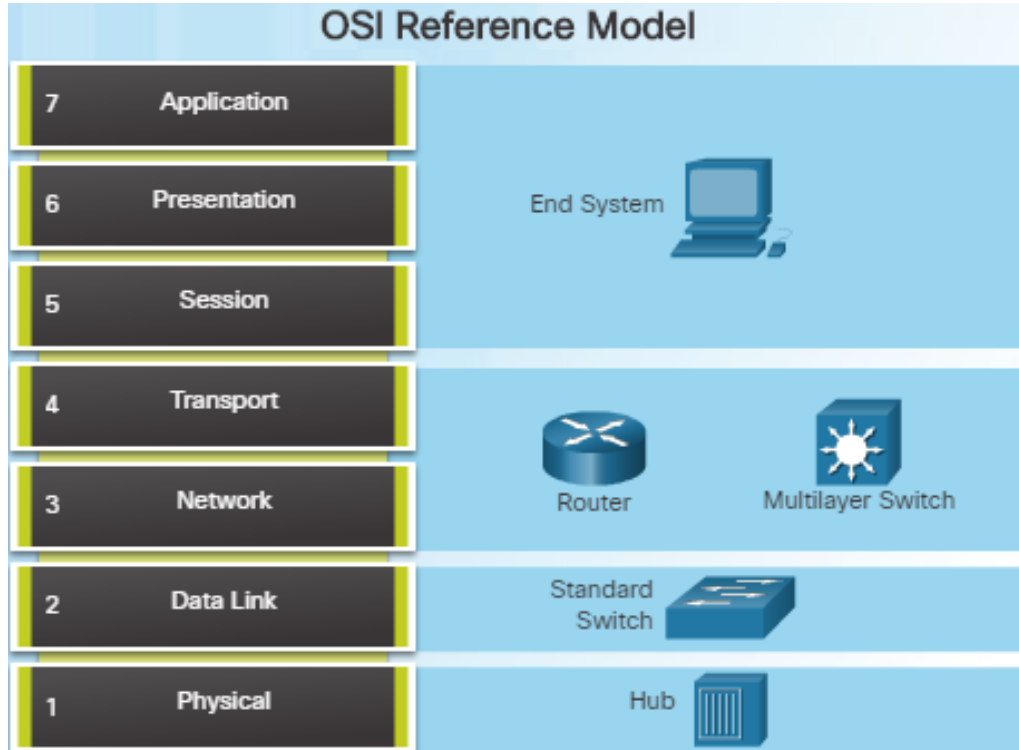
- Step 3. Narrow the scope
 - Determine if the problem is at the core, distribution, or access layer.
 - At the identified layer, analyze the existing symptoms and try to determine which piece of equipment is most likely the cause.
- Step 4. Gather symptoms from suspect devices
 - Using a layered troubleshooting approach, gather hardware and software symptoms from the suspect devices.
 - Is it a hardware or software configuration problem?
- Step 5. Document symptoms
 - If the problem cannot be solved using the documented symptoms, begin the isolating stage of the general troubleshooting process.
 - Gather symptoms from devices using commands/tools, device logs and packet captures.

Questioning End Users

- In many cases, the problem is reported by an end user. This information may often be misleading or vague. Use effective questioning techniques when asking the end users about a network problem they may be experiencing.

Guidelines	Example Open Ended End-User Questions
Ask pertinent questions.	<ul style="list-style-type: none">• What does not work?• What exactly is the problem?• What are you trying to accomplish?
Determine the scope of the problem.	<ul style="list-style-type: none">• Who does this issue affect? Is it just you or others?• What device is this happening on?
Determine when the problem occurred / occurs.	<ul style="list-style-type: none">• When exactly does the problem occur?• When was the problem first noticed?• Were there any error message(s) displayed?
Determine if the problem is constant or intermittent.	<ul style="list-style-type: none">• Can you reproduce the problem?• Can you send me a screenshot or video of the problem?
Determine if anything has changed.	<ul style="list-style-type: none">• What has changed since the last time it did work?
 Use questions to eliminate or discover possible problems.	<ul style="list-style-type: none">• What works?• What does not work?

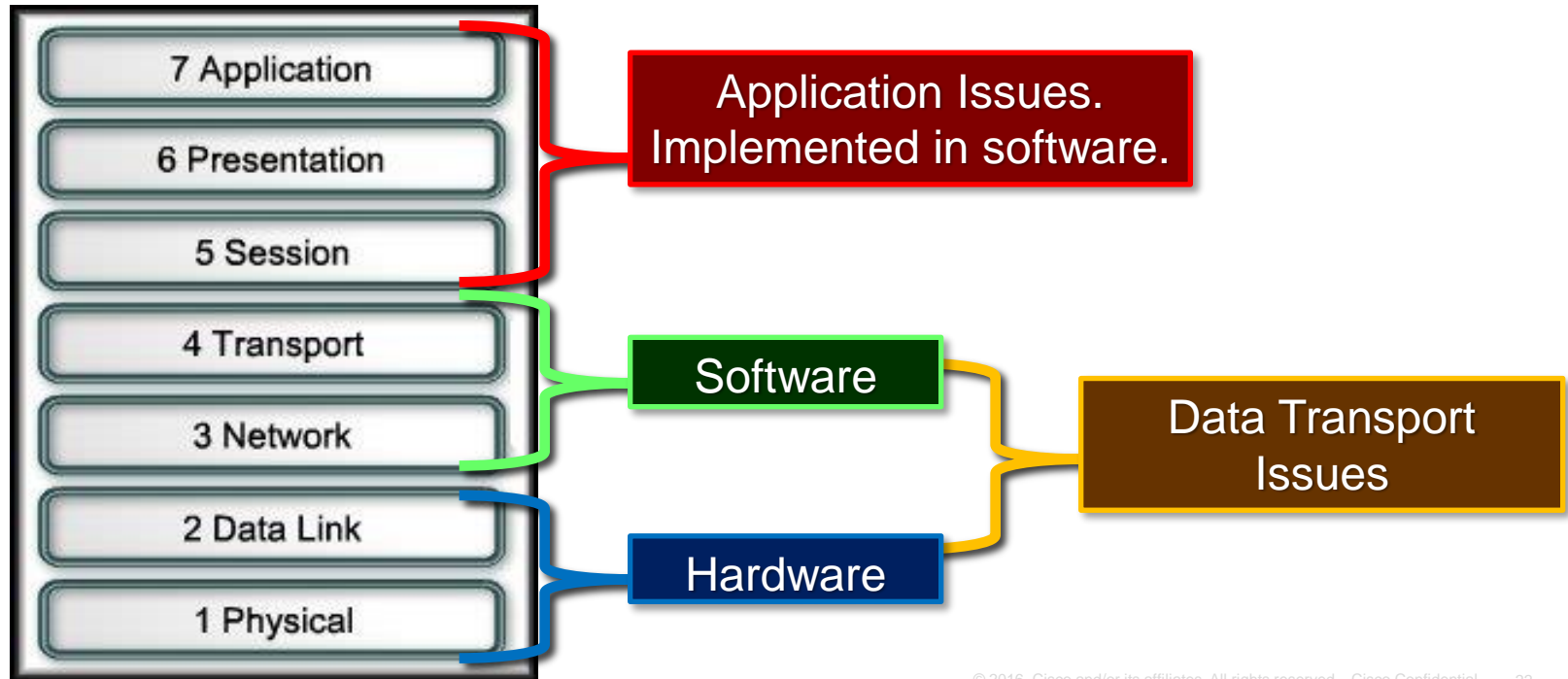
Using Layered Models for Troubleshooting



- If no solution is identified, the network administrator compares the characteristics of the problem to the logical layers of the network to isolate and solve the issue.
- Logical networking models, such as the OSI and TCP/IP models, separate network functionality into modular layers.
- When troubleshooting, these layered models can be applied to the physical network to isolate network problems.

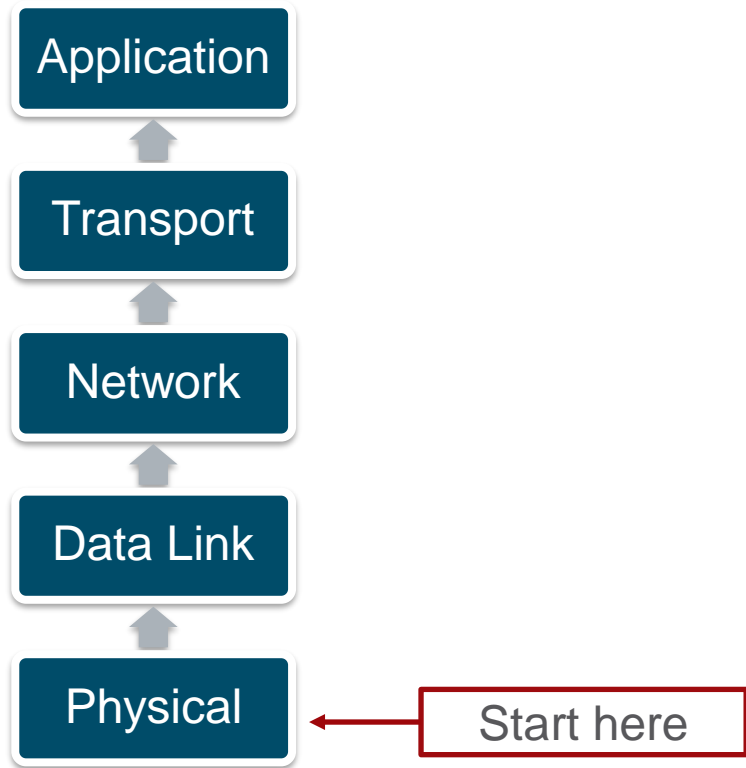
Using Layered Models for Troubleshooting

- Logical networking models, such as the OSI and TCP/IP models, separate network functionality into modular layers.



Isolating the Issue Using Layered Models

Troubleshooting Methods

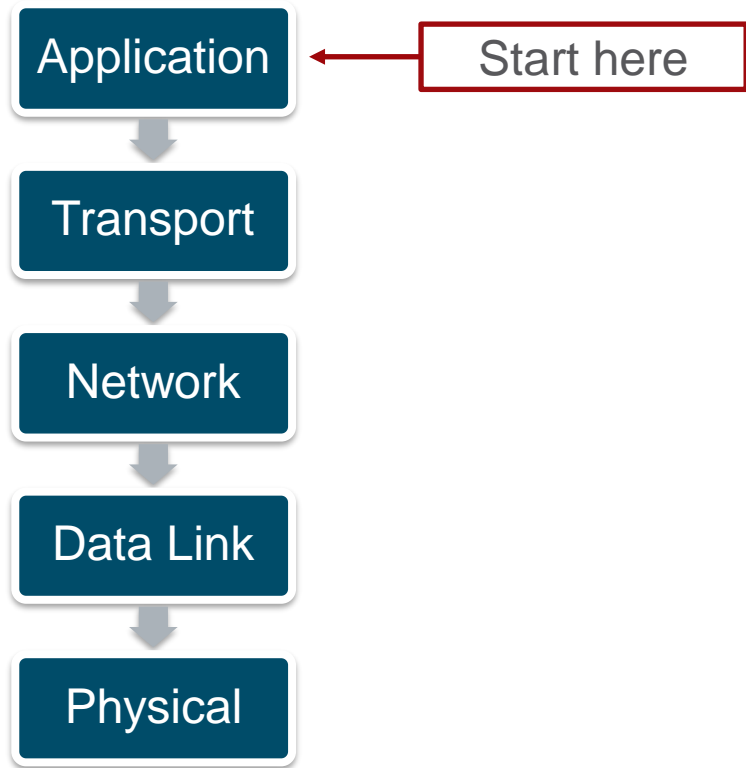


▪ **Bottom-up Troubleshooting Method**

- Start with the physical components of the network and move up through the layers of the OSI model until the cause of the problem is identified
- This is a good approach to use when the problem is suspected to be a physical one.
- Most networking problems reside at the lower levels, so using this method is often effective
- The disadvantage with this method is it requires that you check every device and interface on the network until the cause of the problem is found.

Isolating the Issue Using Layered Models

Troubleshooting Methods

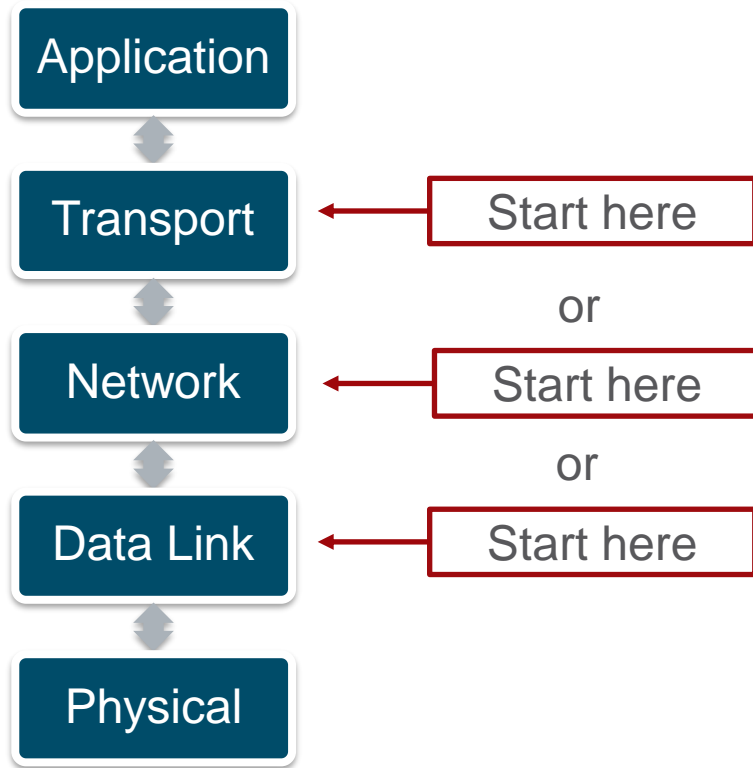


▪ **Top-Down Troubleshooting Method**

- This method starts with troubleshooting the end-user applications and moves down through the layers of the OSI model until the cause of the problem has been identified.
- End-user applications are tested before tackling the more specific networking pieces.
- Use this approach for simpler problems.
- The disadvantage is that it requires checking every network application until the problem is found.

