

CISCO CERTIFIED NETWORK ASSOCIATE EXAM (CCNA)



CLIVE MICALLEF

Table of Contents

1.0 Network Fundamentals	2
2.0 LAN Switching Technologies	18
3.0 Routing Technologies	27
4.0 WAN Technologies	36
5.0 Infrastructure Services	55
6.0 Infrastructure Security	67
7.0 Infrastructure Management	73

1.1 Compare and contrast OSI and TCP/IP models**Protocol Interaction**

HTTP - is an application protocol that governs the way a web server and a web client interact. HTTP defines the content and formatting of the requests and responses that are exchanged between the client and server.

TCP - is the transport protocol that manages the individual conversations. TCP divides the HTTP messages into smaller pieces, called segments. These segments are sent between the web server and client processes running at the destination host. TCP is also responsible for controlling the size and rate at which messages are exchanged between the server and the client.

IP - is responsible for taking the formatted segments from TCP, encapsulating them into packets, assigning them the appropriate addresses, and delivering them to the destination host.

Ethernet - is a network access protocol that describes two primary functions: communication over a data link and the physical transmission of data on the network media. Network access protocols are responsible for taking the packets from IP and formatting them to be transmitted over the media.

Application Layer

DNS –Translates domain names, such as cisco.com, into IP addresses.

BOOTP -Enables a diskless workstation to discover its own IP address, the IP address of a BOOTP server on the network, and a file to be loaded into memory to boot the machine.

DHCP –Dynamically assigns IP addresses to client stations at start-up.

SMTP –Enables clients to send email to a mail server, Enables servers to send email to other servers.

POP3 –Enables clients to retrieve email from a mail server, Downloads email from the mail server to the desktop.

IMAP –Enables clients to access email stored on a mail server, Maintains email on the server.

FTP –Sets rules that enable a user on one host to access and transfer files to and from another host over a network .A reliable, connection-oriented, and acknowledged file delivery protocol.

TFTP –A simple, connectionless file transfer protocol. A best-effort, unacknowledged file delivery protocol. Utilizes less overhead than FTP.

HTTP –Set of rules for exchanging text, graphic images, sound, video, and other multimedia files on the World Wide Web.

Transport Layer

UDP –Enables a process running on one host to send packets to a process running on another host. Does not confirm successful datagram transmission.

TCP –Enables reliable communication between processes running on separate hosts. Reliable, acknowledged transmissions that confirm successful delivery.

Internet Layer

IP –Receives message segments from the transport layer. Packages messages into packets. Addresses packets for end-to-end delivery over an Internet network.

NAT –Translates IP addresses from a private network into globally unique public IP addresses.

ICMP –Provides feedback from a destination host to a source host about errors in packet delivery.

OSPF –Link-state routing protocol. Hierarchical design based on areas. Open standard interior routing protocol.

EIGRP – Cisco proprietary routing protocol. Uses composite metric based on bandwidth, delay, load and reliability.

Network Access Layer

ARP – Provides dynamic address mapping between an IP address and a hardware address.

PPP – Provides a means of encapsulating packets for transmission over a serial link.

Ethernet – Defines the rules for wiring and signalling standards of the network access layer.

Interface Drivers - Provides instruction to a machine for the control of a specific interface on a network device.

OSI Model

7. Application – Contains protocols used for process to process communications.

6. Presentation – Provides for common representation of the data transferred between application layer services.

5. Session – Provides services to the presentation layer to organize its dialogues and to manage data exchange.

4. Transport – Defines services to segment, transfer, and reassemble the data for individual communication between the end device.

3. Network - provides services to exchange the individual pieces of data over the network between identified end devices.

2. Data Link - describe methods for exchanging data frames between devices over a common media.

1. Physical – The physical, mechanical and electrical components.

TCP/IP Model

Application – Represents data to the user, plus encoding and dialog control.

Transport – Supports communication between various devices across diverse networks.

Internet – Determines the best path through the network.

Network Access – Controls the hardware devices and media that make to the network.

Protocol Data Units

Application Layer – Data

Transport Layer – Segment

Network Layer – Packet

Data Link Layer – Frame

Physical Layer – Bits

1.2 Compare and contrast TCP and UDP protocols

	TCP	UDP
Acronym for	Transmission Control Protocol	User Datagram Protocol or Universal Datagram Protocol
Connection	TCP is a connection-oriented protocol.	UDP is a connectionless protocol.
Function	As a message makes its way across the internet from one computer to another. This is connection based.	UDP is also a protocol used in message transport or transfer. This is not connection based which means that one program can send a load of packets to another and that would be the end of the relationship.
Usage	TCP is suited for applications that require high reliability, and transmission time is relatively less critical.	UDP is suitable for applications that need fast, efficient transmission, such as game UDP's stateless nature is also useful for servers that answer small queries from huge numbers of clients.
Use by other protocols	HTTP, HTTPS, FTP, SMTP, Telnet	DNS, DHCP, TFTP, SNMP, RIP, VOIP.
Ordering of data packets	TCP rearranges data packets in the order specified.	UDP has no inherent order as all packets are independent of each other. If ordering is required, it has to be managed by the application layer.
Speed of transfer	The speed for TCP is slower than UDP.	UDP is faster because error recovery is not attempted. It is a "best effort" protocol.
Reliability	There is absolute guarantee that the data transferred remains intact and arrives in the same order in which it was sent.	There is no guarantee that the messages or packets sent would reach at all.
Header Size	TCP header size is 20 bytes	UDP Header size is 8 bytes.
Common Header Fields	Source port, Destination port, Check Sum	Source port, Destination port, Check Sum
Streaming of data	Data is read as a byte stream, no distinguishing indications are transmitted to signal message (segment) boundaries.	Packets are sent individually and are checked for integrity only if they arrive. Packets have definite boundaries which are honored upon receipt, meaning a read operation at the receiver socket will yield an entire message as it was originally sent.
Weight	TCP is heavy-weight. TCP requires three packets to set up a socket connection, before any user data can be sent. TCP handles reliability and congestion control.	UDP is lightweight. There is no ordering of messages, no tracking connections, etc. It is a small transport layer designed on top of IP.
Data Flow Control	TCP does Flow Control. TCP requires three packets to set up a socket connection, before any user data can	UDP does not have an option for flow control

	be sent. TCP handles reliability and congestion control.	
Error Checking	TCP does error checking and error recovery. Erroneous packets are retransmitted from the source to the destination.	UDP does error checking but simply discards erroneous packets. Error recovery is not attempted.
Fields	1. Sequence Number, 2. Ack number, 3. Data offset, 4. Reserved, 5. Control bit, 6. Window, 7. Urgent Pointer 8. Options, 9. Padding, 10. Check Sum, 11. Source port, 12. Destination port	1. Length, 2. Source port, 3. Destination port, 4. Check Sum
Acknowledgement	Acknowledgement segments	No Acknowledgment
Handshake	SYN, SYN-ACK, ACK	No handshake (connectionless protocol)

1.3 Describe the impact of infrastructure components in an enterprise network

- 1.3.a Firewalls
- 1.3.b Access points
- 1.3.c Wireless controllers

APs can be categorized as either **autonomous APs** or **controller-based APs**.

Autonomous APs

Autonomous APs, sometimes referred to as heavy APs, are standalone devices configured using the Cisco CLI or a GUI. Autonomous APs are useful in situations where only a couple of APs are required in the network. Optionally, multiple APs can be controlled using wireless domain services (WDS) and managed using CiscoWorks Wireless LAN Solution Engine (WLSE).

Note: A home router is an example of an autonomous AP because the entire AP configuration resides on the device.

Figure 1 displays an autonomous AP in a small network. If the wireless demands increase, more APs would be required. Each AP would operate independent of other APs and require manual configuration and management.

Controller-Based APs

Controller-based APs are server-dependent devices that require no initial configuration. Cisco offers two controller-based solutions. Controller-based APs are useful in situations where many APs are required in the network. As more APs are added, each AP is automatically configured and managed by a WLAN controller.

Figure 2 displays a controller-based AP in a small network. Notice how a WLAN controller is now required to manage the APs. The benefit of the controller is that it can be used to manage many APs.

Note: Some AP models can operate in either autonomous mode or in controller-based mode.

1.4 Describe the effects of cloud resources on enterprise network architecture

- 1.4.a Traffic path to internal and external cloud services
- 1.4.b Virtual services
- 1.4.c Basic virtual network infrastructure

4.11.1.1 – Cloud Overview

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

Cloud computing 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 personal training needs.
- Enables rapid responses to increasing data volume requirements.

4.11.1.2 – Cloud Services

Cloud services are available in a variety of options, tailored to meet customer requirements.

The three main Cloud computing services are:

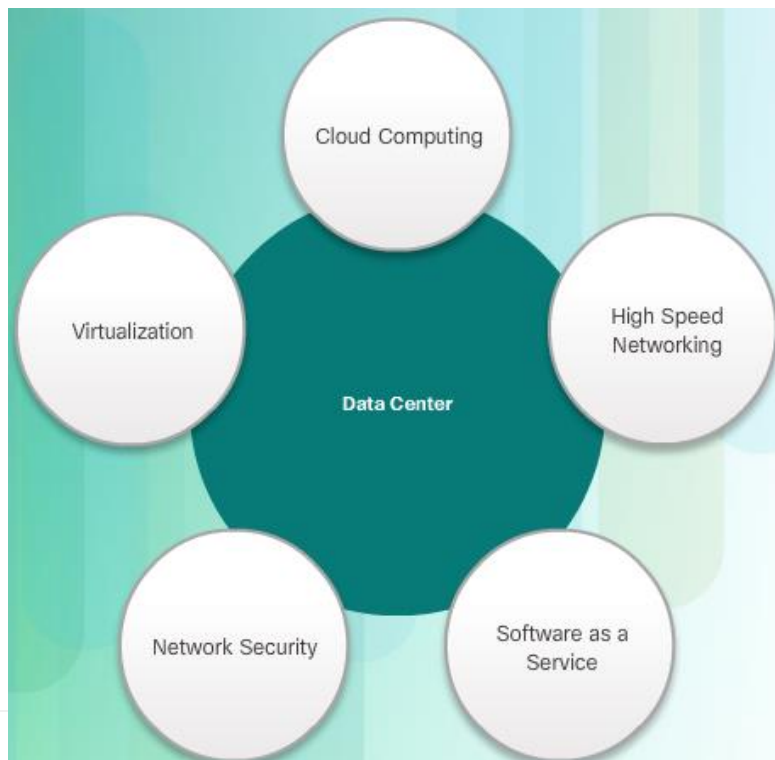
- **Software as a Service (SaaS)**: The Cloud provider is responsible for access to services such as email, communication and office 365 that are delivered over the internet. The user only needs to provide their data.
- **Platform as a Service (PaaS)**: The Cloud provider is responsible for access to the development tools and services used to deliver the applications.
- **Infrastructure as a Service (IaaS)**: The Cloud provider is responsible for access to the network equipment, virtualized network services and supporting network infrastructure.

4.11.1.3 – Cloud Models

- **Public clouds:** Cloud-based applications and services offered in a public cloud are **made available** to the **general population**. Services may be **free** or are offered on a **pay per use** model. Uses the internet to provide services.
- **Private clouds:** Cloud-based applications are services offered in a private cloud are intended for **specific organization** or **entity** such as the **government**. A private cloud can be set up using the organization's private network, through this can be **expensive** to build and maintain. Can also be managed by an outside organization with strict access security.
- **Hybrid clouds:** A hybrid cloud is made **up of two or more clouds** (example: part custom, part public), where each part remains a distinctive object, but both are connected using a single architecture. Individuals on a hybrid cloud would be able to have degrees of access to various services based on user access rights.
- **Custom clouds:** These are clouds built to meet the needs of a **specific industry**, such as **healthcare** or **media**. Custom clouds can be private or public.

4.11.1.4 – Cloud Computing versus Data Centre

- **Data centre:** Typically 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.



Term	Description
✓ Hybrid Cloud	Two or more clouds where each part remains a distinctive object, but both are connected using a single architecture
✓ PaaS	Access to the development tools and services used to deliver the applications
✓ Private Cloud	Applications and services are intended for a specific organization or entity, such as the government
✓ Custom Cloud	Clouds built to meet the needs of a specific industry, such as healthcare or media
✓ IaaS	Access to the network equipment, virtualized network services, and supporting network infrastructure.
✓ Public Cloud	Applications and services are made available to the general population
✓ Cloud	Large numbers of computers connected through a network that can be physically located anywhere
✓ SaaS	Access to services, such as email, communication, and Office 365 that are delivered over the Internet

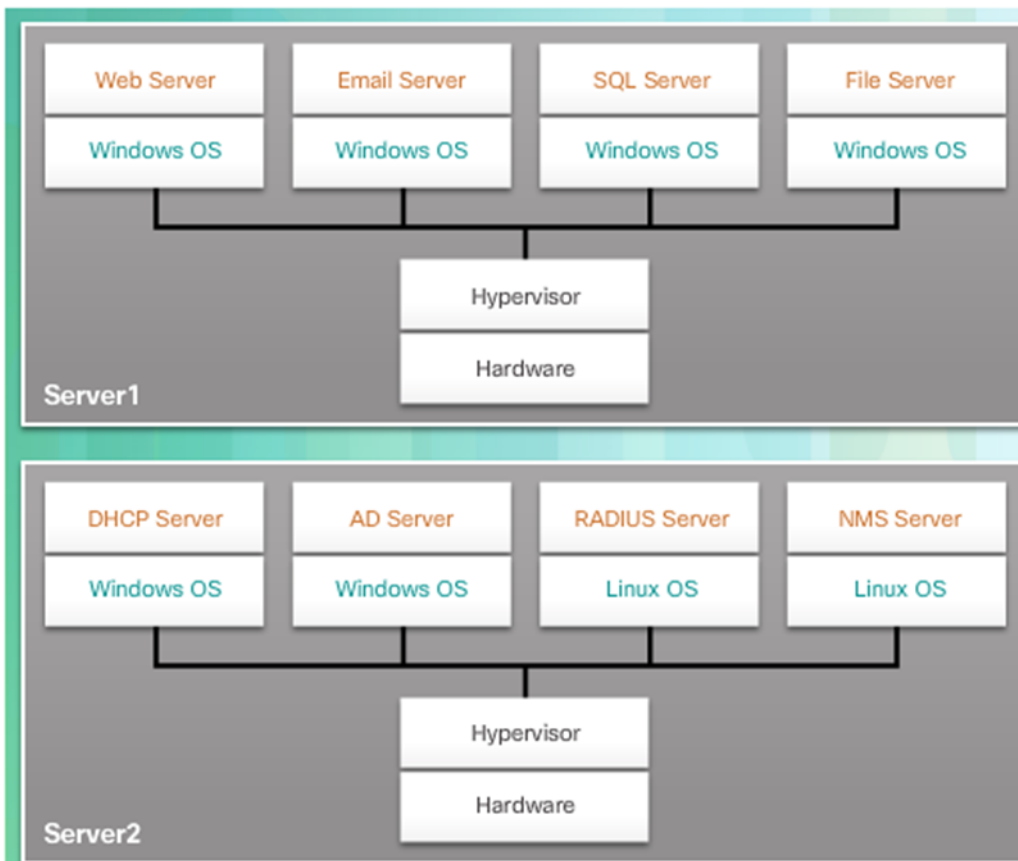
4.11.2.1 – Cloud Computing and Virtualization

Virtualization is the **foundation** of **Cloud computing**.

- **Cloud computing** separates the **application from the hardware**.
- **Virtualization** separates the **OS from the hardware**. Various providers offer Cloud services that can dynamically provision servers as required.

4.11.2.2 – Dedicated Servers

The major problem with this configuration is that when a component fails, the service that is provided by this server becomes unavailable. This is known as a **single point of failure**. Another problem was that dedicated servers were **underused**. Dedicated servers often sat idle for long periods of time waiting until there was a need to deliver the specific service they provide. These servers **wasted energy** and took up more space than was warranted by their amount of service. This is known as server sprawl.

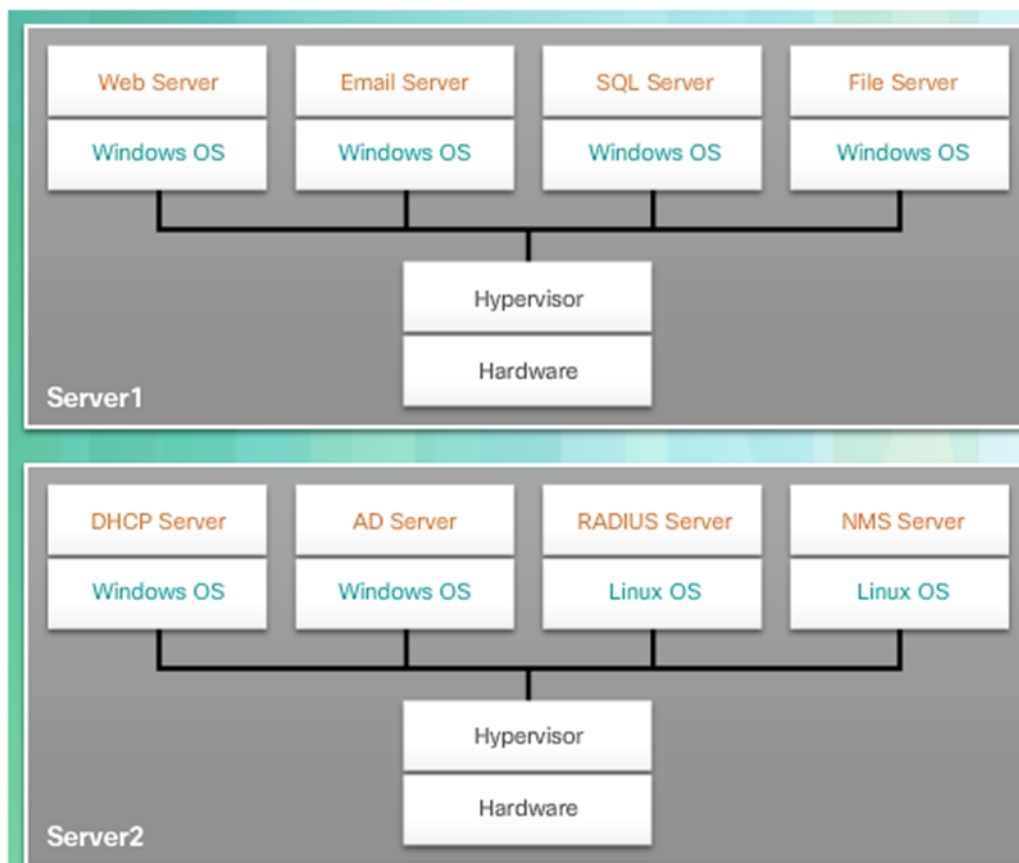


4.11.2.3 – Server Virtualization

Server virtualization takes advantage of **idle resources** and consolidates the number of required servers. This allows for **multiple operating systems** to exist on a **single hardware** platform.

