Learning Outcome

1. **Configure static and default route**
   1.1. **Description, Functions, and Features of Router**
      i. **Router hardware components**
         1. Description of a router

The main job of a router is to forward packets based on a routing table. Every router has at least two IP addresses. It's a characteristic of how routers do their jobs. The router's IP addresses are typically the default gateways to PCs, servers or other networking devices. Routers implement layer 3 or network layer functions.

Routers can connect to service providers and act as gateways to other networks, typically found at the perimeter or edge of the network.

Routers don't always have Ethernet interfaces. Gateway routers can connect to external networks through serial interfaces, DSL connections, and other forms of WAN.

The main internal components of a router are similar to those of any computing device: ***CPU, motherboard, RAM, and ROM***. Cisco routers have different types of memory. They also have flash, where the image of the operating system resides.

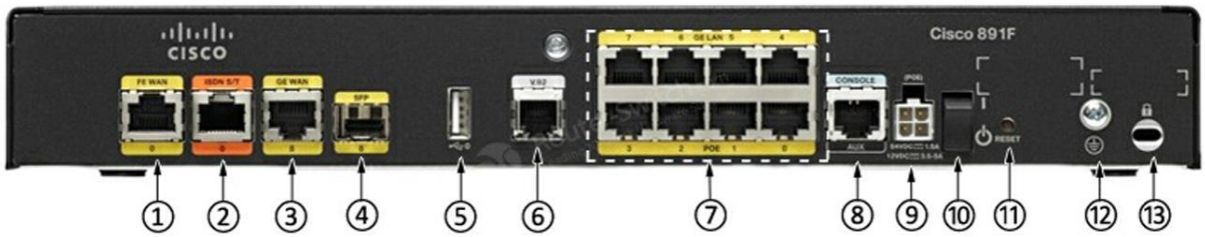
2. Cisco Router's Components

- Interfaces
- The Processor (CPU)
- Internetwork Operating System (IOS)
- RXBoot Image
- RAM
- NVRAM
- ROM
- Flash memory
- Configuration Register

Cisco Router's Interfaces

Interfaces allow us to use the router. They are the various serial ports or Ethernet ports, which we use to connect the router to our LAN.

Let's consider a device Cisco 891F



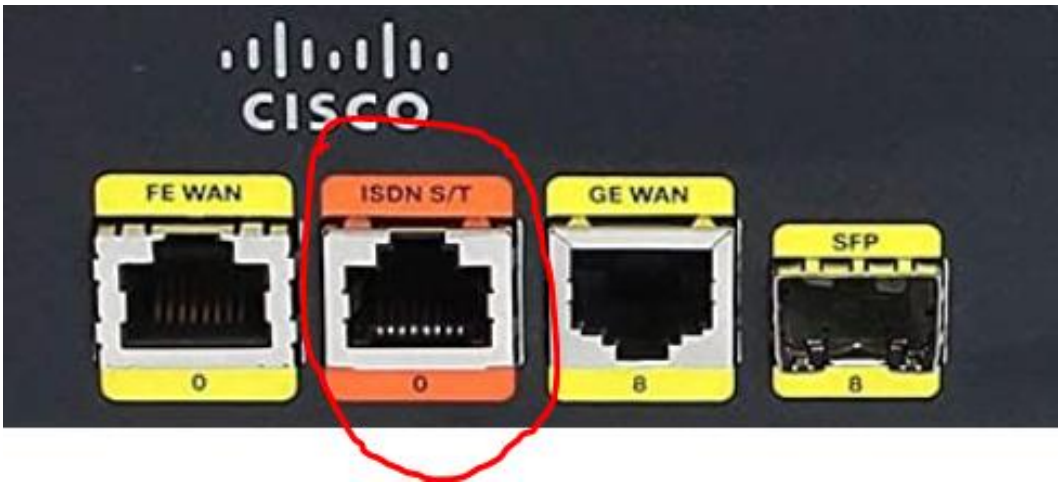
①	Back up WAN port—FE WAN	⑧	Console/Auxiliary port
②	ISDN S/T	⑨	Power connector
③	Primary WAN port—GE WAN	⑩	On/Off switch
④	SFP	⑪	Reset button
⑤	USB port	⑫	Earth ground connection
⑥	V.92 backup	⑬	Kensington security slot
⑦	8 LAN Ethernet Ports (4GE Ports & 4 PoE Ports)		

2.1.1. FE (Fast Ethernet) WAN Port or Backup WAN port

Fast Ethernet WAN Port serves to make backups and load balancing.

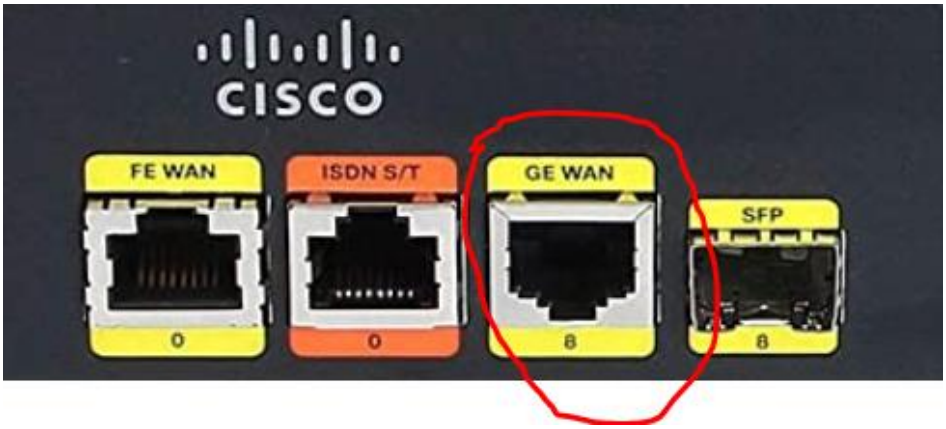
2.1.2. ISDN S/T (Subscriber Terminal)

Integrated Services Digital Network (ISDN) is a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the



digitalized circuits of the Public Switched Telephone Network (PSTN).

2.1.3. Primary WAN port—GE WAN



Gigabit Ethernet (GE) is the evolution beyond Fast Ethernet. It is a lot faster. The "Gigabit" stands for 1 gigabit of data per second, or Gbps. This translates to 1000 Mbps, which you may recognize as being fast.

Dual WAN with FE Port & GE Port

Having two WAN ports, a router can be configured to operate with Dual WAN. This means we can **select two ISP connections to our router**, a primary WAN connected through the GE (Gigabit Ethernet) Port and a secondary WAN connected through FE (Fast Ethernet) port.

There are two modes we can choose to enable when using Dual WAN.

Failover and Failback Mode

In this mode, in order to provide an uninterrupted internet connection, the system will automatically detect our network status by periodically **sending DNS queries to a DNS server** or **sending a ping** to either the default gateway or the address we specified in the configuration.

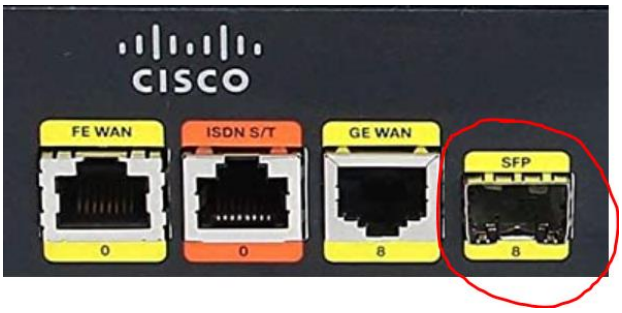
When our primary WAN connected through the GE (Gigabit Ethernet) Port fails, our router will switch to the backup network connected through the FE (Fast Ethernet) port, which allows your Internet connection to continue working after an error has occurred.

When the primary WAN (at GE Port) has been detected and is connected to the internet by using a physical cable, our connection will revert to the Primary WAN as long as **failback** has been enabled.

Load Balance Mode

When the Load Balance Mode is enabled, we can distribute the load between the Primary WAN (at GE Port) and Backup WAN (at FE). By enabling routing rules and adding rules appropriately, we can route requests from a particular device through the Primary WAN or Secondary (Backup) WAN.

2.1.4. SFP (Small Form-factor Pluggable)



An SFP port connection enables the transfer of data between **two faraway network devices** via an SFP transceiver and appropriate cabling. In other words, the port and its corresponding SFP transceiver allow the two network devices to communicate with each other over an extended distance.

SFP socket enables interfacing two faraway network devices using a fiber optic or copper networking cable. **SFP is hot-plugged**. A hot-plugged (also known as hot-swappable) device is a device that is added or removed to the

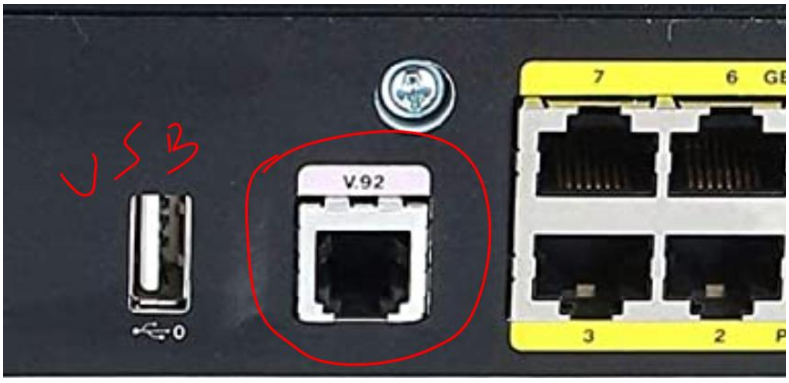
system without having to shut down the operating system or to power off the system.

2.1.5. USB Port

The Universal Serial Bus (USB) ports on the router enable important security and provisioning capabilities, including secure device authentication, storage of removable credentials for establishing secure VPN connections, secure distribution of configuration files, bulk flash storage for files and configuration, and booting from the USB.

Two new features are available to take advantage of these USB ports: USB eToken device support and USB flash support.

2.1.6. V.92 Backup Port



V.92 provides dial backup and remote management functions if the main WAN link fails.

V.92 is an ITU-T recommendation, titled Enhancements to Recommendation V.90, that establishes a modem standard allowing near 56 kb/s download and 48 kb/s upload rates.

2.1.7. 8xLAN Ethernet Ports (4xGE Ports & 4xPoE Ports)

The LAN port allows a computer to connect to a network using a wired connection. 4 among this group of 8 LAN ports are GE (Gigabit Ethernet) ports and the remaining 4 ports are PoE.

Power over Ethernet (PoE) is a technology that passes electric power over twisted-pair Ethernet cable to powered devices (PD), such as wireless access points, IP cameras, and VoIP phones in addition to the data that cable usually carries. **It enables one RJ45 cable to provide both data connection and electric power to PDs instead of having a separate cable for each**.

In a PoE system, power-source equipment (PSE) injects 56.5 V at a maximum current level of 350 mA onto a standard Ethernet LAN cable. Maximum power at the Ethernet switch is 15.4 W per PSE port.

2.1.8. Console/Auxiliary port

The console port is used to connect a computer directly to a router or switch and manage the router or switch since there is no display device for a router or switch. The console port must be used to initially configure routers.

Console vs. AUX

On a router, the console port is used to directly connect the router to a PC using **serial communication** (terminal emulation) programs like **minicom**, **screen**, **Putty** on Linux and HyperTerminal, Putty on Windows. The router is connected to the PC using a console cable and no network connection is involved.

The AUX port is used for a dial in access to the router. *The AUX port is connected to a modem, which in turn is connected to the phone line*. A user with a PC, connected to a modem and phone line, can then dial the phone number of the modem connected with the router and get access to the router console remotely.

2.1.9. Power connector (Supporting PoE)

2.1.10. On/Off Switch

2.1.11. Reset Button

A factory reset button can be used to completely wipe the device. Factory resetting our Cisco router will remove all of our current settings, including our network name and WiFi password.

2.1.12. Earth Ground Connection

Earthing is used to protect people from an electric shock. It does this by providing a path (a protective conductor) for a fault current to flow to the earth. These losses of current may occur, for example, when a damaged power cable is stripped and the electrical wires come into contact with the device's casing. Without an earth or ground wire, the current would pass through the body of the first person who might touch the device: this is electrocution.

2.1.13. Kensington security slot

A Kensington Security Slot is part of an anti-theft system

Cisco Router's Internal Components

1. The Processor (CPU)

All Cisco routers have a main processor that takes care of the main functions of the router. The CPU generates interrupts (IRQ) in order to communicate with the other electronic components in the router. Usually, the CPU utilization on a normal router wouldn't exceed 20%.

2. The IOS

The IOS is the main operating system on which the router runs. The IOS is loaded upon the router's bootup. It usually is around 2 to 5MB in size, but can be a lot larger depending on the router series.

3. The RXBoot Image

The RXBoot image (also known as Bootloader) is nothing more than a "cut-down" version of the IOS located in the router's ROM (Read Only Memory). If you have no Flash card to load the IOS from, you can configure the router to load the RXBoot image, which would give you the ability to perform minor maintenance operations and bring various interfaces up or down.

4. The RAM

The RAM, or Random Access Memory, is where the router loads the IOS and the configuration file. It works exactly the same way as your computer's memory, where the operating system loads along with all the various programs.

5. The NVRAM (No-Volatile RAM)

The NVRAM is a special memory place where the router holds its configuration. When you configure a router and then save the configuration, it is stored in the NVRAM.

6. ROM (Read Only Memory)

The ROM is used to start and maintain the router. It contains some code, like Bootstrap and POST, which helps the router do some basic tests and bootup when it's powered on or reloaded. You cannot alter any of the code in this memory as it has been set from the factory and is Read Only.

7. Flash Memory

EEPROM (Electrical Erasable Programmable Read Only Memory) card. It fits into a special slot normally located at the back of the router and contains nothing more than the IOS image(s). You can write to it or delete its contents from the router's console. Usually, it comes in sizes of 4MB for the smaller routers (1600 series) and goes up from there depending on the router model.

8. Configuration Register

The Configuration Register determines if the router is going to boot the IOS image from its Flash, TFTP server or just load the RXBoot image. This register is a 16-bit register, in other words has 16 zeros or ones. A sample of it in Hex would be the following: 0x2102 and in binary is: 0010 0001 0000 0010.