Isolating the Issue Using Layered Models

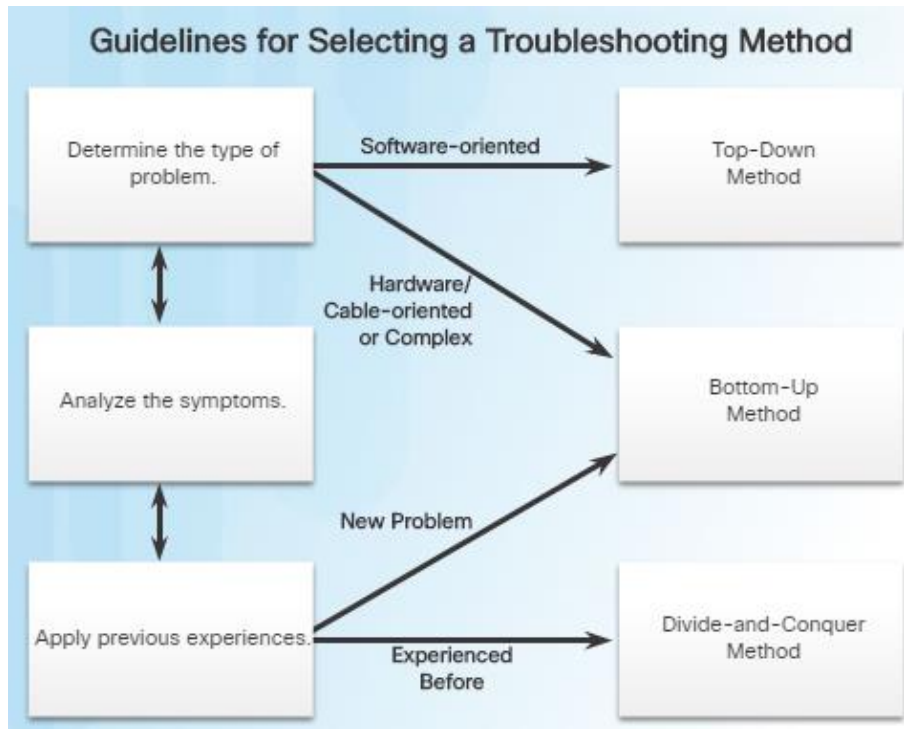
Troubleshooting Methods



▪ Divide-and-Conquer Troubleshooting Method

- The network administrator selects a layer and tests in both directions from that layer.
- Start by collecting user experiences of the problem, document the symptoms, and then, using that information, make an informed guess as to which OSI layer to start your investigation.
- If a layer is functioning properly, all layers below can be assumed to be functioning.

Guidelines for Selecting a Troubleshooting Method



- To quickly resolve network problems, take the time to select the most effective network troubleshooting method. An example:
 - Two IP routers are not exchanging routing information.
 - The last time this type of problem occurred, it was a protocol issue.
 - Therefore, choose the divide-and-conquer troubleshooting method.
 - Analysis reveals that there is connectivity between the routers.
 - Start the troubleshooting process at the physical or data link layer.
 - Confirm connectivity and begin testing the TCP/IP-related functions at the next layer up in the OSI model, the network layer.

Other Troubleshooting Methods



- Educated guess by the network administrator
 - Guess is based on the symptoms of the problem
 - This is more successful when implemented by seasoned network administrators who can rely on their extensive knowledge and experience
- Comparing a working and non-working situation
 - Look for differences between configurations, software versions, and hardware and other device properties.
 - This method can be helpful when the network administrator is lacking an area of expertise or when the problem needs to be resolved quickly.
- Substitution
 - Involves swapping the problematic devices with known, working ones.
 - If the problem remains, the network administrator knows to look elsewhere.
- Follow the Path
 - Used to discover the actual traffic path from source to destination to reduce the scope of troubleshooting

8.2 Troubleshooting Scenarios

Troubleshooting Tools

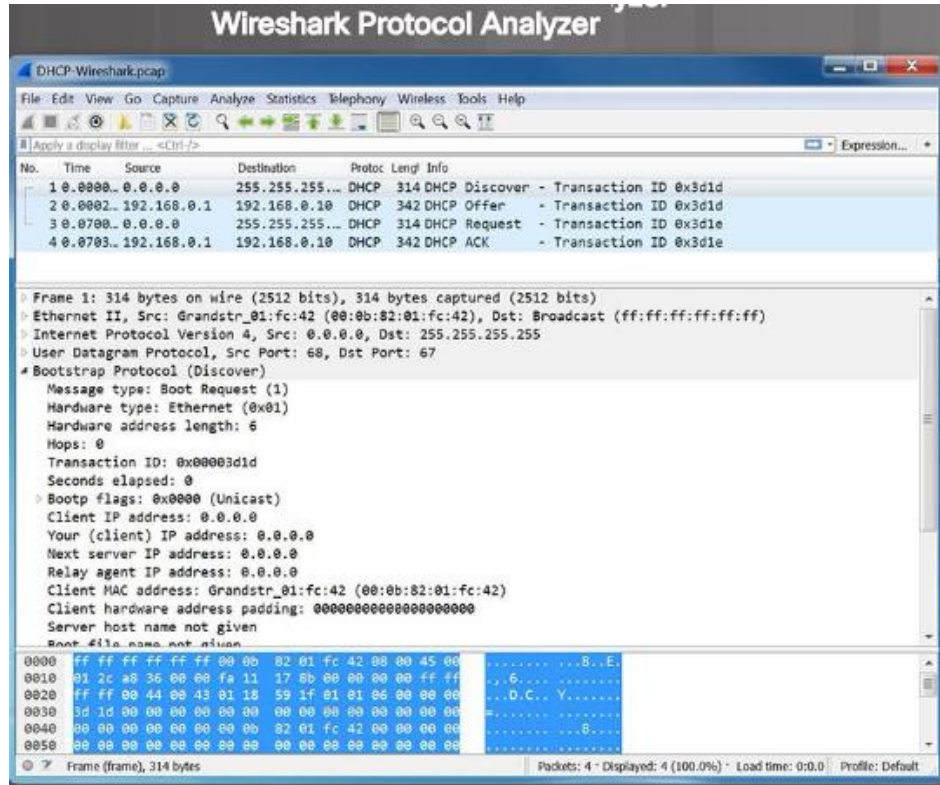
Software Troubleshooting Tools



- Common software troubleshooting tools include these:
 - Network Management System Tools
 - NMS tools include device-level monitoring, configuration, and fault-management tools.
 - These graphical tools can be used to investigate and correct network problems.
- Knowledge Bases
 - On-line network device vendor knowledge bases are very useful.
 - When combined with Internet search engines, a network administrator has access to a vast pool of experience-based information.
- Baselining Tools
 - Many tools for automating the network documentation and baselining process are available. For example:
 - SolarWinds Network Performance Monitor

Troubleshooting Tools

Protocol Analyzers



- Protocol analyzers are useful to investigate packet content while the content is flowing through the network.
- A protocol analyzer decodes the various protocol layers in a recorded frame and presents it in an easy to use format.
- The figure to the left shows a screen capture of the Wireshark protocol analyzer.
- Most protocol analyzers can filter traffic that meets certain criteria. For example, all traffic to and from a particular device can be captured.
- Protocol analyzers are very helpful in troubleshooting network performance problems.

Hardware Troubleshooting Tools

Cable Testers



- There are multiple types of hardware troubleshooting tools including:
 - **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. They can be used to detect broken wires, crossed-over wiring, shorted connections, and improperly paired connections. More expensive time-domain reflectometers (TDRs) are used to pinpoint the distance to a break in a cable.
 - **Cable Analyzers** are multifunctional handheld devices that are used to test and certify copper and fiber cables for different services and standards.

Hardware Troubleshooting Tools (Cont.)

Cable Testers



- **Portable Network Analyzers** are used for troubleshooting switched networks and VLANs.
- By plugging the network analyzer in anywhere on the network, a network engineer can see the switch port to which the devices is connected.
- They can also see the average and peak utilization as well as the VLAN configuration.
- **Network Analysis Module** – The Cisco NAM is a device or software.
- It provides an embedded browser-based interface that generates reports on the traffic that consumes critical network resources.
- The NAM can capture and decode packets and track response times to pinpoint an application problem to a particular network or server.

Troubleshooting Tools

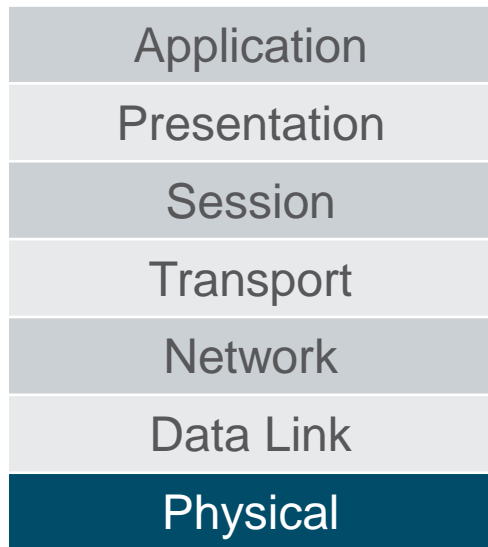
Using a Syslog Server for Troubleshooting

Severity Levels			
	Level	Keyword	Description
Highest Level	0	emergencies	System is unusable
	1	alerts	Immediate action is needed
	2	critical	Critical conditions exist
	3	errors	Error conditions exist
	4	warnings	Warning conditions exist
	5	notifications	Normal (but significant) condition
	6	informational	Informational messages only
Lowest Level	7	debugging	Debugging messages

- Cisco devices can send log messages to several different facilities:
 - Console and Terminal lines
 - Buffered logging
 - SNMP traps
 - External Syslog server

- Recall: Syslog is used by an IP device known as a syslog client to send text-based log messages to another IP device known as the syslog server.
- Implementing a logging facility is a very important part of network security and also for network troubleshooting.
- Network devices can log various types of information including configuration changes, ACL violations, interface status, and many other types of events.
- Syslog messages fall into one of eight levels. The lower the level number, the higher the severity level.

Physical Layer Troubleshooting



- The physical layer is the only layer with physically tangible properties, such as wires, cards, and antennas.
- Because the upper layers of the OSI model depend on the physical layer to function, a network administrator must have the ability to effectively isolate and correct problems at this layer.
- Common symptoms of network problems at the physical layer include:
 - Performance lower than baseline
 - Loss of connectivity
 - Network bottlenecks or congestion
 - High CPU utilization rates
 - Console error messages

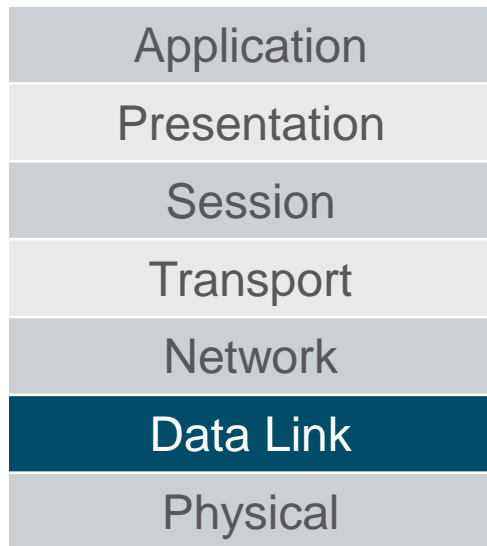
Symptoms and Causes of Network Troubleshooting

Physical Layer Troubleshooting (Cont.)

- Issues that commonly cause network problems at the physical layer include:

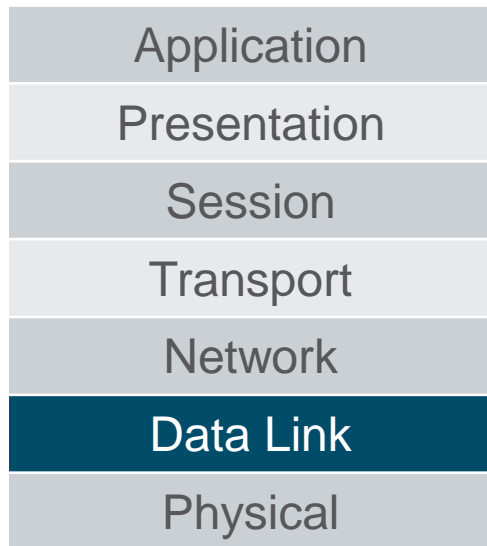
Problem Cause	Description
Power-related	Check the operation of the fans and ensure that the chassis intake and exhaust vents are clear.
Hardware faults	Faulty or corrupt NIC driver files, bad cabling, or grounding problems can cause network transmission errors such as late collisions, short frames, and jabber.
Cabling faults	Look for damaged cables, improper cable, and poorly crimped connectors. Suspect cables should be tested or exchanged with a known functioning cable.
Attenuation	Attenuation can be caused if a cable length exceeds the design limit for the media, or when there is a poor connection resulting from a loose cable, or dirty or oxidized contacts.
Noise	Local electromagnetic interference (EMI) can be generated by many sources, such as crosstalk, nearby electric cables, large electric motors, FM radio stations, police radio, and more.
Interface configuration errors	Causes can include incorrect clock rate, incorrect clock source, and interface not being turned on. This causes a loss of connectivity with attached network segments.
Exceeding design limits	A component could operate sub-optimally if it is being utilized beyond specifications.
CPU overload	Symptoms include processes with high CPU utilization percentages, input queue drops, slow performance, SNMP timeouts, no remote access, no DHCP services, Telnet, and pings are slow or fail to respond.