The **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. Each of these virtual machines runs a complete and separate operating system. With virtualization enterprises can now consolidate the number of servers. For example it is not uncommon for 100 physical servers to be consolidated as virtual machines on top of 10 physical servers using hypervisors.

The use of virtualization normally includes **redundancy** to protect from a single point of failure. Redundancy can be implemented in different ways, if the hypervisors fails, the VM can be restarted on another hypervisor. Also the same VM can be run on two hypervisors concurrently, copying RAM and CPU instructions between them. If one hypervisor fails, the VM continues running on the other hypervisor. The services running on the VMs are also virtual and can be dynamically installed or uninstalled as needed.



4.11.2.4 – Advantages of Virtualization

Major advantages

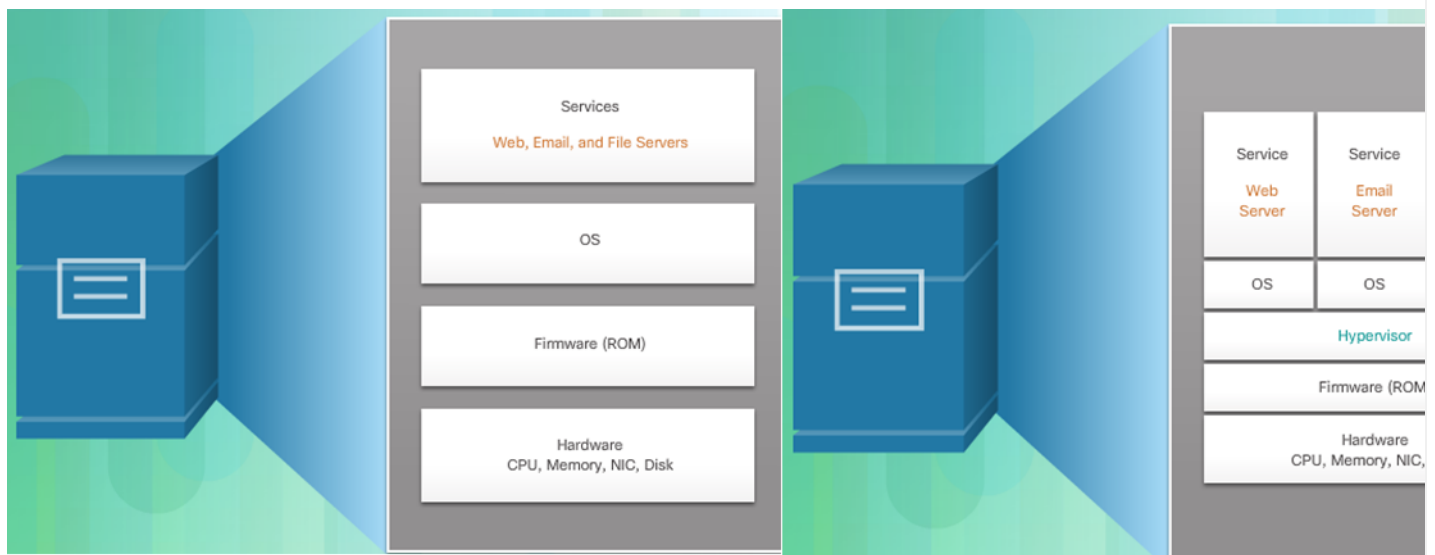
- Reduced cost
- Less equipment is required
- Less energy is consumed
- Less space is required

Other advantages

- Easier prototyping
- Faster server provisioning
- Increased server uptime
- Improved disaster recovery
- Legacy support

4.11.2.5 – Abstraction Layers

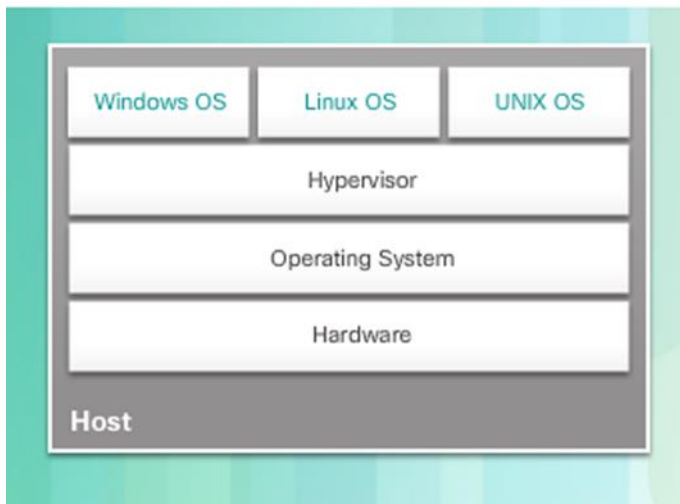
- Services
- OS
- Firmware
- Hardware



4.11.2.6 – Type 2 Hypervisors

A hypervisor is software that creates and runs VM instances. The computer on which hypervisor is supposing one or more VMs is a host machine. Type 2 hypervisors are also called **hosted hypervisors**. This is because the hypervisor is installed on the existing OS, such as MAC OS X, Windows or Linux. Then one or more additional OS instances are installed on the hypervisor.

Figure 1: Type 2 Hypervisor - "Hosted" Approach

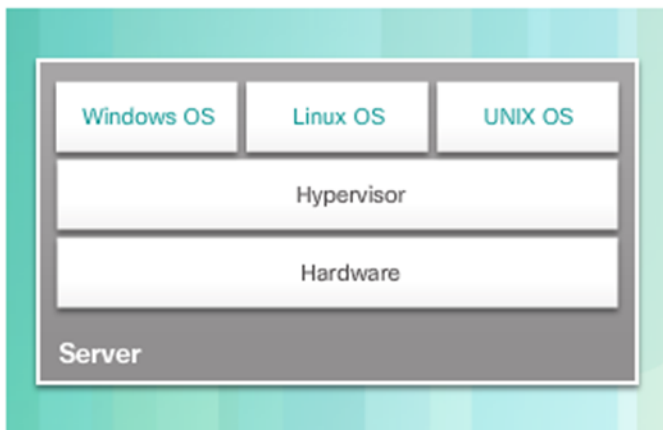


Term	Description
✓ Redundancy	Protection from a single point of failure.
✓ Dedicated Server	When all of a server's RAM, processing power, and hard drive space are devoted to the service provided.
✓ Host Machine	The computer on which a hypervisor is supporting one or more VMs.
✓ Cloud Computing	Separates the application from the hardware.
✓ Hypervisor	A program, firmware, or hardware that adds an abstraction layer on top of the real physical hardware.
✓ Server Virtualization	Takes advantage of idle resources and consolidates the number of required servers.
✓ Virtualization	Separates the OS from the hardware.
✓ Layers of Abstraction	Services, OS, Firmware, and Hardware.

4.11.3.1 – Type 1 Hypervisor

Type 1 hypervisors are also called the “**bare metal**” approach because the hypervisor is installed direct on the hardware. Type 1 hypervisors are usually used on enterprise servers and data centre networking devices.

Figure 1: Type 1 Hypervisor - "Bare Metal" Approach



- Traffic being exchanged **between virtual servers** in a data centre – **East-West traffic**.

1.5 Compare and contrast collapsed core and three-tier architectures

1.6 Compare and contrast network topologies

- 1.6.a Star
- 1.6.b Mesh
- 1.6.c Hybrid

1.7 Select the appropriate cabling type based on implementation requirements

1.8 Apply troubleshooting methodologies to resolve problems

- 1.8.a Perform and document fault isolation

Step	Title	Description
1	Identify the Problem	While tools can be useful, a conversation with the user is often very helpful.
2	Establish a Theory of Probable Causes	This step often yields more than a few probable causes to the problem.
3	Test the Theory to Determine Cause	A technician will often apply a quick procedure to test and see if it solves the problem.
4	Establish a Plan of Action to Resolve the problem and implement the solution	Establish a plan of action to resolve the problem and implement the solution.
5	Verify full system functionality and implement preventive measures	Verify full functionality, implement preventive measures.
6	Document findings, actions and outcomes	Document for future references.

- 1.8.b Resolve or escalate

In some situations, it may not be possible to resolve the problem immediately. A problem should be escalated when it requires a manager's decision, some specific expertise, or network access level unavailable to the troubleshooting technician.

- 1.8.c Verify and monitor resolution

Verification tools include the **ping**, **trace route** and **show** commands.

1.9 Configure, verify, and troubleshoot IPv4 addressing and subnetting

1.10 Compare and contrast IPv4 address types

1.10.a Unicast

Unicast - The process of sending a packet from one host to an individual host.

1.10.b Broadcast

Broadcast - The process of sending a packet from one host to all hosts in the network.

1.10.c Multicast

Multicast - The process of sending a packet from one host to a selected group of hosts, possibly in different networks.

1.11 Describe the need for private IPv4 addressing

1.12 Identify the appropriate IPv6 addressing scheme to satisfy addressing requirements in a LAN/WAN environment

1.13 Configure, verify, and troubleshoot IPv6 addressing

1.14 Configure and verify IPv6 Stateless Address Auto Configuration

1.15 Compare and contrast IPv6 address types

- **1.15.a Global unicast**

A global unicast address is similar to a public IPv4 address. These are globally unique, Internet routable addresses. Global unicast addresses can be configured statically or assigned dynamically.

- **1.15.b Unique local**

Unique local addresses are used for local addressing within a site or between a limited number of sites. These addresses should not be routable in the global IPv6 and should not be translated to a global IPv6 address. Unique local addresses are in the range of FC00::/7 to FDFF::/7.

With IPv4, private addresses are combined with NAT/PAT to provide a many-to-one translation of private-to-public addresses. This is done because of the limited availability of IPv4 address space. Many sites also use the private nature of RFC 1918 addresses to help secure or hide their network from potential security risks. However, this was never the intended use of these technologies, and the IETF has always recommended that sites take the proper security precautions on their Internet-facing router. Unique local addresses can be used for devices that will never need or have access from another network.

- **1.15.c Link local**

Link-local addresses are used to communicate with other devices on the same local link. With IPv6, the term link refers to a subnet. Link-local addresses are confined to a single link. Their uniqueness must only be confirmed on that link because they are not routable beyond the link. In other words, routers will not forward packets with a link-local source or destination address.

- **1.15.d Multicast**

IPv6 multicast addresses are similar to IPv4 multicast addresses. Recall that a multicast address is used to send a single packet to one or more destinations (multicast group). IPv6 multicast addresses have the prefix FF00::/8.

Note: Multicast addresses can only be destination addresses and not source addresses.

There are two types of IPv6 multicast addresses:

- Assigned multicast
- Solicited node multicast

Assigned Multicast

Assigned multicast addresses are reserved multicast addresses for predefined groups of devices. An assigned multicast address is a single address used to reach a group of devices running a common protocol or service. Assigned multicast addresses are used in context with specific protocols such as DHCPv6.

Two common IPv6 assigned multicast groups include:

- **FF02::1 All-nodes multicast group** – This is a multicast group that all IPv6-enabled devices join. A packet sent to this group is received and processed by all IPv6 interfaces on the link or network. This has the same effect as a broadcast address in IPv4. The figure shows an example of communication using the all-nodes multicast address. An IPv6 router sends Internet Control Message Protocol version 6 (ICMPv6) RA messages to the all-node multicast group. The RA message informs all IPv6-enabled devices on the network about addressing information, such as the prefix, prefix length, and default gateway.
- **FF02::2 All-routers multicast group** – This is a multicast group that all IPv6 routers join. A router becomes a member of this group when it is enabled as an IPv6 router with the **ipv6 unicast-routing** global configuration command. A packet sent to this group is received and processed by all IPv6 routers on the link or network.

- 1.15.e Modified EUI 64
- 1.15.f Autoconfiguration
- **1.15. Anycast**

An IPv6 anycast address is any IPv6 unicast address that can be assigned to multiple devices. A packet sent to an anycast address is routed to the nearest device having that address

2.1 Describe and verify switching concepts

- 2.1.a MAC learning and aging
- 2.1.b Frame switching
- 2.1.c Frame flooding
- 2.1.d MAC address table

Switches use **MAC addresses** to **direct network communications** through the switch to the appropriate port toward the destination. A switch is made up of integrated circuits and the accompanying software that controls the data paths through the switch. For a switch to know which port to use to transmit a frame, it must first learn which devices exist on each port. As the switch learns the relationship of ports to devices, it **builds a table** called a **MAC address**, or content addressable memory (CAM) table. CAM is a special type of memory used in high-speed searching applications.

LAN switches determine how to handle incoming data frames by maintaining the MAC address table. A switch builds its MAC address table by recording the MAC address of each device connected to each of its ports. The switch uses the information in the MAC address table to send frames destined for a specific device out the port which has been assigned to that device.

A switch populates the MAC address table based on **source MAC** addresses. When a switch receives an incoming frame with a destination MAC address that is not found in the MAC address table, the switch **forwards the frame** out of **all ports** (flooding) **except** for the **ingress port** of the frame. When the destination device responds, the switch adds the source MAC address of the frame and the port where the frame was received to the MAC address table. In networks with multiple interconnected switches, the MAC address table contains multiple MAC addresses for a single port connected to the other switches.

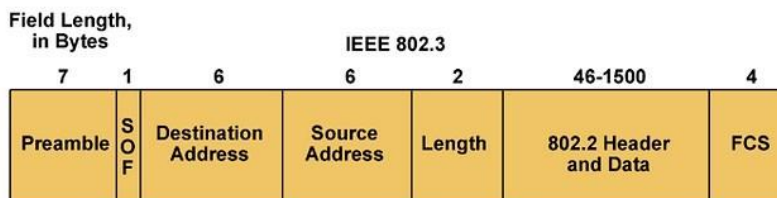
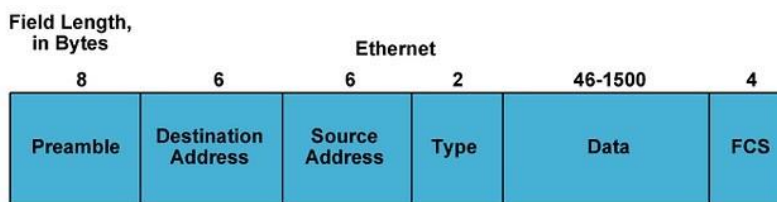
The following steps describe the process of building the MAC address table:

1. The switch receives a frame from PC 1 on Port 1 (Figure 1).
2. The switch examines the source MAC address and compares it to MAC address table.
 - If the address is not in the MAC address table, it associates the source MAC address of PC 1 with the ingress port (Port 1) in the MAC address table (Figure 2).
 - If the MAC address table already has an entry for that source address, it resets the aging timer. An entry for a MAC address is typically kept for five minutes.
3. After the switch has recorded the source address information, the switch examines the destination MAC address.
 - If the destination address is not in the MAC table or if it's a broadcast MAC address, as indicated by all Fs, the switch floods the frame to all ports, except the ingress port (Figure 3).
4. The destination device (PC 3) replies to the frame with a unicast frame addressed to PC 1 (Figure 4).

5. The switch enters the source MAC address of PC 3 and the port number of the ingress port into the address table. The destination address of the frame and its associated egress port is found in the MAC address table (Figure 5).

6. The switch can now forward frames between these source and destination devices without flooding, because it has entries in the address table that identify the associated ports (Figure 6).

2.2 Interpret Ethernet frame format



SOF = Start-of-Frame Delimiter
FCS = Frame Check Sequence

learnCisco

2.3 Troubleshoot interface and cable issues (collisions, errors, duplex, speed)

2.4 Configure, verify, and troubleshoot VLANs (normal/extended range) spanning multiple switches

- 2.4.a Access ports (data and voice)
- 2.4.b Default VLAN

2.5 Configure, verify, and troubleshoot interswitch connectivity

- 2.5.a Trunk ports
- 2.5.b Add and remove VLANs on a trunk
- 2.5.c DTP, VTP (v1&v2), and 802.1Q
- 2.5.d Native VLAN

2.6 Configure, verify, and troubleshoot STP protocols

- 2.6.a STP mode (PVST+ and RPVST+)

Protocol	Standard	Resources Needed	Convergence	Tree Calculation
STP	802.1D	Low	Slow	All VLANs
PVST+	Cisco	High	Slow	Per VLAN
RSTP	802.1w	Medium	Fast	All VLANs
Rapid PVST+	Cisco	Very high	Fast	Per VLAN
MSTP	802.1s, Cisco	Medium or high	Fast	Per Instance

Configure and Verify the BID

Method 1

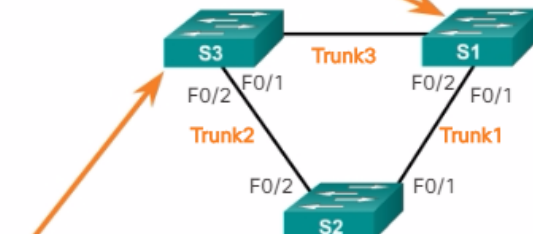
```
s1(config)# spanning-tree VLAN 1 root primary  
s1(config)# end
```

Method 2

```
s3(config)# spanning-tree VLAN 1 priority 24576  
s3(config)# end
```

Method 1

```
s2(config)# spanning-tree VLAN 1 root secondary  
s2(config)# end
```

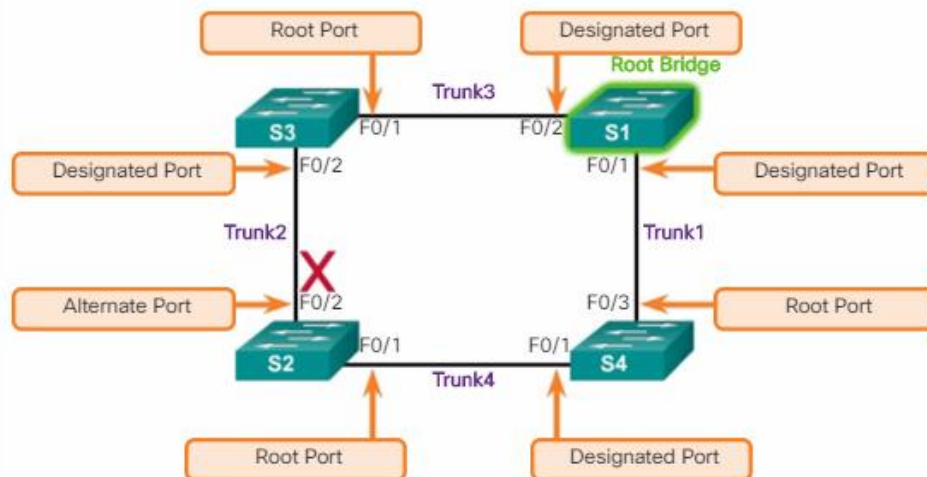


- 2.6.b STP root bridge selection

All switches in the **broadcast domain** participate in the **election process**. After a switch boots, it begins to send out **BPDU frames** every **two** seconds. These BPDUs contain the **switch BID** and the **root ID**.

