CISCO CCNA R&S 6.0
BRIDGING

Clive Micallef

CCNA Bridge

1.1.1.1 – Extended Trace route

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.

1.1.2.1 – Debug Command

Allows the administrator to display these messages in real-time for analysis.

Debug ip icmp

1.1.2.2 – 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.

1.2.1.1 – Basic Troubleshooting Approaches

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.

1.2.1.2 – 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.

1.2.1.3 – Verify and Monitor Solution

Verification tools include the **ping, traceroute and show** commands.

1.2.2.1 – Duplex Operation

If one of the two connected devices is operating in **full duplex** and the other is operating in **half duplex,** a **duplex mismatch** will occur.

1.2.2.2 – Duplex Mismatch

Duplex mismatch may be difficult to troubleshoot as the communication between devices **still occurs** even with ping since small packets may fail to reveal duplex mismatch.

CDP – Cisco Proprietary Protocol can easily detect a duplex mismatch between two cisco devices.

Show interfaces fastethernet 0/5

1.2.3.1 – IP Addressing Issues on IOS Devices

Show ip interface

Show ip interface brief

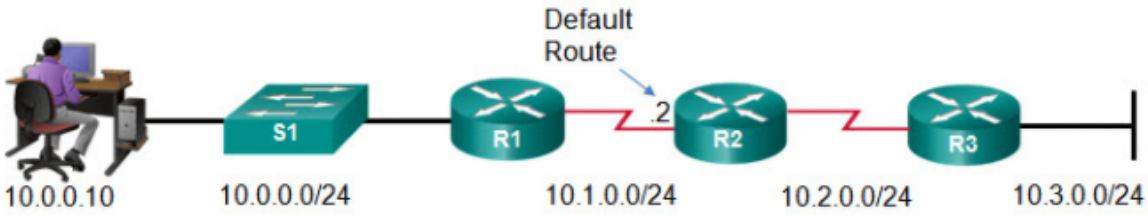
1.2.3.2 – IP addressing Issues on End Devices

Ipconfig

1.2.3.3 Default Gateway Issues

Ipconfig

Show ip route command to list the routing table and verify that the default gateway, known as a default route, has been set. This route is used when the destination address of the packet does not match any other routes in its routing table.



Example 2 shows that the default gateway has been set with a default route of 10.1.0.2.

Example 2: Default gateway displayed in output of show ip route command

```
R1# show ip route

<output omitted>


Gateway of last resort is 10.1.0.2 to network 0.0.0.0


S*    0.0.0.0/0 [1/0] via 10.1.0.2

      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks

C        10.0.0.0/24 is directly connected, GigabitEthernet0/0

L        10.0.0.1/32 is directly connected, GigabitEthernet0/0

C        10.1.0.0/24 is directly connected, Serial0/0/0

L        10.1.0.1/32 is directly connected, Serial0/0/0

R1#
```

1.2.3.4 – Troubleshooting DNS Issues

Domain Name Service (DNS) defines an automated service that matches names such as www.cisco.com with the IP address.

Ipconfig /all

Example 1: DNS Server Information on a PC

```
C:\> ipconfig /all

<some output omitted>


Ethernet adapter Local Area Connection:


   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   Physical Address. . . . . . . . . : F0-4D-A2-DD-A7-B2
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::449f:c2:de06:ebad%10(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.0.0.10(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Monday, November 09, 2015 7:49:48 PM
   Lease Expires . . . . . . . . . . : Thursday, November 19, 2015 7:49:51 AM
   Default Gateway . . . . . . . . . : 10.0.0.1
   DHCP Server . . . . . . . . . . . : 10.0.0.1
   DNS Servers . . . . . . . . . . . : 8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Nslookup – A user can manually place **DNS queries** and analyse the DNS response.

Example 2: The nslookup Command

```
C:\> nslookup

Default Server:  dns-cac-lb-01.rr.com

Address:  209.18.47.61

> cisco.com

Server:  dns-cac-lb-01.rr.com

Address:  209.18.47.61

Non-authoritative answer:

Name:    cisco.com

Addresses:  2001:420:1101:1::a

          72.163.4.161

> quit
```

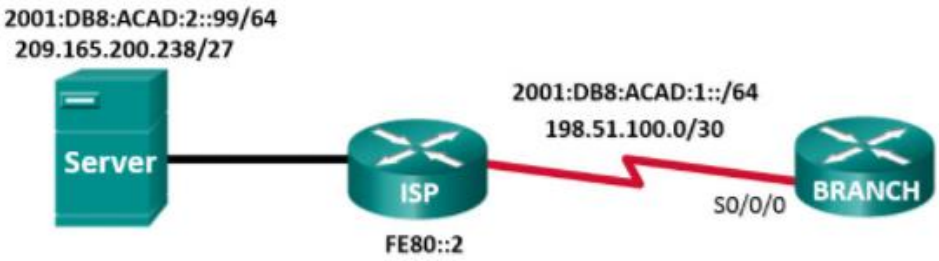
2.1.1.1 – Automatically Installed Local Host Routes

A **host route** is where the destination address is a specific device IP with a subnet mask of **/32** for IPv4 or **/128** for IPv6.

There are **three** ways a host route can be added to the routing table.

- Automatically installed when an IP address is configured on the router.
- Configured as a static host route
- Host route automatically obtained through other methods.

When an active interface on a router is configured with an IP address, a local host route is **automatically** added to the **routing table**. The local routes are marked with **"L"** in the output of the routing table



Show ip route

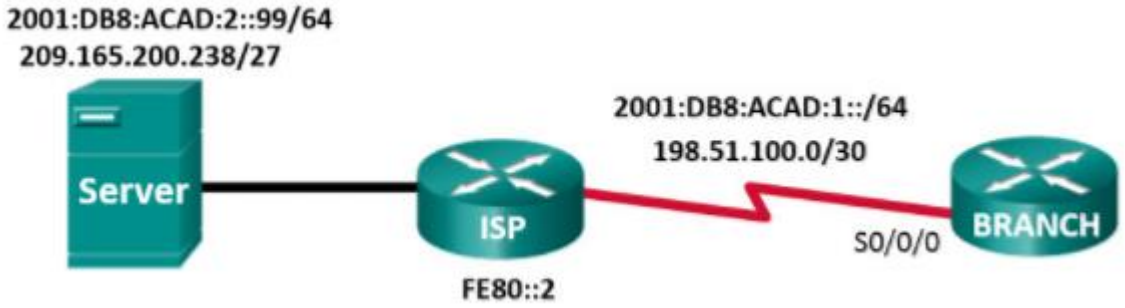
```
L        198.51.100.1/32 is directly connected, Serial0/0/0
```

Show ipv6 route

```
L   2001:DB8:ACAD:1::1/128 [0/0]
     via Serial0/0/0, receive
```

2.1.1.2 – Manually Configured Host Routes

A **Host route** can be manually configured static route to direct traffic to a **specific** destination device, such as an authentication server. The static route uses a destination IP address and a 255.255.255.255 (/32) mask for IPv4 host routes and /128 for IPv6 host routes. Static routes are marked with **'S'** in the output of the routing table.




```
Branch(config)# ip route 209.165.200.238 255.255.255.255 198.51.100.2
Branch(config)# ipv6 route 2001:db8:acad:2::99/128 2001:db8:acad:1::2
```

```
      209.165.200.0/32 is subnetted, 1 subnets
S        209.165.200.38 [1/0] via 198.51.100.2
```

```
S   2001:DB8:ACAD:2::99/128 [1/0]
     via 2001:DB8:ACAD:1::2
```

For **IPv6 static routes**, the next-hop address can be the **link-local address** of the adjacent router. However, you must **specify an interface type** and an **interface number** when using a link-local address as the next hop.

```
Branch(config)# ipv6 route 2001:db8:acad:2::99/128 serial 0/0/0 fe80::2
```

```
S   2001:DB8:ACAD:2::99/128 [1/0]
     via FE80::2, Serial0/0/0
```

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**

2.2.1.3 – Discover Devices Using CDP

```
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 - CVTA, 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)