Data Link Layer Troubleshooting



- Troubleshooting Layer 2 problems can be a challenging process.
- Layer 2 problems cause specific symptoms that, when recognized, will help identify the problem quickly:
 - No functionality or connectivity at the network layer or above
 - Network is operating below baseline performance levels
 - Excessive broadcasts
 - Most common Layer 2 console message is: “line protocol down”

Data Link Layer Troubleshooting (Cont.)



- Issues at the data link layer that commonly result in network connectivity or performance problems include these:
 - Encapsulation errors
 - Encapsulation at one end of a WAN link is configured differently from that on the other end.
 - Address mapping errors
 - In a point-to-multipoint or broadcast Ethernet topology, it is essential that an appropriate Layer 2 destination address be given to the frame.
 - Framing errors
 - A framing error occurs when a frame does not end on an 8-bit byte boundary.
 - Spanning Tree Protocol (STP) failures or loops.
 - Most STP problems are related to forwarding loops that occur when no ports in a redundant topology are blocked and traffic is forwarded in circles indefinitely.

Network Layer Troubleshooting

Application
Presentation
Session
Transport
Network
Data Link
Physical

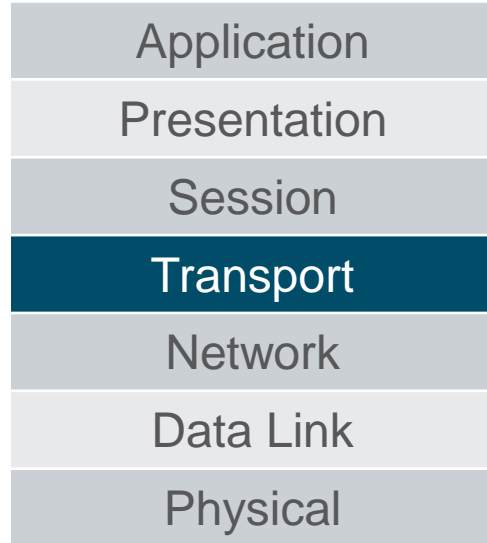
- Network layer problems include any problem that involves a Layer 3 protocol (routed or routing protocols)
- Common symptoms of network layer problems:
 - Network failure
 - Suboptimal performance
- Areas to explore when diagnosing a possible problem involving routing protocols:
 - General network issues
 - Connectivity issues – Also check for Layer 1 or power issues
 - Routing table issues – use **debug**
 - Neighbor issues – check for adjacencies if using routing protocols
 - Check the routing table topology database

Transport Layer Troubleshooting - ACLs

Application
Presentation
Session
Transport
Network
Data Link
Physical

- Network problems can arise from transport layer problems on the router. Improper ACL configuration issues might include:
 - Wrong selection of traffic flow (inbound/outbound)
 - Incorrect order of access control entries
 - Implicit **deny any**
 - Misconfiguration of addresses and IPv4 wildcard masks
 - Selecting both UDP and TCP protocols when unsure
 - Incorrect source and destination ports
 - Incorrect use of the **established** keyword
 - Misconfiguration of uncommon protocols such as VPN and encryption protocols

Transport Layer Troubleshooting – NAT for IPv4



- There are a number of problems with NAT such as not interacting with services like DHCP and tunneling.
- These can include misconfigured NAT inside, NAT outside, or a misconfigured ACL.
- Other issues include interoperability with other network technologies including:
 - BOOTP and DHCP
 - DNS
 - SNMP
 - Tunneling and encryption protocols

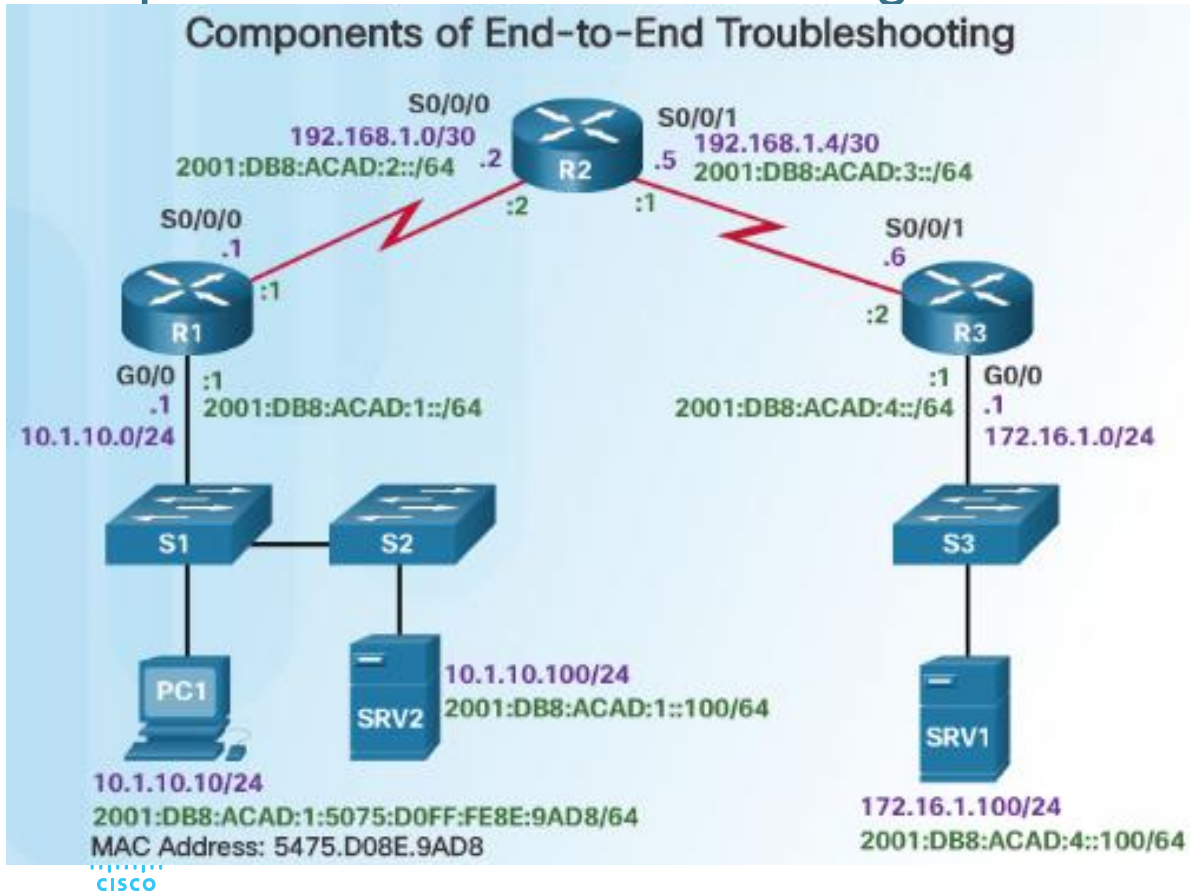
Symptoms and Causes of Network Troubleshooting

Application Layer Troubleshooting

Application
Presentation
Session
Transport
Network
Data Link
Physical

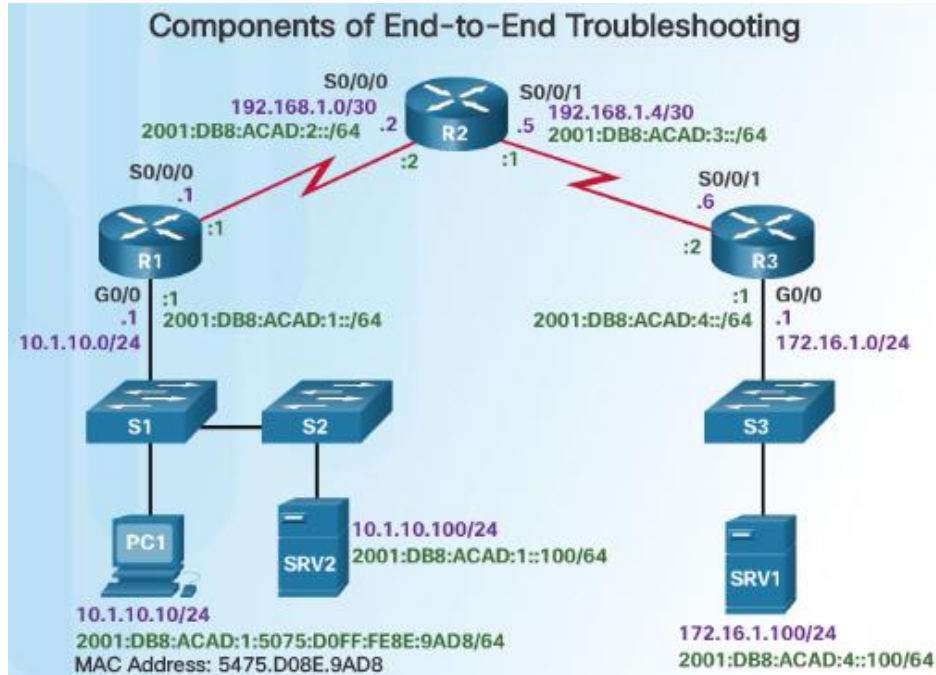
- Most of the application layer protocols provide user services for network management, file transfer, distributed file services, terminal emulation, and email.
- The most widely known and implemented TCP/IP application layer protocols include:
 - SSH/Telnet, HTTP, FTP, TFTP
 - SMTP, POP, SNMP, DNS, NFS
- Application layer problems prevent services from being provided to application programs.
- A problem at the application layer can result in unreachable or unusable resources when the physical, data link, network, and transport layers are functional.

Components of Troubleshooting End-to-End Connectivity



- By employing a structured approach to the troubleshooting process, an administrator can reduce the time it takes to diagnose and solve a problem.
- Sample scenario:
 - The client host PC1 is unable to access applications on server SRV1 or server SRV2.
 - PC1 uses SLAAC with EUI-64 to create its IPv6 global unicast address

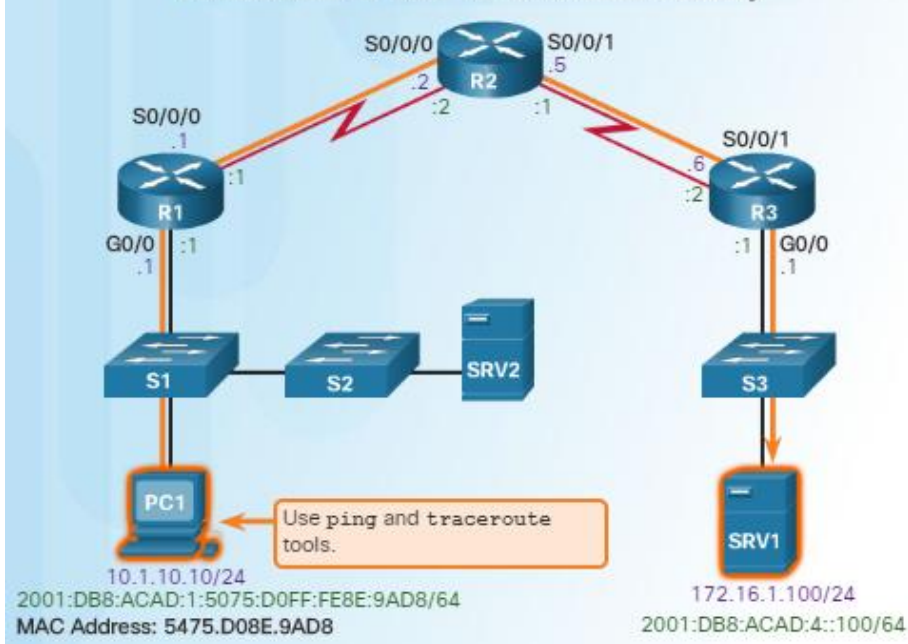
Components of Troubleshooting End-to-End Connectivity (Cont.)



- **Step 1.** Check physical connectivity at the point where network communication stops.
- **Step 2.** Check for duplex mismatches.
- **Step 3.** Check data link and network layer addressing on the local network.
- **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. Manipulate the routing information if necessary.
- **Step 6.** Verify that the transport layer is functioning properly (Telnet can be used).
- **Step 7.** Verify that there are no ACLs blocking traffic.
- **Step 8.** Ensure that DNS settings are correct. There should be a DNS server that is accessible.

End-to-End Connectivity Problem Initiates Troubleshooting

Verification of End-to-End Connectivity



- **Ping** and **traceroute** are the two most common utilities to test end-to-end connectivity.
- The **ping** command uses a Layer 3 protocol that is a part of the TCP/IP suite called ICMP.
 - **ping** uses the ICMP echo request and ICMP echo reply packets.
 - **ping** can be used for IPv4 and IPv6
- The **traceroute** command illustrates the path the IPv4 packets take to reach their destination.
 - The Cisco IOS **traceroute** command can be used for both IPv4 and IPv6
 - The **tracert** command can be used on Windows
- The **traceroute** command is commonly performed when the **ping** command fails.