As the switches forward their BPDU frames, adjacent switches in the broadcast domain read the root ID information from the BPDU frames. If the root ID from a BPDU received is lower than the root ID on the receiving switch, then the receiving switch updates its root ID, identifying the adjacent switch as the root bridge. However, it may not be an adjacent switch. It could be any other switch in the broadcast domain. The switch then forwards new BPDU frames with the lower root ID to the other adjacent switches. Eventually, the switch with the lowest BID ends up being identified as the root bridge for the spanning tree instance.

Link Speed	Cost (Revised IEEE Specification)	Cost (Previous IEEE Specification)
10 Gb/s	2	1
1 Gb/s	4	1
100 Mb/s	19	10
10 Mb/s	100	100



	Port State				
Operation Allowed	Blocking	Listening	Learning	Forwarding	Disabled
Can receive and process BPDUs	YES	YES	YES	YES	NO
Can forward data frames received on interface	NO	NO	NO	YES	NO
Can forward data frames switched from another interface	NO	NO	NO	YES	NO
Can learn MAC addresses	NO	NO	YES	YES	NO

2.7 Configure, verify and troubleshoot STP related optional features

- 2.7.a PortFast
- 2.7.b BPDU guard

PortFast is a **Cisco feature** for PVST+ environments. When a switch port is configured with PortFast that port transitions from **blocking** to **forwarding** state **immediately**, bypassing the usual 802.1D STP transition states (the **listening** and **learning** states). You can use PortFast on access ports to allow these devices to connect to the network immediately, rather than waiting for IEEE 802.1D STP to converge on each VLAN. Access ports are ports which are connected to a single workstation or to a server.

In a valid PortFast configuration, BPDUs should never be received, because that would indicate that another bridge or switch is connected to the port, potentially causing a spanning tree loop. Cisco switches support a feature called BPDU guard. When it is enabled, BPDU guard puts the port in an *error-disabled* state on receipt of a BPDU. This will effectively shut down the port. The BPDU guard feature provides a secure response to invalid configurations because you must manually put the interface back into service.

Cisco PortFast technology is useful for DHCP. Without PortFast, a PC can send a DHCP request before the port is in forwarding state, denying the host from getting a usable IP address and other information. Because PortFast immediately changes the state to forwarding, the PC always gets a usable IP address.

Note: Because the **purpose** of **PortFast** is to **minimize** the **time** that access ports must wait for spanning tree to converge, it should only be used on access ports. If you enable PortFast on a port connecting to another switch, you risk creating a spanning tree loop.

To configure PortFast on a switch port, enter the **spanning-tree portfast** interface configuration mode command on each interface that PortFast is to be enabled, as shown in Figure 2. The **spanning-tree portfast default** global configuration mode command enables PortFast on all nontrunking interfaces.

To configure BPDU guard on a Layer 2 access port, use the **spanning-tree bpduguard enable** interface configuration mode command. The **spanning-tree portfast bpduguard default** global configuration command enables BPDU guard on all PortFast-enabled ports.

2.8 Configure and verify Layer 2 protocols

- 2.8.a Cisco Discovery Protocol

2.2.1.1 – CDP Overview

Cisco Discovery Protocol is a Cisco **proprietary** Layer **2** protocol that is used to gather information about **Cisco** devices with share the same data link.

The device sends **periodic CDP advertisements** to connected devices. These advertisements share **information** about the **type of device** that is discovered, the **name** of the devices, and the number and type of the **interfaces**.

CDP can **assist** in network **design** decisions, **troubleshooting**, and making changes to equipment. CDP can also be used as a network discovery tool to determine the information about the **neighbouring** devices. This information gathered from CDP can help build a logical topology of a network when documentation is missing or lacking in detail.

2.2.1.2 – Configure and Verify CDP

For Cisco devices, CDP is enabled by default. For **security reasons** it may be desirable to **disable** CDP. With CDP an attacker can gather valuable insight about the network layout such as **IP addresses**, **IOS versions** and **types** of devices.

Verify CDP – **show cdp**

Enable CDP – **cdp run**

Disable CDP – **no cdp run**

Enable CDP on interface – **cdp enable**

Disable CDP on interface – **no cdp enable**

Verify CDP and display a list of neighbours (Exec mode) – **show cdp neighbors / show cdp neighbors detail**

Verify CDP on interface (Exec mode) – **show cdp interface**

```
R1# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTIA, M - Two-port Mac Relay

Device ID        Local Intrfce   Holdtme    Capability  Platform  Port ID
S1                Gig 0/1         122        S I        WS-C2960- Fas 0/5
```

The **show cdp neighbors** command provides the following information about each CDP neighbor device:

- **Device identifiers** - The host name of the neighbor device (S1)
- **Port identifier** - The name of the local and remote port (Gig 0/1 and Fas 0/5, respectively)
- **Capabilities list** - Whether the device is a router or a switch (S for switch; I for IGMP is beyond scope for this course)
- **Platform** - The hardware platform of the device (WS-C2960 for Cisco 2960 switch)

- 2.8.b LLDP

2.2.2.1 – LLDP Overview

Cisco devices also support **Link Layer Discovery Protocol (LLDP)** which is a vendor neutral neighbour discovery protocol similar to CDP.

2.2.2.2 – Configure and Verify LLDP

```
Switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# lldp run
```

```
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# lldp transmit
Switch(config-if)# lldp receive
```

```
Switch# show lldp

Global LLDP Information:

    Status: ACTIVE

    LLDP advertisements are sent every 30 seconds

    LLDP hold time advertised is 120 seconds

    LLDP interface reinitialisation delay is 2 seconds
```

2.2.2.3 – Discover Devices using LLDP

Show lldp neighbors

Show lldp neighbors detail

2.9 Configure, verify, and troubleshoot (Layer 2/Layer 3) EtherChannel

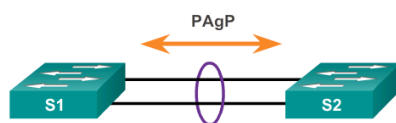
Note: Interface types cannot be mixed; for example, Fast Ethernet and Gigabit Ethernet cannot be mixed within a single EtherChannel.

- Maximum ports: 8 per side (or 16 in total)
- Maximum EtherChannels: *currently* 6 per Cisco IOS Switch
- Only between 2 devices
- Same individual member ports configuration:
 - trunk with same VLAN or access mode
 - configured as layer 2 port
- 2.9.a Static
- 2.9.b PAGP

Port Aggregation Protocol

PAGP modes:

- **On:** Channel member without negotiation (no protocol).
- **Desirable:** Actively asking if the other side can or will participate.
- **Auto:** Passively waiting for the other side.



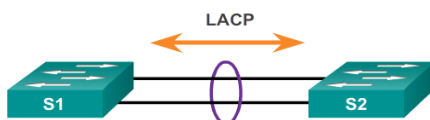
S1	S2	Channel Establishment
On	On	Yes
Auto/Desirable	Desirable	Yes
On/Auto/Desirable	Not Configured	No
On	Desirable	No
Auto/On	Auto	No

- 2.9.c LACP

Link Aggregation Control Protocol

LACP modes:

- **On:** Channel member without negotiation (no protocol).
- **Active:** Actively asking if the other side can or will participate.
- **Passive:** Passively waiting for the other side.



S1	S2	Channel Establishment
On	On	Yes
Active/Passive	Active	Yes
On/Active/Passive	Not Configured	No
On	Active	No
Passive/On	Passive	No

2.10 Describe the benefits of switch stacking and chassis aggregation

A **switch stack** can consist of up to **nine** Catalyst 3750 switches connected through their **StackWise ports**. **One** of the switches **controls** the operation of the stack and is called the **stack master**. The stack master and the other switches in the stack are stack members. **Layer 2 and Layer 3** protocols present the entire switch stack as a single entity to the network. Figure 1 shows the backplane of four Catalyst 3750 switches and how they are connected in a stack.

Every member is **uniquely identified** by its own **stack member number**. All members are eligible masters. If the master becomes **unavailable**, there is an **automatic process** to elect a **new master** from the remaining stack members. One of the factors is the stack member **priority value**. The switch with the **highest stack-member priority**-value becomes the **master**.

One of the primary benefits of switch stacks is that you manage the stack through a **single IP address**. The IP address is a system-level setting and is not specific to the master or to any other member. You can manage the stack through the same IP address even if you remove the master or any other member from the stack.

The master contains the **saved** and **running configuration** files for the stack. Therefore, there is only one configuration file to manage and maintain. The configuration files include the system-level settings for the stack and the interface-level settings for each member. Each member has a current copy of these files for backup purposes.

The switch is managed as a **single switch** including passwords, VLANs, and interfaces. Example 1 shows the interfaces on a switch stack with four 52-port switches. Notice the first number after the interface-type is the stack-member number.

Chassis aggregation is a **Cisco technology** to make two switches operate as a single logical switch. It is similar to stacking but meant for chassis switches like the 6500 and 6800 series switches. It is often used in the core layer and sometimes in the distribution layer.

3.0 Routing Technologies

23%

3.1 Describe the routing concepts

- 3.1.a Packet handling along the path through a network
- 3.1.b Forwarding decision based on route lookup
- 3.1.c Frame rewrite

3.2 Interpret the components of a routing table

- 3.2.a Prefix
- 3.2.b Network mask
- 3.2.c Next hop
- 3.2.d Routing protocol code
- 3.2.e Administrative distance
- 3.2.f Metric
- 3.2.g Gateway of last resort

3.3 Describe how a routing table is populated by different routing information sources

- 3.3.a Admin distance

Administrative Distance Route Source	Default Distance
Connected interface	0
Static route	1
Enhanced IGRP summary route	5
External BGP	20
Internal Enhanced IGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP external route	170
Internal BGP	200
Unknown	255

3.4 Configure, verify, and troubleshoot inter-VLAN routing

- 3.4.a Router on a stick
- 3.4.b SVI

3.5 Compare and contrast static routing and dynamic routing

Static vs. Dynamic Routing

There are two basic methods of building a routing table:

- Static Routing
- Dynamic Routing

A static routing table is created, maintained, and updated by a network administrator, manually. A static route to every network must be configured on every router for full connectivity. This provides a granular level of control over routing, but quickly becomes impractical on large networks.

Routers will not share static routes with each other, thus reducing CPU/RAM overhead and saving bandwidth. However, static routing is not fault-tolerant, as any change to the routing infrastructure (such as a link going down, or a new network added) requires manual intervention. Routers operating in a purely static environment cannot seamlessly choose a better route if a link becomes unavailable.

Static routes have an Administrative Distance (AD) of 1, and thus are always preferred over dynamic routes, unless the default AD is changed. A static route with an adjusted AD is called a floating static route, and is covered in greater detail in another guide.

A dynamic routing table is created, maintained, and updated by a routing protocol running on the router. Examples of routing protocols include RIP (Routing Information Protocol), EIGRP (Enhanced Interior Gateway Routing Protocol), and OSPF (Open Shortest Path First). Specific dynamic routing protocols are covered in great detail in other guides.

Routers do share dynamic routing information with each other, which increases CPU, RAM, and bandwidth usage. However, routing protocols are capable of dynamically choosing a different (or better) path when there is a change to the routing infrastructure.

Do not confuse routing protocols with routed protocols: • A routed protocol is a Layer 3 protocol that applies logical addresses to devices and routes data between networks (such as IP) • A routing protocol dynamically builds the network, topology, and next hop information in routing tables (such as RIP, EIGRP, etc.)

Static vs. Dynamic Routing (continued)

The following briefly outlines the **advantages** and **disadvantages** of **static routing**:

Advantages of Static Routing

- Minimal CPU/Memory overhead
- No bandwidth overhead (updates are not shared between routers)
- Granular control on how traffic is routed

Disadvantages of Static Routing

- Infrastructure changes must be manually adjusted
- No “dynamic” fault tolerance if a link goes down
- Impractical on large network

The following briefly outlines the advantages and disadvantages of dynamic routing:

Advantages of Dynamic Routing

- Simpler to configure on larger networks
- Will dynamically choose a different (or better) route if a link goes down
- Ability to load balance between multiple links

Disadvantages of Dynamic Routing

- Updates are shared between routers, thus consuming bandwidth
- Routing protocols put additional load on router CPU/RAM
- The choice of the “best route” is in the hands of the routing protocol, and not the network administrator

3.6 Compare and contrast distance vector and link state routing protocols

Dynamic Routing Categories

There are two distinct categories of dynamic routing protocols:

- Distance-vector protocols
- Link-state protocols

Examples of distance-vector protocols include RIP and IGRP. Examples of link-state protocols include OSPF and IS-IS.

EIGRP exhibits both distance-vector and link-state characteristics, and is considered a hybrid protocol.

Distance-vector Routing Protocols

All distance-vector routing protocols share several key characteristics:

- Periodic updates of the full routing table are sent to routing neighbors.
- Distance-vector protocols suffer from slow convergence, and are highly susceptible to loops.
- Some form of distance is used to calculate a route’s metric.
- The Bellman-Ford algorithm is used to determine the shortest path.

A distance-vector routing protocol begins by advertising directly-connected networks to its neighbors. These updates are sent regularly (RIP – every 30 seconds; IGRP – every 90 seconds).

Neighbors will add the routes from these updates to their own routing tables. Each neighbor trusts this information completely, and will forward their full routing table (connected and learned routes) to every other neighbor. Thus, routers fully (and blindly) rely on neighbors for route information, a concept known as routing by rumor.

There are several disadvantages to this behavior. Because routing information is propagated from neighbor to neighbor via periodic updates, distance-vector protocols suffer from slow convergence. This, in addition to blind faith of neighbor updates, results in distance-vector protocols being highly susceptible to routing loops.

Distance-vector protocols utilize some form of distance to calculate a route's metric. RIP uses hopcount as its distance metric, and IGRP uses a composite of bandwidth and delay.

Link-State Routing Protocols

Link-state routing protocols were developed to alleviate the convergence and loop issues of distance-vector protocols.

Link-state protocols maintain three separate tables:

- Neighbor table – contains a list of all neighbors, and the interface each neighbor is connected off of. Neighbors are formed by sending Hello packets.
- Topology table – otherwise known as the “link-state” table, contains a map of all links within an area, including each link's status.
- Shortest-Path table – contains the best routes to each particular destination (otherwise known as the “routing table”)

Link-state protocols do not “route by rumor.” Instead, routers send updates advertising the state of their links (a link is a directly-connected network). All routers know the state of all existing links within their area, and store this information in a topology table. All routers within an area have identical topology tables.

The best route to each link (network) is stored in the routing (or shortestpath) table. If the state of a link changes, such as a router interface failing, an advertisement containing only this link-state change will be sent to all routers within that area. Each router will adjust its topology table accordingly, and will calculate a new best route if required.

By maintaining a consistent topology table among all routers within an area, link-state protocols can converge very quickly and are immune to routing loops.

Additionally, because updates are sent only during a link-state change, and contain only the change (and not the full table), link-state protocols are less bandwidth intensive than distance-vector protocols. However, the three link-state tables utilize more RAM and CPU on the router itself.

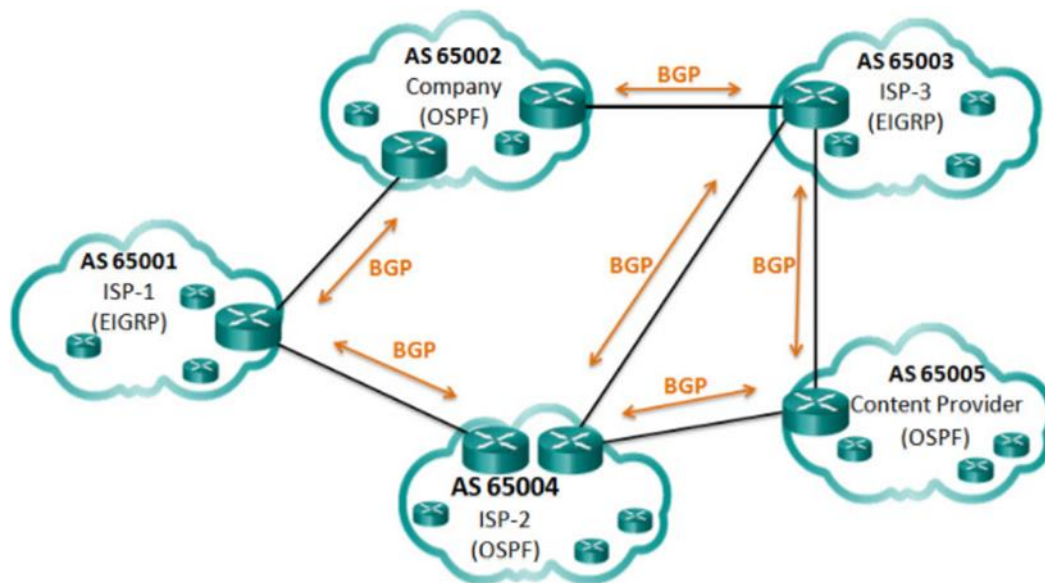
Link-state protocols utilize some form of cost, usually based on bandwidth, to calculate a route's metric. The Dijkstra formula is used to determine the shortest path.