2.2.2.1 – 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

Globally Enabling LLDP

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

Configuring LLDP on the interface

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

Verifying LLDP is operational

```
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

2.3.1.1 – Setting the System Clock

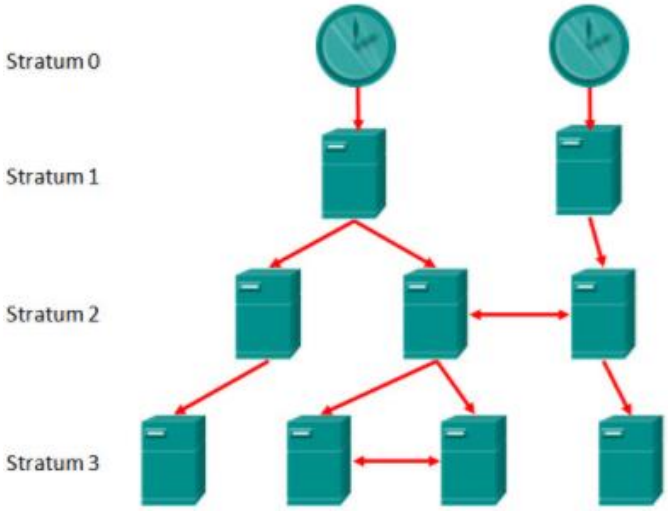
The software clock on a router or switch **starts** when the system **boots** and is the primary source of time for the system. It is important to **synchronize** the time across all devices on the network because all aspects of **managing, securing**, **troubleshooting** and **planning** networks require accurate time stamping.

The data and time can be set:

- **Manually**
- **Configuring a Network Time Protocol (NTP)**

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**

3.1.1.1 VTP Overview

VLAN trunking protocol (VTP) allows a network administrator to **manage VLANs** on a switch configured as a VTP server. The **VTP server distributes** and **synchronizes** VLAN information over **trunk links** to VTP-enabled switches throughout the switched network.

VTP only learns about normal range VLANs (1-1005) .

VTP stores VLAN configuration in a database called vlan.dat.

VTP Components	Definition
VTP Domain	• One or more interconnected switches. • **All** switched in a **domain** share VLAN configuration using **VTP advertisements.** • Switches that are in **different** VTP domains **do not** exchange VTP messages. • A router or Layer 3 switch defines the boundary of each domain.
VTP Advertisements	• **Each** switch in the VTP domain sends **periodic** global configuration **advertisements** from each **trunk port** to a reserved **multicast** address. • Neighbouring switches receive these advertisements and **update** there VTP and VLAN configuration as necessary.
VTP Modes	• A switch can be configured as **a VTP server, client or transparent.**
VTP Password	• Switches in the VTP domain can be also configured with a **password**.

3.1.1.2 – VTP Modes

VTP Mode	Definition
VTP Server	• VTP servers **advertise** the VTP **domain** VLAN information to other VTP-enabled switches in the **same VTP domain.** • VTP servers **store** the VLAN information for the **entire domain in NVRAM.** • The VTP server is where VLANs can be **created, deleted or renamed** for the domain.
VTP Client	• VTP clients function the same way as VTP servers, but you **cannot** create, change or delete VLANs on a VTP client. • A VTP client only stores the VLAN information for the entire domain while the switch is **on**. • A switch reset **deletes** the VLAN information. • You must configure VTP client mode on a switch.
VTP Transparent	• Transparent switches **do not participate** in VTP except to **forward** VTP advertisement to **VTP clients and VTP servers.** • VLANs that are created, renamed or deleted on transparent switches are **local** to the **switch only.** • To create an extended VLAN, a switch must be configured as a VTP transparent switch.

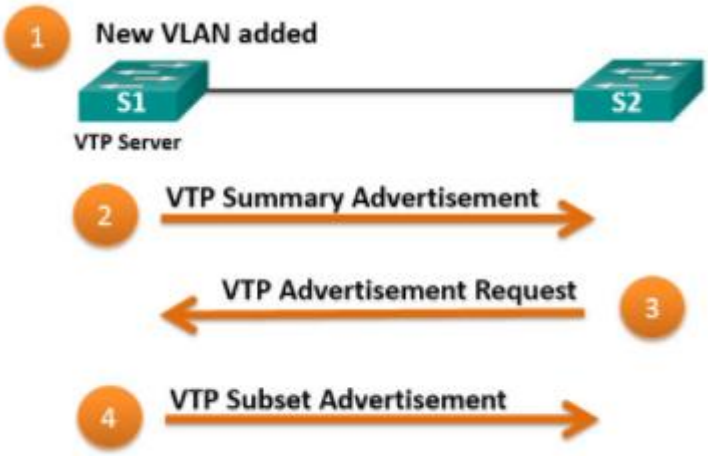
VTP Question	VTP Server	VTP Client	VTP Transparent
What are the differences?	• Managed domain and VLAN configuration. • Multiple VTP Servers can be configured.	• Updates local VTP configuration. • VTP client switches cannot change VLAN configurations.	• Manages local VLAN configurations. • VLAN configurations are not shared with VTP network.
Does it respond to VTP advertisements?	Participates fully.	Participates fully.	Only forward VTP advertisements.
Is the global VLAN configuration preserved on restart?	Yes, Global configuration is stored in NVRAM.	No, global configurations are stored in RAM only.	No, local VLAN configuration is only stored in NVRAM.
Does it update other VTP-enabled switches?	Yes	Yes	No

3.1.1.3 – VTP Advertisements

- **Summary advertisements** – These inform adjacent switches of VTP domain name and configuration revision number.
- **Advertisement request** – These are in response to a summery advertisements message when the summary advertisements contains a higher configuration revision number then the current value.
- **Subset advertisements** – These contain VLAN information including any changes.

By **default**, Cisco switches issue **summary advertisements** every **five minutes.**

The **configuration revision number** is a **32**-bit number that indicates the level of revision for a VTP packet. Each VTP device tracks the VTP configuration revision number that is assigned to it. This information is used to determine whether the received information is more recent than the current version. Each time that you make a VLAN change in a VTP device, the configuration revision is **incremented by one.**



3.1.1.4 – VTP Versions

VTP Version	Definition
VTP Version 1	**Default VTP mode** on all switches. Supports normal range VLANs only.
VTP Version 2	Supports normal range VLANs only. Supports legacy Token Ring networks. Supports advanced features including unrecognized Type-Length-Value (TLV), version-dependant transparent mode and consistency checks.

3.1.1.5 - Default VTP Configuration

Verify VTP Configuration – **show vtp status**

3.1.2.2 – Configure the VTP Server

Configure terminal

Vtp mode server

Vtp domain CCNA

Vtp password cisco

3.1.2.4 – Configure the VTP Clients

Vtp mode client

Vtp domain CCNA

Vtp password cisco

3.1.3.1 – Normal and Extended VLANs

Type	Definition
Normal range VLANs	• Used in **small** and **medium** sized business and enterprise **networks**. • Identified by **VLAN IDs** between **1** and **1005** • **IDs 1 and 1002-1005** and **automatically** created and **cannot** be **removed**. • Configurations are stored within a VLAN database file called **vlan.dat** which is stored in the **flash memory.**
Extended range VLANs	• Used by **service providers** and **large organizations** to extend their infrastructure to a greater number of customers. • Identified by a **VLAN ID** between **1006-4094** • Support **fewer** VLAN features than normal range VLANs. • Configurations are saved in **the running configuration** file.

3.1.4.1 - DTP Trunking Modes

Dynamic Trunking Protocol (DTP) helps switches negotiate and establish **802.1Q** trunk links. DTP is **Cisco proprietary** protocol. A switch port on a Cisco switch supports a number of DTP trunking modes. The trunking mode defines how the port negotiates using DTP to set up a trunk link with its peer port.

DTP is configured using the **switchport mode {access | dynamic {auto | desirable} | trunk}** interface configuration command.

Keyword	Description
Access	• Creates an access port and puts the interface into **permanent nontrunking,** single VLAN interface that sends and receives **nonencapsulated** (non-tagged) **frames**. • The interface becomes a **nontrunk** interface, regardless of whether the neighbouring interface is a trunk interface. • An access port can be assigned to only **one VLAN.**
Auto	• Default switch port mode for all Ethernet interfaces. • Port converts to a **trunk** link only if the **neighbouring port** is set to **trunk** or **desirable**. • If both ports are set to **auto**, the switches will **not negotiate** a **trunk** link.
Desirable	• Configures the interface to actively attempt to convert the link to a **trunk** link. • Port convert to a **trunk** link if the neighbouring port is set to **trunk**, **desirable** or **auto**. • This is the default mode on older switches.
Trunk	• Creates an unconditional **(always on) trunking state.**

DTP Mode	Dynamic Auto	Dynamic Desirable	Trunk	Access port
Dynamic Auto	Access port	Trunk port	Trunk port	Access port
Dynamic Desirable	Trunk port	Trunk port	Trunk port	Access port
Trunk	Trunk port	Trunk port	Trunk port	Limited connectivity
Access	Access port	Access port	Limited connectivity	Access port

3.2.2.1 – Troubleshoot DTP Issues

Problems	Description
Trunk mode mismatches	• One trunk port is configured with trunk mode “**off**" and the other with trunk mode “**on**”. • This configuration error causes the trunk link to **stop** working. • **Correct** the situation by **shutting down** the **interface**, correcting the DTP mode settings and **re-enabling** the interface.
Allowed VLANs on trunks	• The list of **allowed VLANs** on a **trunk** has not been updated with the current VLAN trunking requirements. • In this situation, unexpected traffic or no traffic is being sent over the trunk. • Configure the correct VLANs that are allowed on the trunk.
Native VLAN mismatches	• When native VLANs do not match, the switch will generate informational messages letting you know of the problem. • Ensure that sides of a **trunk link** are using the **same native VLAN**.

3.2.2.2 – Troubleshoot VTP issues

Problems	Description
Incompatible VTP Versions	• VTP versions are **incompatible** with each other. • Ensure that all switches are **capable** of supporting the required **VTP version.**
VTP Password Issues	• If **VTP authentication** is enabled, switches must all have the **same password** configured to participate in VTP. • Ensure that the password is manually configured on all switches in the VTP domain.
Incorrect VTP Mode Name	• An improperly configured VTP domain **affects VLAN synchronization** between switches and if a switch revives the wrong VTP advertisement, the switch **discards** the message. • To avoid incorrectly configured VTP domain name, set the VTP domain name on only one VTP server switch. • All other switches in the same VTP domain will accept and automatically configure their VTP domain name when they revive the first VTP summary advertisement.
All Switches set to VTP Client Mode	• If all switches in the VTP domain are set to **client mode**, you **cannot** create, delete, and manage VLANs. • To avoid losing all VLAN configurations in a VTP domain, configure two switches as VTP servers.
Incorrect Revision Number	• If a switch with the **same VTP domain** name **but** a higher **configuration number** is added to the domain, invalid VLANs can be propagated and / or valid VLANs can be deleted. • The solution is to reset each switch to an earlier configuration and then reconfigure the correct VLANs. • Before adding a switch to a VTP-enabled network, reset the **revision number** on the switch to **0** by assigning it to another false VTP domain and then reassigning it to the correct VTP domain name.

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 **244.0.0.**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 will 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.

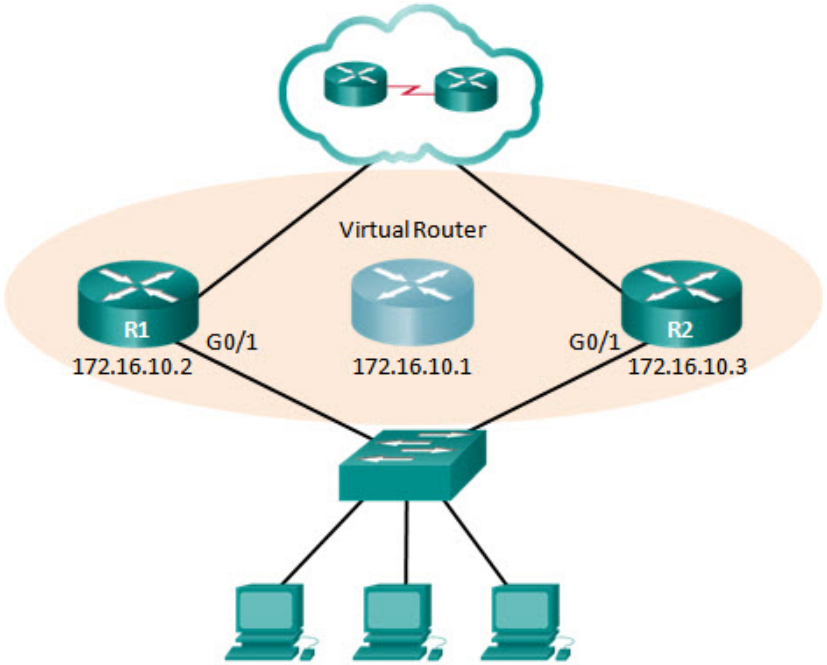
State	Definition
Initial	• This state is entered through a configuration change or when an interface first becomes available.
Learn	• The router has **not determined** the virtual IP address and has not yet seen a hello message from the active router. • In this state the router waits to hear from the active router.
Listen	• 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	• The router **sends periodic hello messages** and actively **participates** in the election of the active and standby router.
Standby	• The router is a **candidate** to become the **next active** router. • The router sends periodic hello messages.
Active	• 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**.

3.5.1.2 – Multiarea OSPF Data Structures

OSPF stores routing information in four main data structures:

- **Interface table** – This table includes a **list of all active interfaces** that have been **enabled for OSPF**. Type 1 LSAs include the subnets associated with each active interface.

- **Neighbour table** – This table is used to **manage neighbour adjacencies** through **hello** timers and **dead** timers. Neighbour entries are added and refreshed with a **hello** is received. Neighbours are **removed** when the **dead** timer **expires**.

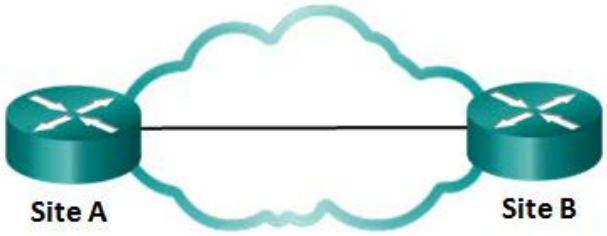
- **Link-state database** – This is the **primary** data structure used by OSPF to store network topology information, It includes **full topology information**. It includes full topological information about each are that the OSPF router is connected to, as well as any paths that are available to reach other networks or autonomous systems.

- **Routing table** – After the SPF algorithm is calculated, the **best routers** to each network are offered to the routing table.

4.1.1.1 – WAN Topologies

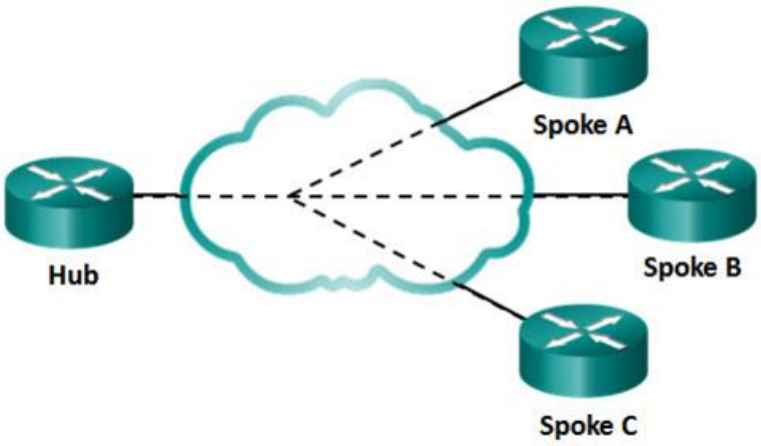
Point to Point

A Point to point topology employs a point to point circuit between two endpoints. Typically involving **dedicated leased-line connections** like TI/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.**



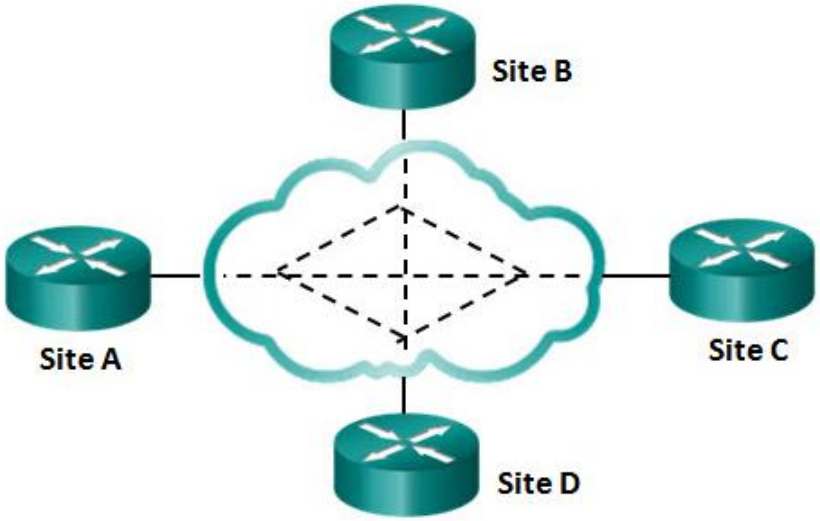
Hub and Spoke

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.**



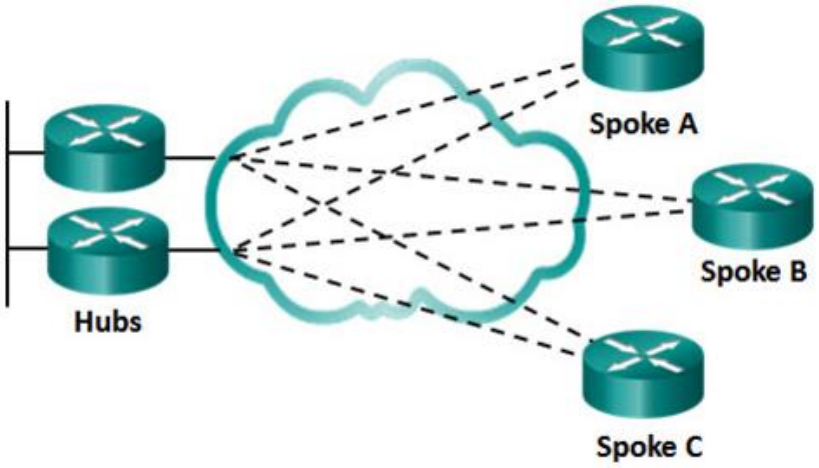
Full Mesh

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



Dual-Homed Topology

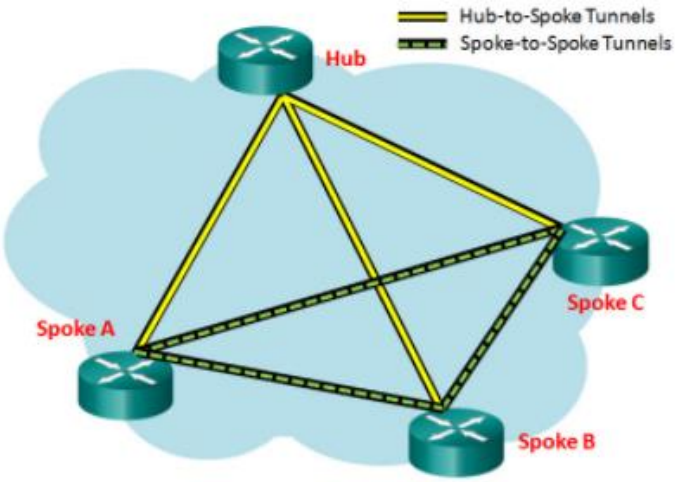
It provides **redundancy**. **More expensive** because there require more networking hardware like routers and switches. The advantage of a dual homed topology is that they offer enhanced network redundancy, load balancing, distributed computing or processing and the ability to implement backup service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



4.2.1.1 – 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)

4.3.1.1 – PPPoE Verification Commands

Show ip interface brief – Verify IPv4 address

Show interface dialer 2 – Verify the MTU and PPP encapsulation