Step 1 – Verify the Physical Layer

- The following IOS commands may be used to verify suspected physical issues:
 - **show processes cpu**
 - **show memory**
 - **show interfaces**
- If device exhibits performance issues and hardware is suspected to be at fault, use the **show interfaces** command and pay attention to the following:
 - Input queue drops
 - Output queue drops
 - Input errors
 - Output errors

```
Router#show interface G0/0
GigabitEthernet0/0 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is d48c.b5ce.a0c0
  (bia d48c.b5ce.a0c0)
  Internet address is 10.1.10.1/24
...

Input queue: 0/75/0 (size/max/drops); Total output drops:0
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0
  abort
  0 watchdog, 1017 multicast, 0 pause input
  0 input packets with dribble condition detected
  0 packets output, 0 bytes, 0 underruns
  0 output errors, 0 collisions, 1 interface resets
  0 unknown protocol drops
  0 babbles, 0 late collision, 0 deferred
  0 lost carrier, 0 no carrier
  0 output buffer failures, 0 output buffers swapped out
```

Step 2 – Check for Duplex Mismatches

```
S1#show interface Fa0/20
FastEthernet0/20 is up, line protocol is up
  Hardware is CN Fast Ethernet, address is
    0010.11c4.7801 (bia 0010.11c4.7801)
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, Auto-speed, media type is 10/100BaseTX
  ...
```

```
S2#show interface Fa0/20
FastEthernet0/20 is up, line protocol is up
  Hardware is CN Fast Ethernet, address is
    0010.11c4.7801 (bia 0010.11c4.7801)
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, Auto-speed, media type is 10/100BaseTX
  ...
```

- Duplex mismatch between two ends of an Ethernet link is another common cause for interface errors.
- Interfaces use autonegotiation to determine link speed and duplex
 - The IEEE 802.3ab Gigabit Ethernet standard mandates the use of autonegotiation for speed and duplex.
 - Most Fast Ethernet NICs also use autonegotiation by default.
- Set the speed and duplex manually on both ends if autonegotiation fails.
 - Point-to-point Ethernet links should always run in full-duplex mode.

Step 3 – Verify Layer 2 and 3 Addressing on the Local Network

```
S1>show mac address-table
      Mac Address Table
```

Vlan	Mac Address	Type	Ports
All	0100.0ccc.ccc	STATIC	CPU
All	0100.0ccc.ccd	STATIC	CPU
1	d48c.b5ce.a0c0	DYNAMIC	Fa0/1
10	000f.34f9.9201	DYNAMIC	Fa0/5
10	5475.d08e.9ad8	DYNAMIC	Fa0/13

```
-----
Total MAC Addresses for this criterion: 5
```

- Look for VLAN assignment issues when troubleshooting end-to-end connectivity issues (**show vlan**)
- The output of the **show mac address-table** command can also be helpful when looking for VLAN assignment issues.

R1

PC1

Step 3 – Verify Layer 2 and 3 Addressing on the Local Network

- The **arp** Windows command can be used to help verify mappings between destination IP addresses and Layer 2 Ethernet addresses.
 - The **arp -d** command can be used to clear the arp cache and allow it to repopulate with updated info.

```
C:\WINDOWS\system32>arp -a
```

```
Interface: 192.168.2.62 --- 0xe
```

Internet Address	Physical Address	Type
10.1.10.1	d48c.b5ce.a0c0	dynamic
10.1.10.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

- The **netsh interface ipv6 show neighbor** Windows command will list all devices that are currently in the neighbor table.
 - By examining the neighbor table, the network administrator can verify that the destination IPv6 addresses map to correct Ethernet addresses.
- The **show ipv6 neighbors** command can be used on a Cisco IOS router.

Step 4 – Verify Default Gateway

```
R1>show ip route
```

```
...
```

```
Gateway of last resort is 192.168.1.2 to network 0.0.0.0
```

```
S* 0.0.0.0/0 [1/0] via 192.168.1.2
```

```
C:\WINDOWS\system32>route print
```

```
IPv4 Route Table
```

```
=====
```

```
Active Routes:
```

Network	Destination	Netmask	Gateway	Interface	Metric
	0.0.0.0	0.0.0.0	10.1.10.2	10.1.10.100	50

- If there is no default route on the router or if the host is configured with the wrong default gateway, then communication between two endpoints on different networks will not work.
- Use the following commands to verify
 - **show ip route / show ipv6 route** to check for the router default route on R1
 - **ipconfig** Windows command to verify if a PC has a default gateway
 - **Route print** Windows command to check the PC routing table for a default gateway
 - **show ipv6 interface GigabitEthernet 0/0** command to verify if router is a member of the correct multicast group.

Step 5 – Verify Correct Path

Examining the IPv6 Routing Table on R1

```
R1# show ipv6 route
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static
       U - Per-user Static route, B - BGP, R - RIP
       I1 - ISIS L1, I2 - ISIS L2, A - ISIS interarea
       IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter
       OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
       ON2 - OSPF NSSA ext 2
S  ::/0 [1/0]
   via 2001:DB8:ACAD:2::2
C  2001:DB8:ACAD:1::/64 [0/0]
   via GigabitEthernet0/0, directly connected
L  2001:DB8:ACAD:1::1/128 [0/0]
   via GigabitEthernet0/0, receive
C  2001:DB8:ACAD:2::/64 [0/0]
   via Serial0/0/0, directly connected
L  2001:DB8:ACAD:2::1/128 [0/0]
   via Serial0/0/0, receive
D  2001:DB8:ACAD:3::/64 [90/41024000]
   via FE80::2, Serial0/0/0
D  2001:DB8:ACAD:4::/64 [90/41024256]
   via FE80::2, Serial0/0/0
L  FF00::/8 [0/0]
   via Null0, receive
R1#
```

- When troubleshooting a connectivity issue, verify the path to the destination network.
- Use either the **show ip route** or **show ipv6 route** command to verify that the route exists to the destination device/network.
- Forwarding packets is based on the longest bit match or longest prefix match. If the destination address in a packet:
 - Does not match any entry in the routing table, then the default route is used; otherwise drop
 - Matches a single entry in the routing table, forward through the interface that is defined in this route.
 - Matches more than one entry in the routing table and the routing entries have the same prefix length, load-balance among the routes that are defined in the routing table.

Step 6 – Verify the Transport Layer

- If the network layer appears to be functioning as expected, but users are still unable to access resources, then troubleshoot the upper layers.
- Most common issues that affect transport: ACL and NAT configuration problems.
- A common tool for testing transport layer functionality is the Telnet utility.
- If a ping is successful to a server, then all layers below the network layer, between the user and the server are operational. Issue is likely to be with Layer 4 or up.
- For example: R1# **telnet 2001:db8:acad:3::2**

```
R1>telnet 2001:db8:acad:3::2 80
Trying 2001:db8:acad:3::2, 80...
% Connection refused by remote host

R1#
```


Troubleshooting IP Connectivity

Step 7 – Verify ACLs

```
R3#show access-lists
Extended IP access list 100
  deny ip 172.16.1.0 0.0.0.255 any (3 match(es))
  permit ip any any

R3#show ip interface Serial0/0/1 | include access list
Outgoing access list is not set
Inbound access list is not set

R3#show ip interface gigabitethernet0/0 | include access
list
Outgoing access list is not set
Inbound access list 100
```

- ACLs may prohibit protocols from passing through the interface in the inbound or outbound direction.
- Use the following commands to display the contents of all ACLs:
 - **show ip access-lists**
 - **show ipv6 access-list**
- Use the following commands to see if there are ACLs set on a particular interface:
 - **show ip interfaces**
 - **show ipv6 interfaces**

Step 7 – Verify DNS

```
C:\WINDOWS\system32>nslookup
Default Server:  router.xyz.com
Address:  10.1.10.1

> SRV1
Server:  router.xyz.com
Address:  192.168.2.1

Name:      SRV1.xyz.com
Addresses:  172.16.1.100
```

- When DNS is used in the network and the DNS server is configured on a device, you can substitute the hostname for the IP address for all IP commands including **ping** and **telnet**.
- On a PC, use the **nslookup** command to check for availability of the DNS server



Questions?

What Did You Learn In This Module?

- Common network documentation includes physical and logical network topologies, network device documentation, and network performance baseline documentation.
- Baselining allows an administrator to document what is considered normal behavior / traffic characteristics of the network
- The troubleshooting process should be guided by structured methods which involve gathering symptoms, isolating the issue, implementing corrective action and documenting the solution
- Several troubleshooting methods may be used depending on the nature of the problem
 - Use bottom-up approach when encountering a new problem or if the problem appears to be a physical issue
 - Use top-down approach when a problem appears to be software in nature
 - Use divide and conquer when a problem seems to be similar to a previously diagnosed issue.

What did I learn in this module? (Cont.)

- Troubleshooting tools include
 - Hardware tools: digital multimeters, cable testers, cable analyzers, portable network analyzers, Cisco Prime NAM,
 - Software tools: NMS tools, knowledge bases, baselining tools, protocol analyzer, and syslog servers.
- When identifying the cause of an issue, it is important to recognize the probable network layer where it lies
 - Physical layer problems cause failures and suboptimal conditions.
 - Data link layer problems are typically caused by encapsulation errors, address mapping errors, framing errors, and STP failures or loops.
 - Network layer problems include IPv4, IPv6, routing protocols (such as EIGRP, OSPF, etc.).
 - Transport layer problems can be misconfigured NAT or ACLs.
 - Application layer problems can result in unreachable or unusable resources.



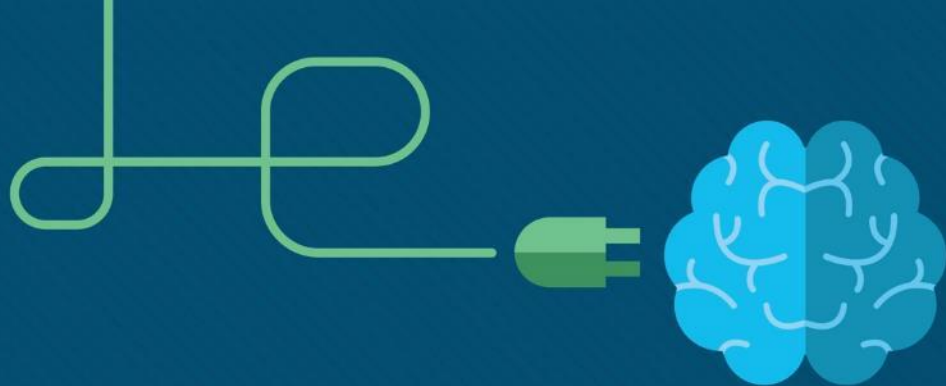


Module 9

Network Evolution

ITNET04

WAN Connectivity



Chapter 7 - Sections & Objectives

- 7.1 Internet of Things
 - Explain the value of the Internet of Things.
 - Describe the Cisco IoT System.
 - Describe the pillars of the Cisco IoT System.
- 7.2 Cloud and Virtualization
 - Explain why cloud computing and virtualization are necessary for evolving networks.
 - Explain the importance of cloud computing.
 - Explain the importance of virtualization.
 - Describe the virtualization of network devices and services.
- 7.3 Network Programming
 - Explain why network programmability is necessary for evolving networks.
 - Describe software-defined networking.
 - Describe controllers used in network programming.

7.1 Internet of Things

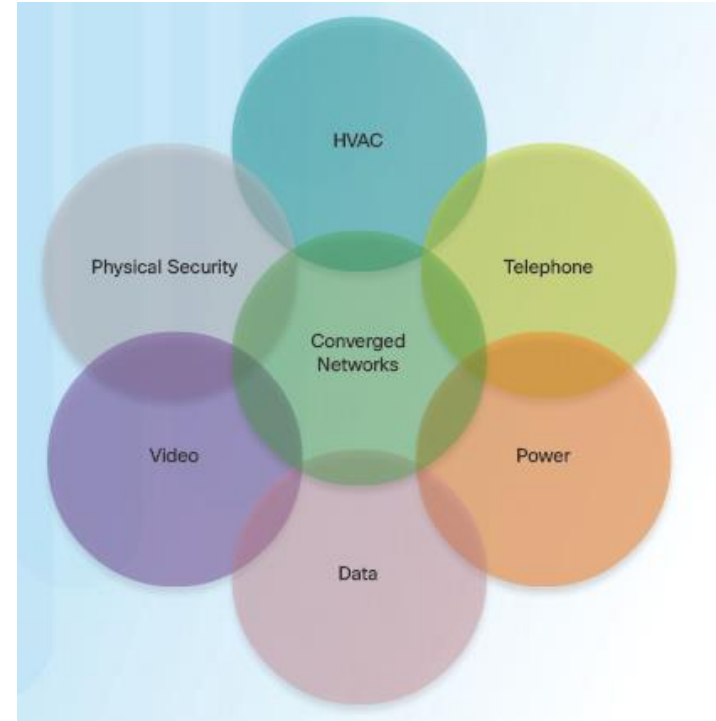
What is the IoT?

- It is predicted that the Internet will interconnect 50 billion things by 2020.
- Using existing and new technologies, we are connecting the physical world to the Internet.
- It is by connecting the unconnected that we transition from the Internet to the Internet of Things (IoT).



The Converged Network and Things

- Dissimilar networks are converging to share the same infrastructure.
- This infrastructure includes comprehensive security, analytics, and management capabilities.
- The connection of the components into a converged network that uses IoT technologies increases the power of the network to help people improve their daily lives.