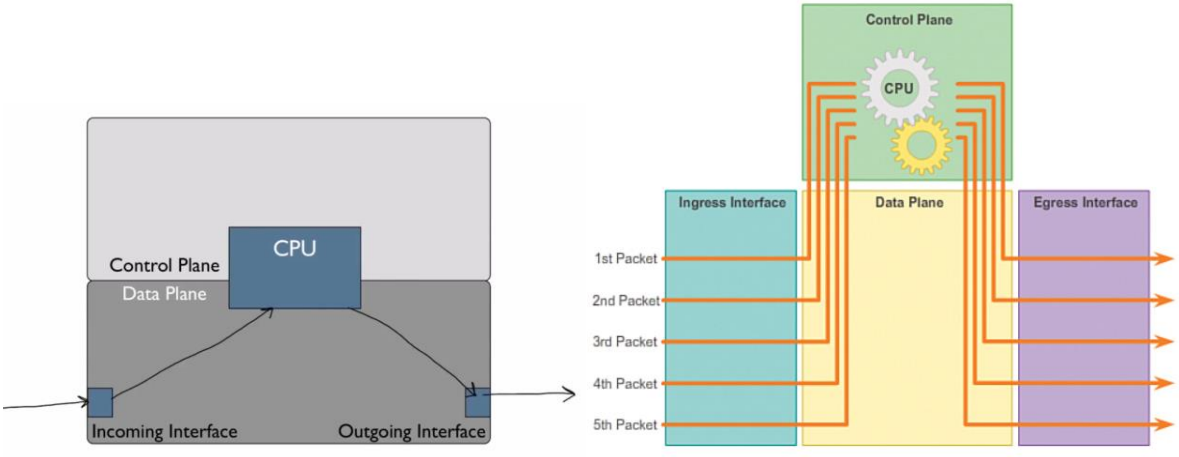
ii. Packet Forwarding mechanisms

Routers support three packet-forwarding mechanisms: **Process forwarding, Fast switching or fast forwarding, and Cisco Express forwarding.**

1. Process switching or Process Forwarding

Process switching is an older packet-forwarding mechanism still available for Cisco routers. When a packet arrives on an interface, it is forwarded to the control plane, where the CPU matches the destination address with an entry in its routing table, and then determines the exit interface and forwards the packet.

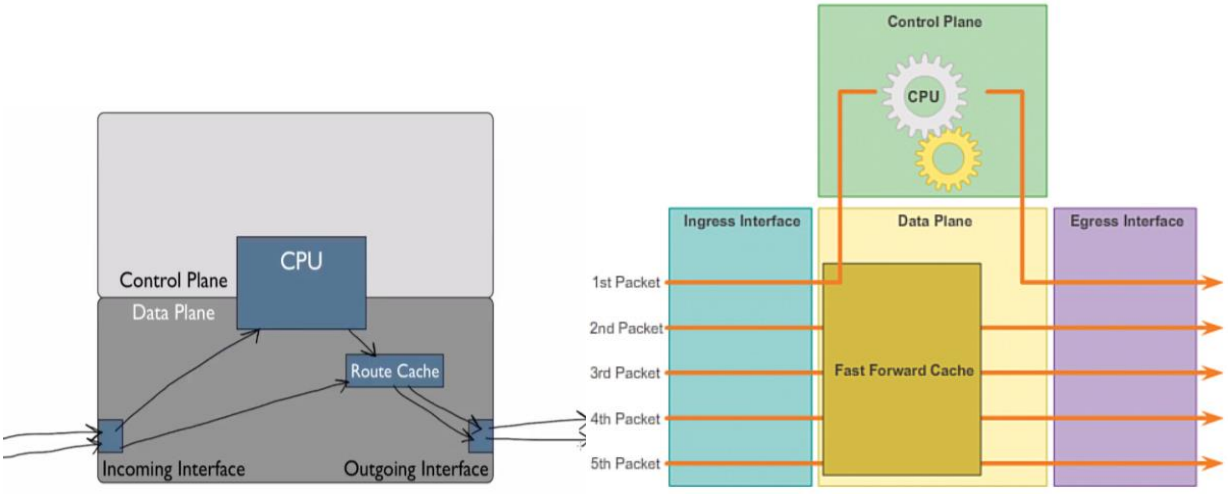
Assuming a traffic flow consisting of five packets all going to the same destination, with process switching, each packet must be processed by the CPU individually.



2. Fast Switching or Fast Forwarding

This is a common packet-forwarding mechanism that uses a fast-switching **cache to store next-hop** information. When a packet arrives on an interface, it is forwarded to the control plane, where the CPU searches for a match in the fast-switching cache. If it is not there, it is process-switched and forwarded to the exit interface. The flow information for the packet is also stored in the fast-switching cache. If another packet going to the same destina tion arrives on an interface, the **next-hop information in the cache is re-used without CPU intervention**

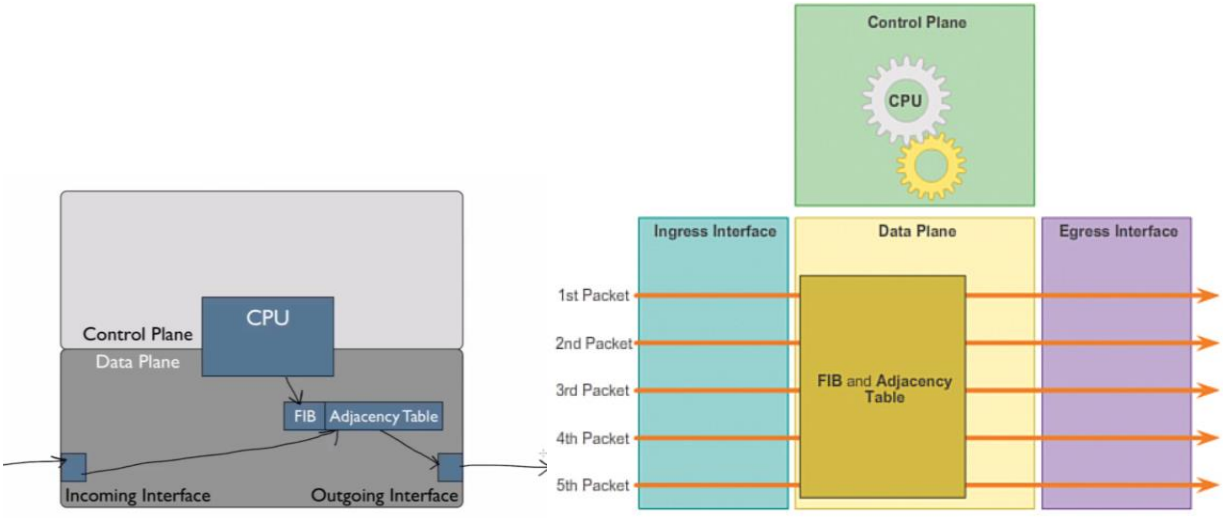
Assuming a traffic flow consisting of five packets all going to the same destination, with fast switching, notice how only the first packet of a flow is process-switched and added to the fast-switching cache. The next four packets are quickly processed based on the information in the fast-switching cache.



Route cache: stores packet-forwarding information for destination networks, this information is learned when the CPU is used to route a packet to each of those networks.

3. Cisco Express Forwarding (CEF)

CEF is the most recent and preferred Cisco IOS packet-forwarding mechanism. Like fast switching, CEF builds a **Forwarding Information Base** (FIB) and an **adjacency table**. However, the table entries are not packet-triggered like fast switching but change-triggered such as when something changes in the network topology. Therefore, when a network has converged, the FIB and adjacency tables contain all the information a router would have to consider when forwarding a packet. **The reverse lookups and next-hop information for routes**, including the interface and Layer 2 information. Cisco Express Forwarding is the fastest forwarding mechanism and the preferred choice on Cisco routers.



FIB (Forwarding information base): Stores layer 3 routing information that it learns from the IP routing table.

Adjacency table: stores information on whom to construct the layer 2 header for a next-hop IP address

A **common analogy** used to describe the three packet-forwarding mechanisms is as follows:

- Process switching solves a problem by doing math long hand, even if it is an identical problem.

- Fast switching solves a problem by doing math long hand one time and remembering the answer for subsequent identical problems.

- CEF solves every possible problem ahead of time in a spreadsheet.

iii. Default Gateways

A default gateway is a hardware connection that helps smooth links between networks, typically enabling one computer to communicate with the different computers on a separate network.

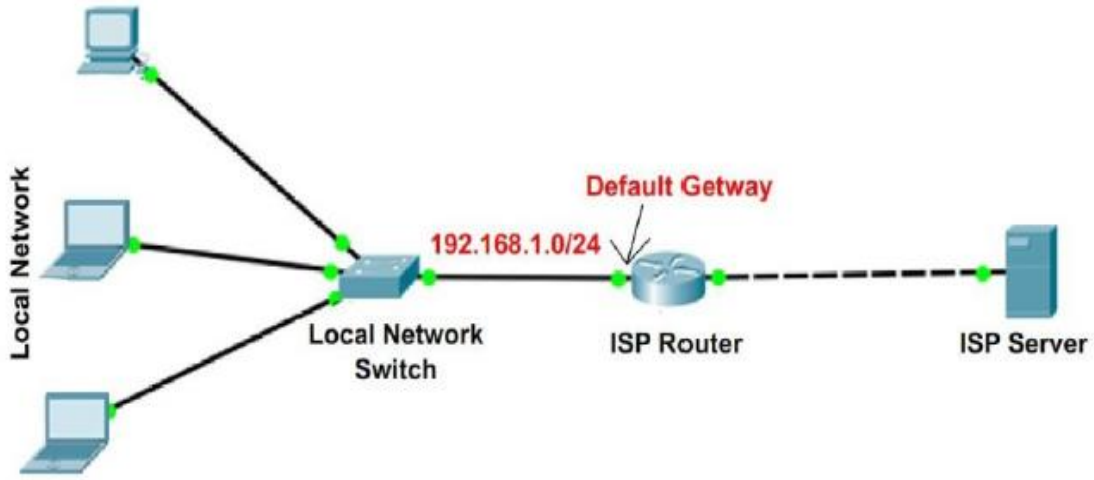
Let's see how we can find the default gateway:

- On Windows we can find the default gateway by the command **ipconfig.**

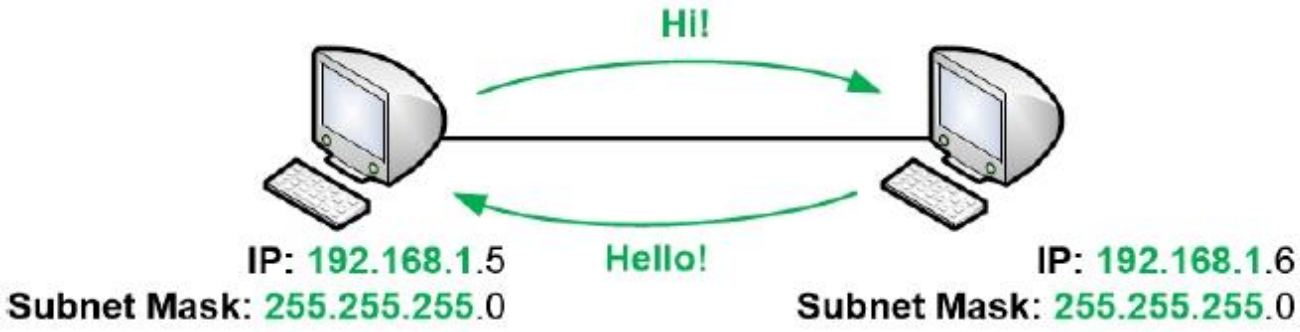
- On Linux we can find the default gateway by the command **ip route | grep default.**

It's also possible to find the default gateway by the command **netstat -r** either on Windows or Linux.

Default gateways are actually routing systems tasked with ensuring the request is sent to the correct destination, even if the sender and receiver practice different network protocols.



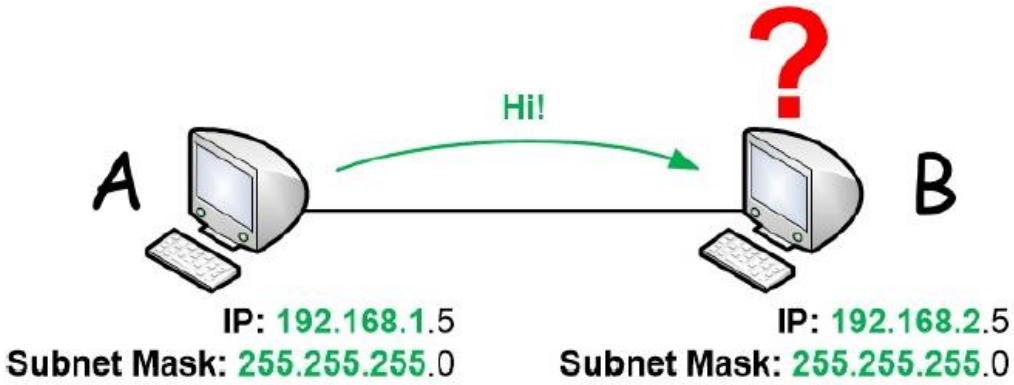
A computer that has an IP address and a Subnet Mask can talk directly with other computers that share the same Subnet Mask and have IP addresses within the same IP network. In fact, when a node sends a packet to another node on the same network the gateway address is not used.



But what about a computer that wants to talk with a node that has an IP address on another IP network?

Let's illustrate the role of a default gateway by an example where computer A belongs to IP network

192.168.1.0 and computer B belongs to IP network 192.168.2.0 – two different IP networks.



Since the communication between two IP networks requires a router to be used, both computers A and B need to communicate via a router. But how does the traffic actually end up in a router?

To find its local router the computer needs a so-called **Default Gateway**, sometimes simply called a **Gateway**. **A Default Gateway** is always a router that can connect to more than one IP network and can route traffic between those IP networks. The router will have its own IP address on each IP network that it connects to.

A computer can only talk with other IP addresses within its own IP network. So for the computer to be able to communicate via a router, at least one of the router's IP addresses must belong to the same IP network as the computer.

When the router hands out an IP address and a Subnet Mask to the computer it also sends out its own IP address to the computer and tells the computer to use that address as its **Default Gateway**.

With the help of the Default Gateway address, the computers can then find their way to all other IP networks in the whole world. The router takes over responsibility for routing the traffic towards the destination on the Internet.

If you are forwarding traffic in the same network, you don't use the default gateway. The host device uses ARP to find the MAC address corresponding to the local IP address for which it is trying to communicate.