```
R1# show interface dialer 2
Dialer2 is up, line protocol is up (spoofing)
  Hardware is Unknown
  Internet address is 10.1.3.1/32
  MTU 1492 bytes, BW 56 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Closed, loopback not set
  Keepalive set (10 sec)
  DTR is pulsed for 1 seconds on reset
```

Show ip route – Verify routing table

Show pppoe session – Verify current active PPPoE session

```
R1# show pppoe session
     1 client session

Uniq ID   PPPoE  RemMAC          Port                 VT  VA         State
           SID   LocMAC                                   VA-st      Type
    N/A      1   30f7.0da3.1641  Gi0/1                Di2 Vi2        UP
                 30f7.0da3.0da1                           UP
```

Show interfaces - Verify local and remote Ethernet MAC addresses of both routers

4.3.1.3 – PPPoE Negotiation

Debug ppp negotiation

```
R1# debug ppp negotiation

*Sep 20 19:05:05.239: Vi2 PPP: Phase is AUTHENTICATING, by the peer

*Sep 20 19:05:05.239: Vi2 LCP: State is Open

<output omitted>

*Sep 20 19:05:05.247: Vi2 CHAP: Using hostname from interface CHAP

*Sep 20 19:05:05.247: Vi2 CHAP: Using password from interface CHAP

*Sep 20 19:05:05.247: Vi2 CHAP: O RESPONSE id 1 len 26 from "Fred"

*Sep 20 19:05:05.255: Vi2 CHAP: I SUCCESS id 1 len 4

<output omitted>

*Sep 20 19:05:05.259: Vi2 IPCP:    Address 10.1.3.2 (0x03060A010302)

*Sep 20 19:05:05.259: Vi2 IPCP: Event[Receive ConfAck] State[ACKsent to Open]

*Sep 20 19:05:05.271: Vi2 IPCP: State is Open

*Sep 20 19:05:05.271: Di2 IPCP: Install negotiated IP interface address 10.1.3.2

*Sep 20 19:05:05.271: Di2 Added to neighbor route AVL tree: topoid 0, address
10.1.3.2

*Sep 20 19:05:05.271: Di2 IPCP: Install route to 10.1.3.2

R1# undebug all
```

There are **four** main points of failure in a **PPP negotiation**:

- No response from the remove device (ISP)
- Link Control Protocol (LCP) is not open
- Authentication failure
- IP Control Protocol (IPCP) failure

4.3.1.4 – PPPoE Authentication

After confirming with the ISP that they use CHAP, verify that the CHAP username and password are correct.

Show running-config | section interface Dialer2

```
R1# show running-config | section interface Dialer2

interface Dialer2

 mtu 1492

 ip address negotiated

 encapsulation ppp

 dialer pool 1

 ppp authentication chap callin

 ppp chap hostname Fred

 ppp chap password 0 Barney
```

Debug ppp negotiation – Verify CHAP username is correct

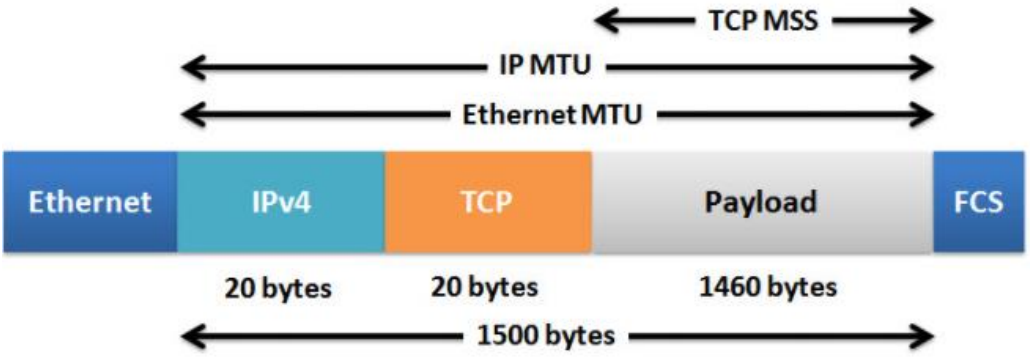
```
R1# debug ppp negotiation

*Sep 20 19:05:05.239: Vi2 PPP: Phase is AUTHENTICATING, by the peer

*Sep 20 19:05:05.239: Vi2 LCP: State is Open

<output omitted>

*Sep 20 19:05:05.247: Vi2 CHAP: Using hostname from interface CHAP

*Sep 20 19:05:05.247: Vi2 CHAP: Using password from interface CHAP

*Sep 20 19:05:05.247: Vi2 CHAP: O RESPONSE id 1 len 26 from "Fred"
```

If the CHAP username or password were **incorrect**, the output from the debug ppp negotiation command would show and **authentication failure message.**