3.7 Compare and contrast interior and exterior routing protocols

RIP, EIGRP and OSPF are **Interior Gateway Protocols (IGPs)** and their customers such as corporations usually use an IGP to route traffic **within their networks**. IGPs are used to exchange routing information within a company network or an autonomous system (AS).

Border Gateway Protocol (BGP) is an **Exterior Gateway Protocol (EGP)** used for the exchange or routing information **between autonomous systems** such as ISPs, companies and content providers.

In a BGP every AS is assigned a unique 16 bit or 32 bit AS number which **uniquely** identifies it on the internet.



Internal routing protocols use a **specific metric** such as OSPF's cost for determining the best paths.

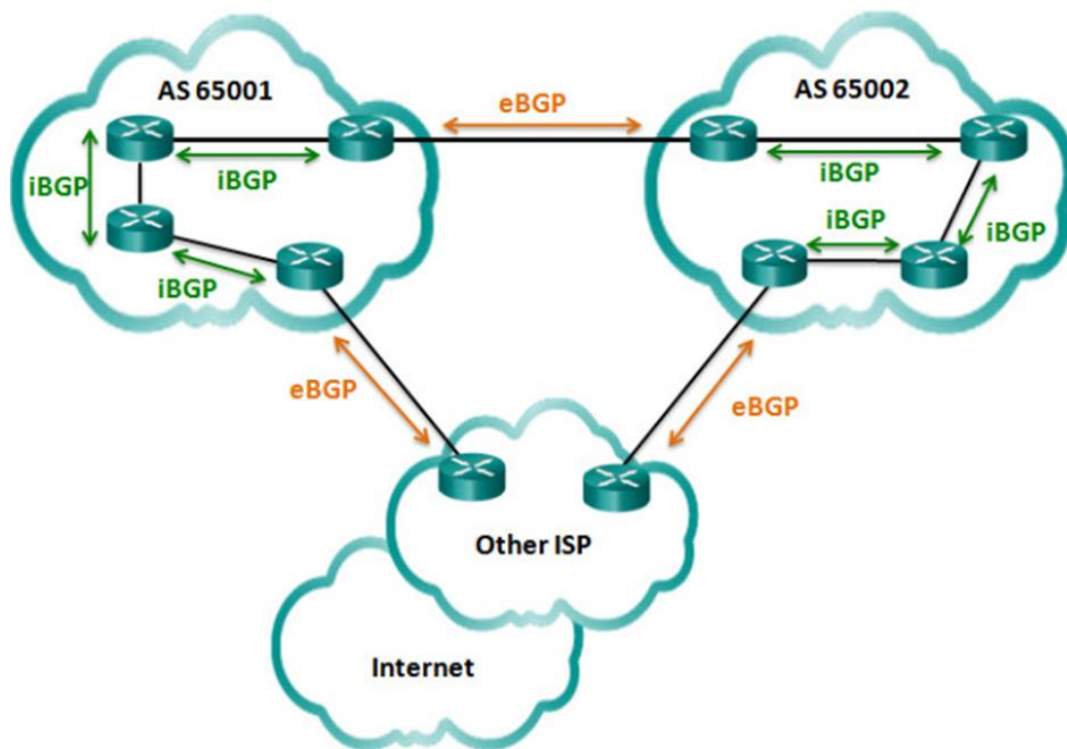
BGP does not use a single metric like IGPs.

IGP routing protocols are used to route traffic within the same organisation and administered by a single organization.

BGP is use to route between networks and administered by two different organizations.

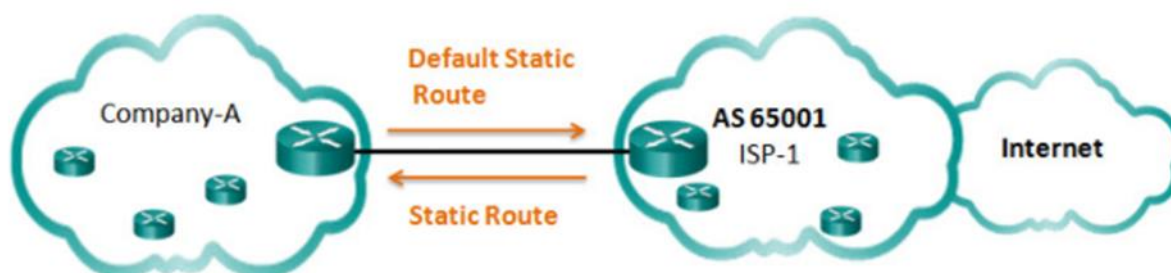
4.4.1.2 – eBGP and iBGP

- **External BGP (eBGP)** – Used between routers in **different** autonomous systems.
- **Internet BGP (iBGP)** – Used between routers in the **same** autonomous systems.



4.4.2.1 – When to use BGP

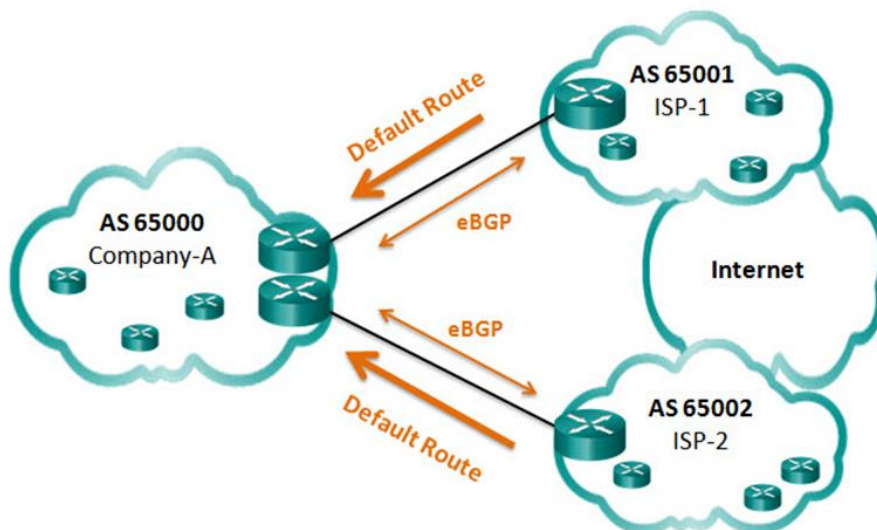
When an AS has connections to **multiple** AS systems, also known as **multi-homed**. Each AS has connections to at least **two** other autonomous systems or BGP peers.



4.4.2.3 – BGP Options

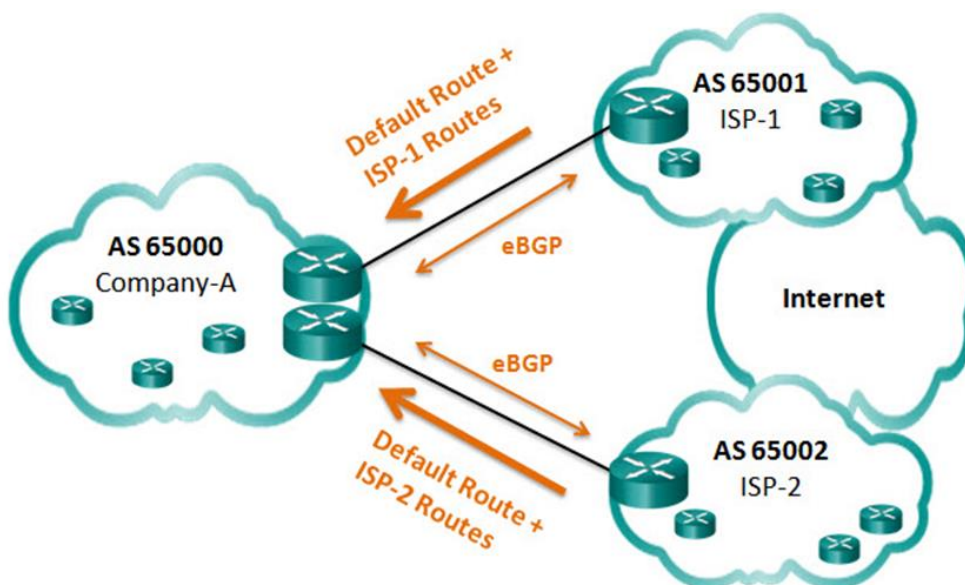
Default Route Only

ISPs advertise a default route to Company-A as shown in the picture below. The arrows indicate that the default is configured on the ISPs. This is the **simplest method** to implement BGP. Sub-optimal routing may occur.



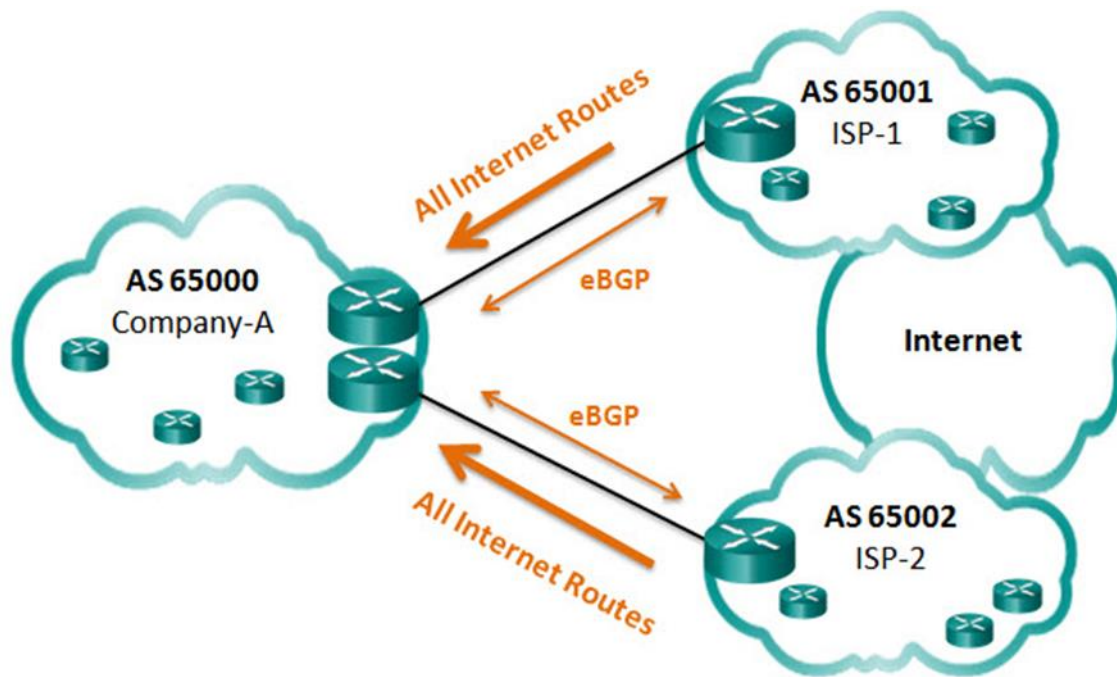
Default Route and ISP Routes

ISPs advertise their **default route** and their network to Company A. This option allows Company A to forward traffic to the appropriate ISP for networks advertised by that ISP. Company A would choose ISP-1 for networks advertised by ISP-1.



All Internet Routes

ISPs advertise all internet routes to Company A. Because Company A receives all internet routes from both ISPs, Company A can determine which ISP to use as the best path to forward traffic for any network. This solves sub optimal routing however Company A's BGP router must contain all internet routes which would currently include routes to over 550,000 networks.



3.8 Configure, verify, and troubleshoot IPv4 and IPv6 static routing

- 3.8.a Default route
- 3.8.b Network route
- 3.8.c Host route
- 3.8.d Floating static

3.9 Configure, verify, and troubleshoot single area and multi-area OSPFv2 for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub, virtual-link, and LSAs)

3.10 Configure, verify, and troubleshoot single area and multi-area OSPFv3 for IPv6 (excluding authentication, filtering, manual summarization, redistribution, stub, virtual-link, and LSAs)

3.11 Configure, verify, and troubleshoot EIGRP for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub)

3.12 Configure, verify, and troubleshoot EIGRP for IPv6 (excluding authentication, filtering, manual summarization, redistribution, stub)

3.13 Configure, verify, and troubleshoot RIPv2 for IPv4 (excluding authentication, filtering, manual summarization, redistribution)

3.14 Troubleshoot basic Layer 3 end-to-end connectivity issues

4.0 WAN Technologies

10%

Hide Details

- 4.1 Configure and verify PPP and MLPPP on WAN interfaces using local authentication
- 4.2 Configure, verify, and troubleshoot PPPoE client-side interfaces using local authentication
- 4.3 Configure, verify, and troubleshoot GRE tunnel connectivity

4.4 Describe WAN topology options

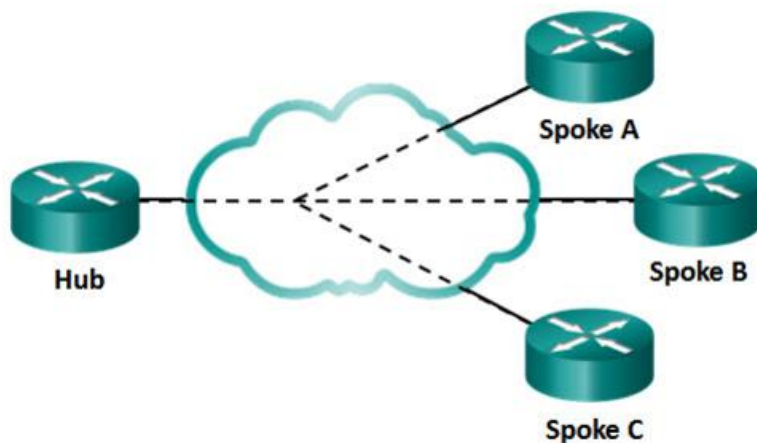
- 4.4.a Point-to-point

A Point to point topology employs a point to point circuit between two endpoints. Typically involving **dedicated leased-line connections** like T1/E1 lines. It Involves a **Layer 2 transport** service through the **ISP network**. A point to point connection is **transparent** to the customer network as if there was a **direct physical link**.



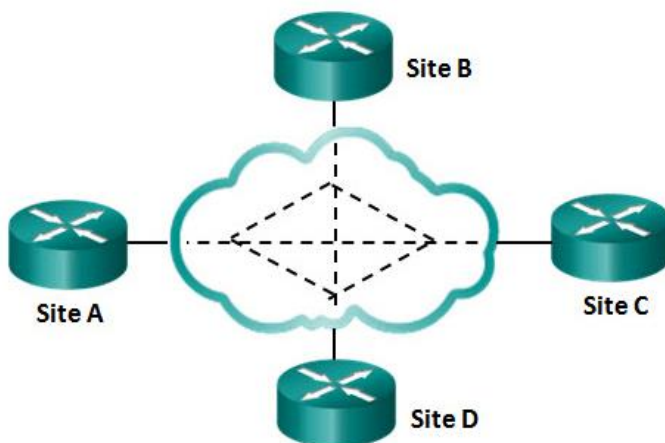
- 4.4.b Hub and spoke

If a private network connection between multiple sites is required, Hub and spoke is used. With a hub and spoke a **single interface** to the **hub** can be **shared** by **all spoke** circuits. This topology is also an example of a **single homed topology**.



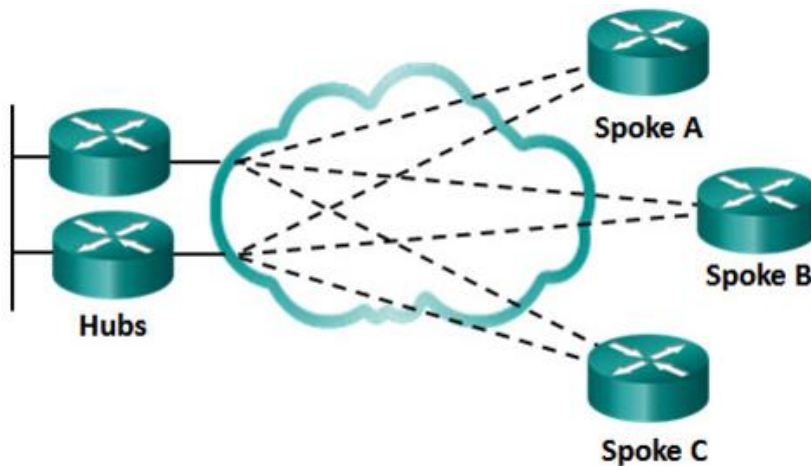
- 4.4.c Full mesh

Any site can communicate **directly** with any **other site**. The disadvantage here is the large number of virtual circuits that need to be configured and maintained.



- 4.4.d Single Homed vs
- Dual-homed

It provides **redundancy**. **More expensive** because there require more networking hardware like routers and switches. The advantage of a dual homed topology is that they offer enhanced network redundancy, load balancing, distributed computing or processing and the ability to implement backup service provider connections.



4.5 Describe WAN access connectivity options

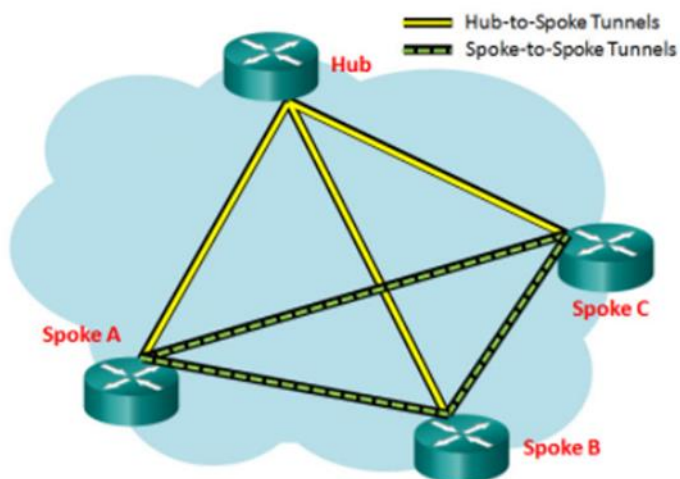
- 4.5.a MPLS
- 4.5.b Metro Ethernet
- 4.5.c Broadband PPPoE

- 4.5.d Internet VPN (DMVPN, site-to-site VPN, client VPN)

4.2.1.1 – DMVPN

Dynamic Multipoint VPN (DMVPN) is a **Cisco** software solution for building **multiple VPNs** in an easy, dynamic and scalable manner. The goal is to **simplify** the **configuration** while easily and flexibly connecting central office sites with branch sites. This is called hub and spoke.