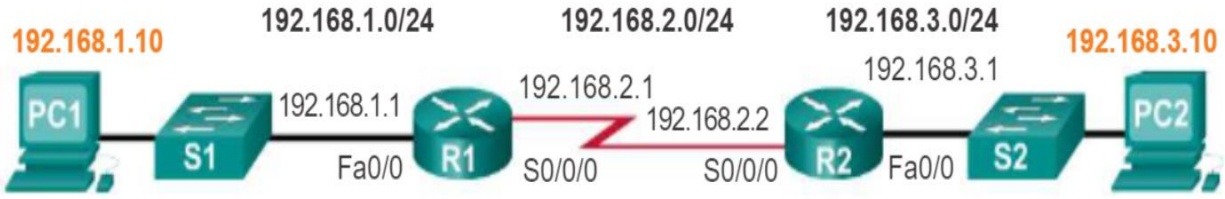
iv. Document network addressing

When designing a new network or mapping an existing network, the network should be documented. At a minimum, the documentation should identify:

- Device names
- Interfaces used in the design
- IP addresses and subnet masks
- Default gateway addresses

In order to capture the information regarding the network two useful network documents must be created:

Document 1: Topology diagram that provides a visual reference that indicates the physical connectivity and logical Layer 3 addressing.



Often created using software, such as Microsoft Visio.

Document 2: Addressing table that captures device names, interfaces, IPv4 addresses, subnet masks, and default gateway addresses.

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

v. Console access

Every Cisco router or switch has a console port (also known as the management port) on its backside. Console port is used to connect a computer directly to a router or switch and manage the router or switch since there is no display device for a router or switch.

The console port is the only one way to initially configure routers before setting up virtual teletypes (VTY) i.e SSH and Telnet.

SSH or telnet allows us to connect to the router from anywhere on the network without any need of a console cable.

A special type of cable, known as rollover cable is used to connect the Serial/COM port of the computer to the router or switch console port. One end of the cable is RJ49 type while the other end is DB9.

DB9 Connector to RJ45 Cat5 Ethernet Adapter Cable

Fig: DB9 Connector to RJ45 Cat5 Ethernet Adapter Cable for Routers Network

Rollover wire cable

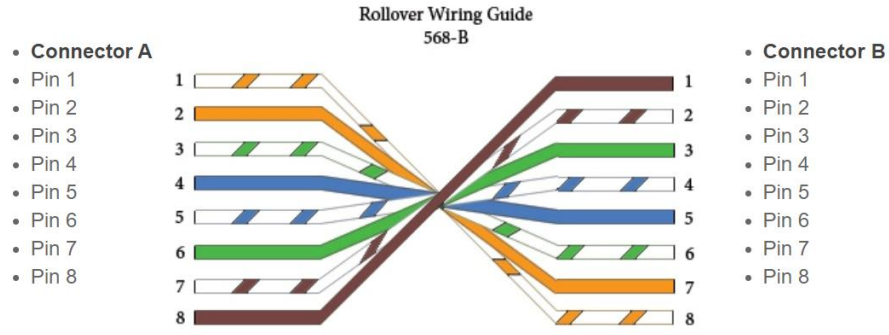
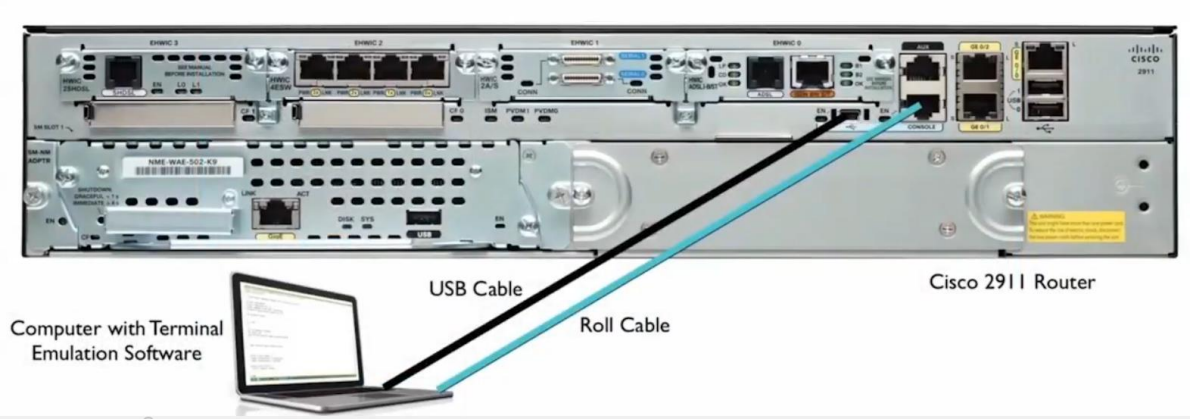


Fig: Rollover wire cable

And because newer laptops don't have Serial ports on them, we have to use a USB to Serial adapter.

Fig: USB to Serial Adapter Cable (USB to RS232, USB to DB9)

Accessing the CLI (Command Line Interface) via PuTTY with a Console Connection



https://www.youtube.com/watch?v=jlRRsIgfHU8&t=121s&ab_channel=DavidBombal

Step 1: Connect the computer to the router or switch using a standard 9-pin serial cable.

On Windows PC:

Step 2: Right-click on the Windows logo/Start button and click on Device Manager to open it.

Let's look for a COM port to input to PuTTY. In fact, when connecting a console cable between a router/switch into a computer it assigns a COM port number to a computer. That COM port is different from COM1.

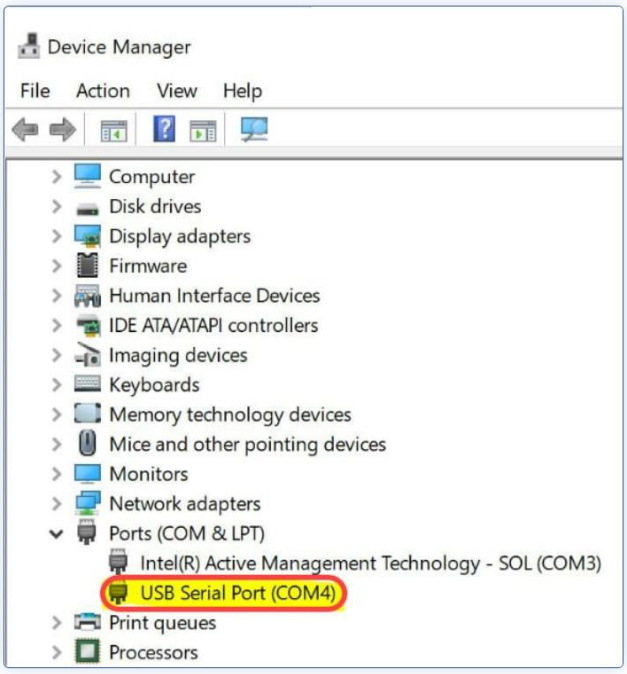
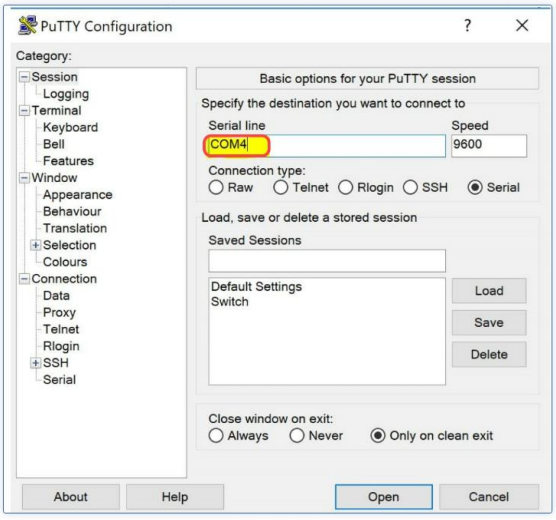
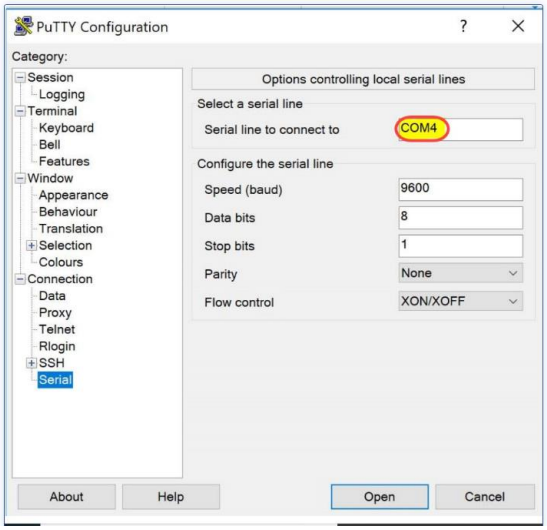


Fig1: choosing a Serial port in Device Manager

On the picture above COM4 is to be used for the Serial line to make the connection.





Another way to find a COM port for the console cable is to open the CMD terminal and type the command **mode**. Then go looking for the COM# other than COM1.

Step 3: Open the PuTTY application and proceed with it,

After clicking on the button "Open" below window will open:

Finally, you will be ready to configure your router or switch.

On the Linux PC

When we use Linux we do not necessarily need to use puTTY for console access.

1. We can easily use a screen

Make sure screen is installed by typing

sudo apt install screen -y

Then...
sudo screen /dev/ttyUSB0

2. We can also use minicom

https://www.youtube.com/watch?v=vUp9TergyhQ&ab_channel=MichaelSt.John

type: dmesg |grep tty

Start By Setting it up

sudo minicom -s

Press F to set Hardware Flow Control in No

Press Enter

Press the down arrow 3 times to get to Save setup as dfl ("Save as default")

Press Enter

Press the down arrow 3 times

Press Enter

1. Let's plug our USB-to-Serial cable in

2.Type **ls -l /dev/ttyUSB0**

Type **sudo minicom**

If you get the error message "Device /dev/ttyUSB0 is locked" do:

sudo killall -9 minicom

Then...

Type **sudo minicom**

3. But if you still want to use puTTY just install it:

sudo apt install putty

vi. Loopback Interface configuration

The ***loopback interface*** is a logical interface internal to the router. It is not assigned to a physical port and can therefore never be connected to any other device.

A loopback interface is a virtual interface that is always up and reachable as long as at least one of the IP interfaces on the switch or router is operational. As a result, a loopback interface is useful for debugging tasks since its IP address can always be pinged if any other switch interface is up.

The loopback interface is useful in testing and managing a Cisco IOS device because it ensures that at least one interface will always be available. For example, *it can be used for testing purposes*, such as testing internal routing processes, by emulating networks behind the router.

The steps to configure a loopback interface on a router are:

Step 1: Create the loopback interface using the interface loopback number in global configuration mode.

Step 2: Add a description. Although optional, it is a necessary component for documenting a network.

Step 3: Configure the IP address.

For example, the following commands configure a loopback interface of the R1 router:

```
R1# configure terminal

R1(config)# interface loopback 0

R1(config-if)# description Loopback Interface
R1(config-if)# ip address 10.0.0.1 255.255.255.0

R1(config-if)# exit

R1(config)#
```

Note:

- **configure** can be shortened to **conf**
- **terminal** to **t**
- **interface** to **int**

A loopback interface is always enabled and therefore does not require a no-shutdown command. Multiple loopback interfaces can be enabled on a router. The IPv4 address for each loopback interface must be unique and unused by any other interface.

IPv4 and IPv6 Loopback Addresses of computers:

- The IPv4 loopback address is 127.0.0.0/8 and the most commonly used loopback address is 127.0.0.1
- The IPv6 loopback address is ::1

vii. Path determination

1. Routing Decisions

A primary function of a router is to determine the best path to use to send packets. To determine the best path, the router searches its routing table for a network address that matches the destination IP address of the packet.

Source of routing information:

- Directly connected network
- Static routing configuration
- Dynamic routing configuration
- Default routing configuration

The routing table search results in one of three path determinations:

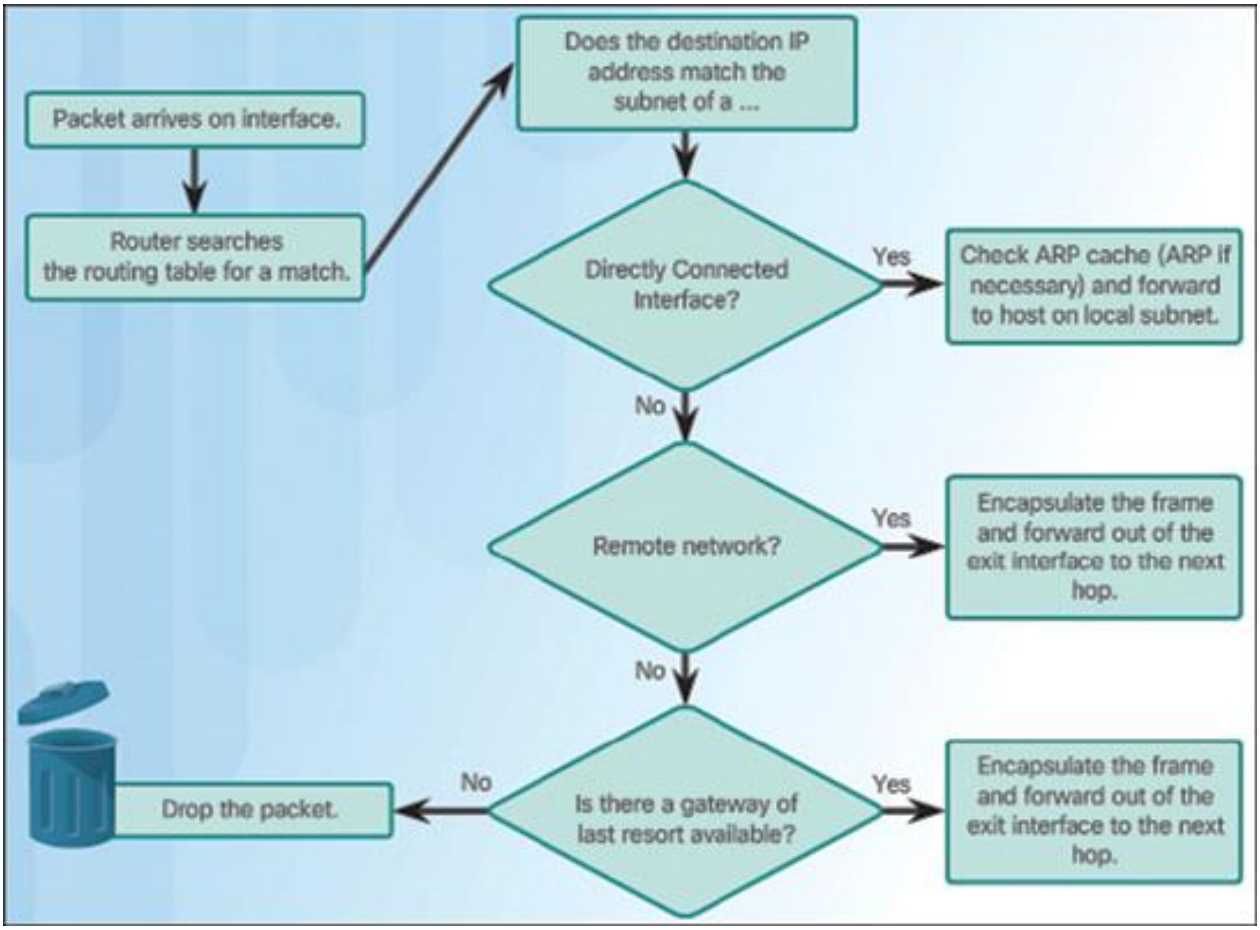
- Directly connected network: If the destination IP address of the packet belongs to a device on a network that is directly connected to one of the interfaces of the router, that packet is forwarded directly to the destination device. This means that the destination IP address of the packet is a host address on the same network as the interface of the router.