```
*Sep 20 19:05:05.247: Vi2 CHAP: I FAILURE id 1 Len 26 MSG is "Authentication
failure"
```

4.3.1.5 – PPPoE MTU Size

The **default MSS** size is 1460 bytes, when the default MTU is 1500 bytes. However, PPPoE supports an MTU of only 1492 bytes in order to accommodate the **additional 8-byte PPPoE header.**



Adjusting MTU size

Interface g0/0

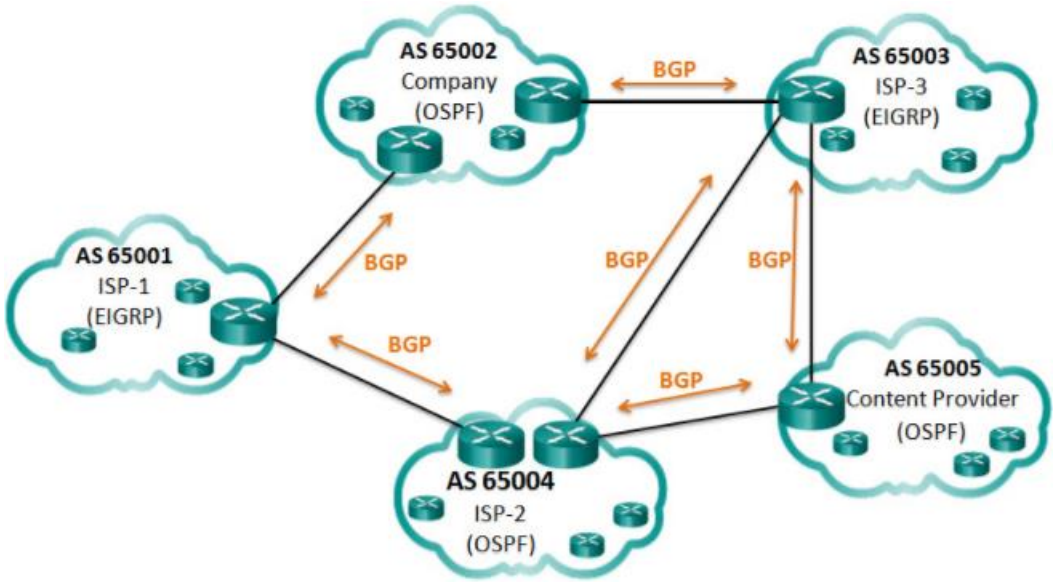
Ip tcp adjust-mss 1452

4.4.1.1 – IGP and EGP 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.

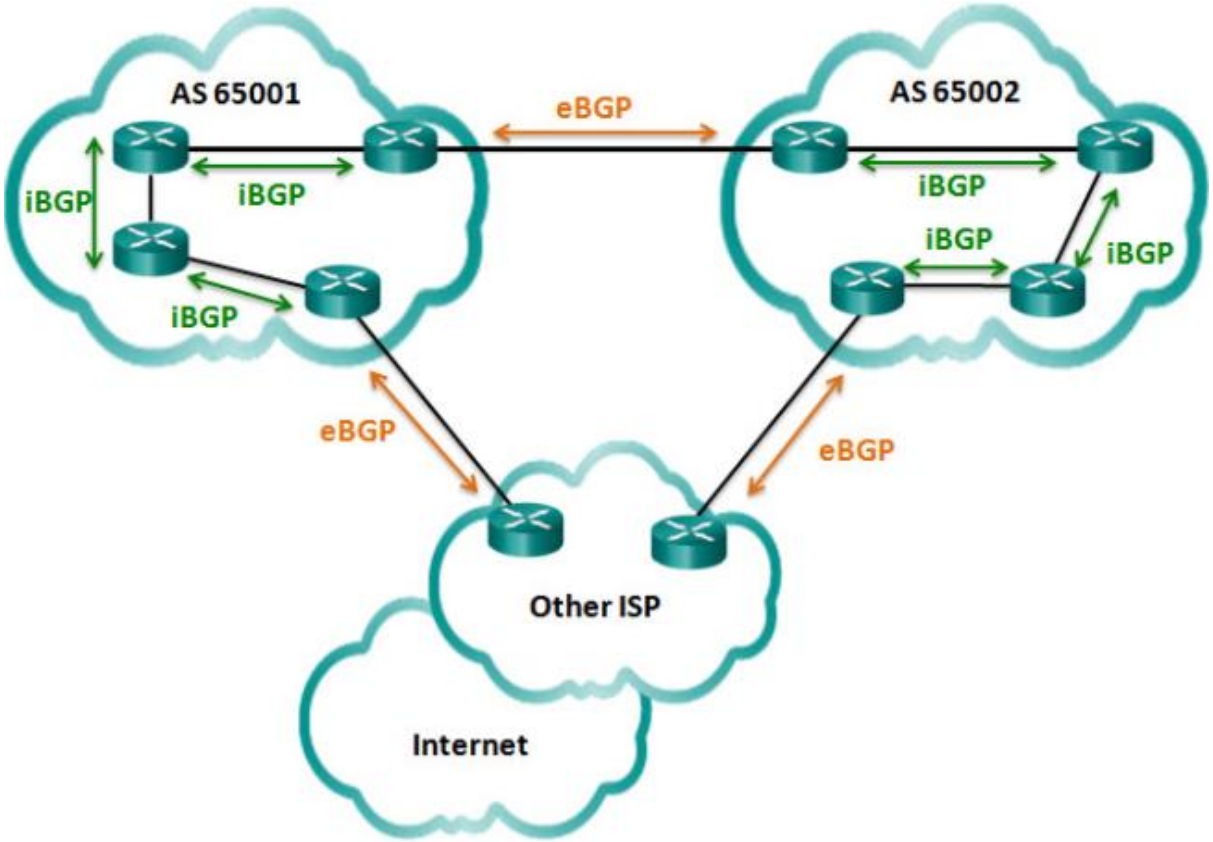
BGP does not use a single metric like IGPs.

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.

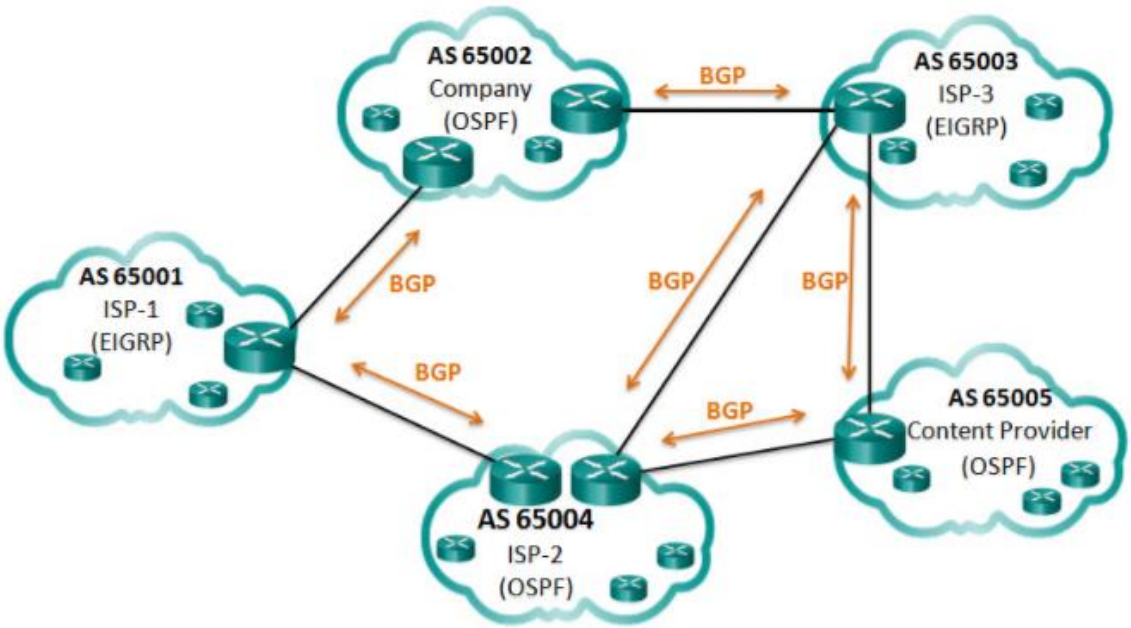
4.4.1.2 – eBGP and iBGP

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



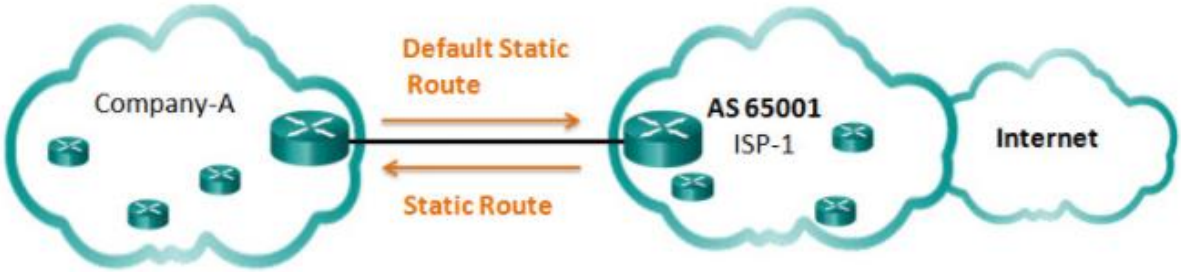
4.4.2.1 – When to use BGP

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.



4.4.2.2 – When not to use BGP

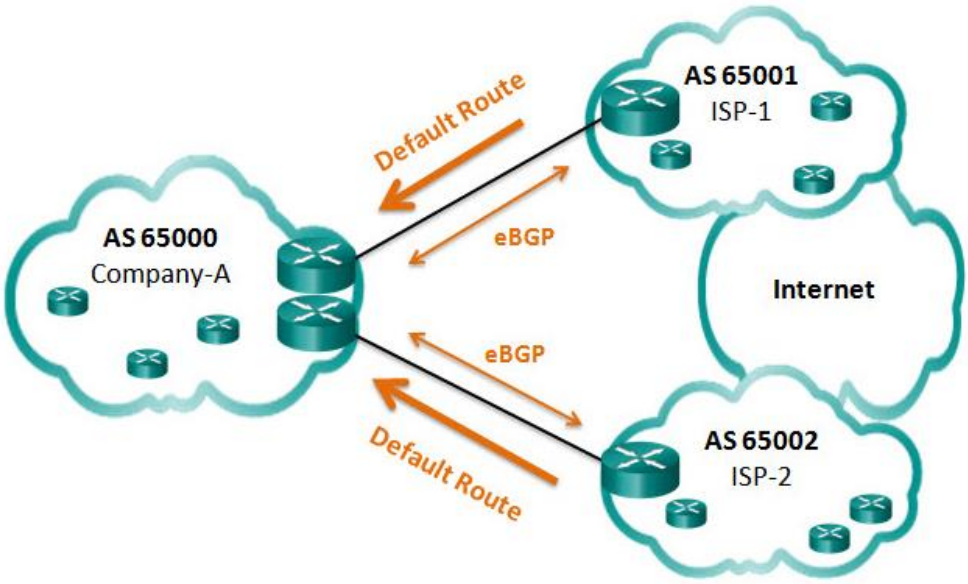
- When there is a **single connection** to the internet or another AS.
- When there is a **limited understanding** of BGP.



4.4.2.3 – BGP Options

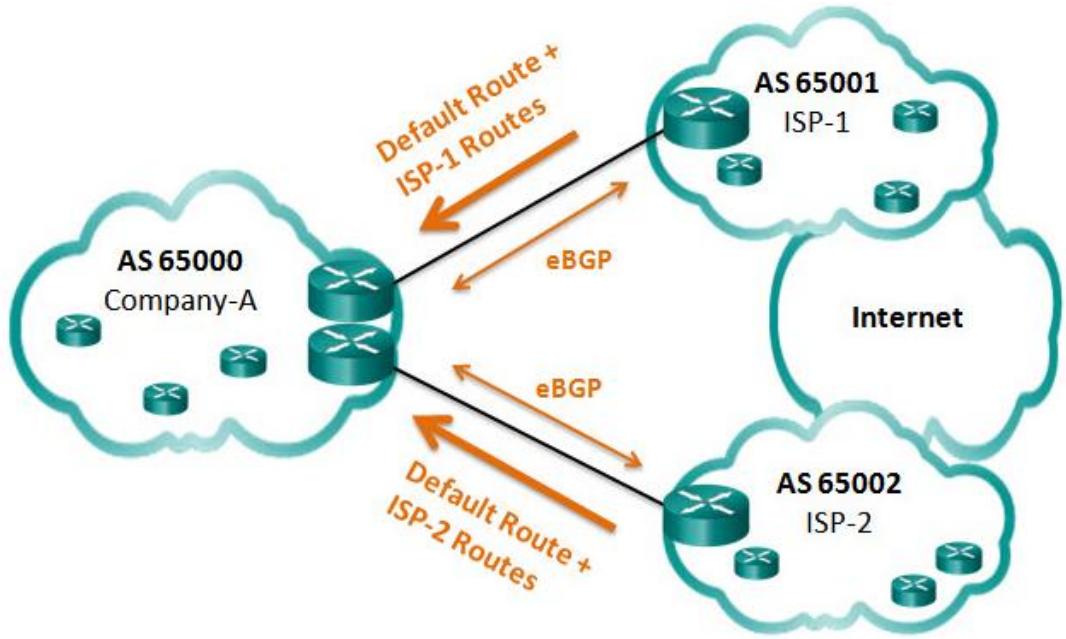
Default Route Only

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.



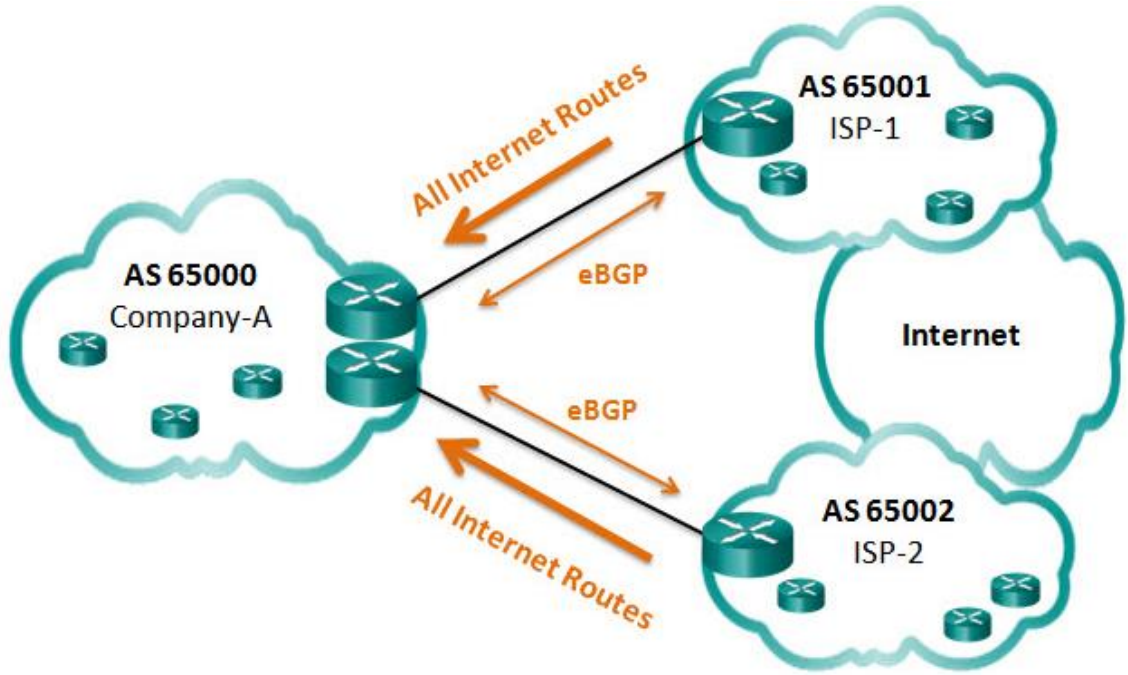
Default Route and ISP Routes

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.



4.4.3.1 – Steps to configure eBGP

Step 1: Enable BGP routing.

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

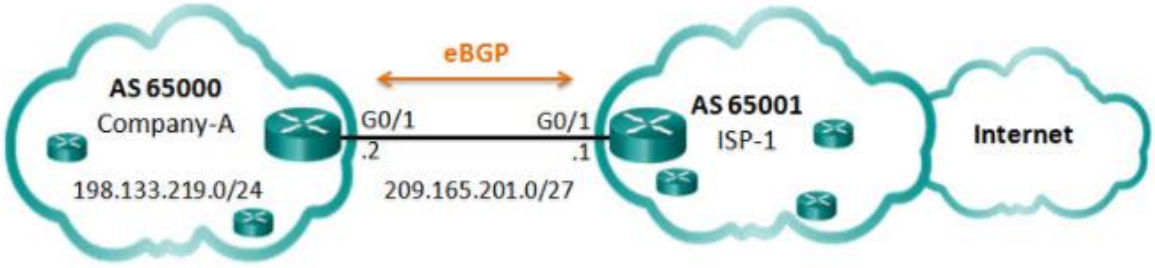
Step 3: Advertise network(s) originating from this AS.

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 it's 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 adverted 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
```