The Six Pillars of the Cisco IoT System

- Cisco IoT System uses six pillars to identify foundational elements.



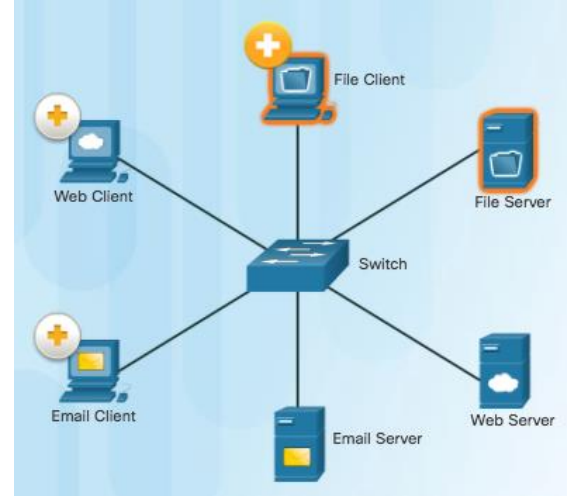
The Network Connectivity Pillar

- All IoT devices (sensors, actuators, etc) need network connectivity to communicate and perform automated tasks
- Network equipment needed varies depending on the type of network.
 - LANs
 - PANs
 - WANs
 - WLANs
- Home networks typically consist of a wireless broadband router, while business networks will have multiple switches, APs, a firewall or firewalls, routers, and more.

The Fog Computing Pillar

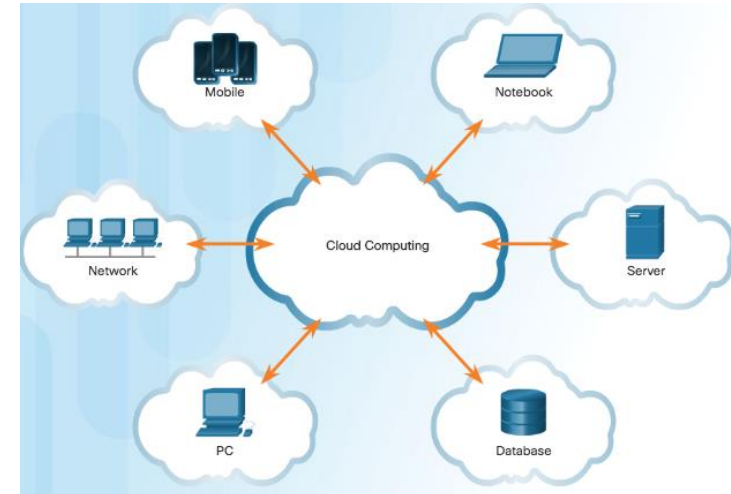
■ Fog computing

- This IoT network model identifies a computing infrastructure closer to the network edge.
- Edge devices run applications locally and make immediate decisions.
- Data does not need to be sent over network connections.
- Enhances resiliency by allowing IoT devices to operate when network connections are lost.
- Enhances security by keeping sensitive data from being transported beyond the edge where it is needed.



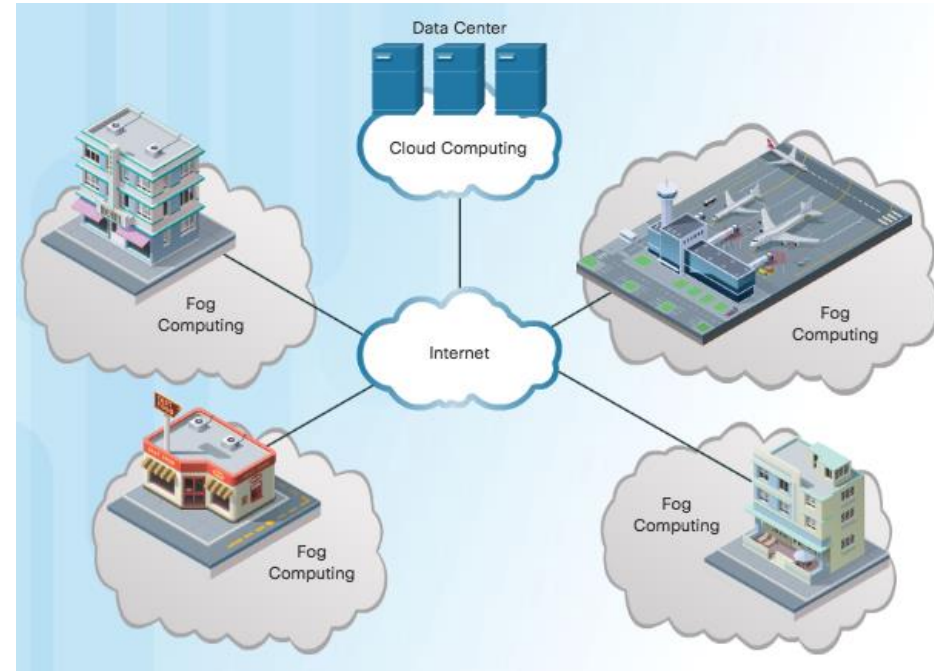
Client-Server Model

Cloud Computing Model



The Fog Computing Pillar

- Fog computing
 - This IoT network model identifies a computing infrastructure closer to the network edge.
 - Edge devices run applications locally and make immediate decisions.
 - Data does not need to be sent over network connections.
 - Enhances resiliency by allowing IoT devices to operate when network connections are lost.
 - Enhances security by keeping sensitive data from being transported beyond the edge where it is needed.



Fog Computing Model

The Security Pillar

- IoT introduces new attack vectors not typically encountered with normal enterprise networks.
- Cybersecurity solutions include:
 - Operational Technology (OT) specific security – OT is the hardware and software that keeps power plants running and manages factory process lines.
 - IoT Network security – Includes network and perimeter security devices.
 - IoT Physical security - Cisco Video Surveillance IP Cameras.



Cisco Industrial
Security Appliance



Cisco FirePOWER Appliance



Cisco Video
Surveillance
Cameras

Data Analytics Pillar

- IoT can connect billions of devices capable of creating exabytes of data every day. To provide value, this data must be rapidly processed and transformed into actionable intelligence.
 - Need to bring centers of data together and take advantage of data.

ANALYTICS & AUTOMATION:
a new approach

aggregate

Integrate data in
the right context at
the right time

analyze

Extract valuable
information from
data

automate

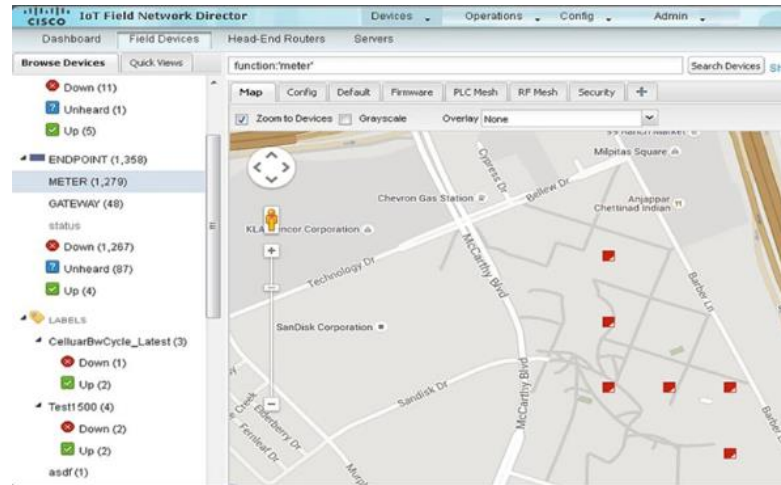
Automatically give
feedback to people
in order to make
better decisions

engage

Give personalized
experiences for
people

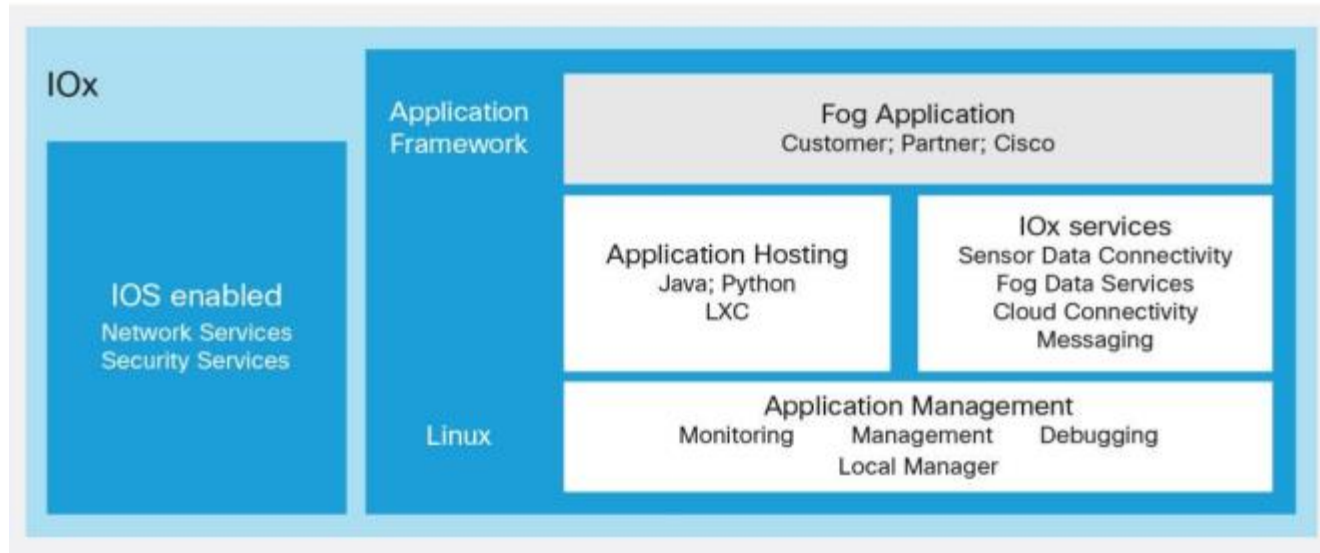
Management and Automation Pillar

- IoT expands the size and diversity of the network to include the billions of smart objects that sense, monitor, control, and react. Each of these areas also has distinctive requirements, including the need to track specific metrics.
- Cisco management and automation products can be customized for specific industries to provide enhanced security and control and support.
- Management Tools: Cisco IoT Field Network Director, Cisco Prime, Cisco Video Surveillance Manager, and more.



Application Enablement Platform Pillar

- Provides the infrastructure for application hosting and application mobility between cloud and Fog computing.
- Cisco IOx which is a combination of Cisco IOS and Linux, allows routers to host applications close to the objects they need to monitor, control, analyze, and optimize.



7.2 Cloud and Virtualization

If you were to host your own E-commerce website,
what hardware and software would you need?

What if you could just 'rent' everything and pay only
for what you use?

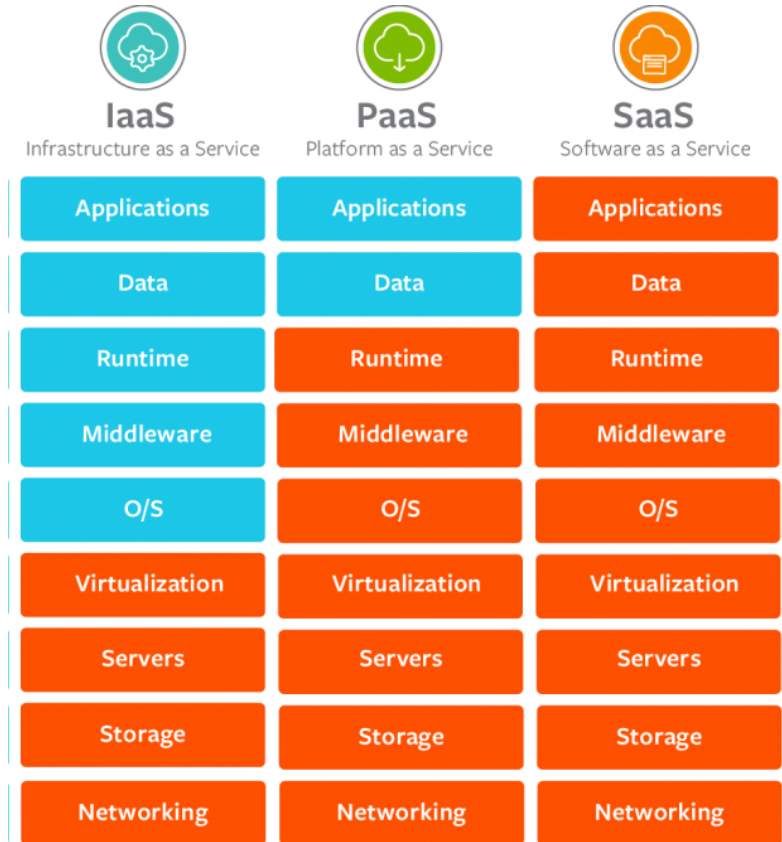
Cloud Computing Overview

- The “pay-as-you-go” model where capital expenditures are transferred to operating expenses.
- Large numbers of networked computers physically located anywhere.
- Providers rely heavily on virtualization to allow customers to reduce operational costs by using resources more efficiently.
- Supports a variety of data management issues:
 - Enables access to organizational data anywhere and at any time
 - Streamlines the organization’s IT operations by subscribing only to needed services
 - Eliminates or reduces the need for onsite IT equipment, maintenance, and management
 - Reduces cost for equipment, energy, physical plant requirements, and personnel training needs
 - Enables rapid responses to increasing data volume requirements

Cloud Computing

Cloud Services

- **Software as a Service (SaaS):** Access to services, such as email and Office 365 that are delivered over the Internet.
- **Platform as a Service (PaaS):** Access to the development tools and services used to deliver the applications.
- **Infrastructure as a Service (IaaS):** Access to the network equipment, virtualized network services, and supporting network infrastructure.
- **IT as a Service (ITaaS):** IT Professionals support applications, platforms and infrastructure.