- Remote network: If the destination IP address of the packet belongs to a remote network, then the packet is forwarded to another router. Remote networks can only be reached by forwarding packets to another router.

- No route determined: If the destination IP address of the packet does not belong to either a connected or remote network, the router determines if there is a Gateway of ***Last Resort available.***

A Gateway of Last Resort is set when a default route is configured on a router. If there is a default route, the packet is forwarded to the Gateway of Last Resort. If the router does not have a default route, then the packet is discarded. If the packet is discarded, the router sends an ICMP (Internet Control Message Protocol) Unreachable message to the source IP address of the packet.

The logic flowchart in the figure below illustrates the router packet-forwarding decision process.



2. Best Path

Determining the best path involves the evaluation of multiple paths to the same destination network and selecting the optimum or shortest path to reach that network. Whenever multiple paths to the same network exist, each path uses a different exit interface on the router to reach that network.

The best path is selected by a routing protocol based on the value or metric it uses to determine the distance to reach a network. **A metric** is a quantitative value used to measure the distance to a given network. The best path to a network is the path with the lowest metric.

Dynamic routing protocols typically use their own rules and metrics to build and update routing tables. The routing algorithm generates a value, or a metric, for each path through the network. Metrics can be based on either a single characteristic or several characteristics of a path.

The following lists some dynamic protocols and the metrics they use:

- Routing Information Protocol (RIP): Hop count

- Open Shortest Path First (OSPF): Cisco routers use a cost based on cumulative bandwidth from source to destination

- Enhanced Interior Gateway Routing Protocol (EIGRP): Bandwidth, delay, load, reliability

EIGRP Metric Calculation:

Metric = 256 * [(10^7 / minimum bandwidth) + (sum of delays / 10)]

https://www.youtube.com/watch?v=ZMSYx7HRlXs&ab_channel=NetworkingwithRich

3. Load Balancing

What happens if a routing table has two or more paths with identical metrics to the same destination network?

When a router has two or more paths to a destination with equal cost metrics, then the router forwards the packets using both paths equally. This is called **equal cost load balancing**. The routing table contains the single destination network, but has multiple exit interfaces, one for each equal cost path. The router forwards packets using the multiple exit interfaces listed in the routing table.

If configured correctly, load balancing can increase the effectiveness and performance of the network. ***Equal cost load balancing*** can be configured to use both dynamic routing protocols and static routes.

By default, Cisco routers can load balance up to ***four equal cost*** paths. The maximum number of equal cost paths depends on the routing protocol and IOS version.

EIGRP supports equal cost load balancing and is also the only routing protocol to support unequal cost load balancing. **Unequal cost load balancing** is when a router distributes traffic over network interfaces, even those that are different distances from the destination address.

NOTE: EIGRP supports unequal cost load balancing by using the **variance** command.

https://www.youtube.com/watch?v=qA8_JxBy5-Q&ab_channel=Learnet

4. Administrative Distance

It is possible for a router to be configured with multiple routing protocols and static routes. If this occurs, the routing table may have *more than one route source* for the same destination network.

For example, if both RIP and EIGRP are configured on a router, both routing protocols may learn of the same destination network. However, each routing protocol may decide on a different path to reach the destination based on that routing protocol's metrics.

RIP chooses a path based on hop count, **whereas EIGRP** chooses a path based on its composite metric.

How does the router know which route to use?

Cisco IOS uses what is known as the administrative distance (AD) to determine the route to install into the IP routing table.

The AD represents the "**trustworthiness**" of the route; the lower the AD, the more trustworthy the route source. For example, a static route has an AD of 1, whereas an EIGRP-discovered route has an AD of 90. Given two separate routes to the same destination, the router chooses the route with the lowest AD. When a router has the choice of a static route and an EIGRP route, the static route takes precedence. Similarly, a directly connected route with an AD of 0 takes precedence over a static route with an AD of 1.

Table below lists various routing protocols and their associated ADs.

Route Source	**Administrative Distance**
Connected	0
Static	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90

Route Source	Administrative Distance
IGRP	100
OSPF	110
IS-IS (**Intermediate System to Intermediate System**)	115
RIP	120
External EIGRP	170
Internal BGP	200
Unknown	255

viii. Routing table

A routing table, or routing information base (RIB), is a data table stored in a router or a network host that lists the routes to particular network destinations, and in some cases, metrics (distances) associated with those routes.

Static routes are entries made in a routing table by non-automatic means and which are fixed rather than being the result of routing protocols and associated network topology discovery procedures.

A routing table is a **database** that keeps track of paths, like a map, and uses these to determine which way to forward traffic. A routing table is a data file in **RAM** that is used to store route information about directly connected and remote networks. Nodes can also share the contents of their routing table with other nodes.

When a router interface is configured with ***an IP address and subnet mask***, the interface becomes a host on that attached network.

A remote network is a network that can only be reached by sending the packet to another router. Routing table entries to remote networks may be either dynamic or static.

Dynamic routes are routes to remote networks that were learned automatically by the router through a dynamic routing protocol.

Static routes are routes that a network administrator manually configured.

See below a typical routing table:

Destination	Subnet mask	Interface
128.75.43.0	255.255.255.0	Eth0
128.75.43.0	255.255.255.128	Eth1
192.12.17.5	255.255.255.255	Eth3
default		Eth2

The entry corresponding to the default gateway configuration is a network destination of 0.0.0.0 with a network mask (netmask) of 0.0.0.0. The Subnet Mask of the default route is always 255.255.255.255.

Entries of a Routing Table

Each packet contains information about its origin and destination. Routing Table provides the device with instructions for sending the packet to the next hop on its route across the network.

Routing table entries can be used to store the following types of routes: Directly Attached Network IDs, Remote Network IDs, Host Routes, Default Route, and Destination

Each entry in the routing table consists of the following entries:

1. Network ID: The network ID or destination corresponding to the route.

2. Subnet Mask: The mask that is used to match a destination IP address to the network ID.

3. Next Hop: The IP address to which the packet is forwarded

4. Outgoing Interface: Outgoing interface the packet should go out to reach the destination network.

5. Metric: A common use of the metric is to indicate the minimum number of hops (routers crossed) to the network ID.

3. How are Routing Tables populated?

- Using Static Routing (manually): Tables for static network devices do not change unless a network administrator manually changes them.

-Using Dynamic Routing (automatically): In dynamic routing, devices build and maintain their routing tables automatically by using routing protocols to

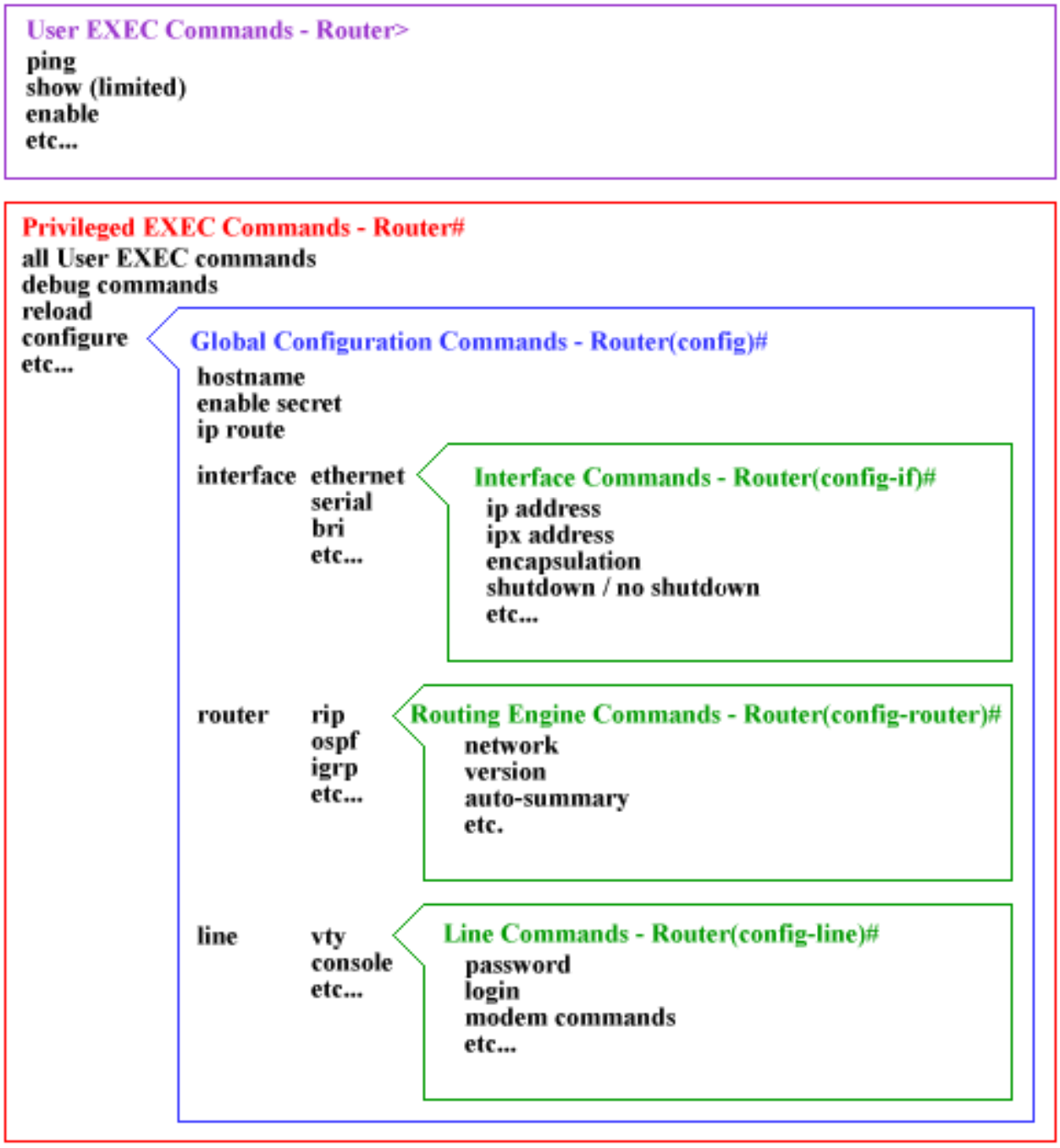
exchange information about the surrounding network topology. Dynamic routing tables allow devices to "listen" to the network and respond to occurrences like device failures and network congestion.

Note that the routing tables are not specific to Cisco devices. Even your Windows operating system has a routing table that can be displayed using the **route print** command.

Linux as well has a routing table that can be displayed using the **route** command.

Cisco IOS Command Hierarchy

Router>	- User EXEC mode
Router#	- Privileged EXEC mode
Router(config)#	- Global Configuration mode (notice the # sign indicates this is accessible only at privileged EXEC mode)
Router(config-if)#	- Interface level within configuration mode
Router(config-router)#	- Routing engine level within configuration mode
Router(config-line)#	- Line level (vty, tty, async) within configuration mode

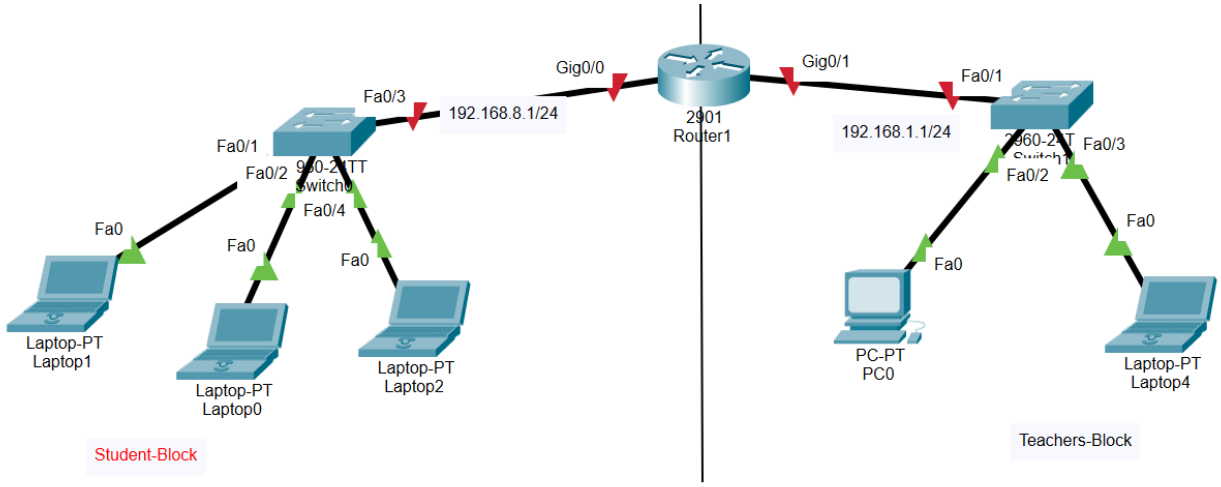


Practical session

- Basics router configuration
- DHCP Configuration

DHCP configuration

1. DHCP configuration on CISCO Router



Configuration	Student-block	Teachers-block
IP addresses	192.168.8.0 to 192.168.8.255	192.168.1.0 to 192.168.1.255
Available IP addresses for hosts	192168.8.5 to 192.168.8.254	192.168.1.10 to 192.168.1.254
Subnet mask	255.255.255.0	255.255.255.0
Default Gateway	192.168.8.1	192.168.1.1
Reserved	192.168.8.1 to 192.168.8.5	192.168.1.1 to 192.168.1.10

Sequence of Commands

Go up to configure terminal

```
Router>en

Router# conf t
```

Configure the interface on the student-block

```
Router(config)# int Gi0/0
Router(config-if)# ip add 192.168.8.1 255.255.255.0
Router(config-if)# no sh
Router(config-if)#exit
```

Configure the interface on the Teachers-block

```
Router(config)# int Gi0/1
Router(config-if)# ip add 192.168.1.1 255.255.255.0
Router(config-if)# no sh
Router(config-if)#exit
```

Configure DHCP on the Student-block

```
Router(config)#ip dhcp excluded-address 192.168.8.0 192.168.8.5
Router(config)#ip dhcp pool Student-block
Router(dhcp-config)#default-router 192.168.8.1
Router(dhcp-config)#network 192.168.8.0 255.255.255.0
Router(dhcp-config)#exit
```

Configure DHCP on the Teacher-block

```
Router(config)#ip dhcp excluded-address 192.168.1.0 192.168.1.10
Router(config)#ip dhcp pool Teacher-block
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#exit
```

Saving the configuration

```
router #copy running-config startup-config
or
router# write memory
```

Verifying the DHCP Server

```
router #show ip dhcp pool Teacher-block
router#show ip dhcp pool student-block
```

CONFIGURING STATIC AND DEFAULT ROUTES

1. Initial Configuration

This section describes how to use the setup command facility to configure a hostname for the router, set passwords, and configure an interface for communication with the management network.