With DMVPNs, branch sites can also communicate **directly** with other branch sites.



DMVPN is built using the following **technologies**:

- Next Hop Resolution Protocol (NHRP)
- Multipoint Generic Routing Encapsulation tunnels (mGRE)
- IP Security encryption (IPsec)

4.6 Configure and verify single-homed branch connectivity using eBGP IPv4 (limited to peering and route advertisement using Network command only)

4.4.3.1 – Steps to configure eBGP

Step 1: Enable BGP routing.

Step 2: Configure BGP neighbor(s) (peering).

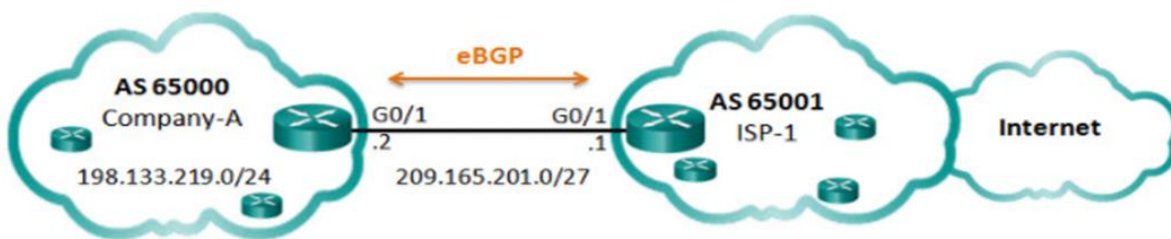
Step 3: Advertise network(s) originating from this AS.

4.4.3.2 – BGP Sample Configuration

Using eBGP,

Company A in AS 65000 will advertise its 198.133.219.0/24 network to ISP-1 as AS 65001.

ISP-1 will advertise a default route in its eBGP updates to Company A.



```
Company-A(config)# router bgp 65000
Company-A(config-router)# neighbor 209.165.201.1 remote-as 65001
Company-A(config-router)# network 198.133.219.0 mask 255.255.255.0
```

```
ISP-1(config)# router bgp 65001
ISP-1(config-router)# neighbor 209.165.201.2 remote-as 65000
ISP-1(config-router)# network 0.0.0.0
```

Router bgp – Enables BGP and identifies the AS number

Neighbour – Identifies the BGP peer and its AS number

Network – Enters the network address into the local BGP table.

Mask – Used when the network being advertised is different than its class-full equivalent.

4.4.3.3 – Verify eBGP

Show ip route – Verify routes advertised by the BGP neighbour are present in the IPv4 routing table.

```
Company-A# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
<output omitted>

Gateway of last resort is 209.165.201.1 to network 0.0.0.0

B* 0.0.0.0/0 [20/0] via 209.165.201.1, 00:36:03
    10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    198.133.219.0/24 is directly connected, GigabitEthernet0/0
L    198.133.219.1/32 is directly connected, GigabitEthernet0/0
    209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C    209.165.201.0/27 is directly connected, GigabitEthernet0/1
L    209.165.201.2/32 is directly connected, GigabitEthernet0/1
```

Show ip bgp – Verify that received and advertised IPv4 networks are in the BGP table.

```
Company-A# show ip bgp
BGP table version is 3, local router ID is 209.165.201.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
               x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

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

Show ip bgp summary – Verify IPv4 BGP neighbours and other BGP information

```
Company-A# show ip bgp summary
BGP router identifier 209.165.201.2, local AS number 65000
BGP table version is 3, main routing table version 3
2 network entries using 288 bytes of memory
2 path entries using 160 bytes of memory
2/2 BGP path/bestpath attribute entries using 320 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 792 total bytes of memory
BGP activity 2/0 prefixes, 2/0 paths, scan interval 60 secs

Neighbor      V    AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
209.165.201.1 4    65001    66     66      3    0    0 00:56:11      1
```

4.7 Describe basic QoS concepts

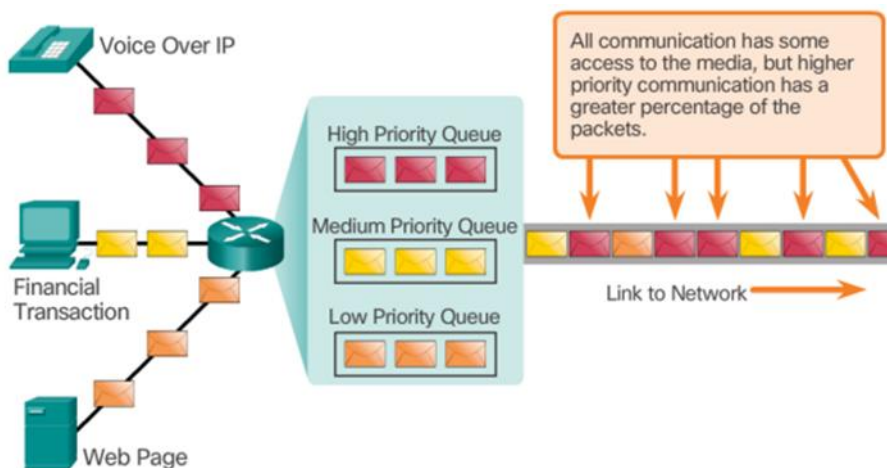
- 4.7.a Marking
- 4.7.b Device trust
- 4.7.c Prioritization
 - 4.7.c. [i] Voice
 - 4.7.c. [ii] Video
 - 4.7.c. [iii] Data
- 4.7.d Shaping
- 4.7.e Policing
- 4.7.f Congestion management

4.9.1.1 – Prioritizing Traffic

Quality of Service (QoS) is an ever increasing requirement of networks today. New applications available to users such as **voice** and **live video** transmission create higher expectations for the quality of the received services.

Congestion occurs when the **demand for bandwidth exceeds** the **amount available**. When simultaneous communications are attempted across the network, the demand for network bandwidth can exceed its availability, creating network congestion.

When the volume of traffic is greater than what can be transported across the network, devices **queue** or **hold** the packets in memory **until resources become available** to transmit them. Queuing packets causes delay because new packets cannot be transmitted until previous packets have been processed. If the number of packets to be queued continues to increase, the **memory queues** fill up and **packets are dropped**.

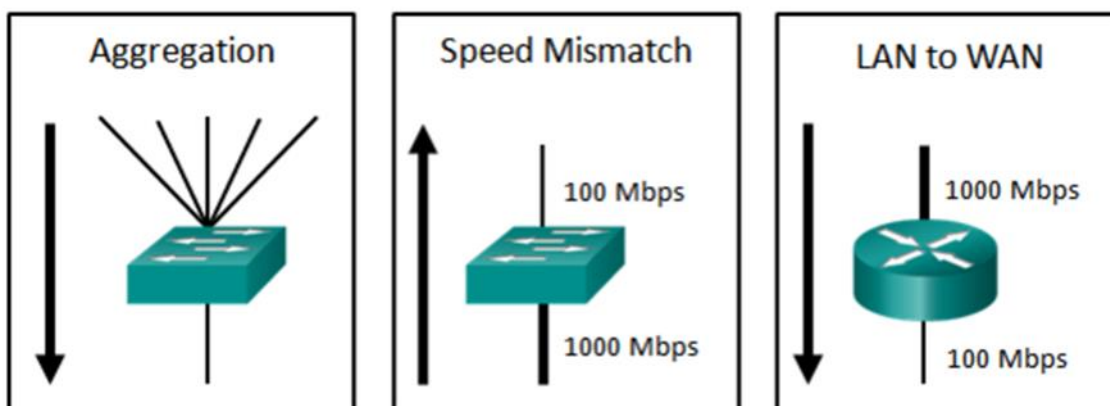


4.9.1.2 – Bandwidth, Congestion, Delay and Jitter

Network bandwidth is measured in the number of **bits** that can be transmitted in a **single second** or **bits per seconds (bps)**. Network administrators most often refer to the performance of network devices by describing the bandwidth or interfaces expresses.

Network congestion causes **delay**. Variations in delay cause **jitter**. An interface experiences congestion when it is presented with more traffic than it can handle.

Examples of Congestion Points



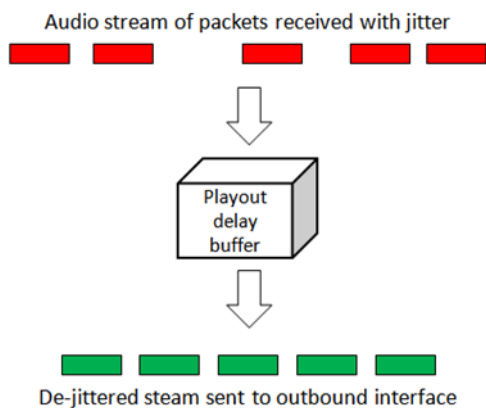
A device only implements QoS when it is experiencing some congestion.

Delay or **latency** refers to the **time** it takes for a **packet** to travel from the **source** to the **destination**. These are both fixed delays and variable delays.

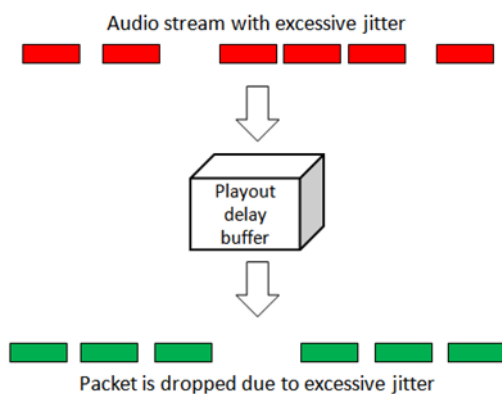
Delay	Description
Code delay	<ul style="list-style-type: none">The fixed amount of time it takes to compress data at the source before transmitting to the first interworking device, usually a switch.
Packetization delay	<ul style="list-style-type: none">The fixed time it takes to encapsulate a packet with all the necessary header information.
Queuing delay	<ul style="list-style-type: none">The variable amount of time a frame or packet waits to be transmitted on the link.
Serialization delay	<ul style="list-style-type: none">The fixed amount of time it takes to transmit a frame from the NIC to the wire.
Propagation delay	<ul style="list-style-type: none">The variable amount of time it takes for the frame to traverse the links between the source and destination.
De-jitter delay	<ul style="list-style-type: none">The fixed amount of time it takes to buffer a flow of packets and then send them out in evenly spaced intervals.

4.9.1.3 – Packet Loss

Without QoS mechanisms in place, packets are processed in the order which they are **received**. When **congestion occurs**, routers and switches begin to **drop packets**. This means that time-sensitive packets, such as real-time video and voice will be dropped with the same frequency as data that is not time-sensitive, such as email and web.




If the jitter is so large that it causes packets to be received out of the range of this buffer, the out of range packets are discarded and dropouts are heard in the audio.



4.9.2.2 – Voice

Voice traffic is **predictable** and **smooth**. It does **not consume** a lot of **network resources**, however it is very **sensitive** to **delays** and **dropped packets** and it cannot be re-transmitted if lost. Therefore it must receive a **higher priority**.



Voice

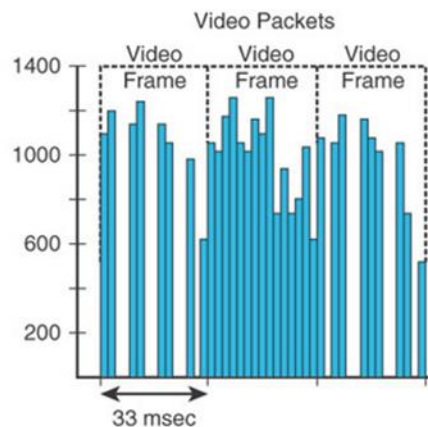
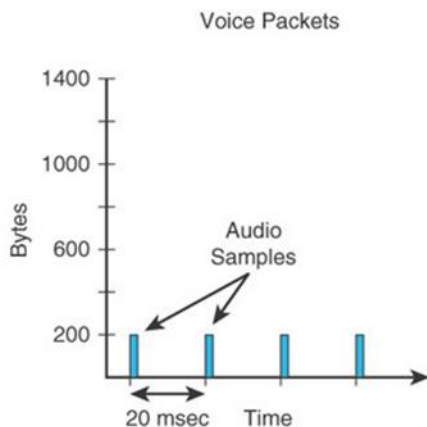
- Smooth
- Benign
- Drop sensitive
- Delay sensitive
- UDP priority


One-Way Requirements

- Latency ≤ 150 ms
- Jitter ≤ 30 ms
- Loss $\leq 1\%$
- Bandwidth (30–128Kbps)

4.9.2.3 – Video

Without QoS and a significant amount of extra bandwidth capacity, video quality typically **degrades**. Video traffic tends to be **unpredictable**, **inconsistent** and **bursty** compared to voice traffic.





Video

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

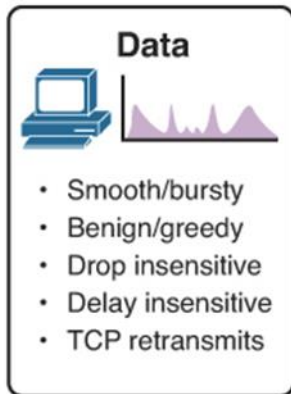
One-Way Requirements

- Latency ≤ 200 -400 ms
- Jitter ≤ 30 -50 ms
- Loss ≤ 0.1 -1%
- Bandwidth (384Kbps–20 + Mbps)

4.9.2.4 – Data

Most applications use either **TCP** or **UDP**. Unlike UDP, **TCP** performs **error recovery**. Data applications that have no tolerance for data loss such as email and web pages use TCP to ensure that if packets are lost in transit they will be resent.

However some TCP application can be very **greedy**, consuming a large portion of **network capacity**. FTP will consume as much bandwidth as it can get when you download a large file, such as a movie or game.



4.9.3.1 – Queuing Overview

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. A number of queuing algorithms are available such as:

- First-In, First-Out (FIFO)
- Weighted Fair Queuing (WFQ)
- Class-Based Weighted Fair Queuing (CBWFQ)
- Low Latency Queuing (LLQ)

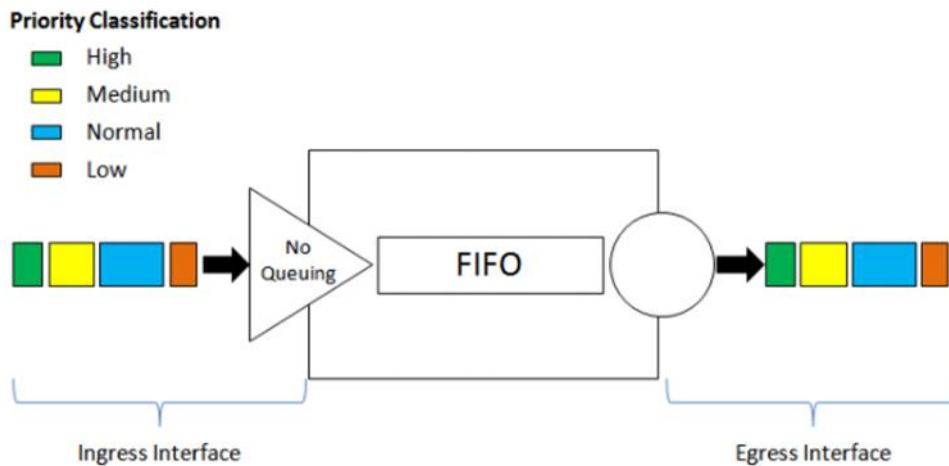
4.9.3.2 – First In First Out (FIFO)

Buffering and forwarding packets in the order of arrival.

FIFO has no concept of priority or classes of traffic and consequently makes no decision about packet priority. There is only one queue and all packets are treated equally.

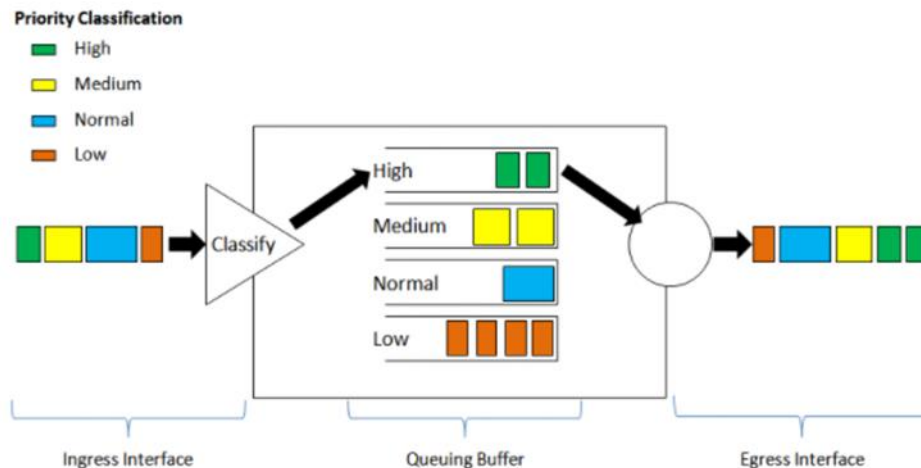
When no other queuing strategies are configured, all interfaces except serial interfaces at E1 (2.048Mbps) and below use FIFO by default.

Serial interfaces at E1 and below use WFQ by default.



4.9.3.3 – Weighted Fair Queuing (WFQ)

WFQ is an automated scheduling method that provides fair bandwidth allocation to all network traffic. WFQ applies priority or weights to identified traffic and classifies it into conversations or flows.



WFQ then determines how much bandwidth each flow is allowed relative to other flows. The flow-based algorithm used by WFQ simultaneously schedules interactive traffic to the front of a queue to reduce response time. It then fairly shares the remaining bandwidth among high bandwidth flows.

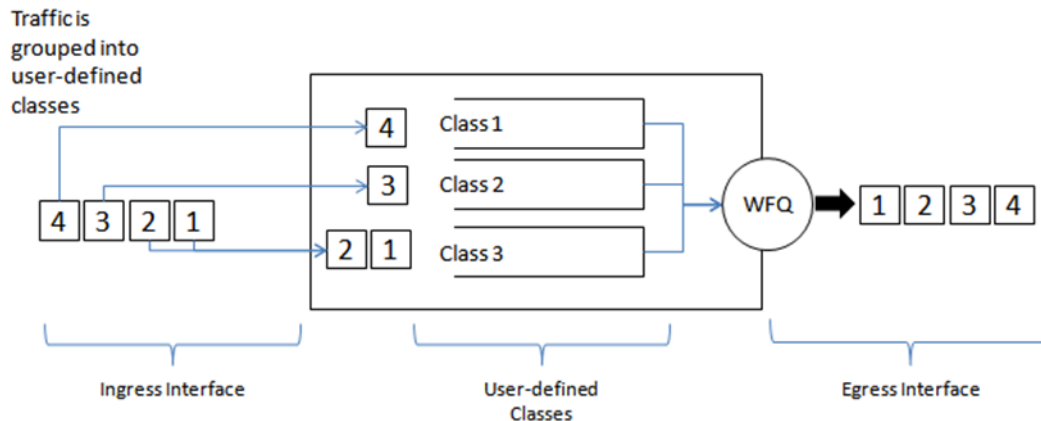
WFQ classifies traffic into different flows based on packet header addressing including such characteristics as **source** and **destination IP addresses**, **MAC addresses**, **port numbers**, **protocol**, **Type of Service**. The ToS value in the IP header can be used to **classify traffic**.

Limitations

- WFQ is **not supported** with **tunnelling** and **encryption** because these features modify the packet content information required by WFQ for classification.
- **Not as precise** as CBWFQ.

4.9.3.4 – Class Based Weighted Fair Queuing (CBWFQ)

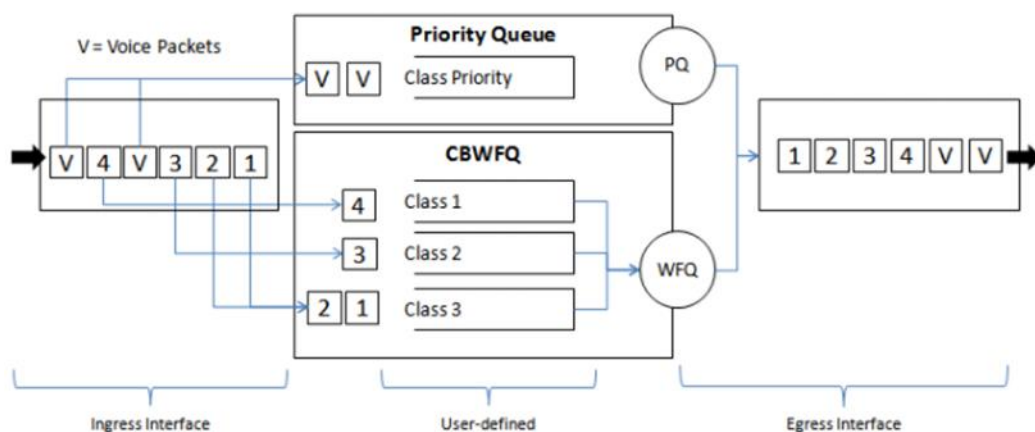
CBWFQ extends the standard WFQ **functionality** to provide support for user-defined traffic classes. For CBWFQ you define traffic classes based on **match criteria** including protocols, ACLs and input interfaces. Packets satisfying the match criteria for a class constitute the traffic to that class. A FIFO queue is reserved for each class and traffic belonging to a class is directed to the queue for that class.



After a queue has reached its configured **queue limit**, adding more packets to the class **causes tail drop** to take effect depending on how class policy is configured. Tail drop means a router simply **discards any packets** that arrive at the tail end of a queue that has completely use its packet holding resources. This is the default queuing response to congestion. Tail drop **treats** all traffic **equally**.

4.9.3.5 – Low Latency Queuing (LLQ)

LLQ brings strict priority queuing (PQ) to CBWFQ. Strict PQ allows delay-sensitive data such as **voice** to be sent **before packets in other queues**. LLQ provides strict priority queuing for CBWFQ, reducing jitter in voice conversations.



4.10.1.1 – Selecting an Appropriate QoS Policy Model

Model	Description
Best effort Model	Not really an implementation as QoS is not explicitly configured. Use when QoS is not required.
Integrated Services (IntServ)	Provides very high QoS to IP packets with guaranteed delivery. It defines a signalling process for application to signal to the network that that require special QoS for a period and that bandwidth should be reserved. However, IntServ can severely limit the scalability of a network .
Differentiated Services (DiffServ)	Provides high scalability and flexibility in implementing QoS. Network device recognise traffic classes and provide different levels of QoS to different traffic classes.

4.10.1.2 – Best Effort

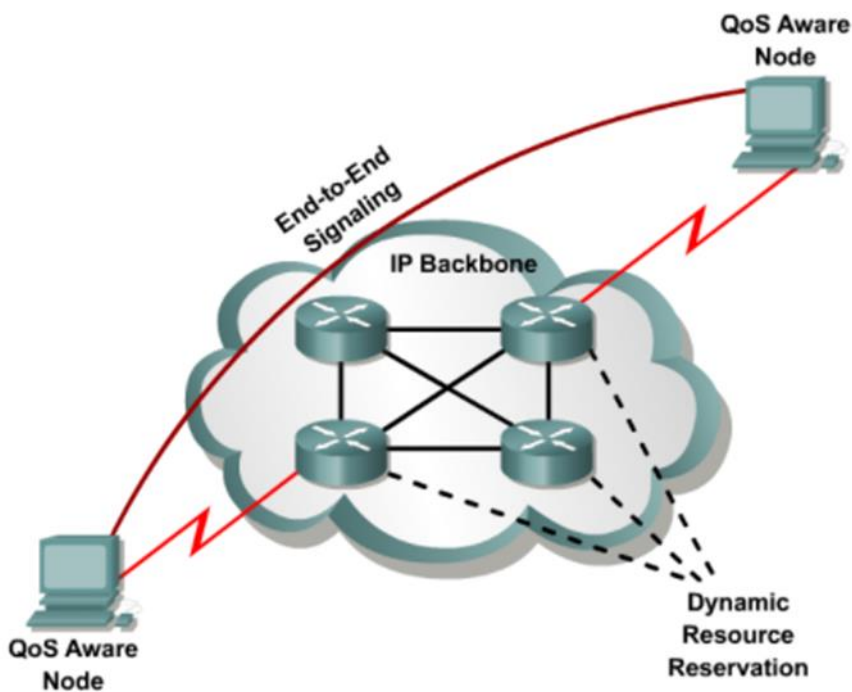
The best effort model **treats all network packets in the same way**. Without QoS, the network cannot tell the difference between packets and as a result cannot treat packets preferentially.

Benefits	Drawbacks
<ul style="list-style-type: none">• Most scalable.• Scalability is only limited by bandwidth limits.• No special QoS mechanisms are required.• The easiest and quickest model to deploy.	<ul style="list-style-type: none">• No Guarantees of delivery.• Packets will arrive whenever they can and in any order possible.• No packets have preferential treatment.• Critical data is treated the same as other data.

4.10.1.3 – Integrated Services

IntServ provides a way to deliver the **end to end QoS** that real time applications require by explicitly managing network resources to provide QoS to specific user packet streams called microflows. It uses resource reservation and admission control mechanisms as building blocks to establish and maintain QoS.

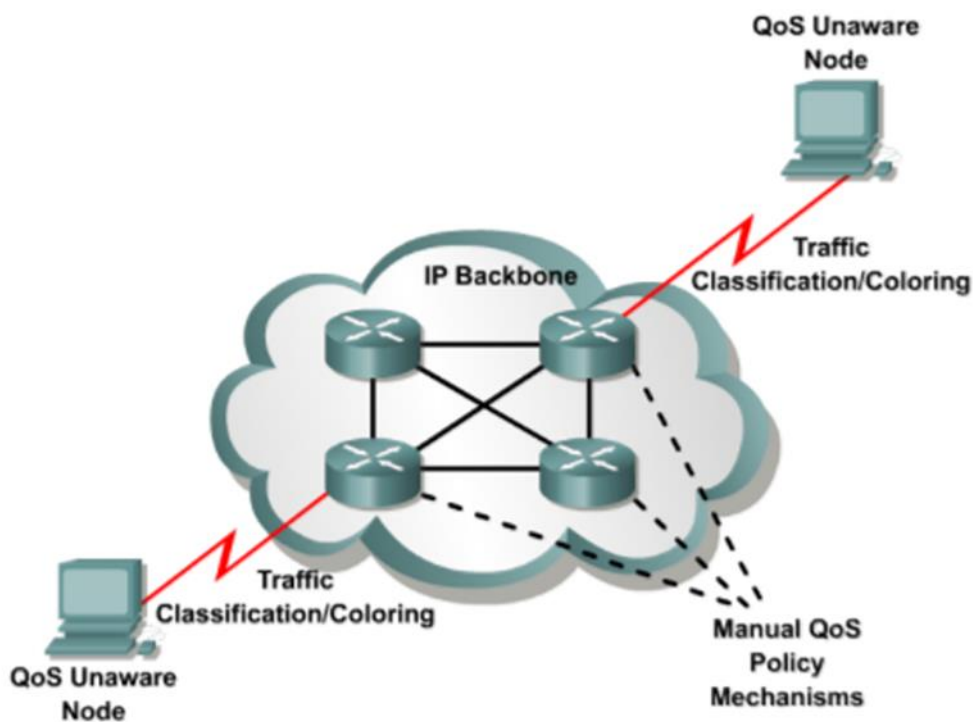
Benefits	Drawbacks
<ul style="list-style-type: none">• Explicit end to end resource admission control.• Per-request policy admission control.• Signalling of dynamic port numbers.	<ul style="list-style-type: none">• Resource intensive due to the stateful architecture requirement for continuous signalling.• Flow-based approach not scalable to large implementations such as the internet.



4.10.1.4 – Differentiated Services

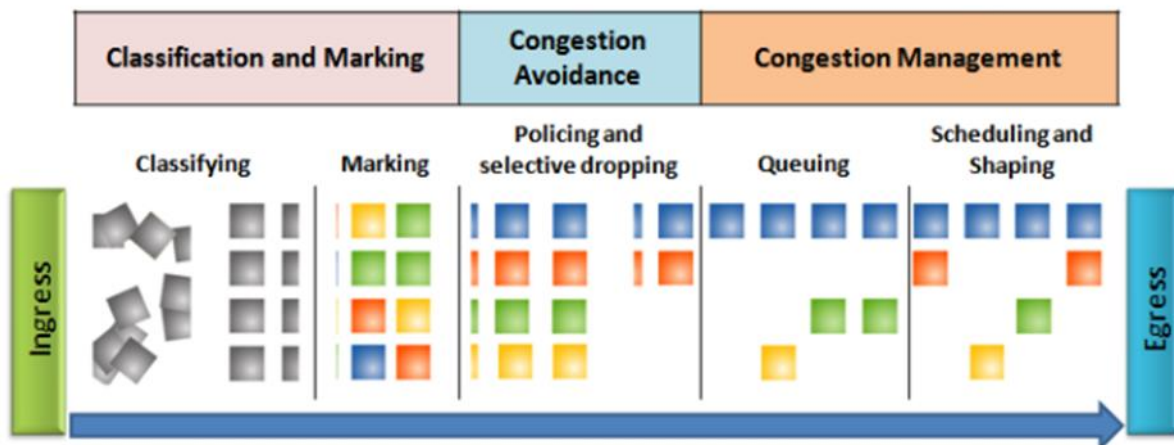
DiffServ QoS model specifies a **simple** and **scalable** mechanism for classifying and managing network traffic and providing QoS guarantees on modern IP networks. DiffServ can provide **low-latency guaranteed service** to critical network traffic such as voice or video while providing simple best effort traffic guarantees to non-critical services such as web traffic or file transfers.

Benefits	Drawbacks
<ul style="list-style-type: none">• Highly scalable.• Provides many different levels of quality.	<ul style="list-style-type: none">• No absolute guarantee of service quality.• Requires a set of complex mechanisms to work in covert throughout the network.



4.10.2.2 – QoS Tools

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



Ethernet Class of Service (CoS) Values

Value	Description
7	Reserved
6	Reserved
5	Voice bearer (voice traffic)
4	Videoconferencing
3	Call Signaling
2	High-Priority Data
1	Medium-Priority Data
0	Best-Effort Data

Ethernet Class of Service (CoS) Values

Value	Description
7	Network
6	Internet
5	Critical
4	Flash-override
3	Flash
2	Immediate
1	Priority
0	Routine

Term	Description
✓ Traffic Policing	When the traffic rate reaches the configured maximum rate, excess traffic is dropped.
✓ Congestion Avoidance	Queuing and scheduling methods where excess traffic is buffered while it waits to be sent on an egress interface.
✓ WRED algorithm	Provides buffer management and allows TCP traffic to throttle back before buffers are exhausted.
✓ Classification	Determines what class of traffic packets or frames belong to.
✓ Traffic Shaping	Retains excess packets in a queue and then schedules the excess for later transmission over increments of time.
✓ Marking	Adding a value to the packet header.
✓ ECN bits	Used to identify a Layer 2 QoS marking.
✓ 802.1Q	An IEEE specification for implementing VLANs in Layer 2 switched networks.

5.1 Describe DNS lookup operation

5.2 Troubleshoot client connectivity issues involving DNS

5.3 Configure and verify DHCP on a router (excluding static reservations)

- 5.3.a Server