4.5.1.1 – Troubleshooting IPv6 ACLs Overview

Show ipv6 access-list

Show running-config

Most common errors:

- Entering ACLs in the wrong order
- Not specifying adequate ACL rules
- Wrong ACL name
- Wrong Interface
- Wrong direction

4.6.1.1 – DHCP Snooping

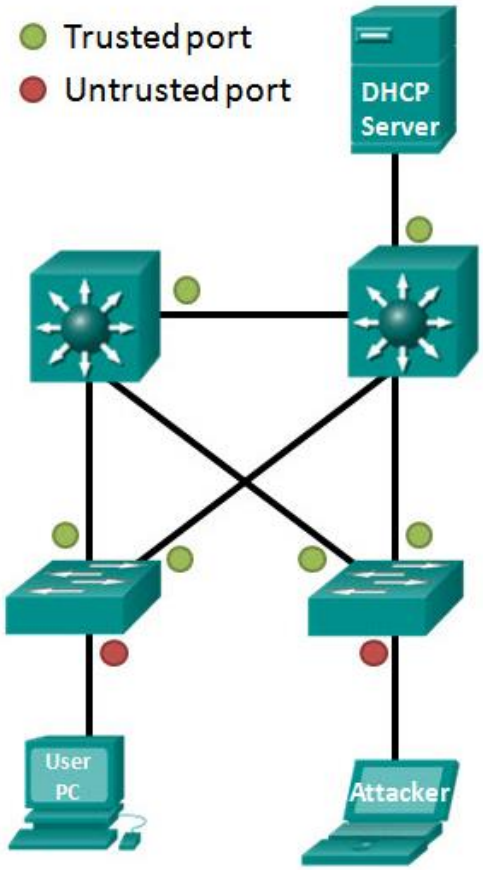
A DHCP spoofing attack occurs when a rouge DHCP server is connected to the network and provides **false IP configuration** parameters to legitimate clients. DHCP spoofing is **dangerous** because clients can be leased IP information such as **malicious DNS server** addresses, **malicious default gateways**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



4.6.1.2 – AAA with RADIUS and TACACS+

To keep **malicious users** from gaining access to sensitive network equipment and services, administers 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:

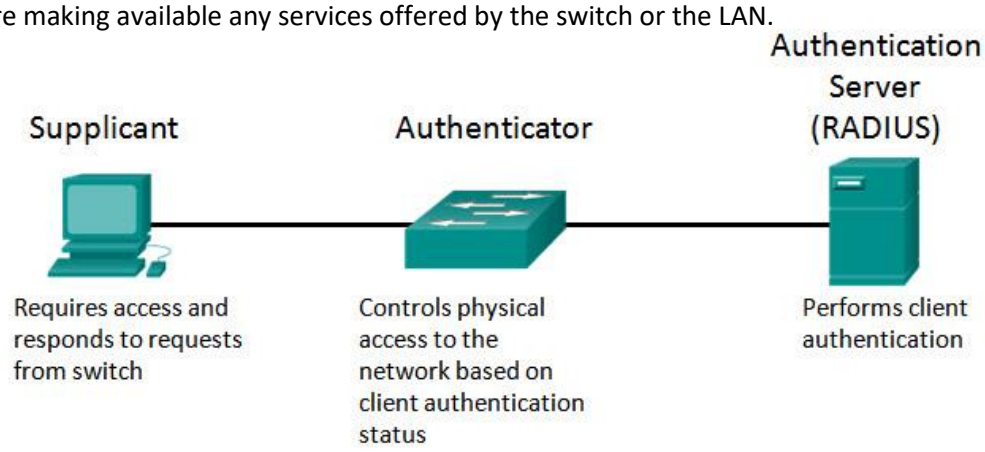
- Separates authentication and authorization
- **Encrypts all communication**
- Utilizes TCP port 49

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**)

4.6.1.3 – 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.

4.7.1.1 – SNMPv3 Overview

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 – Confiure SNMP group user featues 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
```

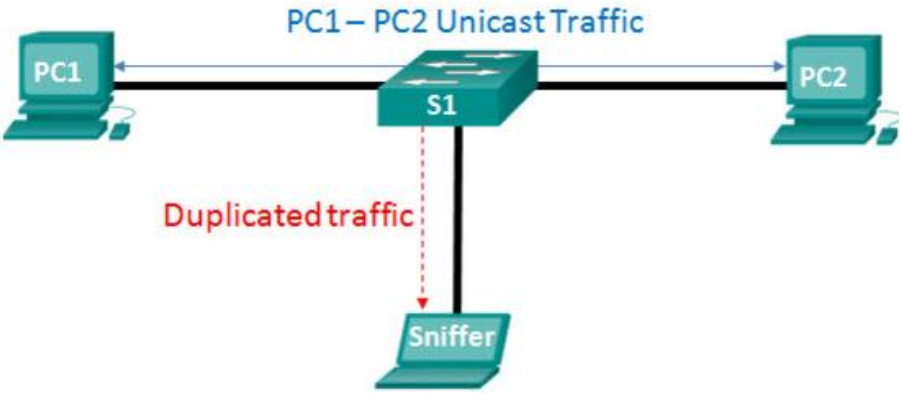
Show snmp user BOB

```
R1# show snmp user BOB


User name: BOB

Engine ID: 800000090300FC994775C3E0

storage-type: nonvolatile     active

Authentication Protocol: SHA

Privacy Protocol: AES128

Group-name: ADMIN
```

4.8.1.1 – Port Mirroring

A packet analyser is typically software such as **Wireshark** that captures packets **entering** and **exiting** a **network interface card**.

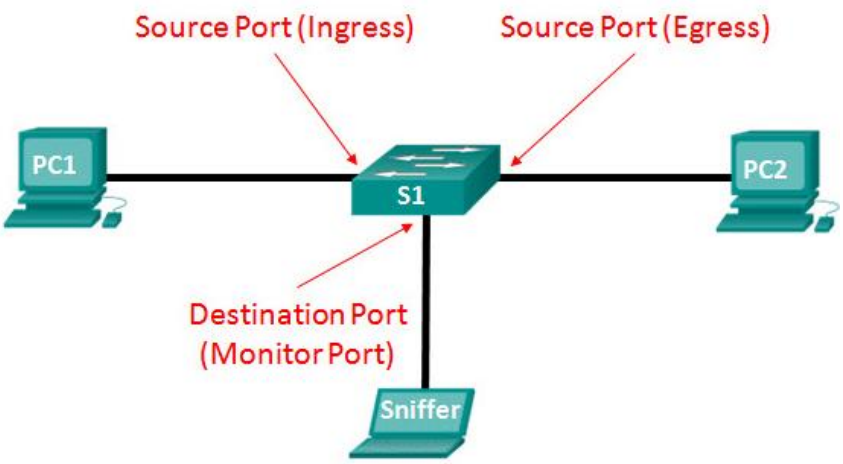
The **port mirroring** feature allows a switch to **copy** and **send Ethernet frames** from specific ports to the destination port connected to a packet analyser. The original frame is still forwarded in the usual manner.



4.8.1.2 – 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:

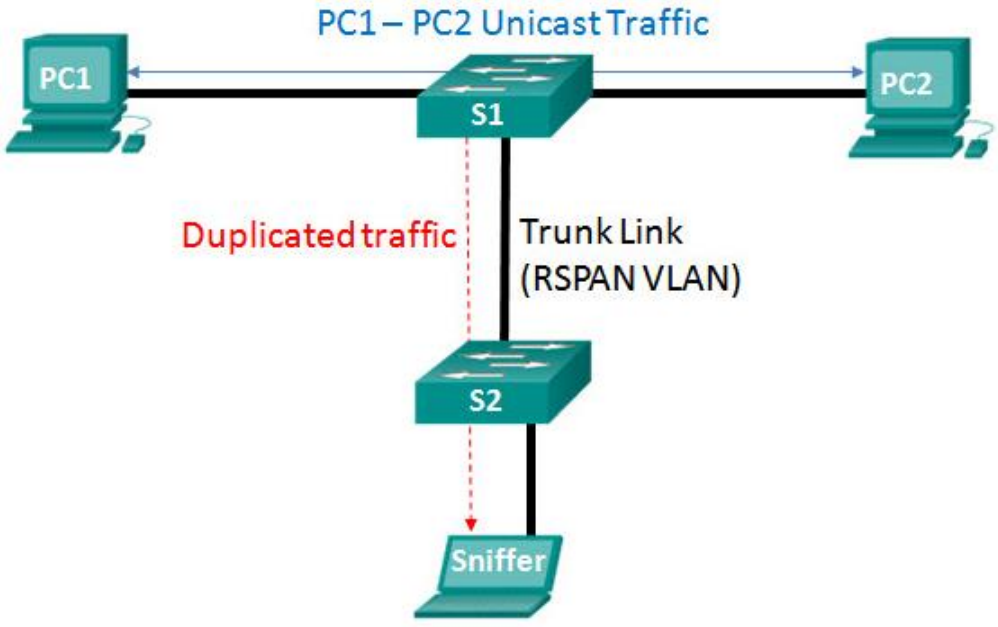
- The **destination port** cannot be a **source port**, and the **source port** cannot be a **destination port**.
- The number of destination port is **platform-dependant.**
- The destination port is no longer a normal switch port. **Only monitored traffic passes** through that port.

4.8.1.3 – Remote SPAN

RSPAN allows **source** and **destination ports** to be in **different switches**. RSPAN is useful in campus networks where a packet analyser is most likely not connected to the same switch on which you need to capture traffic.

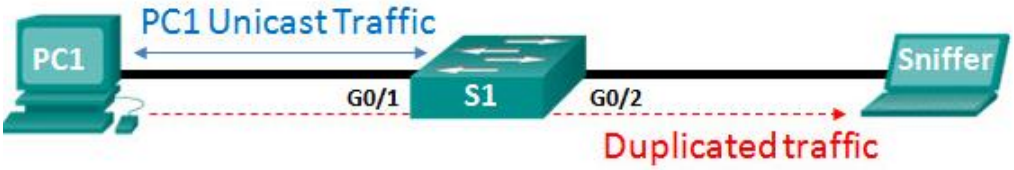
Term	Definition
RSPAN source session	• Source port / VLAN to **copy** traffic from
RSPAN destination session	• Destination VLAN / port to **send** traffic to
RSPAN VLAN	• A unique VLAN is **required** to transport the traffic from one switch to another. • VLAN is configured with the "**remote-span**" vlan configuration command. • This VLAN must be **defined** on **all switches** in the **path** and must be allowed on **trunk** ports between the source and destination.

Remote SPAN uses **two sessions**, one session as the **source** and one session to **copy or receive** the traffic from a VLAN.



4.8.2.1 – Local SPAN Configuration

Configure Local SPAN




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

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

Verify Local SPAN

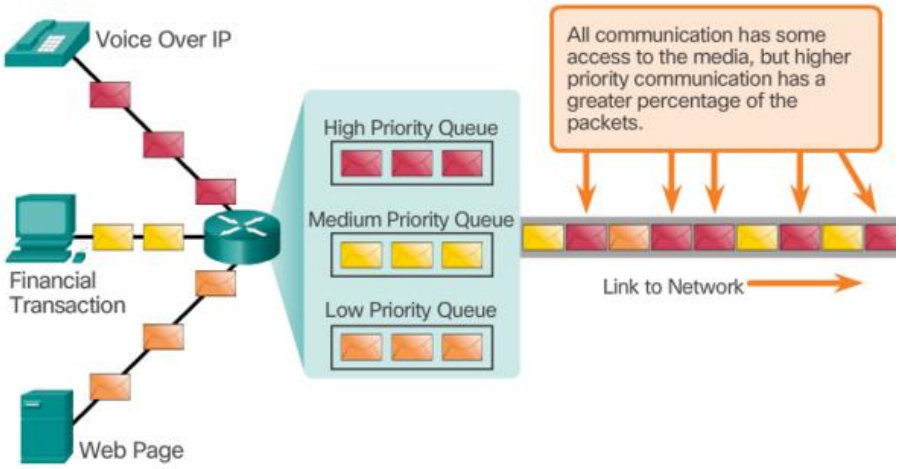
```
S1# show monitor