Cloud Computing

Cloud Models

- **Public clouds:**

- Application and services made available to the general population and uses the Internet to provide services.
- Services may be free or are offered on a pay-per-use model

- **Private clouds:**

- Applications and services are intended for a specific organization or entity, such as the government.
- Can be set up using the organization's private network (expensive though!)

- **Hybrid clouds:**

- Made up of two or more clouds (example: part private, part public), where each part remains a distinctive object, but both are connected using a single architecture.

- **Community clouds:**

- Created for exclusive use by a specific community. e.g. healthcare organizations must remain compliant with policies and laws (e.g., HIPAA) that require special authentication and confidentiality.

Cloud Computing versus Data Center

- **Data center:** Typically a data storage and processing facility run by an in-house IT department or leased offsite.
- **Cloud computing:** Typically an off-premise service that offers on-demand access to a shared pool of configurable computing resources. These resources can be rapidly provisioned and released with minimal management effort.

Cloud computing is possible because of data centers.



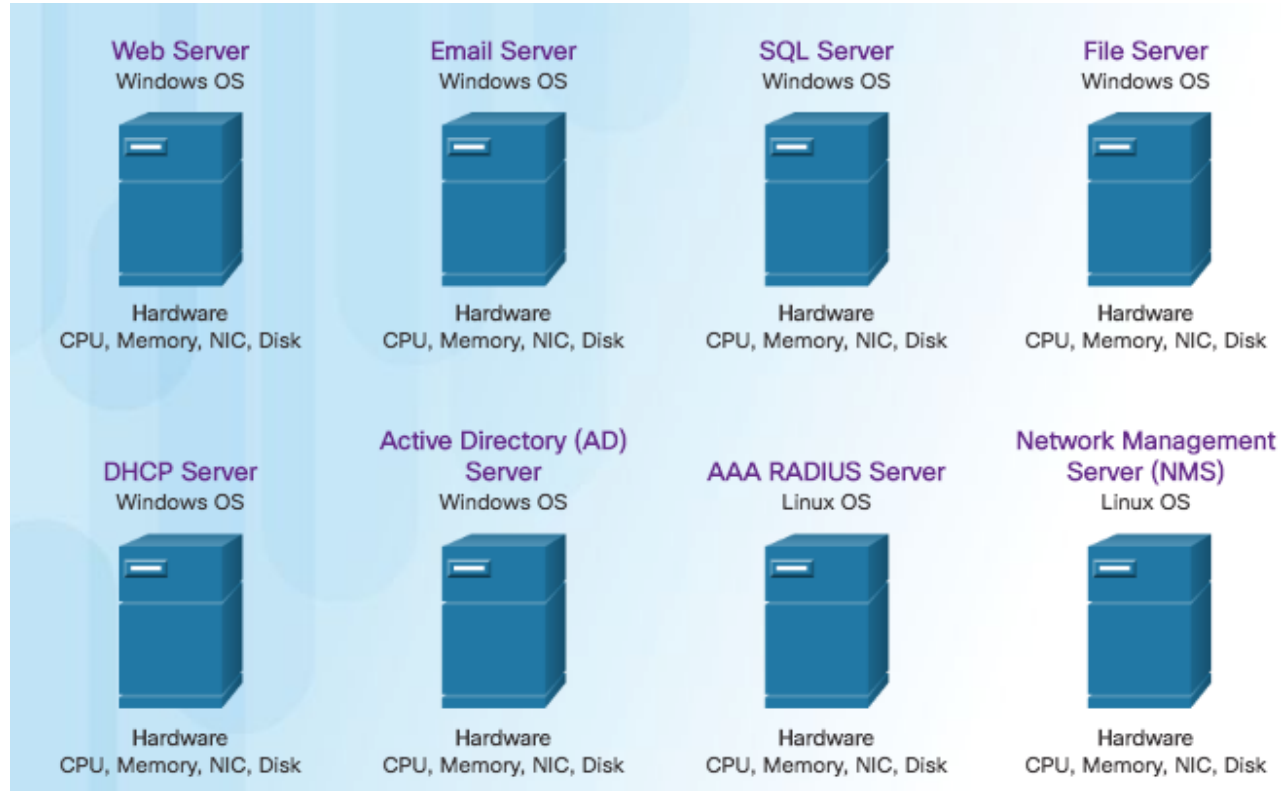
Cloud computing is often a service provided by data centers.

Cloud Computing and Virtualization

- Virtualization is the foundation of cloud computing. Without it, cloud computing would not be possible.
- Cloud computing separates the application from the hardware.
- Virtualization separates the OS from the hardware.
- Amazon Elastic Compute cloud (Amazon EC2) web service provides a simple way for customers to dynamically provision the computer resources they need. These virtualized instances of servers are created on demand in Amazon's EC2.

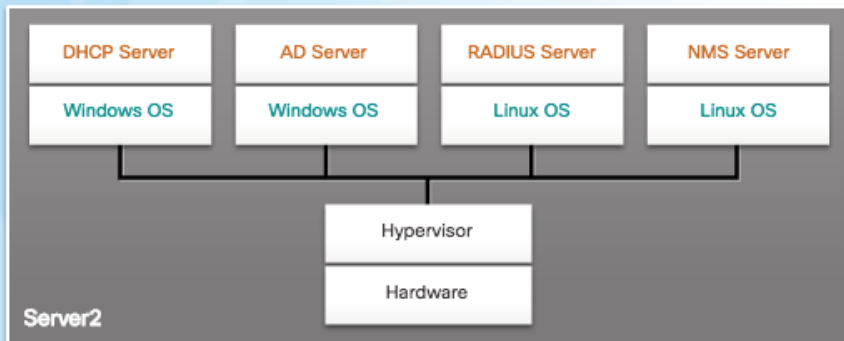
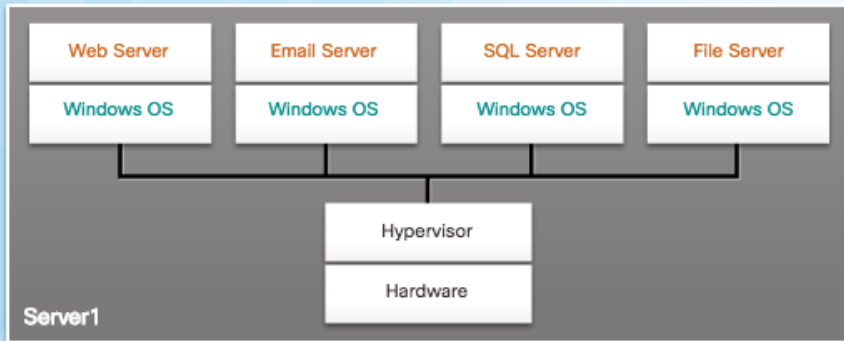
Virtualization

Dedicated Servers



Server Virtualization

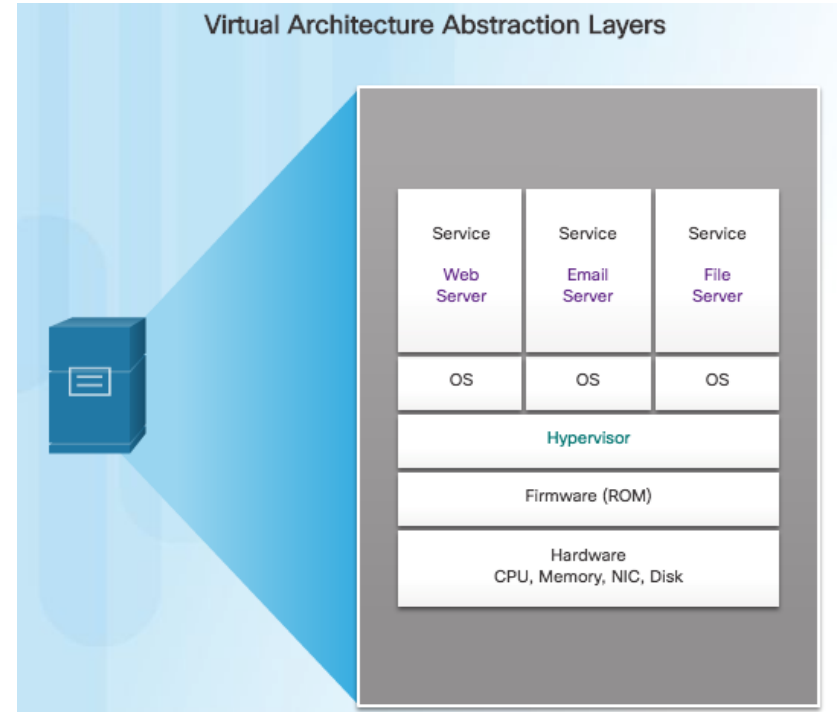
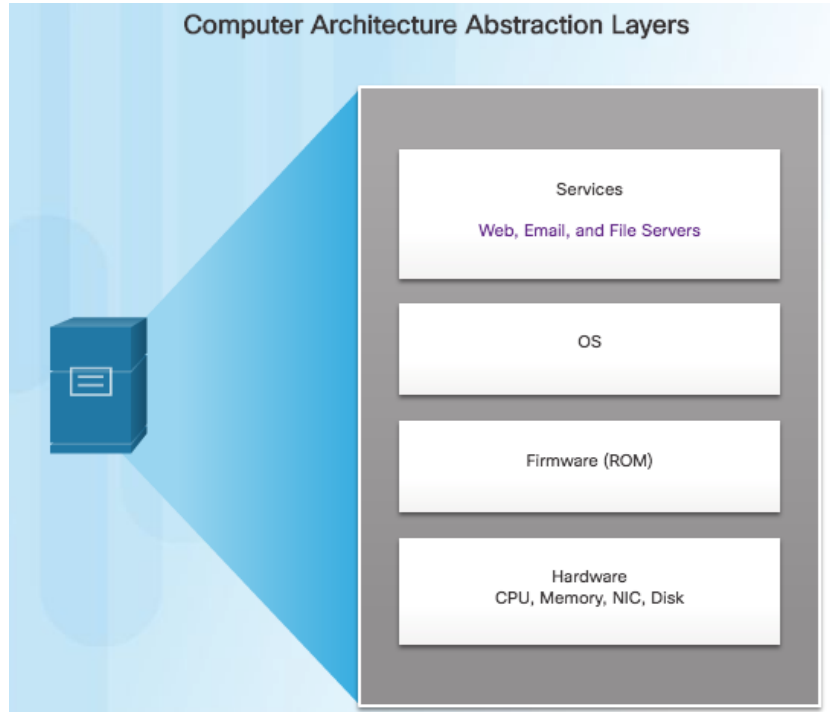
Hypervisor OS Installation



- Hypervisor is a program, firmware, or hardware that adds an abstraction layer on top of the real physical hardware.
- The abstraction layer is used to create virtual machines which have access to all the hardware of the physical machine such as CPUs, memory, disk controllers, and NICs.
- In the figure, the previous eight dedicated servers have been consolidated into two servers using hypervisors to support multiple virtual instances of the operating systems.
- It is not uncommon for 100 physical servers to be consolidated as virtual machines on top of 10 physical servers that are using hypervisors.

Abstraction Layers

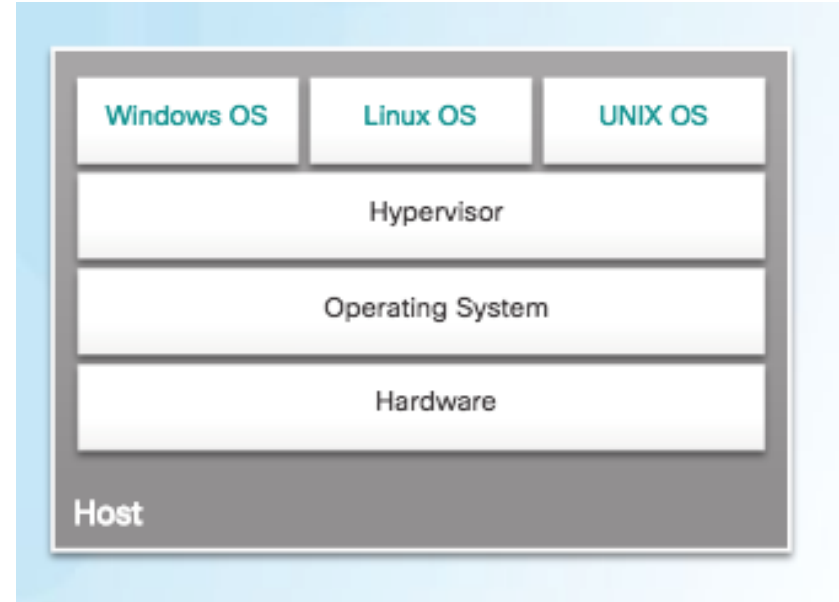
- A hypervisor is software installed between firmware and the OS that creates and runs virtual machine instances
- The computer, on which a hypervisor is supporting one or more VMs, is a host machine.