If the following messages appear at the end of the startup sequence, the setup command facility has been invoked automatically:

```
--- System Configuration Dialog ---
At any point, you may enter a question mark '?' for help.
Use ctrl-c to abort the configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Would you like to enter the initial configuration dialog? [yes/no]:
No
```

The setup command facility prompts you for basic information about your router and network, and it creates an initial configuration file. After the configuration file is created, you can use the CLI or Security Device Manager to perform additional configuration.

The prompts in the setup command facility vary, depending on your router model, the installed interface modules, and the software image. The following example and the user entries (in bold) are shown as examples only.

Note: If you make a mistake while using the setup command facility, you can exit and run the setup command facility again. Press Ctrl-C, and enter the setup command at the privileged EXEC mode prompt (Router#).

Step 1: To proceed using the setup command facility, enter yes:

```
Would you like to enter the initial configuration dialog?
[yes/no]: yes
```

Step 2: When the following messages appear, enter yes to enter basic management setup:

```
At any point you may enter a question mark '?' for help.

Use ctrl-c to abort configuration dialog at any prompt.

Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity

for management of the system, extended setup will ask you
```

```
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: yes
```

Step 3: Enter a hostname for the router (this example uses Router):

```
Configuring global parameters:

Enter host name [Router]: Router
```

Step 4: Enter an **enable secret password**. This password is encrypted (more secure) and cannot be seen when viewing the configuration:

```
The enable secret is a password used to protect access to
privileged EXEC and configuration modes. This password, after
entered, becomes encrypted in the configuration.
Enter enable secret: xxxxxx
```

Step 5: Enter an **enable password** that is different from the enable secret password. This password is not encrypted (less secure) and can be seen when viewing the configuration:

```
The enable password is used when you do not specify an
enable secret password, with some older software versions, and
some boot images.
Enter enable password: xxxxxx
```

Step 6: Enter the **virtual terminal password**, which prevents unauthenticated access to the router through ports other than the console port:

```
The virtual terminal password is used to protect
access to the router over a network interface.
Enter virtual terminal password: xxxxxx
```

Step 7: Respond to the following prompts as appropriate for your network:

```
Configure SNMP Network Management? [yes]:

Community string [public]:
```

A summary of the available interfaces is displayed.

We can get a summary of the available interfaces by running this command:
show ip interface brief

Below is the screenshot I got while working on CISCO 891F

```
Current interface summary

Any interface listed with OK? value "NO" does not have a valid configuration

Interface              IP-Address      OK? Method Status                Protocol
Async3                 unassigned      YES unset  down                  down
BRI0                   unassigned      NO  unset  down                  down
BRI0:1                 unassigned      YES unset  down                  down
BRI0:2                 unassigned      YES unset  down                  down
FastEthernet0          unassigned      NO  unset  down                  down
GigabitEthernet0       unassigned      YES unset  down                  down
GigabitEthernet1       unassigned      YES unset  down                  down
GigabitEthernet2       unassigned      YES unset  down                  down
GigabitEthernet3       unassigned      YES unset  down                  down
GigabitEthernet4       unassigned      YES unset  down                  down
GigabitEthernet5       unassigned      YES unset  down                  down
GigabitEthernet6       unassigned      YES unset  down                  down
GigabitEthernet7       unassigned      YES unset  down                  down
GigabitEthernet8       unassigned      NO  unset  down                  down
Vlan1                  unassigned      YES unset  down                  down
```

Step 8: Choose one of the available interfaces for connecting the router to the management network:

```
Enter interface name used to connect to the management network
from the above interface summary: FastEthernet0
```

Step 9: Respond to the following prompts as appropriate for your network:

```
Configuring interface FastEthernet0:
Use the 100 Base-TX (RJ-45) connector? [yes]: yes
Operate in full-duplex mode? [no]: no
Configure IP on this interface? [yes]: yes
IP address for this interface: 172.1.2.3
Subnet mask for this interface [255.255.0.0] : 255.255.0.0
Class B network is 172.1.0.0, 26 subnet bits; mask is /16
```

Are routers full duplex?

Cisco router's and switch's interfaces have the capability to work at full duplex as well as half duplex. By default, interface works on auto-negotiation mode, which negotiates the duplex and speed of the link between the 2 devices connected in the segment of the network.

Step 10: The configuration is displayed. You have nothing to do here. The following information ensues from hitting enter after entering the subnet mask on precedent step.

```
The following configuration command script was created:
hostname Router
enable secret 5 $1$D5P6$PYx41/lQIASK.HcSbfO5q1
enable password xxxxxx
line vty 0 4
password xxxxxx
snmp-server community public
!
no ip routing
!
interface FastEthernet0
no shutdown
speed 100
half-duplex
ip address 172.1.2.3 255.255.0.0
!
```

Step 11: Respond to the following prompts. Enter 2 to save the initial configuration.

```
[0] Go to the IOS command prompt without saving this config.

[1] Return back to the setup without saving this config.

[2] Save this configuration to nvram and exit.

Enter your selection [2]: 2

Building configuration...

Use the enabled mode 'configure' command to modify this
configuration.

Press RETURN to get started! RETURN key
```

The user prompt is displayed.

```
Router>
```

Step 12: Verify the initial configuration

•To verify that the interfaces are operating correctly and that the interfaces and line protocol are in the correct state i.e. up or down, enter the command

show interfaces

•To display a summary status of the interfaces configured for IP, enter the command

show IP interface brief (Do show ip interface brief: issue this command while you are in global configuration mode)

•To verify that you configured the correct hostname and password, enter the command.

Make sure you're at the privileged EXEC mode prompt (Router# and not Router>). To go to EXEC mode just enter either the command **en** or the command **enable**

You'll be asked to enter the password enter **xxxxxx** as configured above.

show configuration

show inventory: this command will display the information regarding the module of the router

•To display a collection of information about a router (e.g. version, up-time, memory, Cisco IOS image, and installed interfaces), enter the command.

Show version

•To display detailed information about the configuration and operation of a router interface, enter the command

show interface interface-id

To exit the EXEC mode you can simply enter the command:

exit

Now that we have completed and verified the initial configuration, we can configure the static route.

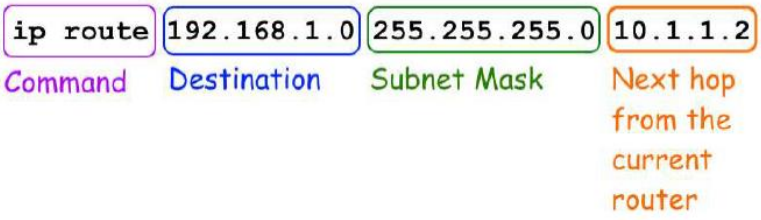
Notice the initial configuration can be skipped in the future as long as we already covered it.

2.1. Static Routing

The term static refers to the fact that entries in the routing table are manually added and are therefore permanent (or static) by nature.

A static route is a pre-determined pathway that a packet must travel to reach a specific host or network

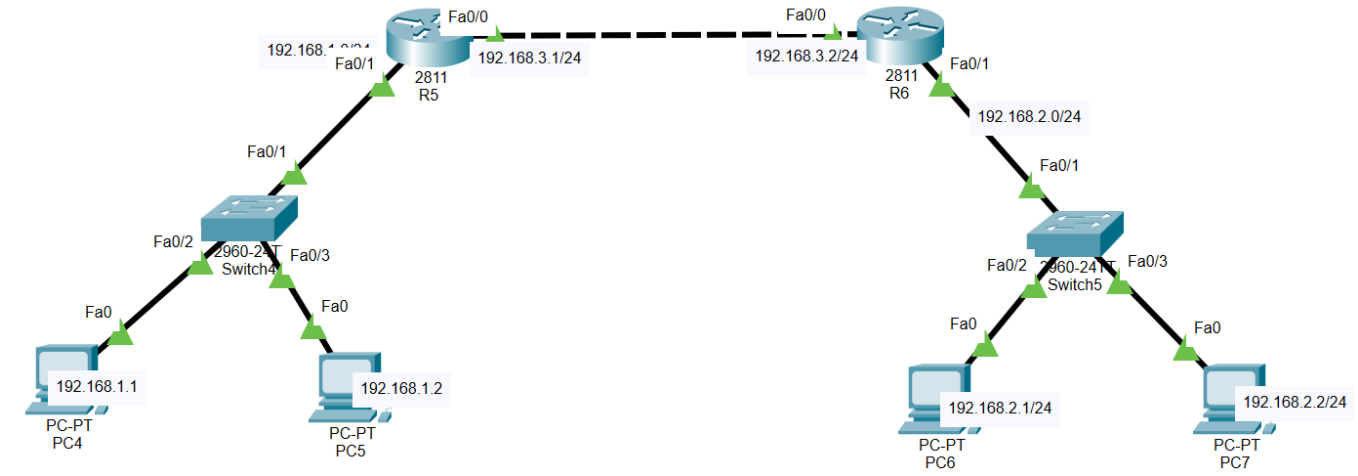
Due to this manual approach, static routing is most appropriate to use in smaller network deployments where addresses are fairly fixed and where the number of connected networks are limited to a few.



Types of static routes

- **Static network routes** is a static route that points to a specific network address (also known as a **network prefix or** here we can specify the **egress interface)**
- **Static host route:** a static route that points to a specific IP address (as evidenced by a 32-bit subnet mask)
- **Static default route:** a static route that acts as a default route (also known as a **gateway of last resort**) for the router use if the router doesn't have more specific routing information for a given network.
- **Floating static route:** A static route whose **Administrative Distance** (AD) is configured higher (and is therefore less attractive) that the AD of a dynamic routing protocol that knows a different route to the same destination.

STATIC NETWORK ROUTE



To configure a basic IP static route, perform these steps.

1. **Configure the router name**

Router>en
Router#conf t
Router(config)#hostname R5

2. **Configure the IP address on the first interface**

R5(config)#interface fa0/1
R5(config-if)#ip add
R5(config-if)#ip address 192.168.1.3 255.255.255.0
R5(config-if)#no shutdown
R5(config-if)#exit

3. **Configure the IP address on the Second interface**

R5(config)#interface fa0/0
R5(config-if)#ip address 192.168.3.1 255.255.255.0
R5(config-if)#no shutdown
R5(config-if)#exit

4. **Configure the static route**

R5(config)#ip route 192.162.2.0 255.255.255.0 Fa0/0
R5(config)#exit

5. **Save the configuration to NVRAM**

R5#copy running-config startup-config
R5#

Configure the second Router

1. **Set the router hostname**

```
Router>en
Router#conf t
Router(config)#hostname R6
```

2. **Configure the router's first interface**

```
R6(config)#interface fa0/0
R6(config-if)#ip address 192.168.3.2 255.255.255.0
R6(config-if)#no shutdown
```

3. **Configure the second interface**

```
R6(config-if)#exit
R6(config)#interface fa0/1
R6(config-if)#ip address 192.168.2.1 255.255.255.0
R6(config-if)#no shutdown
```

4. **Configure the static route**

Enter the IP address and prefix length, or enter the IP address and network mask for the route destination network. On the same command line, enter the IP address for the next hop.

```
R6(config-if)#exit
R6(config)#ip route 192.168.1.0 255.255.255.0 Fa0/0 or
R6(config)#ip route 192.168.1.0 255.255.255.0 192.168.3.1 or
R6(config)#ip route 192.168.1.0 255.255.255.0 192.168.3.1
R6(config)#
```

Static routing is when the administrator manually configures a router to send traffic for particular destinations in preconfigured directions.