Session 1

---------

Type                   : Local Session

Source Ports           :

    Both               : Gi0/1

Destination Ports      : Gi0/2

    Encapsulation      : Native

          Ingress      : Disabled
```

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 deceived 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 continuous to increase, the **memory queues** fill up and **packets** are **dropped**.

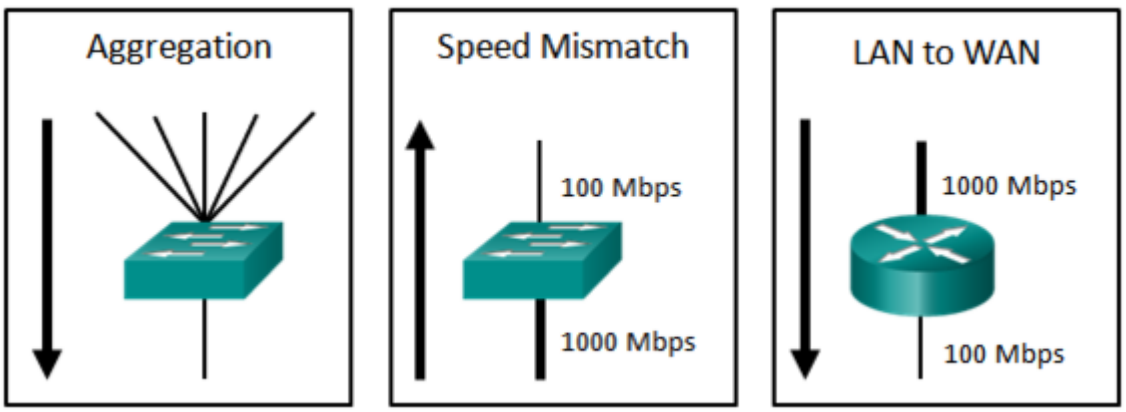


4.9.1.2 – Bandwidth, Congestion, Delay and Jitter

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



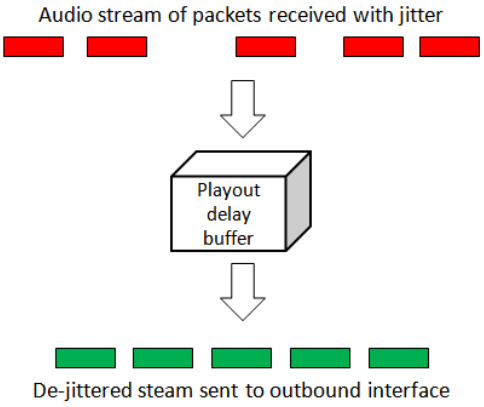
A device only implements QoS when it is experiencing some congestion.

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.

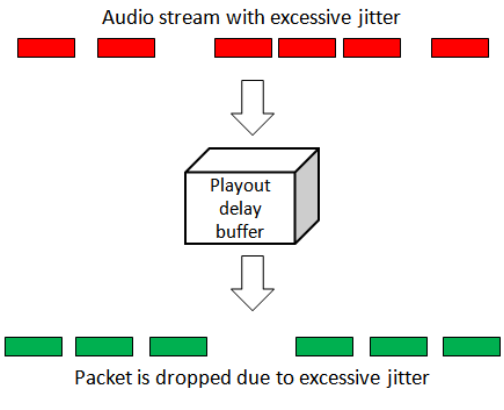
Delay	Description
Code delay	• The fixed amount of time it takes to **compress data at the source** before transmitting to the first interworking device, usually a switch.
Packetization delay	• The fixed time it takes to **encapsulate** a **packet** with all the necessary header information.
Queuing delay	• The variable amount of time a frame or packet waits to be **transmitted on the link**.
Serialization delay	• The fixed amount of time it takes to **transmit** a **frame** from the **NIC** to the **wire**.
Propagation delay	• The variable amount of time it takes for the frame to **travers** the links between the **source** and **destination**.
De-jitter delay	• 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.

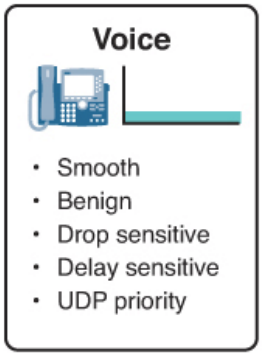


If the jitter is so large that it causes packets to be received out of the range of this buffer, the out of range packets are discarded and dropouts are heard in the audio.



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**.

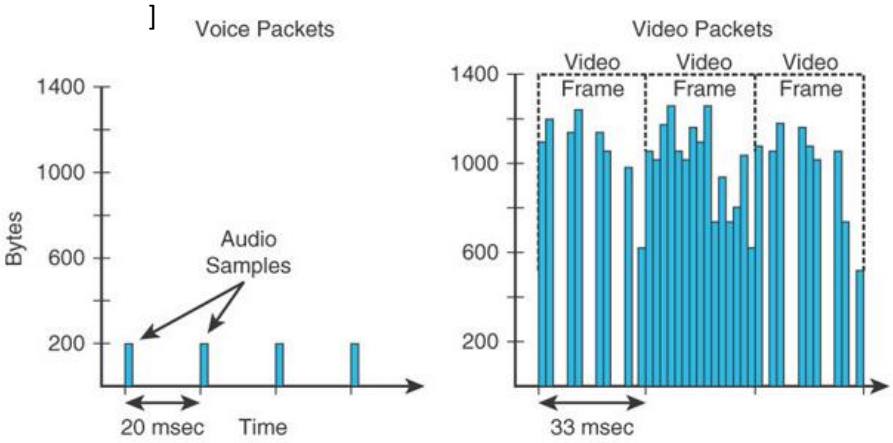


One-Way Requirements
- Latency ≤ 150 ms
- Jitter ≤ 30 ms
- Loss ≤ 1%
- Bandwidth (30–128Kbps)

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.

]

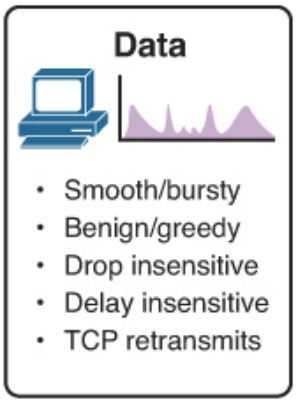


One-Way Requirements
- Latency ≤ 200-400 ms
- Jitter ≤ 30-50 ms
- Loss ≤ 0.1-1%
- Bandwidth (384Kbps–20 + Mbps)

4.9.2.4 – Data

Most applications us 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 list 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)