```
R1(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.9
R1(config)# ip dhcp excluded-address 192.168.10.254
R1(config)# ip dhcp pool LAN-POOL-1
R1(dhcp-config)# network 192.168.10.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.10.1
R1(dhcp-config)# dns-server 192.168.11.5
R1(dhcp-config)# domain-name example.com
R1(dhcp-config)# end
R1#
```

- 5.3.b Relay

```
R1(config)# interface g0/0
R1(config-if)# ip helper-address 192.168.11.6
R1(config-if)# end
```

- 5.3.c Client

Configuring a Router as DHCP Client



```
SOHO(config)# interface g0/1
SOHO(config-if)# ip address dhcp
SOHO(config-if)# no shutdown
SOHO(config-if)#
*Jan 31 17:31:11.507: %DHCP-6-ADDRESS_ASSIGN: Interface
GigabitEthernet0/1 assigned DHCP address 209.165.201.12, mask
255.255.255.224, hostname SOHO
SOHO(config-if)# end
SOHO# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 209.165.201.12/27
  Broadcast address is 255.255.255.255
  Address determined by DHCP
<output omitted>
```


- 5.3.d TFTP, DNS, and gateway options

5.4 Troubleshoot client- and router-based DHCP connectivity issues

5.5 Configure, verify, and troubleshoot basic HSRP

- **5.5.a Priority**
- **5.5.b Preemption**
- **5.5.c Version**

3.4.1.1 – HSRP Overview

Hot Standby Router Protocol (HSRP) was designed by **Cisco** to allow for gateway redundancy without any additional configuration on end devices. Routers configured with HSRP work together to present themselves as a single virtual default gateway (router) to end devices.

One of the routers is selected by HSRP to be the **active** router. The **active** router will act as the **default gateway** for end devices.

The other router will become the **standby** router. If the active router **fails**, the **standby** router will **automatically** assume the role of the **active** router. It will assume the role of the default gateway for end devices. This does **not** require any configuration on the end devices.

Both the HSRP **active** router and the **standby** router present a single default gateway address to end devices. The default gateway address is a **virtual IP address** along with **virtual MAC address** that is **shared** amongst **both** HSRP routers.

End devices use this **virtual IP address** as their default gateway address.

3.4.1.2 – HSRP Versions

The default version for Cisco IOS 15 is version 1. HSRP version 2 provides the following enhancements:

- **HSRPv1** uses the multicast address of **224.0.0.2**. **HSRP version 2** uses that IPv4 multicast address **224.0.0.102** or the IPv6 multicast address **FF02::66** to send hello packets.
- **HSRPv2** expands the number of **supported groups**. HSRP version **1** supports group numbers from **0 to 255**. HSRP version **2** supports group numbers from **0 to 4095**.
- **HSRPv2** adds support for **MD5 authentication**.

3.4.1.3 – HSRP Priority and Preemption

The role of the active and standby routers is determined during HSRP election process. By default, the router with the numerically highest IP address is elected as the active router. However, it is always better to know how your network will operate under normal conditions rather than leaving it to chance.

HSRP Priority

HSRP priority can be used to **determine** the **active router**. The routers with the **highest** HSRP priority will become the **active** router. By **default**, the HSRP priority is **100**. If the priorities are **equal**, the router with the numerically **highest IP address** is elected as the **active** router.

Standby priority (0-255)

HSRP Preemption

By **default**, after a router becomes the **active** router, it will **remain** the active router even if another router comes online with a higher HSRP priority.

To **force** a new **HSRP election process**, Preemption must be enabled. With **Preemption** enabled, a router that comes online with a higher HSRP priority will assume the role of the **active** router.

Standby preempt

3.4.1.4 – HSRP States

When an **interface** is configured with HSRP or is first activated with an existing HSRP configuration, the router **sends and receives HSRP hello packets** to begin the process of determining which state it will assume in the HSRP group.

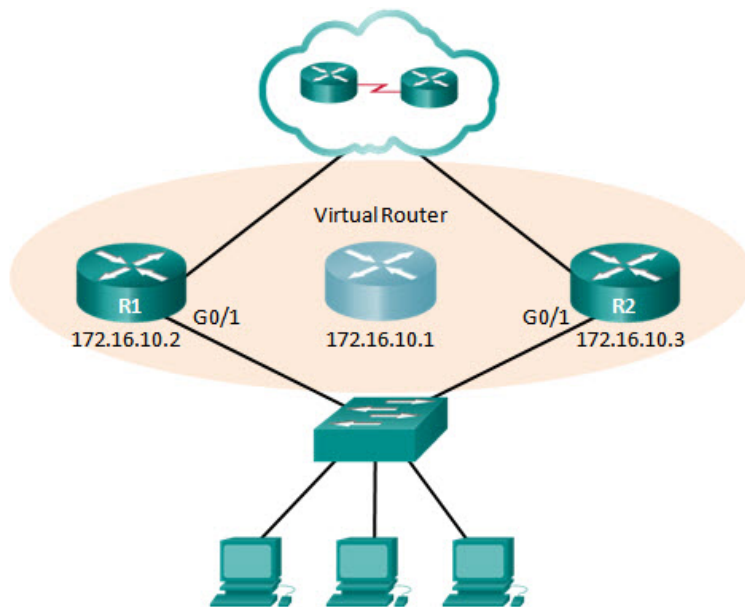
State	Definition
Initial	<ul style="list-style-type: none">• This state is entered through a configuration change or when an interface first becomes available.
Learn	<ul style="list-style-type: none">• The router has not determined the virtual IP address and has not yet seen a hello message from the active router.• In this state the router waits to hear from the active router.
Listen	<ul style="list-style-type: none">• The router knows the Virtual IP address, but the router is neither the active or standby router.• It listens for hello messages from those routers.
Speak	<ul style="list-style-type: none">• The router sends periodic hello messages and actively participates in the election of the active and standby router.
Standby	<ul style="list-style-type: none">• The router is a candidate to become the next active router.• The router sends periodic hello messages.
Active	<ul style="list-style-type: none">• The router currently forwards packets that are sent to the group virtual MAC address.• The router sends periodic hello messages.

3.4.1.5 – HSRP Timers

The **active** and **standby** HSRP routers send **hello** packets to the HSRP group **multicast address** every **3 seconds** by default. The standby router will become active if it does **not receive** a **hello** messages from the active router after **10 seconds**. You can lower these timer settings to speed up the failover or Preemption. However do not set hello timer below **1** second or hold timer below **4** seconds.

3.4.2.1 – HSRP Configuration Commands

- Step 1. Configure HSRP version 2.
- Step 2. Configure the virtual IP address for the group.
- Step 3. Configure the priority for the desired active router to be greater than 100.
- Step 4. Configure the active router to preempt the standby router in cases where the active router comes online after the standby router.



Example 1: HSRP Configuration for R1 and R2