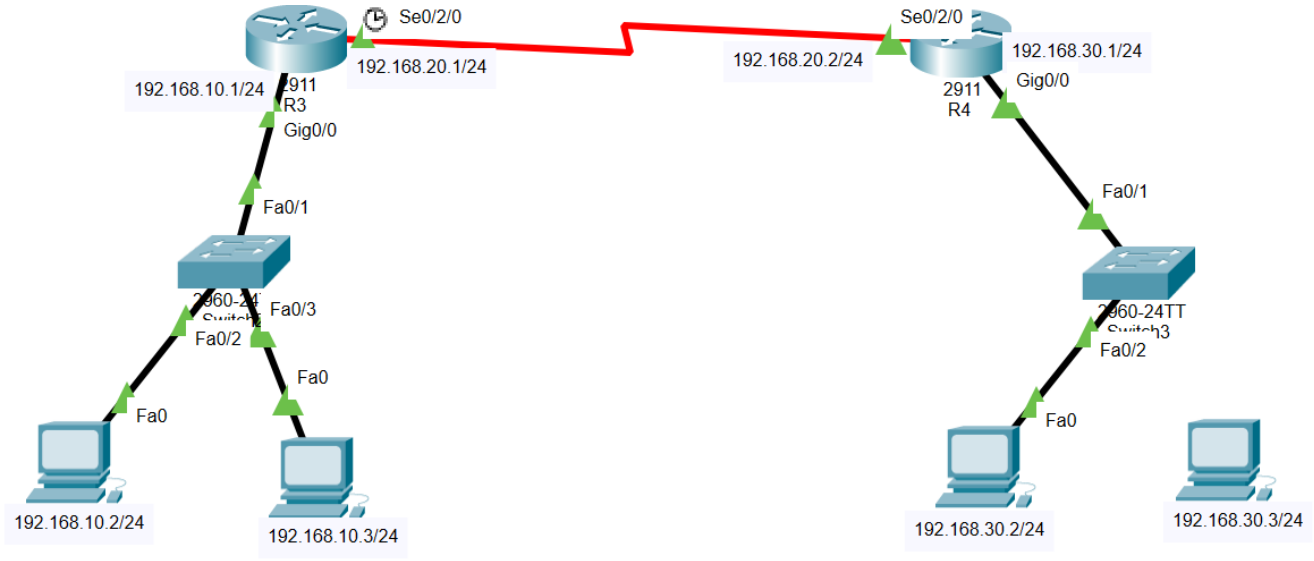
Configuring a default static route

A static default route is an entry that allows the router to send traffic to another router if the router doesn't have an entry for the destination.

You can manually create a default static route that the router uses if there are no other default routes to a destination.

If the default route is a protocol route, that protocol needs to be enabled to resolve static routes. Use the IP route next-hop command to allow protocol resolution through the default route.

If the default route itself is a static route, you must configure the IP route next-hop-enable-default command to resolve other static routes through the default route. You may also configure recursive lookup to resolve the next hop.



Perform these steps to configure a default route.

Write the following commands on R3:

1. **Configure the IP address on the interface Serial 0/2/0**

R3(config)#interface s0/2/0
R3(config-if)#ip address 192.168.20.1 255.255.255.0 //Assigning the IP address on the interface
R3(config-if)#clock rate 1280000 //assign the CPU speed
R3(config-if)#no shutdown
R3(config-if)#exit

2. **Configure the IP address on the interface GigabitEthernet 0/0**

R3(config)#interface g0/0
R3(config-if)#ip address 192.168.10.1 255.255.255.0
R3(config-if)#no shutdown

3. **Configure the default route**

R3(config)#ip route 0.0.0.0 0.0.0.0 192.168.20.2 //default route
R3(config)#exit

4. **Save the configurations**

R3#copy running-config startup-config

Write the following commands on R4:

1. Configure the IP address on the interface Serial 0/2/0

R4(config)#interface s0/2/0
R4(config-if)#ip address 192.168.20.2 255.255.255.0 //Assigning the IP address on the interface
R4(config-if)#no shutdown
R4(config-if)#exit

2. Configure the IP address on the interface GigabitEthernet 0/0

```
R4(config)#interface g0/0
R4(config-if)#ip address 192.168.30.1 255.255.255.0
R4(config-if)#no shutdown
```

3. Configure the default route

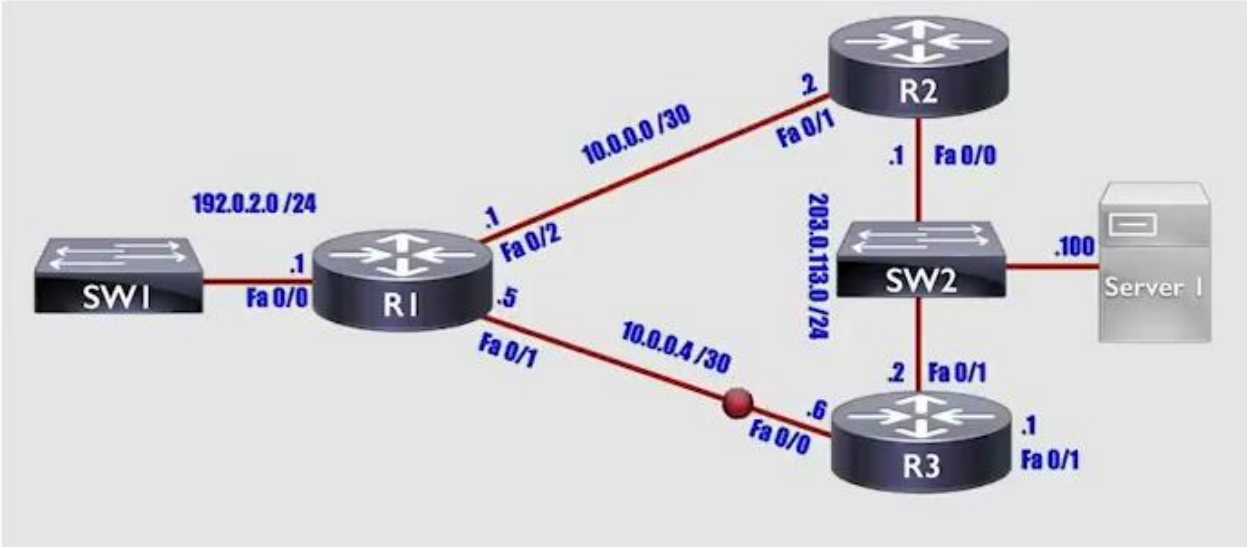
```
R4(config)#ip route 0.0.0.0 0.0.0.0 192.168.20.1 //default route
R4(config)#exit
```

4. Save the configurations

R4#copy running-config startup-config

STATIC HOST ROUTE CONFIGURATION

The entry that allows you to route traffic for a specific host



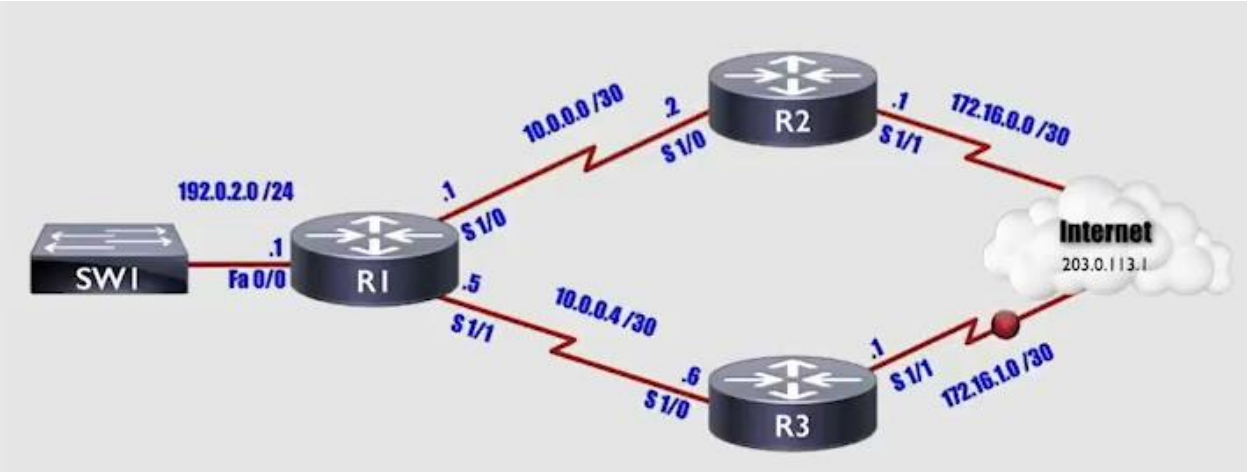
R1# conf t
R1(config)# ip route 203.0.113.0 255.255.255.0 10.0.0.6
R1(config)# ip route 203.0.113.100 255.255.255.255 10.0.0.2 // **here we specify the server**
//R1(config)# ip route 203.0.113.100 255.255.255.255 10.0.0.2 permanent (This can be configured permanently by adding the keyword "**permanent**")

R1(config)#end

Floating static route configuration

A router has two static route entries but prefers one (primary) and the second acts as a backup

If the primary static route can't be used, it will be deleted from the routing table and the second static route will be installed.



R1# conf t

R1(config)# ip route 203.0.113.0 255.255.255.0 10.0.0.2 125 (125: administrative distance)

R1(config)#end

Q: What is the difference between the default route and the default gateway?

Reference:
https://www.ciscopress.com/articles/article.asp?p=2180209&seqNum=7

3. Apply class full and classless routing protocol

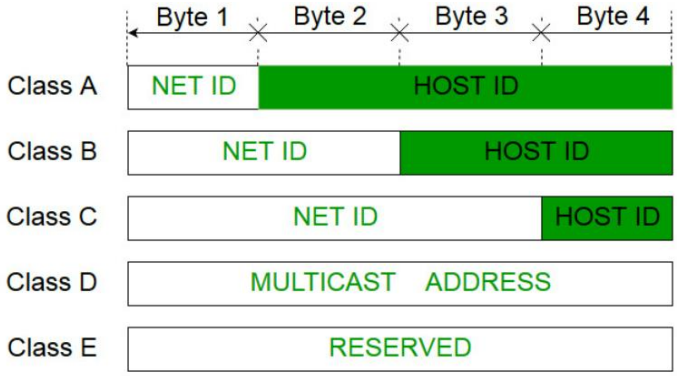
3.1. Class full IP addressing

IP Header Classes:

Class	Address Range	Subnet masking	Example IP	Leading bits	Max number of networks	Application
IP Class A	1 to 126	255.0.0.0	1.1.1.1	8	128	Used for large number of hosts.
IP Class B	128 to 191	255.255.0.0	128.1.1.1	16	16384	Used for medium size network.
IP Class C	192 to 223	255.255.255.0	192.1.11.1	24	2097157	Used for local area network.
IP Class D	224 to 239	NA	NA	NA	NA	Reserve for multi-tasking.
IP Class E	240 to 254	NA	NA	NA	NA	This class is reserved for research and Development Purposes.

Note:

1. Class A addresses **127.0.0.0 to 127.255.255.255** cannot be used and is reserved for **loopback** and diagnostic functions or is used for internal testing on the local machine.
2. Class B addresses **169.254.1.0 to 169.254.254.255**. Automatic Private IP Addressing (APIPA), DHCP clients automatically configure an IP address and subnet mask when a DHCP server is not available. The device chooses its own IP address in the range 169.254.1.0 through to 169.254. 254.255.
3. **0.0.0.0** address indicates the client isn't connected to a TCP/IP network, and a device may give itself 0.0.0.0 address when it is offline.



Limitations of classful IP addressing

- Risk of running out of address space
- Class boundaries did not encourage efficient allocation of address space

The private IP address of a system is the IP address that is used to communicate within the same network. Using private IP data or information can be sent or received within the same network.

The public IP address of a system is the IP address that is used to communicate outside the network. A public IP address is basically assigned by the ISP (Internet Service Provider).

Private Address Ranges

- Class A: 10.0. 0.0 to 10.255.255.255
- Class B: 172.16. 0.0 to 172.31.255.255
- Class C: 192.168. 0.0 to 192.168.255.255

IPV6 (Internet Protocol version 6)

Benefits of IPv6

- ✓ Increased address space: $5x10^{28}$ address for each person on the planet
- ✓ Simplified header (IPv4 header: 12 fields, IPv6 header: 8 fields)
- ✓ No broadcasts
- ✓ Security and mobility features built-in
- ✓ No fragmentation: MTU discovery is performed for each session
- ✓ Can coexist with IPv4 during a migration (dual stack, IPv6 over IPv4)

IPv6 address structure

IPv6 is a 128-bits address having an address space of 2^128, which is way bigger than IPv4. In IPv6 we use Colon-Hexa representation. There are 8 groups and each group represents 2 Bytes.

In IPv6 representation, we have three addressing methods:

- Unicast
- Multicast
- Anycast

1. IPv6 unicast addresses

Unicast addresses represent a single interface. Packets addressed to a unicast address will be delivered to a specific network interface.

There are three types of IPv6 unicast addresses:

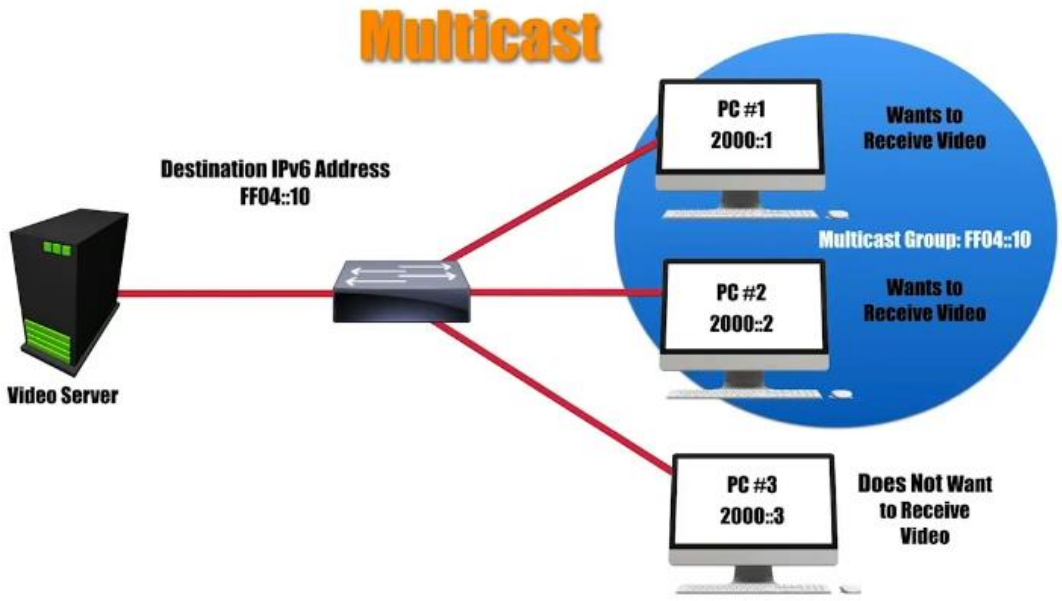
- ✓ **Global unicast** – similar to IPv4 public IP addresses. These addresses are assigned by the IANA and used on public networks. They have a prefix of **2000::/3**, (all the addresses that begin with binary **001**).
- ✓ **Unique local –** similar to IPv4 private addresses. They are used in private networks and aren't routable on the Internet. These addresses have a prefix of **FD00::/8**.
- ✓ **Link local –** these addresses are used for sending packets over the local subnet. Routers do not forward packets with these addresses to other subnets. IPv6 requires a link-local address to be assigned to every network interface on which the IPv6 protocol is enabled. These addresses have a prefix of **FE80::/10**.