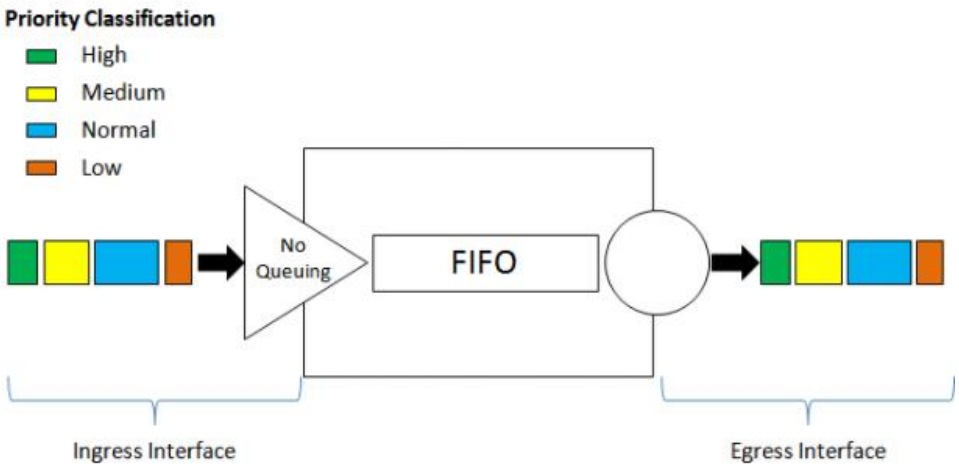
4.9.3.2 – First In First Out (FIFO)

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.

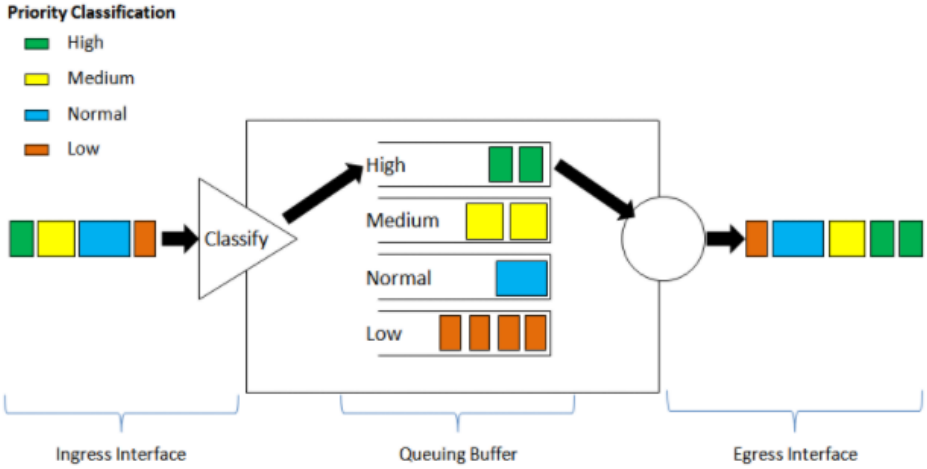
When no other queuing strategies are configured, all interfaces except serial interfaces at E1 (2.048Mbps) and below use FIFO by default.

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.

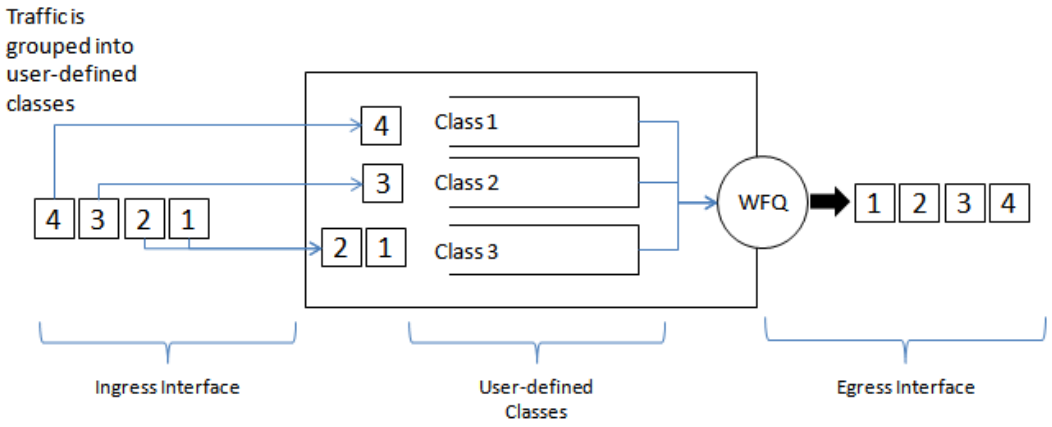
WFQ classifies traffic into different flows based on packet header addressing including such characteristics as **source** and **destination IP addresses**, **MAC addresses**, **port numbers**, **protocol**, **Type of Service**. The ToS value in the IP header can be used to **classify traffic**.

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)

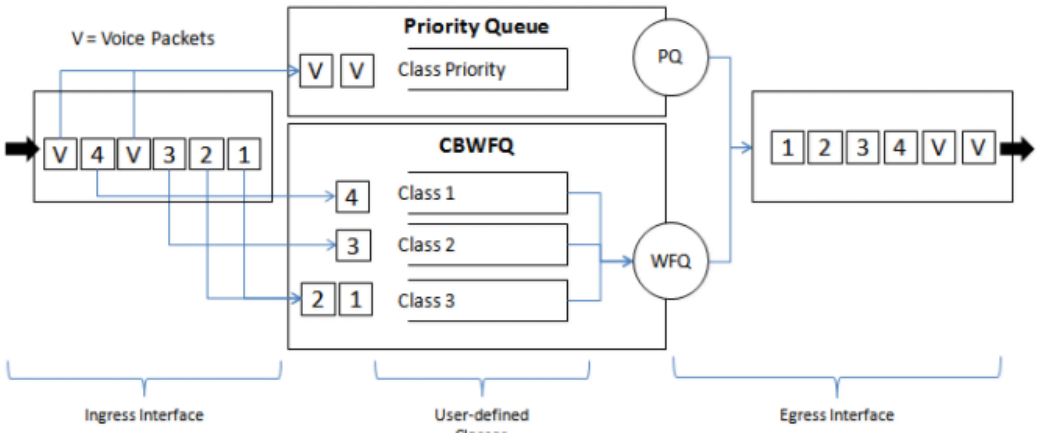
CBWFQ extends the standard WFQ **functionality** to provide support for user-defined traffic classes. For CBWFQ you define traffic classes based on **match criteria** including protocols, ACLs and input interfaces. Packets satisfying the match criteria for a class constitute the traffic to that class. 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 devise recognise traffic classes and proved different levels of QoS to different traffic classes.

4.10.1.2 – Best Effort

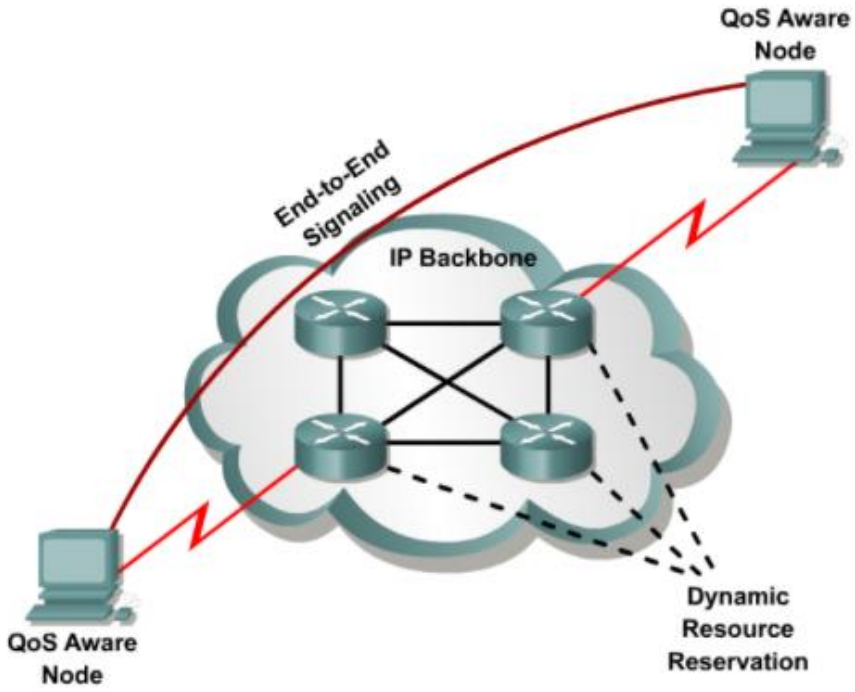
The best effort model **treats all network packets in the same way.** Without QoS, the network cannot tell the difference between packets and as a result cannot treat packets preferentially.

Benefits	Drawbacks
• **Most scalable.** • Scalability is only limited by bandwidth limits. • **No special QoS mechanisms are required.** • The **easiest** and **quickest** model to deploy.	• **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.

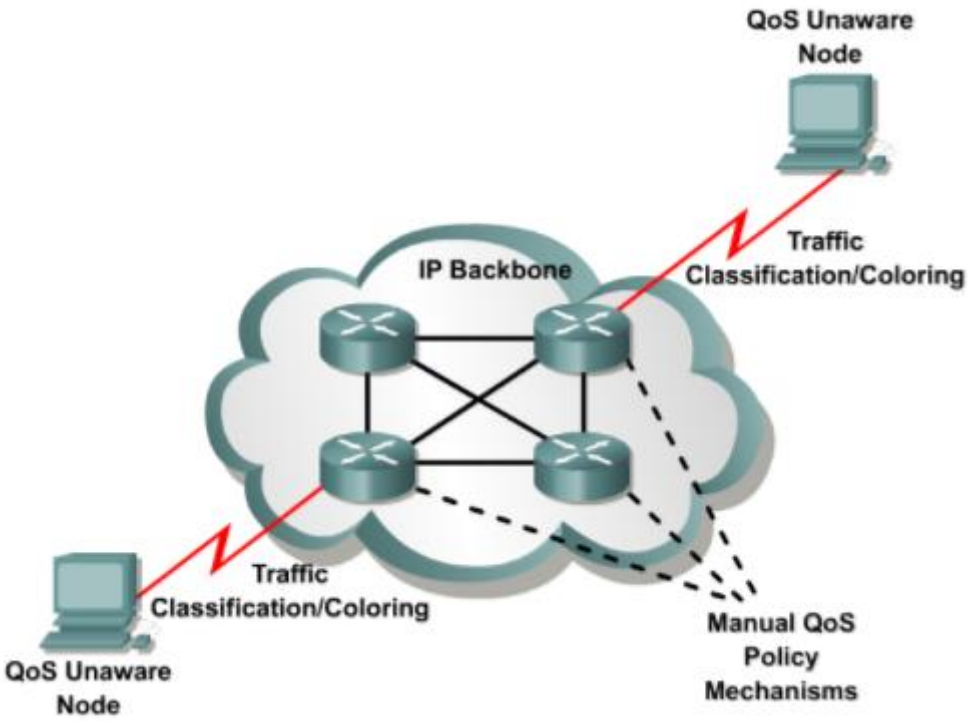
Benefits	Drawbacks
• Explicit **end to end** resource admission control. • **Per-request policy** admission control. • **Signalling** of **dynamic port** numbers.	• **Resource intensive** due to the stateful architecture requirement for continuous signalling. • Flow-based approach **not scalable** to large implementations such as the internet.



4.10.1.4 – Differentiated Services

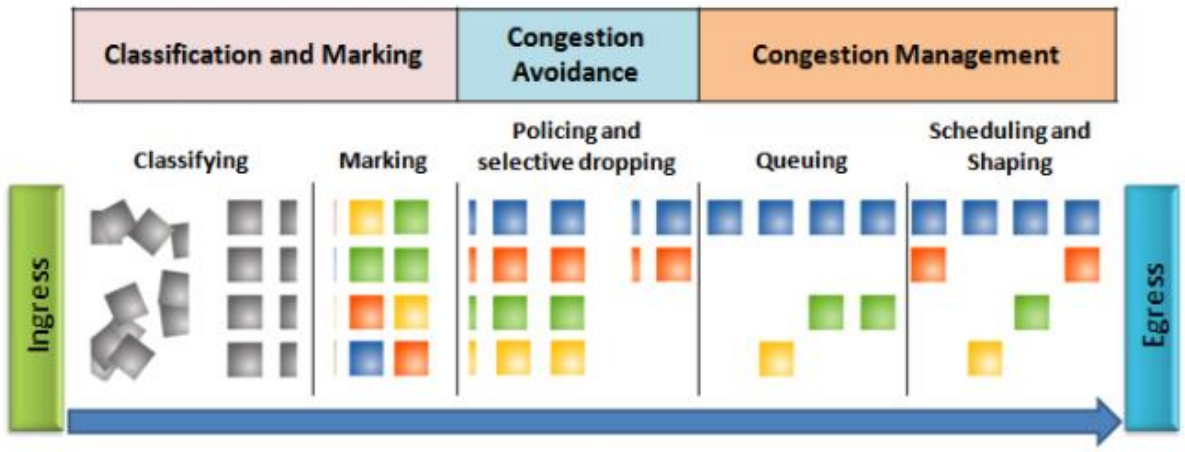