```
R1(config)# interface g0/1
R1(config-if)# ip address 172.16.10.2 255.255.255.0
R1(config-if)# standby version 2
R1(config-if)# standby 1 ip 172.16.10.1
R1(config-if)# standby 1 priority 150
R1(config-if)# standby 1 preempt
R1(config-if)# no shutdown
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
R2(config)# interface g0/1
R2(config-if)# ip address 172.16.10.3 255.255.255.0
R2(config-if)# standby version 2
R2(config-if)# standby 1 ip 172.16.10.1
R2(config-if)# no shutdown
```

3.4.2.3 – HSRP Verification

Show standby

```
R1# show standby

GigabitEthernet0/1 - Group 1 (version 2)

  State is Active

    5 state changes, last state change 01:02:18

  Virtual IP address is 172.16.10.1

  Active virtual MAC address is 0000.0c9f.f001

    Local virtual MAC address is 0000.0c9f.f001 (v2 default)

  Hello time 3 sec, hold time 10 sec

    Next hello sent in 1.120 secs

  Preemption enabled

  Active router is local

  Standby router is 172.16.10.3, priority 100 (expires in 9.392 sec)

  Priority 150 (configured 150)

  Group name is "hsrp-Gi0/1-1" (default)
```

Show standby brief

```
R1# show standby brief

                P indicates configured to preempt.
                |
Interface    Grp  Pri P State    Active        Standby        Virtual IP
Gi0/1        1   150 P Active    local         172.16.10.3    172.16.10.1
```

3.4.2.3 – HSRP Debug Commands

Debug standby packets – View the receiving and sending of hello packets every 3 seconds.

Debug standby terse – View HSRP events.

Debug standby errors

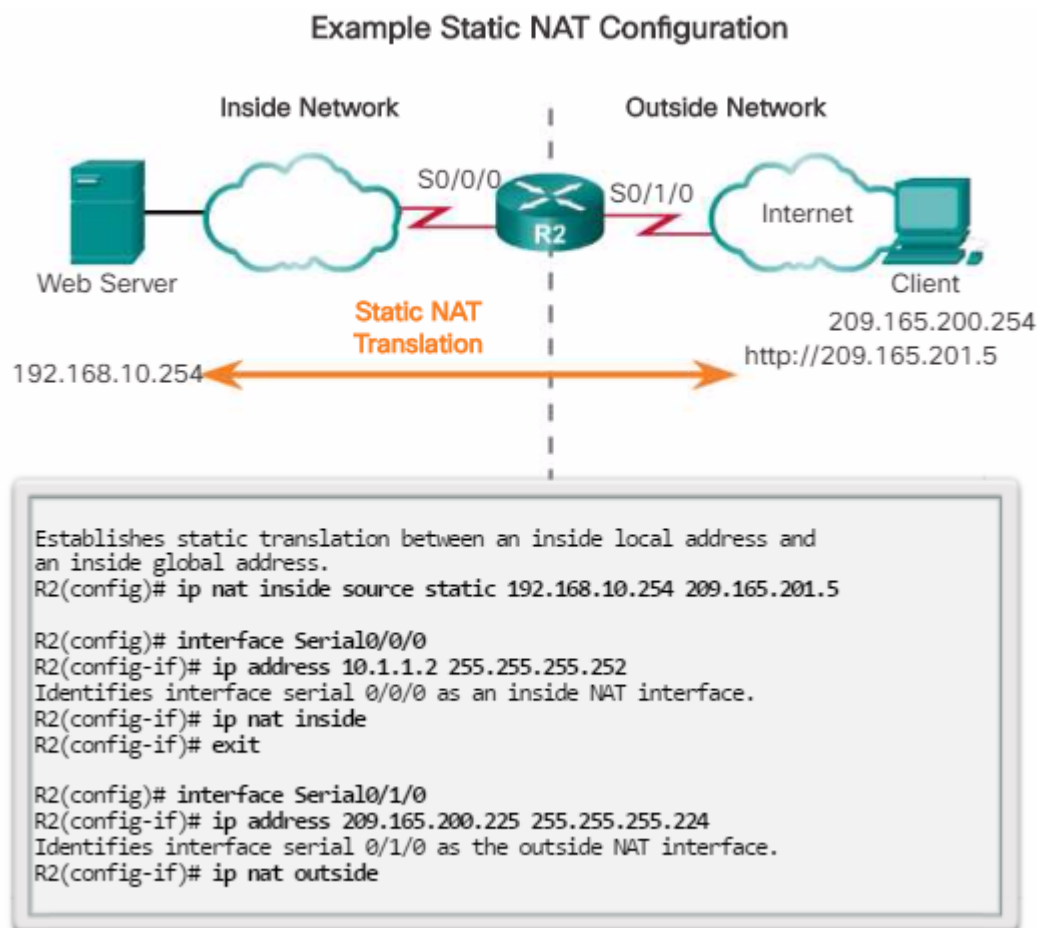
Debug standby events

3.4.3.3 – Common HSRP Configuration Issues

- The HSRP routers are **not connected** to the **same network** segment.
- The HSRP routers are **not configured** with **IP** addresses from the **same subnet**. HSRP hello packets are local and not routed beyond the network.
- The HSRP routers are not configured with the **same virtual IP address**.
- The HSRP routers are not configured with the **same HSRP group number**.
- End devices are not configured with the **correct default gateway address**.

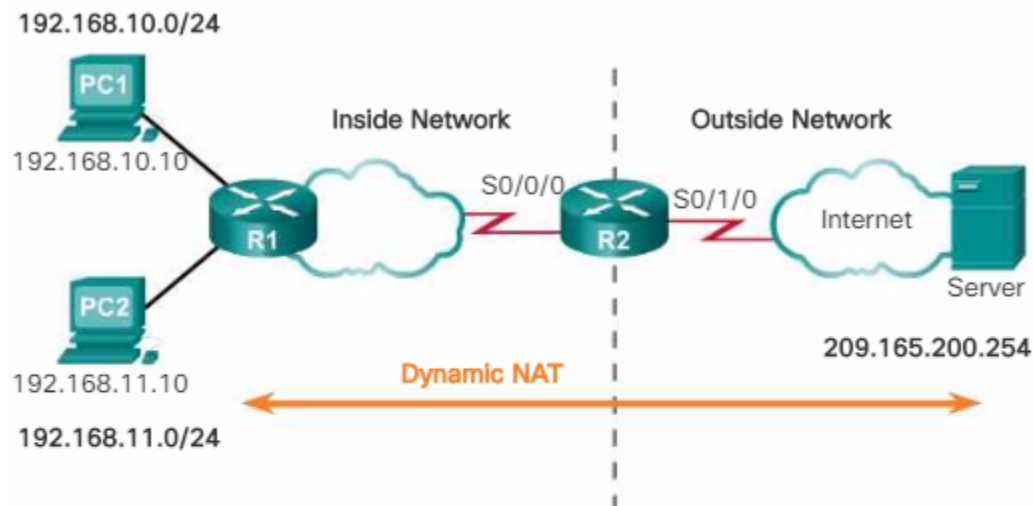
5.6 Configure, verify, and troubleshoot inside source NAT

- **5.6.a Static**



- 5.6.b Pool

Example Dynamic NAT Configuration



Defines a pool of public IPv4 addresses under the pool name NAT-POOL1.

```
R2(config)# ip nat pool NAT-POOL1 209.165.200.226  
209.165.200.240 netmask 255.255.255.224
```

Defines which addresses are eligible to be translated.

```
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
```

Binds NAT-POOL1 with ACL 1.

```
R2(config)# ip nat inside source list 1 pool NAT-POOL1
```

Identifies interface serial 0/0/0 as an inside NAT interface.

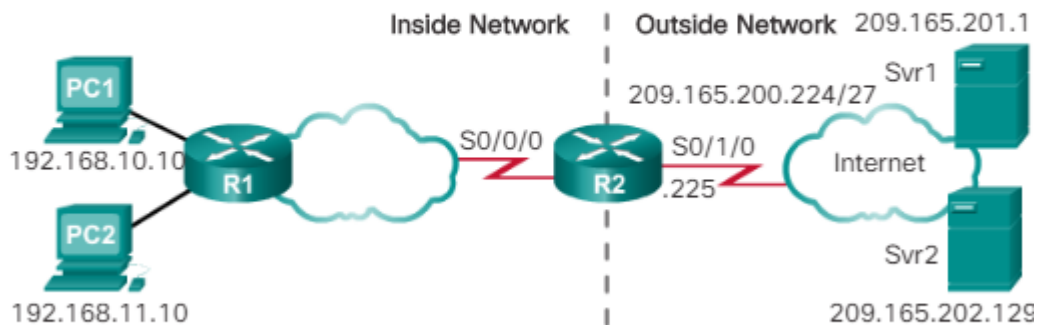
```
R2(config)# interface Serial0/0/0  
R2(config-if)# ip nat inside
```

Identifies interface serial 0/1/0 as an outside NAT interface.

```
R2(config)# interface Serial0/1/0  
R2(config-if)# ip nat outside
```


- 5.6.c PAT

Example PAT with Address Pool



Define a pool of public IPv4 addresses under the pool name NAT-POOL2.

```
R2(config)# ip nat pool NAT-POOL2 209.165.200.226 209.165.200.240 netmask 255.255.255.224
```

Define which addresses are eligible to be translated.

```
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
```

Bind NAT-POOL2 with ACL 1.

```
R2(config)# ip nat inside source list 1 pool NAT-POOL2 overload
```

Identify interface serial 0/0/0 as an inside NAT interface.

```
R2(config)# interface Serial0/0/0
```

```
R2(config-if)# ip nat inside
```

Identify interface serial 0/1/0 as the outside NAT interface.

```
R2(config)# interface Serial0/1/0
```

```
R2(config-if)# ip nat outside
```

Verifying Static NAT Translations

The static translation is always present in the NAT table.

```
R2# show ip nat translations
Pro Inside global  Inside local  Outside local  Outside global
--- 209.165.201.5  192.168.10.254  ---          ---
R2#
```

The static translation during an active session.

```
R2# show ip nat translations
Pro Inside global  Inside local  Outside local  Outside global
--- 209.165.201.5  192.168.10.254  209.165.200.254  209.165.200.254
R2#
```

Verifying Static NAT Statistics

```
R2# clear ip nat statistics

R2# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Peak translations: 0
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/0/0
Hits: 0 Misses: 0
<output omitted>
```

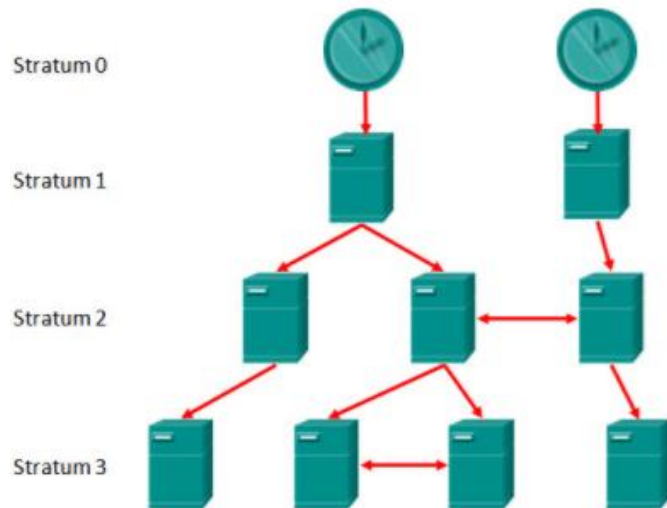
Client PC establishes a session with the web server

```
R2# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Peak translations: 2, occurred 00:00:14 ago
Outside interfaces:
  Serial0/1/0
Inside interfaces:
  Serial0/0/0
Hits: 5 Misses: 0
<output omitted>
```

5.7 Configure and verify NTP operating in a client/server mode

2.3.1.2 - NTP Operation

NTP networks use a **hierarchical** system of time sources. Each level in this hierarchical system is called a **stratum**. The **stratum** level is defined as the number of **hop counts** from the **authoritative source**.



Stratum 0 – Authoritative time sources

Stratum 1 – Directly connected to the authoritative time sources.

Stratum 2 and lower - Connected to stratum 1 device through network connections. Stratum 2 devices, such as NTP clients, synchronize their time using the NTP packets from stratum 1 servers. They could also act as servers for stratum 3 devices.

2.3.1.3 – Configure and Verify NTP

Verify the Time Source – **show clock detail**

Configure NTP Server – **ntp server 209.165.200.225**

Verify NTP Associations – **show ntp associations**

Verify NTP Status – **show ntp status**

6.1 Configure, verify, and troubleshoot port security

- 6.1.a Static
Static secure MAC addresses - MAC addresses that are manually configured on a port by using the **switchport port-security mac-address *mac-address*** interface configuration mode command. MAC addresses configured in this way are stored in the address table and are added to the running configuration on the switch.
- 6.1.b Dynamic
Dynamic secure MAC addresses - MAC addresses that are dynamically learned and stored only in the address table. MAC addresses configured in this way are removed when the switch restarts.
- 6.1.c Sticky
Sticky secure MAC addresses - MAC addresses that can be dynamically learned or manually configured, then stored in the address table and added to the running configuration.
- 6.1.d Max MAC addresses
Maximum number of secure MAC addresses for the interface; valid values are from 1 to 1025.
- 6.1.e Violation actions
- **Protect** - When the number of secure MAC addresses reaches the limit allowed on the port, packets with unknown source addresses are dropped until a sufficient number of secure MAC addresses are removed, or the number of maximum allowable addresses is increased. There is no notification that a security violation has occurred.
- **Restrict** - When the number of secure MAC addresses reaches the limit allowed on the port, packets with unknown source addresses are dropped until a sufficient number of secure MAC addresses are removed, or the number of maximum allowable addresses is increased. In this mode, there is a notification that a security violation has occurred.
- **Shutdown** - In this (**default**) violation mode, a port security violation causes the interface to immediately become error-disabled and turns off the port LED. It increments the violation counter. When a secure port is in the error-disabled state, it can be brought out of this state by entering the **shutdown** and **no shutdown** interface configuration mode commands.

Security Violation Modes

Violation Mode	Forwards Traffic	Sends Syslog Message	Displays Error Message	Increases Violation Counter	Shuts Down Port
Protect	No	No	No	No	No
Restrict	No	Yes	No	Yes	No
Shutdown	No	No	No	Yes	Yes

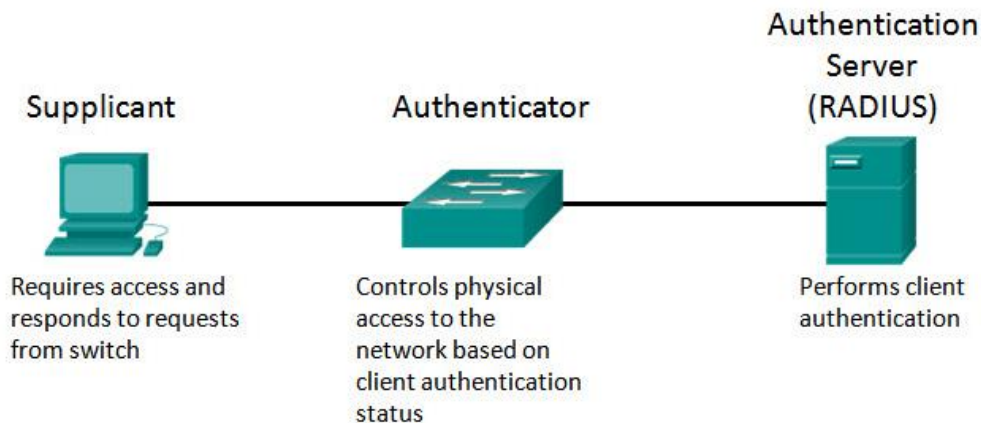
- 6.1.f Err-disable recovery