Virtualization

Hypervisors

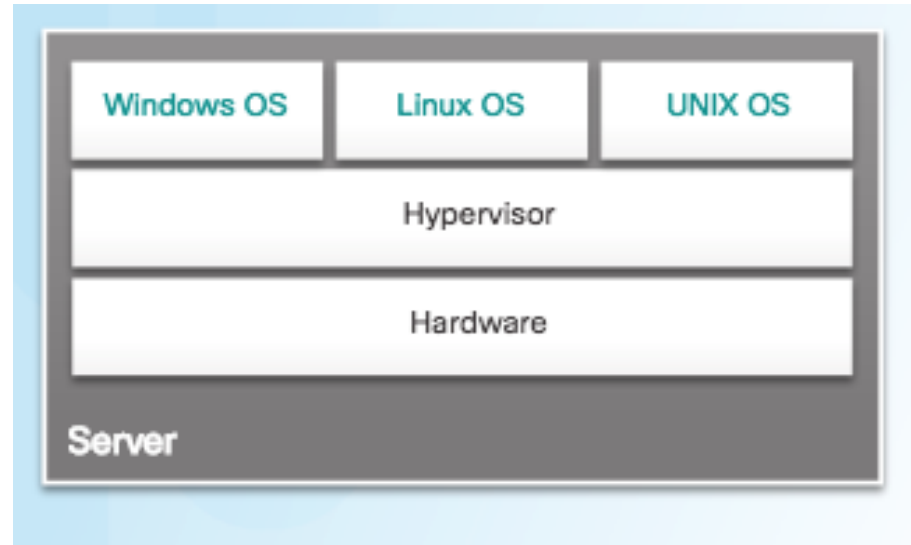
- Type 2 hypervisors (a.k.a. hosted hypervisors) and are installed on top of the existing OS.
- Examples:
 - Virtual PC
 - VMware Workstation
 - Oracle VM VirtualBox
 - VMware Fusion
 - Mac OS X Parallels



Virtualization

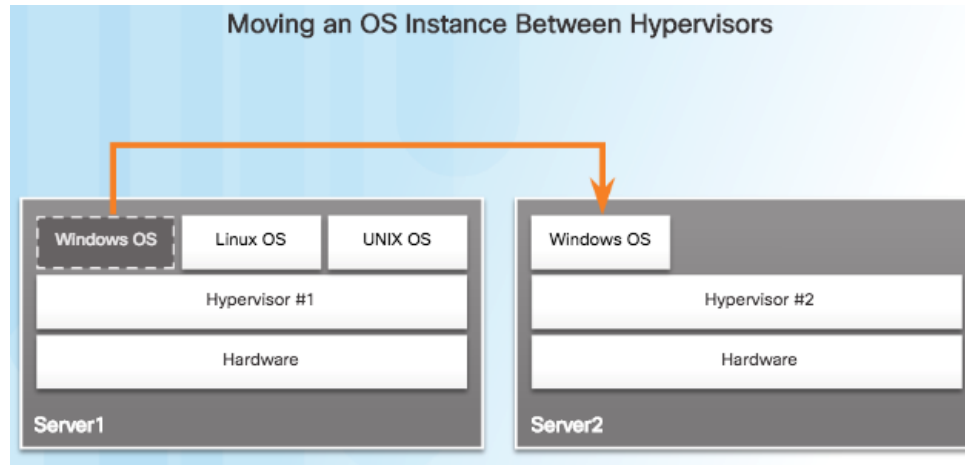
Hypervisors

- Type 1 hypervisors (a.k.a bare-metal hypervisors) are installed directly on the hardware.
 - Usually for enterprise servers and data centers
 - Have direct access to the hardware resources hence have better scalability, performance, and robustness.
- Examples:
 - VMware ESXi
 - Xen
 - Microsoft Hyper-V



Installing a VM on a Hypervisor

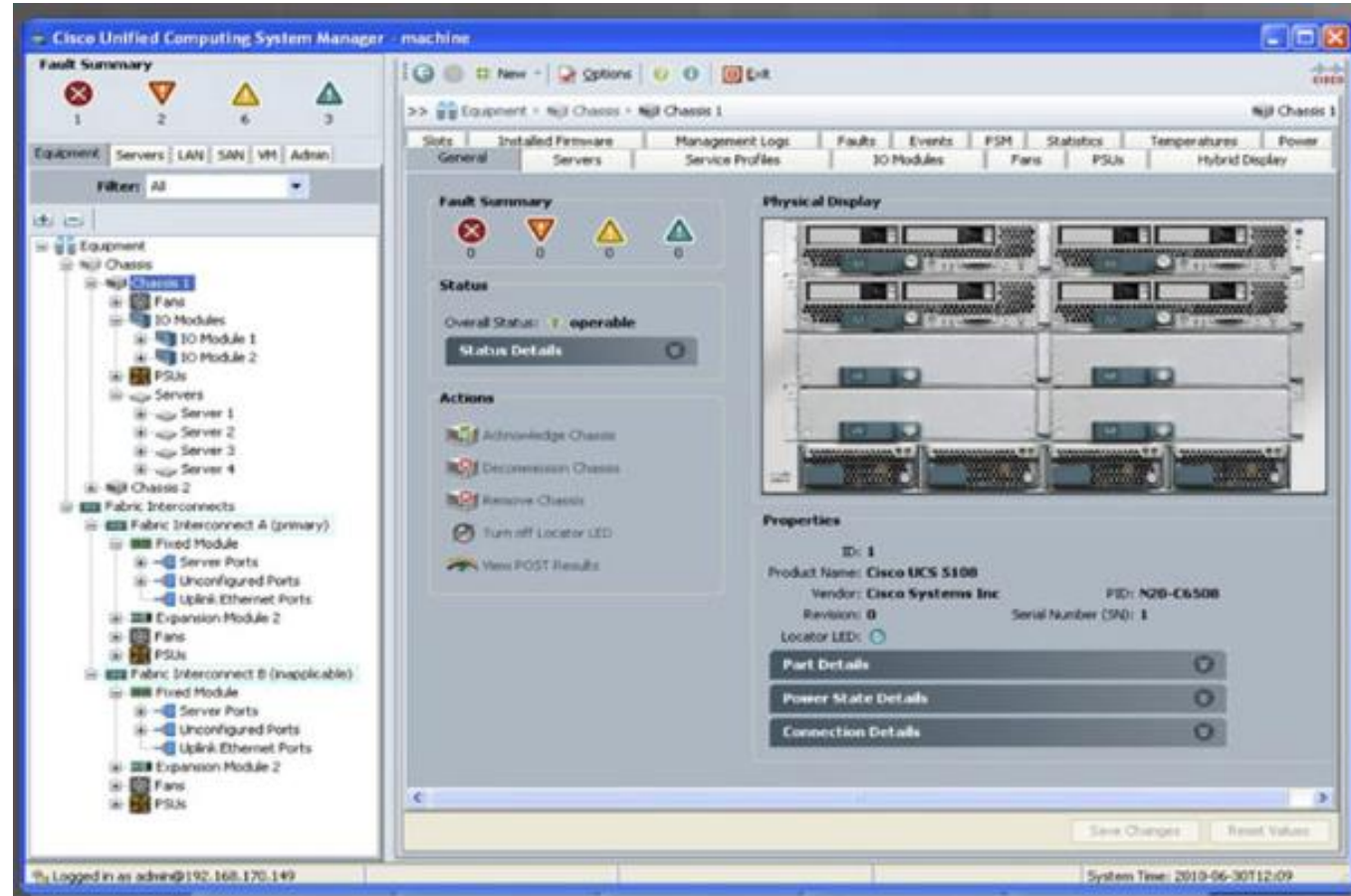
- Type 1 hypervisors require a “management console” to manage the hypervisor.
- Management software is used to manage multiple servers using the same hypervisor.
- The management console can automatically consolidate servers and power on or off servers as required.



Assume that Server1 in the figure becomes low on resources. To make more resources available, the management console moves the Windows instance to the hypervisor on Server2.

Installing a VM on a Hypervisor (Cont.)

- The management console provides recovery from hardware failure.
- If a server component fails, the management console automatically and seamlessly moves the VM to another server.



Advantages of Virtualization

- One major advantage of virtualization is overall reduced cost:
 - Less equipment is required - Server consolidation and lower maintenance costs.
 - Less energy is consumed - Consolidating servers lowers the monthly power and cooling costs.
 - Less space is required - Fewer servers, network devices, and racks reduce the amount of required floor space.
- Additional benefits of virtualization:
 - Easier prototyping
 - Faster server provisioning
 - Increased server uptime
 - Improved disaster recovery
 - Legacy Support

Virtual Network Infrastructure

Network Virtualization

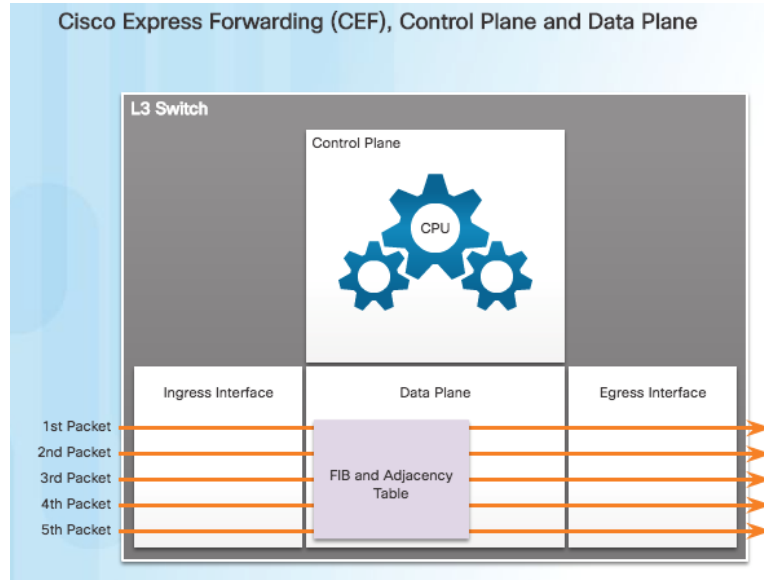
- Server virtualization hides server resources from server users. but can create problems used with traditional network architectures.
- Virtual LANs (VLANs) used by VMs must be assigned to the same switch port as the physical server running the hypervisor
 - VMs are movable and network settings must migrate together with them.
 - Network administrator must be able to add, drop, and change network resources and profiles.
- Traffic flows differ substantially from the traditional client-server model.
 - Typically, a data center has a considerable amount of traffic being exchanged between virtual servers (referred to as East-West traffic).
 - Traffic flows change in location and intensity over time, requiring a flexible approach to network resource management.
 - Quality of Service (QoS) and security level reconfigurations for individual flows can be tiem consuming in large enterprises using multivendor equipment

7.3 Network Programming

Software-Defined Networking

Control Plane and Data Plane

- A network device contains the following planes:
 - Control plane - Regarded as the brains of a device. Used to make forwarding decisions. Information sent to the control plane is processed by the CPU.
 - Data plane - Also called the forwarding plane, this plane is the switch fabric connecting the various network ports on a device. The data plane of each device is used to forward traffic flows.



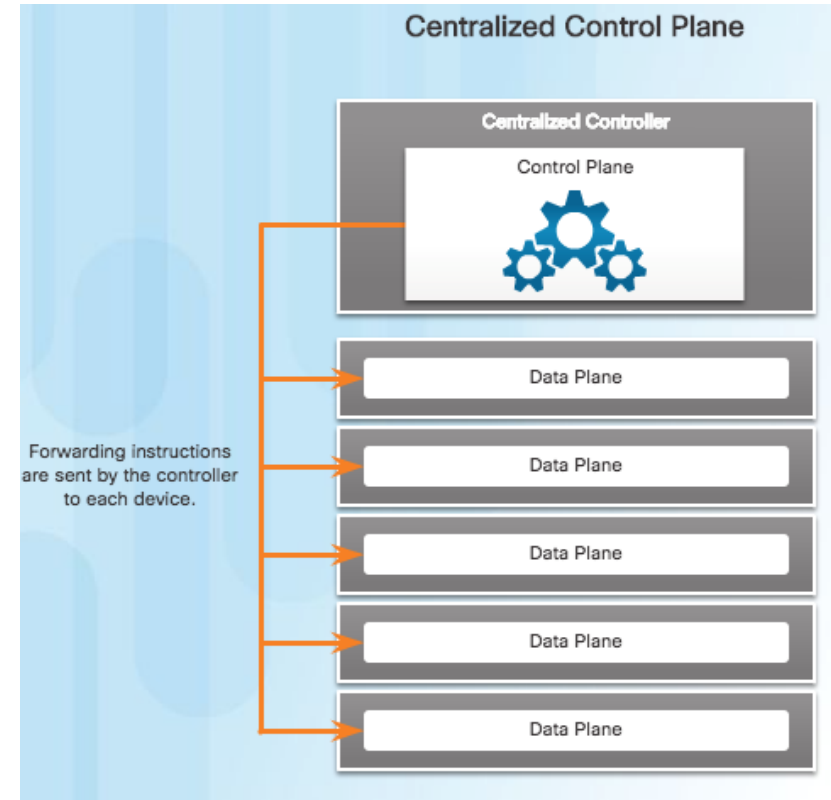
CEF is an advanced, Layer 3 IP switching technology that enables forwarding of packets to occur at the data plane without consulting the control plane.

Packets are forwarded directly by the data plane based on the information contained in the Forwarding Information Base (FIB) and adjacency table, without needing to consult the information in the control plane.

Software-Defined Networking

Control Plane and Data Plane (Cont.)

- To virtualize the network, the control plane function is removed from each device and is performed by 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.