2. Multicast Address:

Multicast Address is used by multiple hosts, called as Group, acquires a multicast destination address. These hosts need not be geographically together. If any packet is sent to this multicast address, it will be distributed to all interfaces corresponding to that multicast address.

Some examples of IPv6 well-known multicast addresses include the following:

- **ff02::1:** All IPv6 devices
- **ff02::2:** All IPv6 routers
- **ff02::5:** All OSPFv3 routers
- **ff02::a:** All EIGRP (IPv6) routers

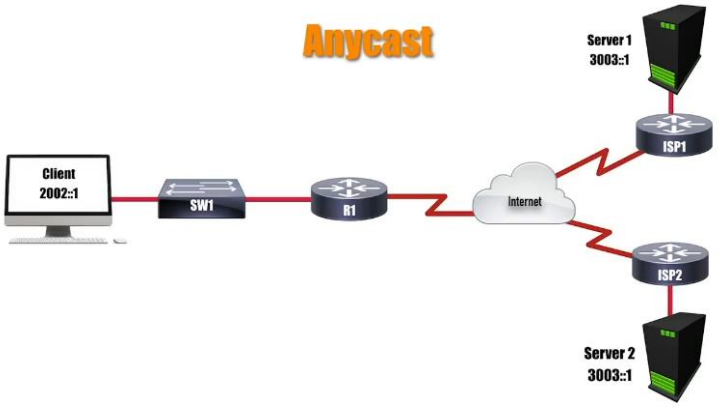


3. Anycast Address:

Anycast Address is assigned to a group of interfaces. Any packet sent to an anycast address will be delivered to only one member interface (mostly the nearest host possible).

Note: Broadcast is not defined in IPv6.

There is no special prefix for an IPv6 anycast address. An IPv6 anycast address uses the same address range as global unicast addresses.



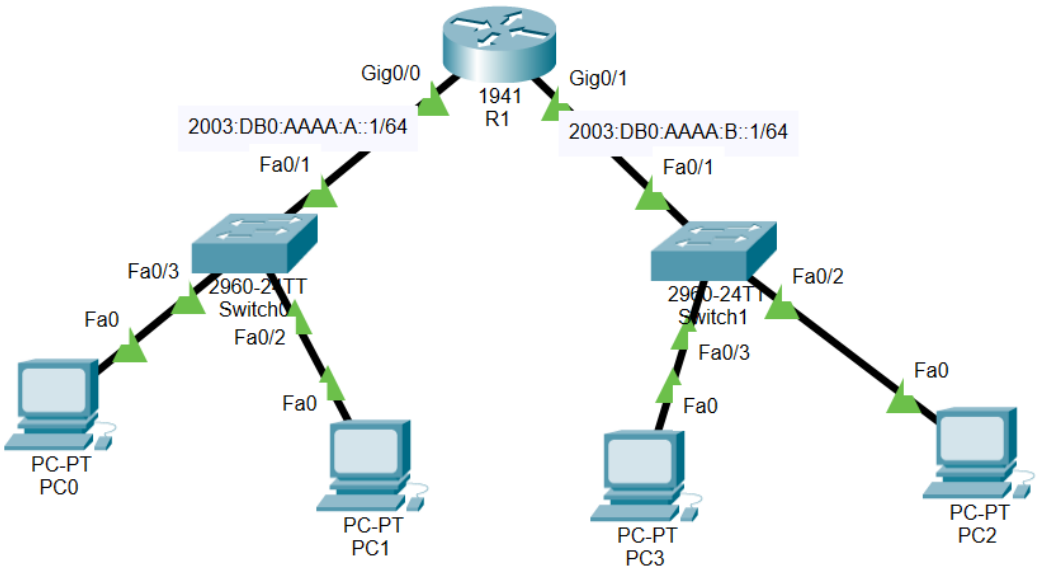
Loopback address:

Written as ::1 also known as localhost (127 zeros)

IPv6 addressing in Packet tracer

Considering the below network:

-Enable the communication between PC0 and PC2 or PC0 and PC3



Assigning the IPV6 on the router's interfaces:

Router# configure terminal
Router(config)# ipv6 unicast-routing //First enable unicast routing on the router
Router(config)#interface g0/0
Router(config-if)#ipv6 enable //Automatically the link local address is assigned to the router
Router(config-if)# ipv6 address 2003:DB0:AAAA:A::1/64
Router(config)#interface g0/1
Router(config-if)#ipv6 enable //Automatically the link local address is assigned to the router
Router(config-if)# ipv6 address 2003:DB0:AAAA:B::1/64
Note: For PC0, PC1, PC2, and PC3 enable autoconfiguration
Verification: Ping PC2 in PC0

Router#show ipv6 interface G0/0

Router#show ipv6 interface brief

3.2. Review of Sub-netting

Subnetting is a method of dividing a single physical network into logical sub-networks (subnets). Its purpose is to divide a huge network into a collection of smaller, interconnected networks to reduce traffic.

Subnetting is aimed to achieve the following targets in the network:

- Reallocating IP Addresses
- Improving Network Security
- Improves Network Speed
- Efficiency

Disadvantages of Subnetting

- Subnetting increases the network's complexity.
- More subnets mean more IP addresses are wasted because each subnet has its own *network address* and *broadcast address.*
- As we increase more subnets in the network, the maintenance process becomes challenging.

The easy way of solving subnetting questions is to use a table that contains subnet, host, and subnet mask (in shortened format) or you can use some mathematical calculations as usual

For example:

1. With /24 network

Subnet	1	2	4	8	16	32	64	128	256
Host	256	128	64	32	16	8	4	2	1
Subnet Mask	/24	/25	/26	/27	/28	/29	/30	/31	/32

Example 2: with /16 network

Subnet	1	2	4	8	16	32	64	128	256	512	1024	2048	4096	8192	16384	32768	65536
Host	65536	32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1
Subnet Mask	/16	/17	/18	/19	/20	/21	/22	/23	/24	/25	/26	/27	/28	/29	/30	31	/32

Example: subnetting with class C address

Network address = 192.168.10.0 (This is found by performing the AND operation between provided IP address and new subnet mask)

- ✓ CIDR = 26 => 192.168.10.0/26
- ✓ 26 bits are ON, so subnet mask =255.255.255.192
- ✓ Block size =256-192 =64
- ✓ No. of subnets= 22= 4
- ✓ No. of hosts per subnet= 26-2 =64-2 =62

Subnets	Network address	Broadcast address
1st subnet	192.168.10.0	192.168.10.63
2nd subnet	192.168.10.64	192.168.10.127
3rd subnet	192.168.10.128	192.168.10.191
4th subnet	192.168.10.192	192.168.10.255

Valid host range

Subnets	Valid host range
1st subnet	192.168.10.1-192.168.10.62
2nd subnet	192.168.10.65 -192.168.10.126
3rd subnet	192.168.10.129-192.168.10.190
4th subnet	192.168.10.193- 192.168.10.254

Questions:

1. What is the Network ID, Broadcast Address, First Usable IP, or Last Usable IP on the subnetwork that the node 192.168.1.15/26 belongs to?
   Note that for getting a Network ID you use AND operation between given IP and subnet Mask.
   Answer:
   - Network ID (First IP in the subnet): 192.168.1.0
   - Broadcast address (last IP in the subnet): 192.168.1.63
   - First Usable IP (the address after the network ID): 192.168.1.1
   - Last Usable IP (the address before the broadcast address): 192.168.1.62
2. How many subnets and hosts per subnet can you get from the network 192.168.1.0 255.255.255.224?
   Answer:
   Subnet Bits = 2^3 = 8
   Host Bits = 2^5-2 = 30
3. Given the following IP address 192.168.64.0/24, create three equal separate networks of RCA. One for the Administration office, the other for students, and the last for Teachers. List each network ID, subnet mask, Host ID range, number of usable host addresses, and broadcast ID for each created network.
   Answer:
4. Suppose you have a class B ID: 172.16.0.0/16, and you are requested to create 4 new subnets.
   a. What is the new subnet?
   b. How many usable host IPs for each subnet?
   c. List each network I D, the usable IP range, and Broadcast IP for each subnet.

Answer:
New subnet mask: CIDR=/18=255.255.192.0
Block size=256-192=64 on the second Octet
Host per subnet= 2^{14}
Usable host Per subnet= $2^{14}-2$

Network ID	Host Range (16,382)	Broadcast ID
172.16.0.0	172.16.0.1 - 172.16.63.254	172.16.63.255
172.16.64.0	172.16.64.1 - 172.16.127.254	172.16.127.255
172.16.128.0	172.16.128.1 - 172.16.191.254	172.16.191.255
172.16.192.0	172.16.192.1 - 172.16.255.254	172.16.255.255

5. Given the following IP address: 172.16.0.0/16. You are requested to create 1000 subnets.
   a. What is the new subnet mask for all subnets?
   b. How many usable host IPs are there for each new subnet?
   c. List all network IPs, host range, and broadcast IPs (At least 4 first subnets and 4 last subnets).

Answer:

Bits to borrow (10 Bits)= 255.255.11111111.11000000=> 255.255.255.192 in CIDR/26
New subnet mask=255.255.255.192
Block size: 256-192=64 (Iteration on the third octet)

Network ID	Host Range	Broadcast ID
172.16.0.0	172.16.0.1 - 172.16.0.62	172.16.0.63
172.16.0.64	172.16.0.65 - 172.16.0.126	172.16.0.127
172.16.0.128	172.16.0.129 - 172.16.0.190	172.16.0.191
172.16.0.192	172.16.0.193 - 172.16.0.254	172.16.0.255
172.16.1.0	172.16.1.1 - 172.16.1.62	172.16.1.63
172.16.1.64	172.16.1.65 - 172.16.1.126	172.16.1.127
172.16.1.128	172.16.1.129 - 172.16.1.190	172.16.1.191
172.16.1.192	172.16.1.193 - 172.16.1.254	172.16.1.255
172.16.2.0	172.16.2.1 - 172.16.2.62	172.16.2.63
172.16.2.64	172.16.2.65 - 172.16.2.126	172.16.2.127
172.16.2.128	172.16.2.129 - 172.16.2.190	172.16.2.191
172.16.2.192	172.16.2.193 - 172.16.2.254	172.16.2.255
...	...	...
172.16.254.0	172.16.254.1 - 172.16.254.62	172.16.254.63
172.16.254.64	172.16.254.65 - 172.16.254.126	172.16.254.127
172.16.254.128	172.16.254.129 - 172.16.254.190	172.16.254.191
172.16.254.192	172.16.254.193 - 172.16.254.254	172.16.254.255

3.3. VLSM and IP addressing

VLSM stands for Variable Length Subnet Mask where the subnet design uses more than one mask in the same network which means more than one mask is used for different subnets of a single class A, B, C or a network.
It is used to increase the usability of subnets as they can be of variable size. It is also defined as the process of subnetting of a subnet.

Steps for solving VLSM questions:

Step1: Arrange the network in descending order (Largest to small)

Step2: Pick a subnet for the largest network

Step3: Pick the next largest network to work with

Step4: continue this process until you reach the last

Question:

Suppose there is an administrator that has four departments to manage. These are the sales and purchase department with 120 computers, the development department with 50 computers, the accounts department with 26 computers and the management department with 5 computers.
If the administrator has IP 192.168.1.0/24, department-wise IPs can be allocated by following these steps:

1. For each segment select the block size that is greater than or equal to the actual requirement which is the sum of host addresses, broadcast addresses, and network addresses. Make a list of subnets possible:
   Table of possible subnets list

SLASH NOTATION	HOSTS/SUBNETS
/24	254
/25	126
/26	62
/27	30
/28	14
/29	6
/30	2

2. Arrange all the segments in descending order based on the block size that is from highest to lowest requirement.
   - `Sales and Purchase: 120`
   - `Development: 50`
   - `Accounts: 26`
   - `Management: 5`

3. The highest IP available has to be allocated to highest requirement so the sales and purchase department gets 192.168.1.0/25 which has 126 valid addresses that can easily be available for 120 hosts.
   The subnet mask used is 255.255.255.128

4. The next segment requires an IP to handle 50 hosts. The IP subnet with network number 192.168.1.128/26 is the next highest which can be assigned to 62 hosts thus fulfilling the requirement of development department. The subnet mask used is 255.255.255.192
5. Similarly, the next IP subnet 192.168.1.192/27 can fulfill the requirements of the accounts department as it has 30 valid hosts IP which can be assigned to 26 computers. The mask used is 255.255.255.224
6. The last segment requires 5 valid hosts IP which can be fulfilled by the subnet 192.168.1.224/29 which has the mask as 255.255.255.248 is chosen as per the requirement. The IP with the mask 255.255.255.240 could be chosen but it has 14 valid host IPs and the requirement is less in comparison so the one that is comparable with the requirement is chosen.

   Thus, there is less IP wastage in VLSM as compared to FLSM.