```
S1(config)# interface FastEthernet 0/18
S1(config-if)# shutdown
Sep 20 06:57:28.532: %LINK-5-CHANGED: Interface
FastEthernet0/18, changed state to administratively down
S1(config-if)# no shutdown
Sep 20 06:57:48.186: %LINK-3-UPDOWN: Interface
FastEthernet0/18, changed state to up
Sep 20 06:57:49.193: %LINEPROTO-5-UPDOWN: Line protocol on
Interface
FastEthernet0/18, changed state to up
```

6.2 Describe common access layer threat mitigation techniques

- 6.2.a 802.1x

The IEEE 802.1X standard defines a port-based access control and authentication protocol that **restricts unauthorized workstation** from connecting to a LAN through **publicly accessible switch ports**. The authentication server authenticates each workstation that is connected to a switch port before making available any services offered by the switch or the LAN



Client (Supplicant) – This is usually the **802.1X enabled port** on the device that **requests access** to LAN and switch services and then responds to requests from the switch.

Switch (Authenticator) – Controls physical access to the network based on the authentication status of the client. The switch acts as an intermediary (proxy) between the client and the authentication server. It **requests identifying information** from the client **verifies** that **information** with the **authentication server** and **relays a response** to the client.

Authentication Server – Performs the actual authentication of the client. The authentication server **validates** the **identity** of the **client** and **notifies** the **switch** whether the client is authorized to access the LAN and switch services. The authentication service is **transparent** to the client.

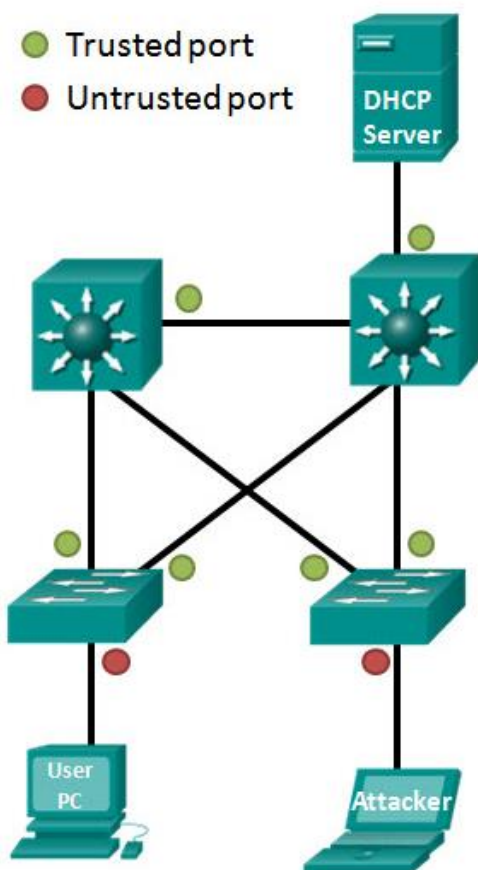
- 6.2.b DHCP snooping

A DHCP spoofing attack occurs when a rogue DHCP server is connected to the network and provides **false IP configuration** parameters to legitimate clients. DHCP spoofing is **dangerous** because clients can be leased IP information such as **malicious DNS server** addresses, **malicious default gateways** and **malicious IP assignments**.

DHCP snooping **builds** and maintains a database called the **DHCP Snooping Binding Database** (also known as the DHCP Snooping Binding Table). This database includes the client MAC address, IP address, DHCP lease time, binding type, VLAN number, and interface information on each untrusted switch port or interface.

DHCP snooping recognizes two types of ports:

- **Trusted DHCP ports** – Only ports connecting to **upstream DHCP servers** should be trusted. These ports should lead to legitimate DHCP servers replying with DHCP offer and DHCP Ack messages. Trusted ports must be explicitly identified in the configuration
- **Untrusted ports** – These ports connect to **hosts** that should not be providing DHCP server messages. By Default all switch ports are untrusted.



- 6.2.c Nondefault native VLAN

6.3 Configure, verify, and troubleshoot IPv4 and IPv6 access list for traffic filtering

- 6.3.a Standard
- 6.3.b Extended
- 6.3.c Named

6.4 Verify ACLs using the APIC-EM Path Trace ACL analysis tool

6.5 Configure, verify, and troubleshoot basic device hardening

- 6.5.a Local authentication
- 6.5.b Secure password
- 6.5.c Access to device
 - 6.5.c. [i] Source address
 - 6.5.c. [ii] Telnet/SSH
- 6.5.d Login banner

6.6 Describe device security using AAA with TACACS+ and RADIUS

To keep **malicious users** from gaining access to sensitive network equipment and services, administrators must enable **access control**. Access control limits who or what can use specific resources. IT also limits the service or options that are available after access is granted.

Common authentication methods:

- **Simple password authentication** – Involves using the “**Password**” and “**login**” line configuration commands to protect console, vty and aux ports. Also the **weakest** and **least secure** method because it provides **no accountability**.
- **Local database authentication** – This involves creating **local user accounts** with the “**username**” name “**secret**” password global configuration commands and then configuring the “**login local**” command on the console, vty and aux ports. This provides **additional security** because an attacker is required to know a user and password and provides **more accountability** since the username is **recorded** when a user logs in.

A better and much more scalable solution is to have all devices refer to a database or usernames and passwords hosted on a central server. **Authentication, Authorization and Accounting (AAA)** framework to help secure device access is used.

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

A device enabled with AAA can be configured to **refer to an external user database** for user **authentication, authorization** and **accounting**.

TACACS+ Factors:

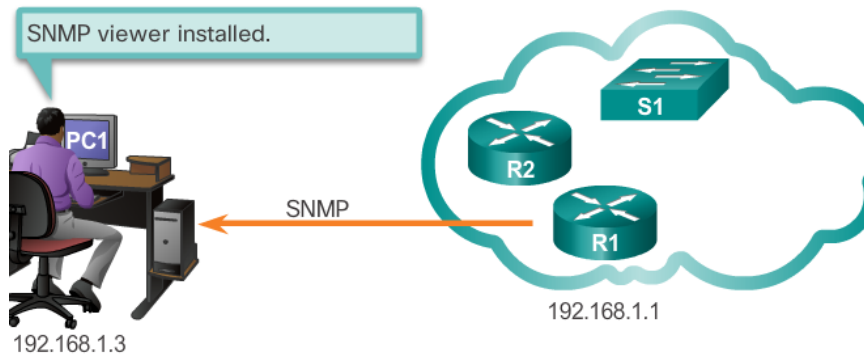
- Separates authentication and authorization
- **Encrypts all communication**
- Utilizes TCP port 49

RADIUS Factors:

- Combines RADIUS authentication and authorization as one process
- **Encrypts only the password**
- Utilizes UDP
- **Supports remote-access technologies** 802.1X and Session Initiation Protocol (SIP)

7.1 Configure and verify device-monitoring protocols

- 7.1.a SNMPv2



```
R1(config)# snmp-server community batonaug ro SNMP_ACL
R1(config)# snmp-server location NOC_SNMP_MANAGER
R1(config)# snmp-server contact Wayne World
R1(config)# snmp-server host 192.168.1.3 version 2c batonaug
R1(config)# snmp-server enable traps
R1(config)# ip access-list standard SNMP_ACL
R1(config-std-nacl)# permit 192.168.1.3
```

```
R1# show snmp
Chassis: FTX1636848Z
Contact: Wayne World
Location: NOC_SNMP_MANAGER
0 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  0 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  0 Get-next PDUs
  0 Set-request PDUs
  0 Input queue packet drops (Maximum queue size 1000)
19 SNMP packets output
  0 Too big errors (Maximum packet size 1500)
  0 No such name errors
  0 Bad values errors
  0 General errors
  0 Response PDUs
  19 Trap PDUs
SNMP Dispatcher:
```

R1# **show snmp community**

Community name: IIMI
Community Index: cisco0
Community SecurityName: IIMI
storage-type: read-only active

Community name: batonaug
Community Index: cisco7
Community SecurityName: batonaug
storage-type: nonvolatile active access-list: SNMP_ACL

Community name: batonaug@1
Community Index: cisco8
Community SecurityName: batonaug@1
storage-type: nonvolatile active access-list: SNMP_ACL

- 7.1.b SNMPv3

Simple Network Management Protocol version 3 **authenticates** and **encrypts packets** over the network to provide **secure access** to devices. Adding authentication and encryption to SNMPv3 addresses the vulnerabilities of earlier version of SNMP.

4.7.1.2 – SNMPv3 Configuration Steps

Step 1 – Configure an ACP that will permit access to authorized SNMP managers.

- **Ip access-list standard acl name**
- **Permit source**

Step 2 – Configure and SNMP view to identify which MIB object identifiers(OIDs) that the SNMP manager will be able to read.

- **Snmp-view 'view-name old-tree' (included/Excluded)**

Step 3 – Configure SNMP group features with the snmp-server group command.

- Configure a name for the group.
- Set the SNMP version to 3 with the v3 keyword.
- Require authentication and encryption with the priv keyword.
- Associate a view to the group and give it read only access with the read command.
- Specify the ACL configured in Step 1.
- **Router(config)# snmp-server group group-name v3 priv read view-name access [acl-number | acl-name]**

Step 4 – Configure SNMP group user features with the snmp-server user command.

Configure a username and associate the user with the group name that was configured in Step 3.

- Set the SNMP version to 3 with the v3 keyword.
- Set the authentication type to either md5 or sha and configure an authentication password. SHA is preferred and should be supported by the SNMP management software.
- Require encryption with the priv keyword and configure an encryption password.
- **Router(config)# snmp-server user username group-name v3 auth {md5 | sha} auth-password priv {des | 3des | aes {128 | 192 | 256}} privpassword**

```
R1(config)# ip access-list standard PERMIT-ADMIN
R1(config-std-nacl)# permit 192.168.1.0 0.0.0.255
R1(config-std-nacl)# exit
R1(config)# snmp-server view SNMP-RO iso included
R1(config)# snmp-server group ADMIN v3 priv read SNMP-RO access PERMIT-ADMIN
R1(config)# snmp-server user BOB ADMIN v3 auth sha cisco12345 priv aes 128
cisco54321
R1(config)# end
```

4.7.1.3 – SNMPv3 Verification

Show snmp group

```
R1# show snmp group

groupname: ILMI                                security model:v1
contextname: <no context specified>           storage-type: permanent
readview : *ilmi                               writeview:
*ilmi
notifyview: <no notifyview specified>
row status: active
```

```
R1# show snmp user BOB

User name: BOB
Engine ID: 800000090300FC994775C3E0
storage-type: nonvolatile      active
Authentication Protocol: SHA
Privacy Protocol: AES128
Group-name: ADMIN
```

- 7.1.c Syslog

```
R1(config)# logging 192.168.1.3
R1(config)# logging trap 4
R1(config)# logging source-interface g0/0
R1(config)# interface loopback 0
R1(config-if)#
*Jun 12 22:06:02.902: %LINK-3-UPDOWN: Interface Loopback0,
changed state to up
*Jun 12 22:06:03.902: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback0, changed state to up
*Jun 12 22:06:03.902: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to
host 192.168.1.3 port 514 started - CLI initiated
R1(config-if)# shutdown
R1(config-if)#
*Jun 12 22:06:49.642: %LINK-5-CHANGED: Interface Loopback0,
changed state to administratively down
*Jun 12 22:06:50.642: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback0, changed state to down
R1(config-if)# no shutdown
R1(config-if)#
*Jun 12 22:09:18.210: %LINK-3-UPDOWN: Interface Loopback0,
changed state to up
*Jun 12 22:09:19.210: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback0, changed state to up
R1(config-if)#
```

```
R1# show logging | include changed state to up
*Jun 12 17:46:26.143: %LINK-3-UPDOWN: Interface
GigabitEthernet0/1, changed state to up
*Jun 12 17:46:26.143: %LINK-3-UPDOWN: Interface Serial0/0/1,
changed state to up
*Jun 12 17:46:27.263: %LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet0/1, changed state to up
*Jun 12 17:46:27.263: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Serial0/0/1, changed state to up
*Jun 12 20:28:43.427: %LINK-3-UPDOWN: Interface
GigabitEthernet0/0, changed state to up
```

Syslog Severity Level

Severity Name	Severity Level	Explanation
Emergency	Level 0	System Unusable
Alert	Level 1	Immediate Action Needed
Critical	Level 2	Critical Condition
Error	Level 3	Error Condition
Warning	Level 4	Warning Condition
Notification	Level 5	Normal, but Significant Condition
Informational	Level 6	Informational Message
Debugging	Level 7	Debugging Message

Summary

The time on Cisco network devices can be synchronized using NTP.

Cisco network devices can log syslog messages to an internal buffer, the console, a terminal line, or an external syslog server. A network administrator can configure the types of messages to be collected and where to send the time-stamped messages.

The SNMP protocol has three elements: the Manager, the Agent, and the MIB. The SNMP manager resides on the NMS, while the Agent and the MIB are on the client devices. The SNMP Manager can poll the client devices for information, or it can use a TRAP message that tells a client to report immediately if the client reaches a particular threshold. SNMP can also be used to change the configuration of a device. SNMPv3 is the recommended version because it provides security. SNMP is a comprehensive and powerful remote management tool. Nearly every item available in a **show** command is available through SNMP.

NetFlow is a Cisco IOS technology that is the standard for collecting IP operational data from IP networks. NetFlow efficiently measures what network resources are being used and for what purposes. NetFlow uses header fields to distinguish between data flows. NetFlow is a “push” technology, where the client device initiates the sending of data to a configured server.

7.2 Troubleshoot network connectivity issues using ICMP echo-based IP SLA

7.3 Configure and verify device management

- 7.3.a Backup and restore device configuration
- 7.3.b Using Cisco Discovery Protocol or LLDP for device discovery
- 7.3.c Licensing
- 7.3.d Logging
- 7.3.e Timezone
- 7.3.f Loopback

7.4 Configure and verify initial device configuration

7.5 Perform device maintenance

- 7.5.a Cisco IOS upgrades and recovery (SCP, FTP, TFTP, and MD5 verify)
- 7.5.b Password recovery and configuration register
- 7.5.c File system management

7.6 Use Cisco IOS tools to troubleshoot and resolve problems

- 7.6.a Ping and traceroute with extended option

This is **helpful** when **troubleshooting routing loops**, determining the exact **next-hop router** or to help determine where **packets** are getting **dropped** by a **router** or **denied** by a **firewall**.

An ICMP '**Time exceeded**' error message – a router in the path has **seen** and **discarded** the packet.

AN ICMP '**Destination unreachable**' error message – a router has **received** the packet, but **discarded** it because it could **not be delivered**.

Different trace route options – Protocol, Target IP address, Source Address, Numeric display, Timeout, Probe count, Max time to live, Port number.

- 7.6.b Terminal monitor

While IOS log messages are sent to the console by **default**, these same log messages are **not sent** to the virtual lines by default. Because debug messages are log messages, this behavior prevents any debug-related messages from being displayed on VTY lines.

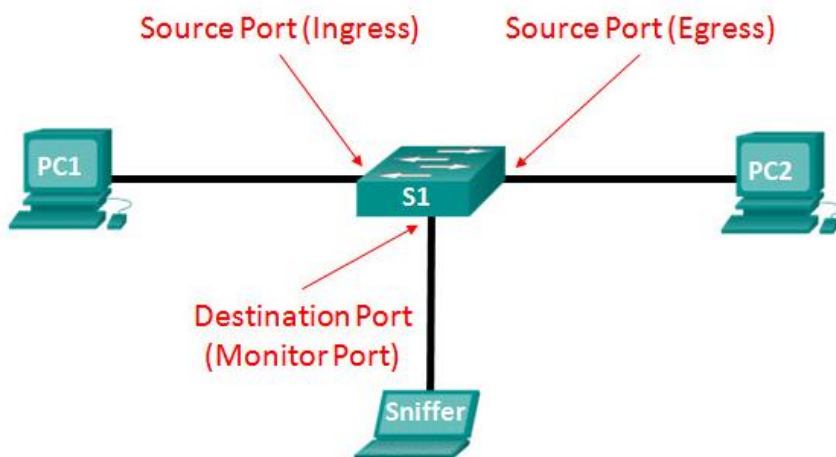
To display log messages on a **terminal** (virtual console), use the **terminal monitor** privileged EXEC command.

- 7.6.c Log events

- 7.6.d Local SPAN

Switched Port Analyser (SPAN) feature on Cisco switches is a **type of port mirroring** that sends copies of the frame entering a port out another port on the same switch. It is common to find a device running a **packet analyser**, an **Intrusion Detection System (IDS)** or an **Intrusion Prevention System (IPS)** **connected** to that port.

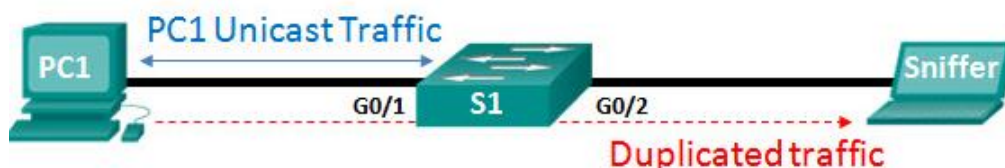
Term	Definition
Ingress traffic	Traffic that enters the switch
Egress traffic	Traffic that leaves the switch
Source (SPAN) port	Port monitored with SPAN
Destination (SPAN) port	Port that monitors source ports, usually where a packet analyser, IDS or IPS is connected . Also called a monitor port.
SPAN session	An association of a destination port with one or more source ports
Source VLAN	The VLAN monitored for traffic analysis



Although SPAN can support multiple source ports under the same session or an entire VLAN as the traffic source, a SPAN session **does not support both**.

Things to consider:

- The **destination port** cannot be a **source port**, and the **source port** cannot be a **destination port**.
- The number of destination port is **platform-dependant**.
- The destination port is no longer a normal switch port. **Only monitored traffic passes** through that port.



```
Switch1(config)# monitor session 1 source interface GigabitEthernet 0/1
Switch1(config)# monitor session 1 destination interface GigabitEthernet 0/2
```

```
S1# show monitor

Session 1
-----

Type                : Local Session
Source Ports        :
    Both            : Gi0/1
Destination Ports    : Gi0/2
    Encapsulation    : Native
    Ingress          : Disabled
```

7.7 Describe network programmability in enterprise network architecture

- 7.7.a Function of a controller
- 7.7.b Separation of control plane and data plane
- 7.7.c Northbound and southbound APIs