DiffServ QoS model specifies a **simple** and **scalable** mechanism for classifying and managing network traffic and providing QoS guarantees on modern IP networks. DiffServ can provide **low-latency guaranteed service** to critical network traffic such as voice or video while providing simple best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

Benefits	Drawbacks
• **Highly scalable.** • Provides many **different levels** of **quality**.	• 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	• Session or flows are **analysed** to determine what traffic class that belong to. • One determined, the packets are marked.
Congestion avoidance tools	• 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	• 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.

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 delivers over the internet. The user is 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.

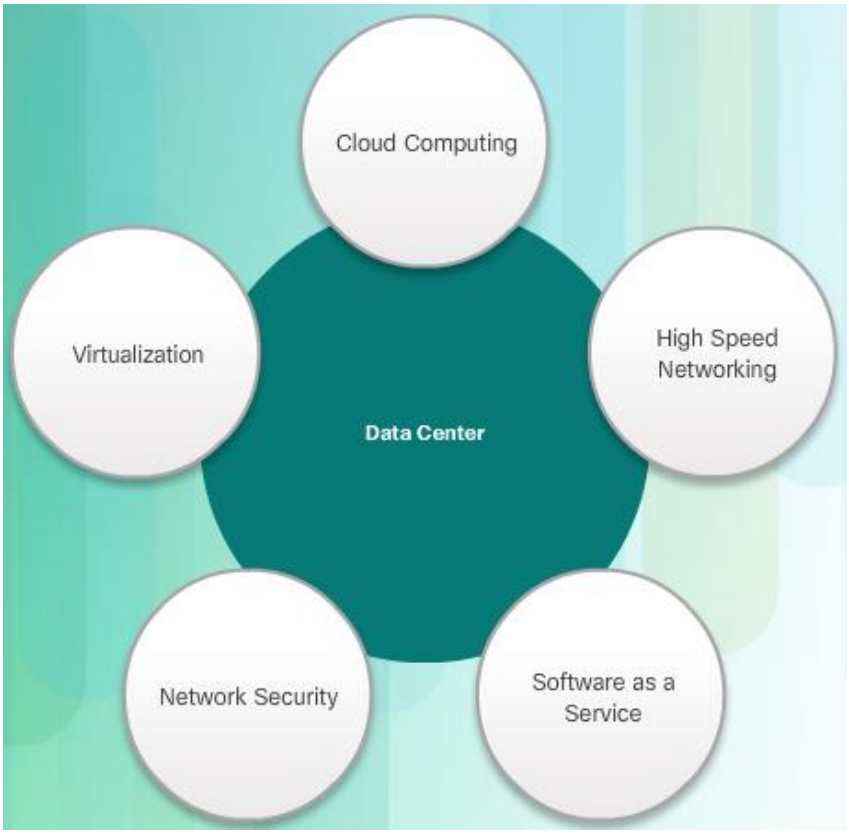
- **Private clouds:** Cloud-based applications are services offered in a private cloud are intended for **specific organization** or **entity** such as the **government**. A private cloud can be set up using the organization's private network, through this can be **expensive** to build and maintain. 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.

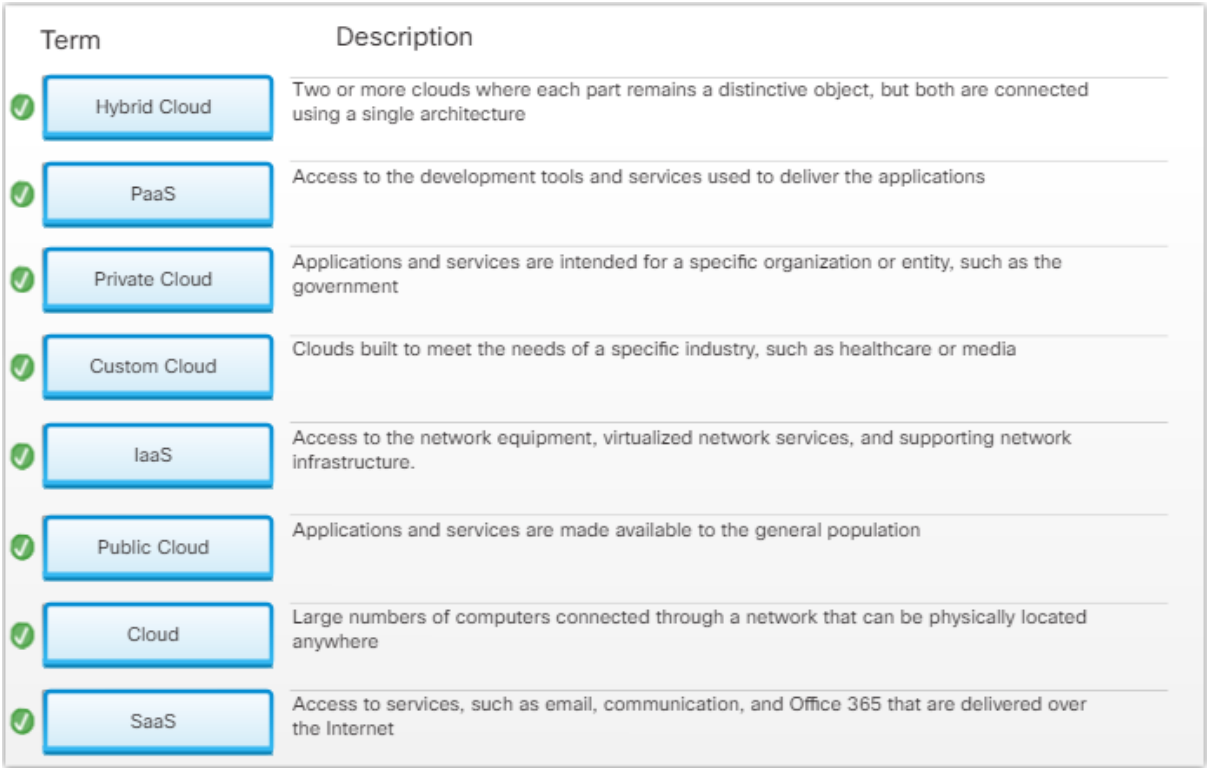
- **Custom clouds:** These are clouds built to meet the needs of a **specific industry**, such as **healthcare** or **media**. Custom clouds can be private or public.

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.



4.11.1.5


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

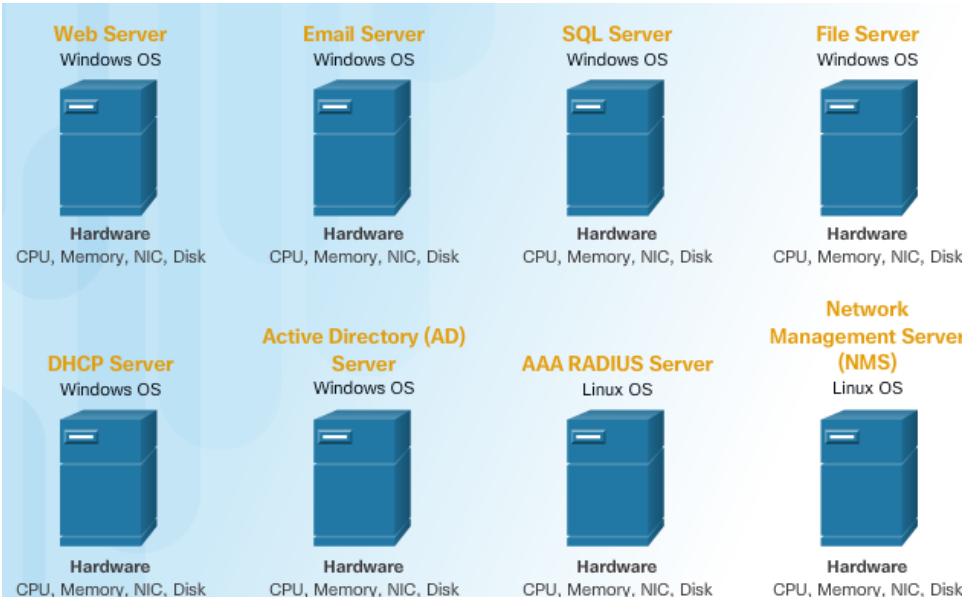
4.11.2.1 – Cloud Computing and Virtualization

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.

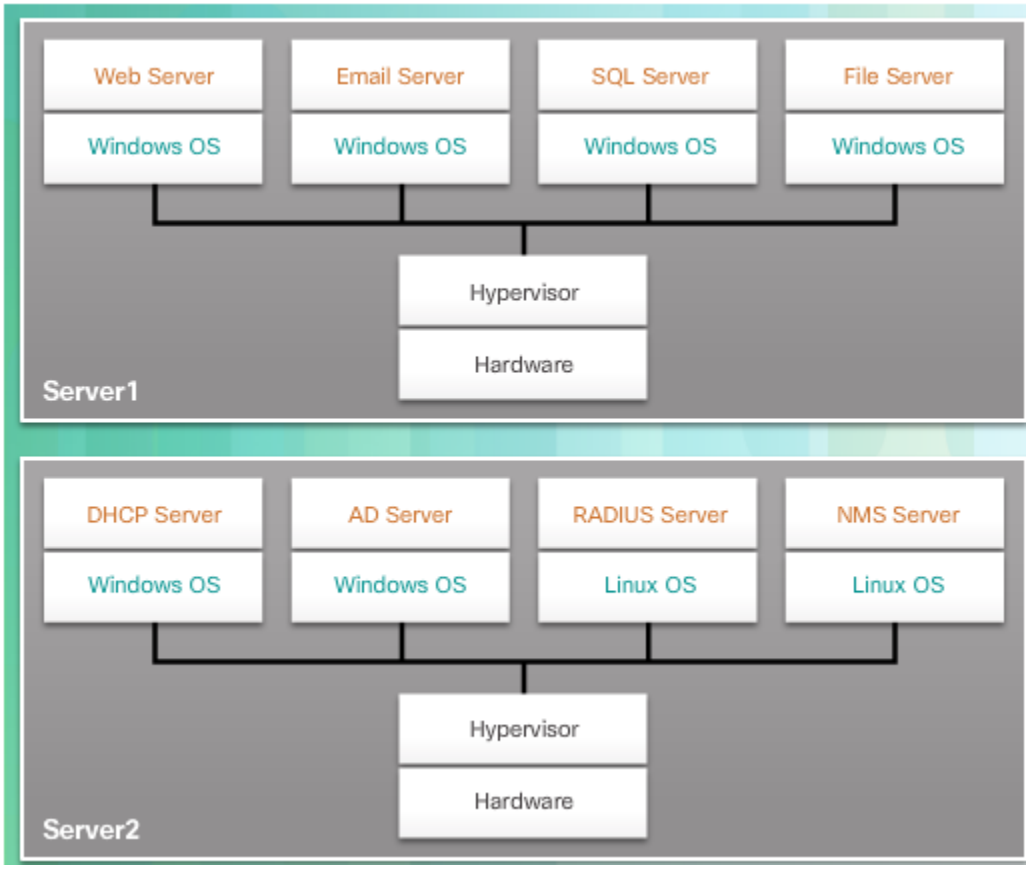


4.11.2.3 – Server Virtualization

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

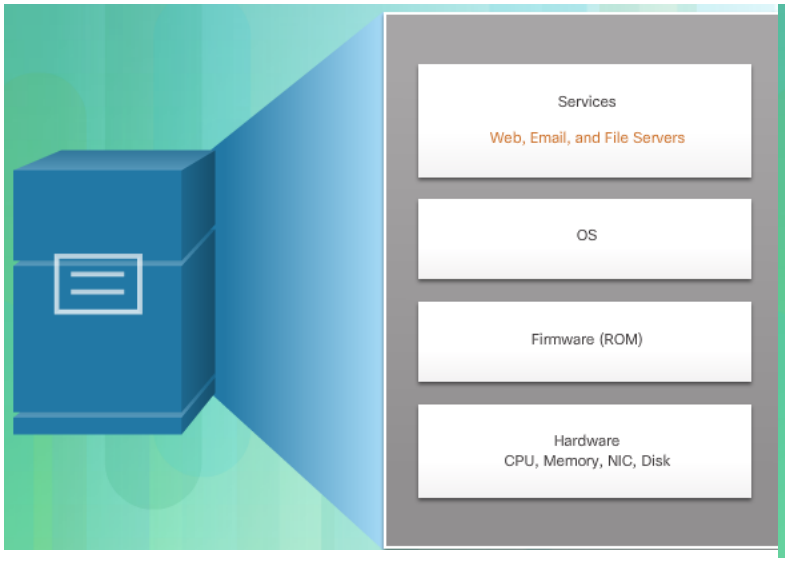
Other advantages

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

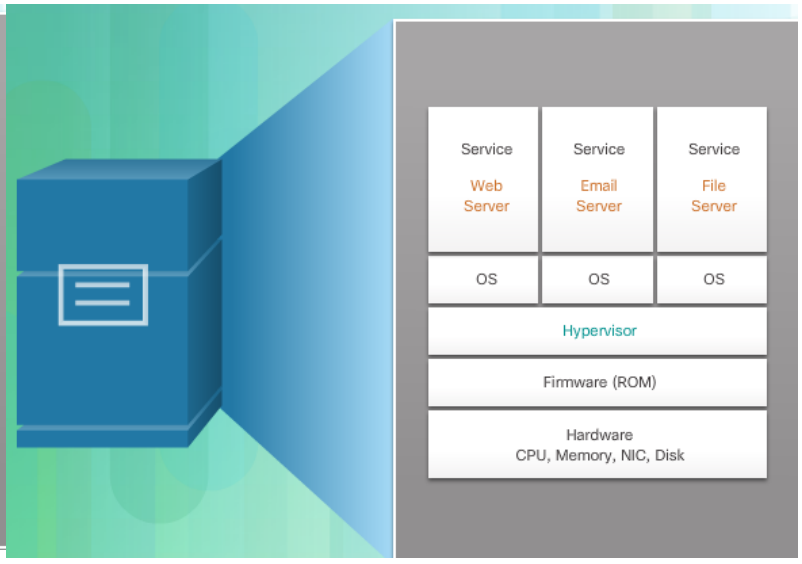
4.11.2.5 – Abstraction Layers

- Services
- OS
- Firmware
- Hardware

Computer Architecture



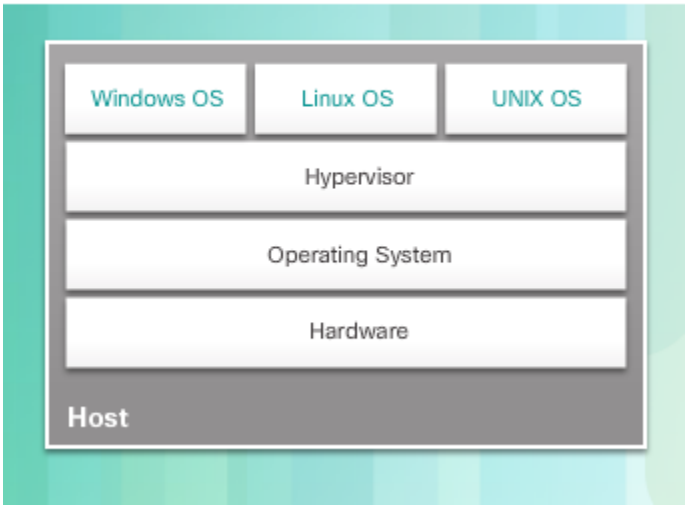
Virtual Architecture



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



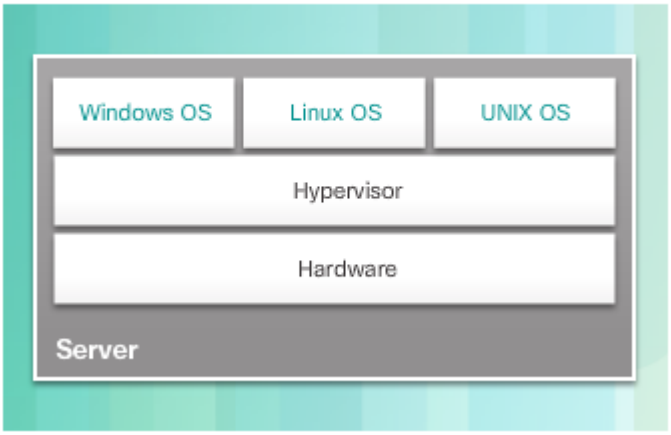
4.11.2.7

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.**