Software-Defined Networking

Virtualizing the Network

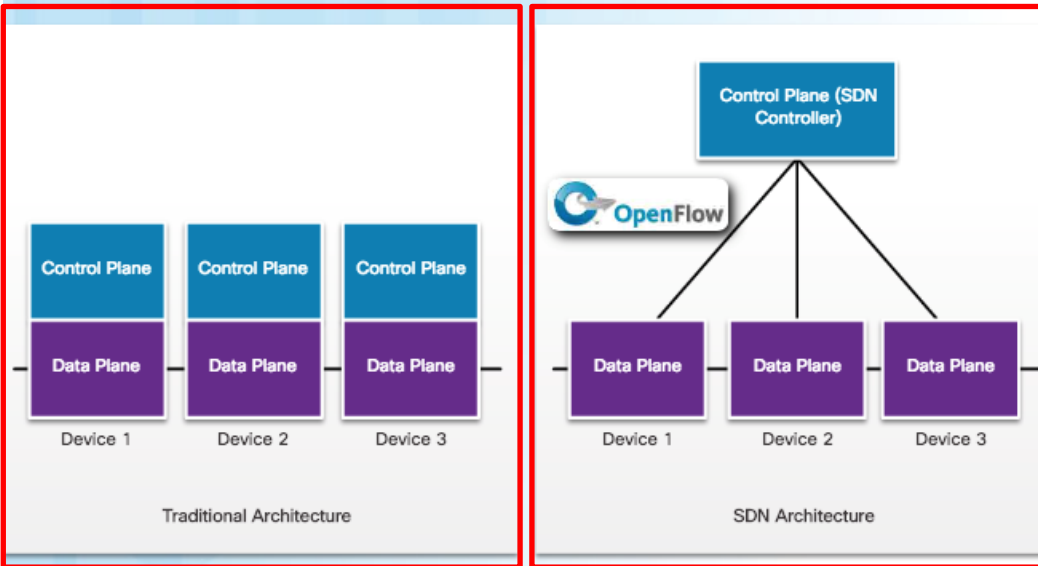
- Two major network architectures have been developed to support network virtualization:
 - Software Defined Networking (SDN) - A network architecture that virtualizes the network.
 - Cisco Application Centric Infrastructure (ACI) - A hardware solution for integrating cloud computing and data center management.
- These are some other network virtualization technologies, some of which are included as components in SDN and ACI:
 - OpenFlow - The OpenFlow protocol is a basic element in building SDN solutions.
 - OpenStack - This approach is a virtualization and orchestration platform available to build scalable cloud environments and provide an infrastructure as a service (IaaS) solution.



Software-Defined Networking

SDN Architecture

Traditional and SDN Architectures

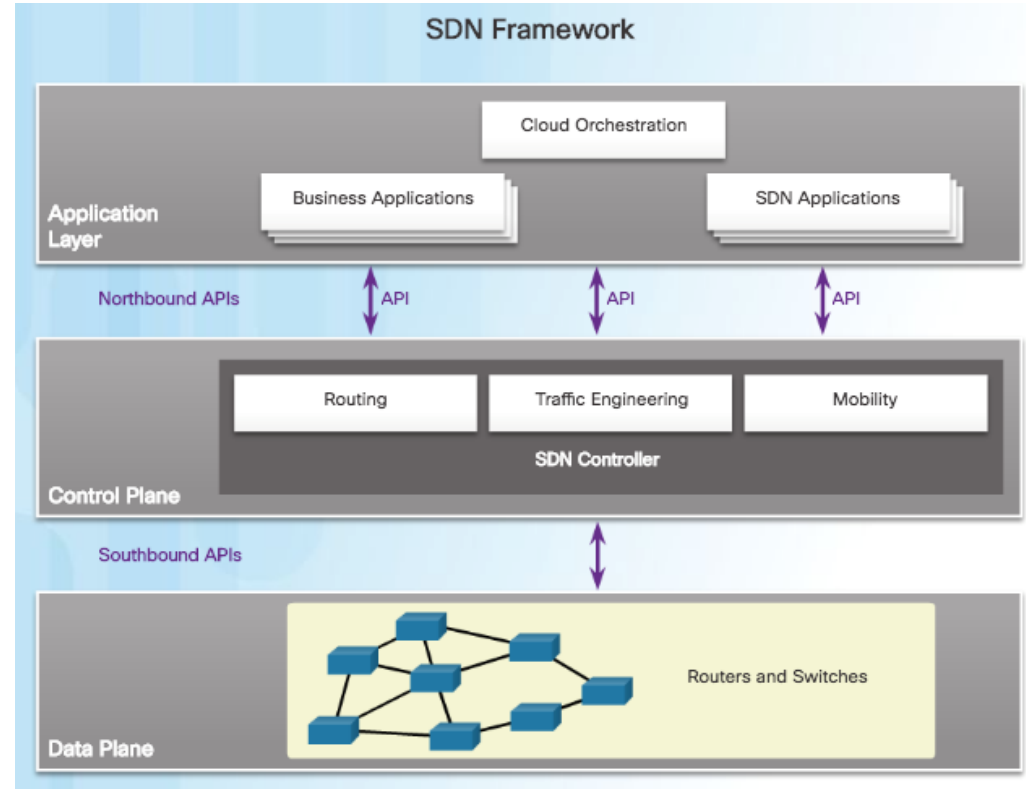


- In a traditional router or switch architecture, the control plane and data plane functions occur in the same device. Routing decisions and packet forwarding are the responsibility of the device operating system.
- Software defined networking (SDN) is a network architecture that virtualizes the control plane. The control plane is from each network device to a central network intelligence and policy-making entity called the *SDN controller*.

Software-Defined Networking

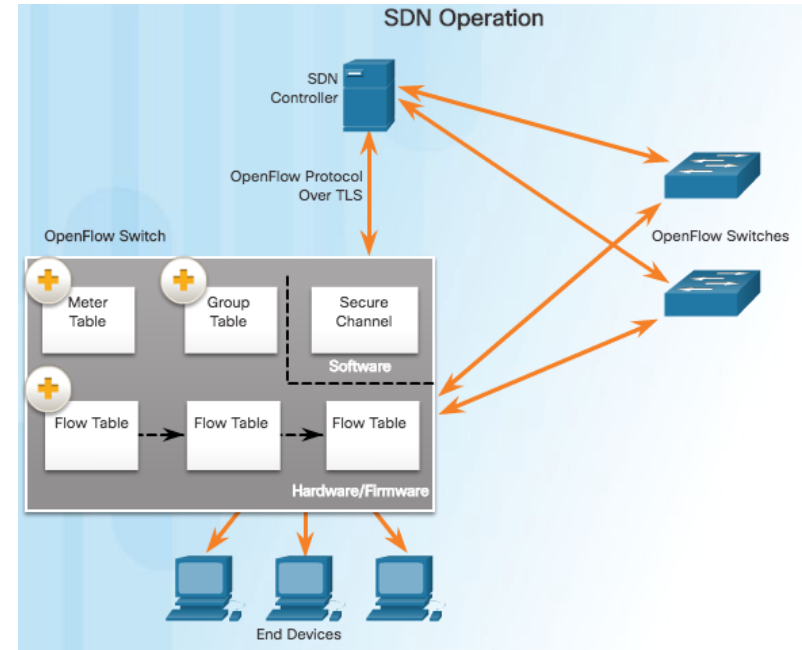
SDN Architecture (Cont.)

- The SDN controller enables network administrators to manage and dictate how the data plane of virtual switches and routers should handle network traffic.
- Northbound APIs communicate with the upstream applications. These APIs help network administrators shape traffic and deploy services.
- Southbound APIs control the behavior of virtual switches and routers. OpenFlow is the original and widely implemented southbound API.
- Note: An API is a set of standardized requests that define the methods by which an application can request services from another application.



SDN Controller and Operations

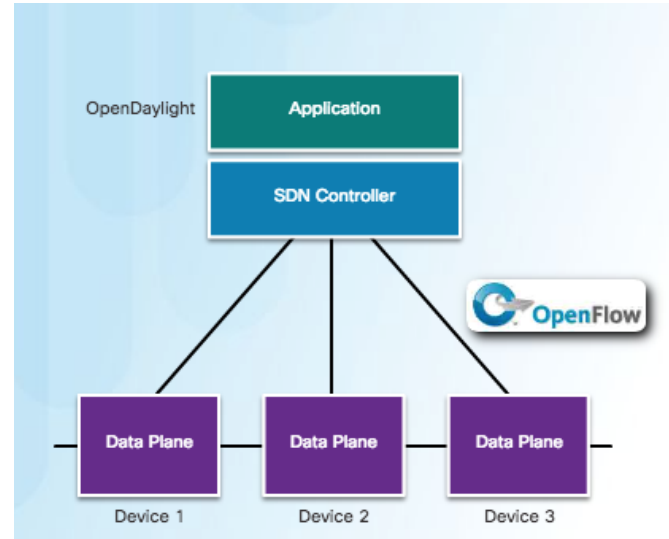
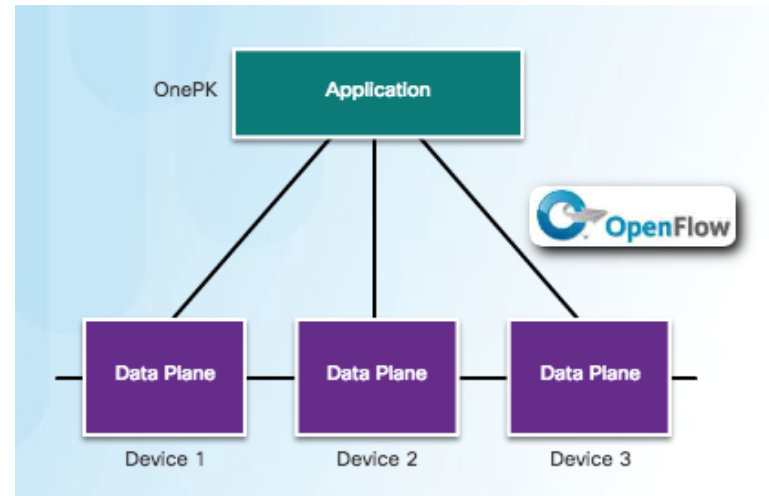
- SDN controller defines the data flows that occur in the SDN Data Plane. A flow could consist of all packets with the same source and destination IP addresses, or all packets with the same VLAN identifier.
- Each flow traveling through the network must first get permission from the SDN controller. If 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.
- The controller populates and the switches manage the flow tables. Each OpenFlow switch connects to other OpenFlow switches. They can also connect to end-user devices that are part of a packet flow.
- To the switch, a flow is a sequence of packets that matches a specific entry in a flow table.



Controllers

SDN Types

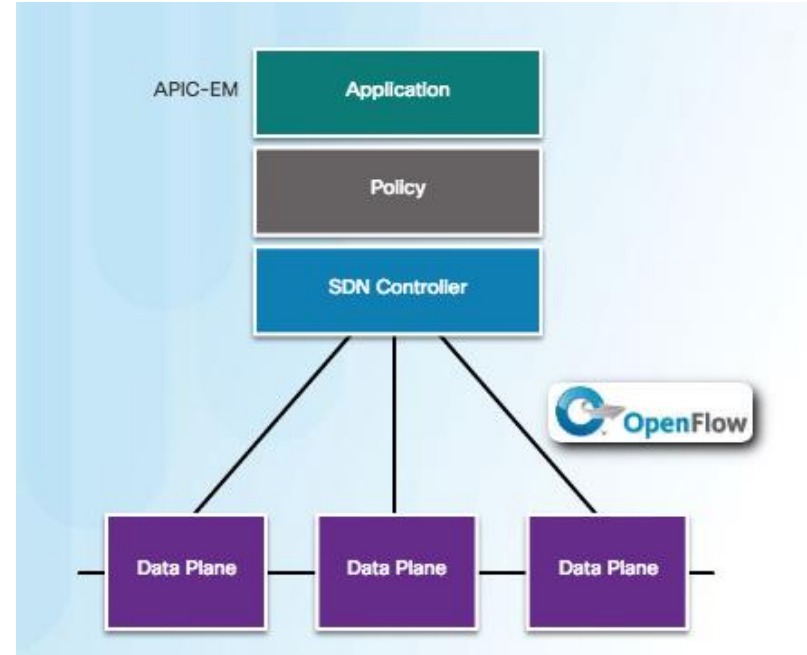
- Device-based SDN
 - The devices are programmable by applications running on the device itself or on a server in the network.
 - Cisco OnePK is an example of a device-based SDN. It enables programmers to build applications to integrate and interact with Cisco devices.
- Controller-based SDN
 - Uses a 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.



Controllers

SDN Types (Cont.)

- Policy-based SDN
 - Similar to controller-based SDN where a centralized controller has a view of all devices in the network.
 - Includes an additional Policy layer. Uses built-in applications that automate advanced configuration tasks via a guided workflow and user-friendly GUI.
 - Considered to be most robust, providing for a simple mechanism to control and manage policies across the entire network.
 - Cisco APIC-EM is an example of this type of SDN.





Questions?

1. Reflection paper for ITNET – **September 24 (Friday) 9PM**
2. Course feedback: **September 20 (Monday) 9 PM**
3. Case Project
 - Docu and simulation: **September 18 (Saturday)**
 - Peer Evaluation: **September 21**

Next Week

1. Final Exam: **September 20 (Monday) 8-11 AM**
2. *Data privacy review and end of course survey completion – **September 25 (12 noon)**