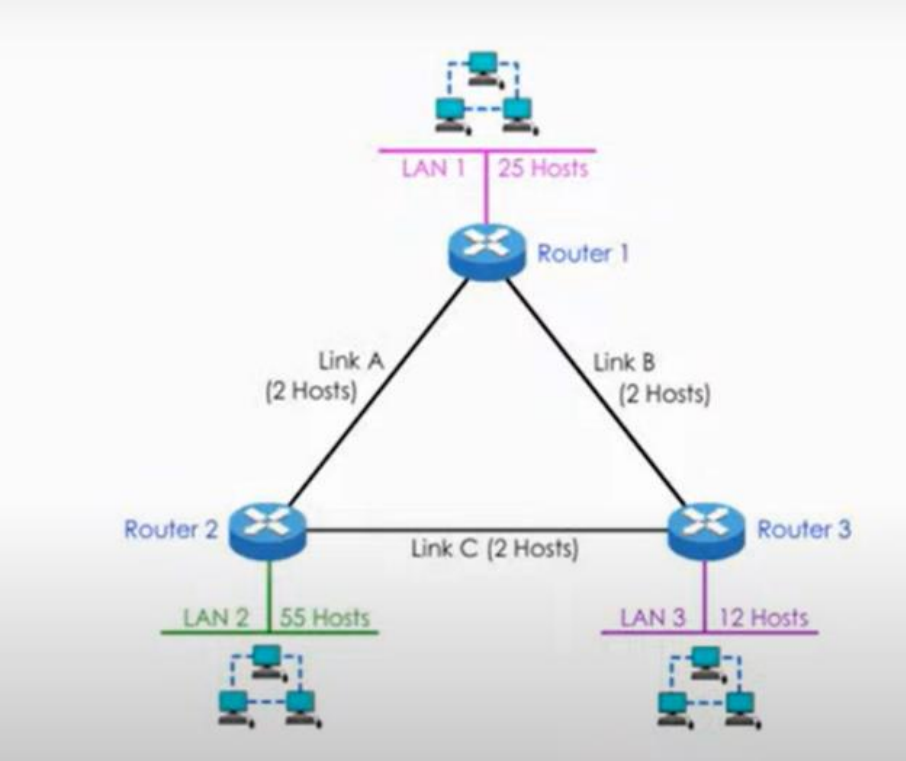
   Advantages of VLSM over FLSM

SN	VLSM (Variable Length Subnet Mask)	FLSM(Fixed Length Subnet Mask)
1	The size is variable and it can have variable number of hosts thus making the IP addressing more efficient by allowing a routed system of different mask length to suit requirements.	All subnets are of equal size and have equal number of hosts
2	Minimum wastage of IP addresses	Wastage of IP addresses
3	It is preferred for public IP addresses as the best option.	FLSM is preferred for private IP addresses

Question 2: Corporate headquarters provided your office a portion of their class B subnet to use at a new office location. Allocate the minimum number of addresses (Using CIDR notation) needed to accommodate each department. Range given: 172.30.232.0/24

- HR: 57 devices
- Sales: 100 devices
- IT: 12 devices
- Finance: 25 devices

Question 3: The network consists of three local area networks: LAN 1, LAN 2, and LAN3. These three LANs are connected with three serial links: Link A, link B, and link C. With an ID range - 192.168.4.0/24, please design an IP plan for the network using VLSM. LAN1 has 25 hosts, LAN2 has 55 hosts, LAN 3 has 12 hosts and Links A,B, and C have 2 hosts each.



Final answer:

Network ID	Subnet Mask	Host	Network
192.168.4.0	/26	64	LAN 2
192.168.4.64	/27	32	LAN 1
192.168.4.96	/28	16	LAN 3
192.168.4.112	/30	4	Link A
192.168.4.116	/30	4	Link B
192.168.4.120	/30	4	Link C
192.168.4.124	/30	4	Unused
192.168.4.128	/26	64	Unused
192.168.4.192	/26	64	Unused

3.4. SUMMARIZATION/SUPERNETTING

Summarization is reverse process of subnetting. In subnetting, you divided one large network into subnets but in summarization, you will combine small subnets to make large network

Purpose of using summarization:

- Reduce the size of routing table. So that router can analyze the routing table faster.
- It will be easy for router to send a summary route rather than individual subnets.

Example:

Consider an ISP providing services to homes. It might create a /30 network for every home, each having only one assignable host identifier. It might create a /16 supernet of all the addresses, broken out further into regional /24 supernets. Routers outside the ISP infrastructure use /16 to send packets in; the ISP uses the /24s to push packets toward the appropriate regional routers, which use the /30s to reach the home networks.

Route Summarization

A summarized route can increase the performance of a router by limiting the routing table and reducing routing traffic.

Consider the following question:

Question1: You have a router with four different LANs attached:

- Network 1 = 192.168.0.0/24
- Network 2 = 192.168.1.0/24
- Network 3 = 192.168.2.0/24
- Network 4 = 192.168.3.0/24

How would you summarize these networks with a single statement?

Answer:

Step 1: Convert all four IP addresses to binary and align them in a list:

Decimal	Binary
192.168.0.0	11000000.10101000.00000000.00000000
192.168.1.0	11000000.10101000.00000001.00000000
192.168.2.0	11000000.10101000.00000010.00000000
192.168.3.0	11000000.10101000.00000011.00000000

Step 2: In the binary section of the grid, count the common bits from left to right. In this example, the first two octets are identical, so we know the first 16 bits are common across all four networks. In addition, the first six bits of the third octet are also common. It may be easier to draw a line through all four binary numbers at the point where the bit pattern changes.

Step 3: Count the number of common bits in the mask. In this example, the first 22 bits are common across all four networks. The answer is 192.168.0.0/22.

Question2: Consider the following router which has six different network:

1. Network 1 = 10.10.0.0/16
2. Network 2 = 10.11.0.0/16
3. Network 3 = 10.12.0.0/16
4. Network 4 = 10.13.0.0/16
5. Network 5 = 10.14.0.0/16
6. Network 6 = 10.15.0.0/16

How would you summarize these networks with a single statement?

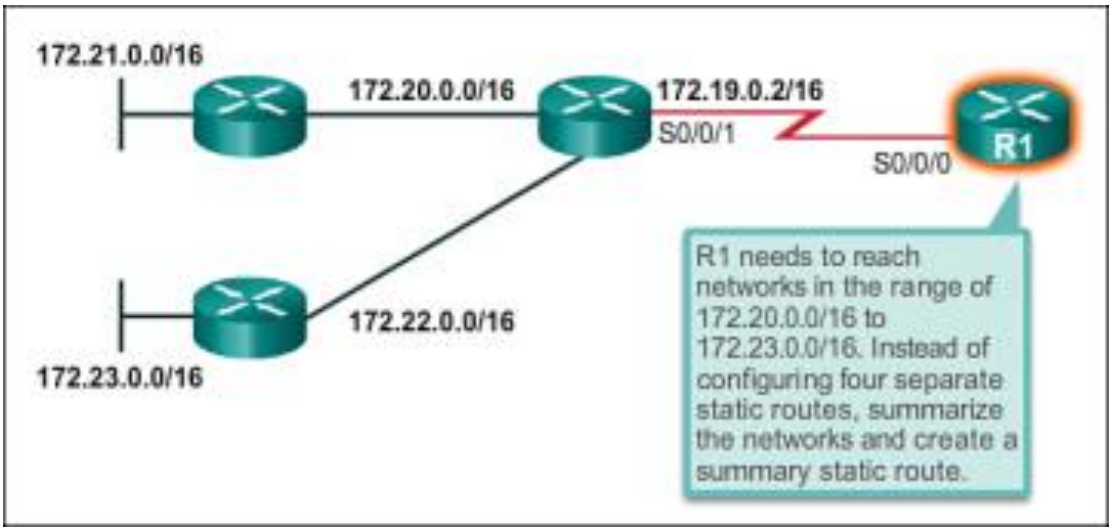
Answer:

Decimal	**Binary**
10.10.0.0	00001010.00001010.00000000.00000000
10.11.0.0	00001010.00001011.00000000.00000000
10.12.0.0	00001010.00001100.00000000.00000000
10.13.0.0	00001010.00001101.00000000.00000000
10.14.0.0	00001010.00001110.00000000.00000000
10.15.0.0	00001010.00001111.00000000.00000000

The first octet is identical and so are the first five bits of the second octet. The answer is 10.8.0.0/13

Summary static route configuration

Route summarization, also known as route aggregation, is the process of advertising a contiguous set of addresses as a single address with a less-specific, shorter subnet mask. CIDR is a form of route summarization and is synonymous with the term supernetting.

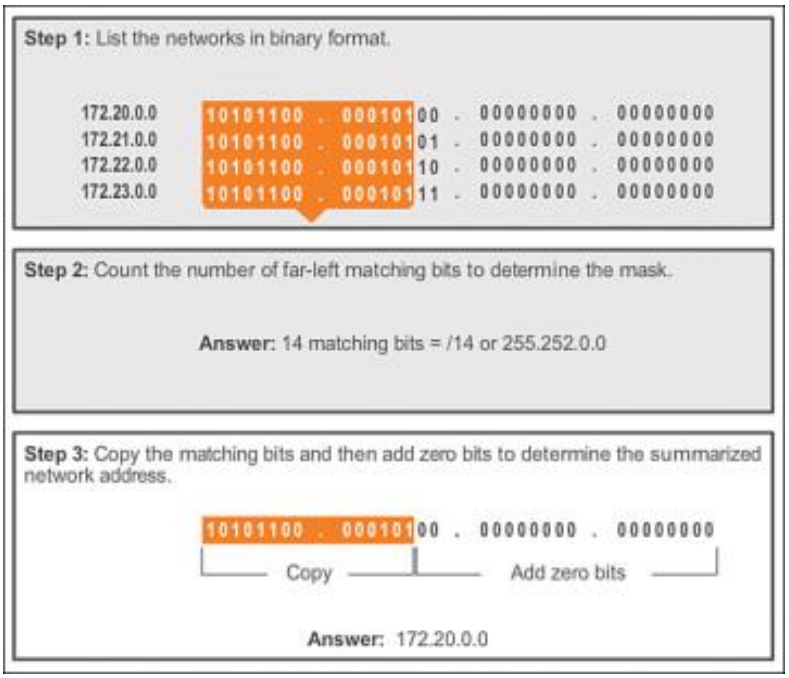


Step 1. List the networks in binary format.

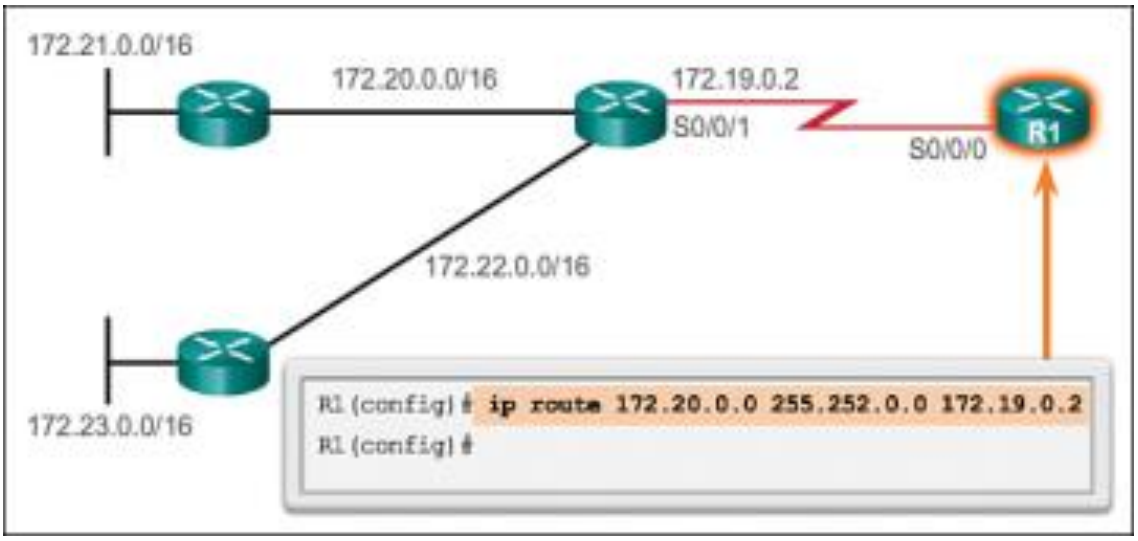
Step 2. Count the number of far-left matching bits to determine the mask for the summary route.

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

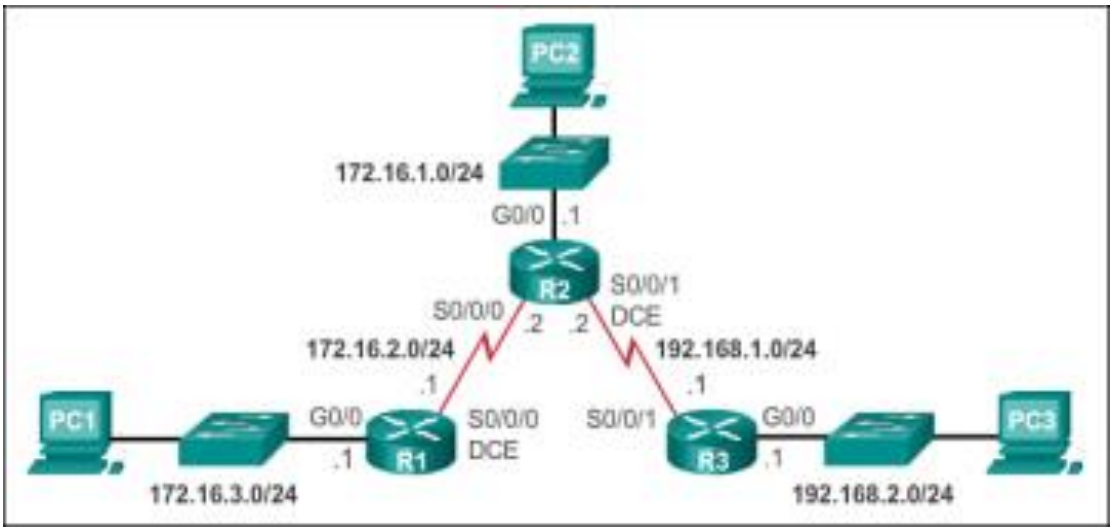
The four networks: 172.20.0.0/16, 172.21.0.0/16, 172.22.0.0/16, and 172.23.0.0/16—can be summarized into the single network address and prefix **172.20.0.0/14**.



Then configure the summary static route as follow:



Q: How can we configure the summarized static route on R3?



Dynamic Routing protocols configuration

Routing protocols can be classified into different groups according to their characteristics. Specifically, routing protocols can be classified by their:

- **Purpose**: Interior Gateway Protocol (IGP) or Exterior Gateway Protocol (EGP)

    1. Interior Gateway Protocol (IGP): RIP, OSPF and EIGRP
    2. Exterior Gateway Protocol (IGP): BGP, EGP

- **Operation**: Distance vector protocol, link-state protocol, or path-vector protocol
    1. Distance vector protocol: RIP, EIGRP
    2. Link-state protocol: OSPF
    3. Path-vector protocol: BGP
- **Behavior**: Classful (legacy) or classless protocol

    - RIPv1 and IGRP, are **Classful (legacy protocols**) and are only used in older networks
    - RIPv2, EIGRP, OSPF, IS-IS, and BGP are classless routing protocol

Routing Protocol	Distance-Vector	Link-State	Path-Vector
RIP	✓		
OSPF		✓	
EIGRP	✓		
BGP			✓

- **RIPv1 routing protocol**
    - **i. RIPv1 Operation**

RIPv1 stands for Routing Information Protocol version 1. It uses Classful routing. The regula678ir routing updates do not carry subnet details and do not support Variable Length subnet masks (VLSM). This is the drawback of RIPv1, due to which it is not possible to have various-sized subnets in the same network class.

Its main functions are:

- To find out the most effective way to route data on a network
- To avoid routing loops

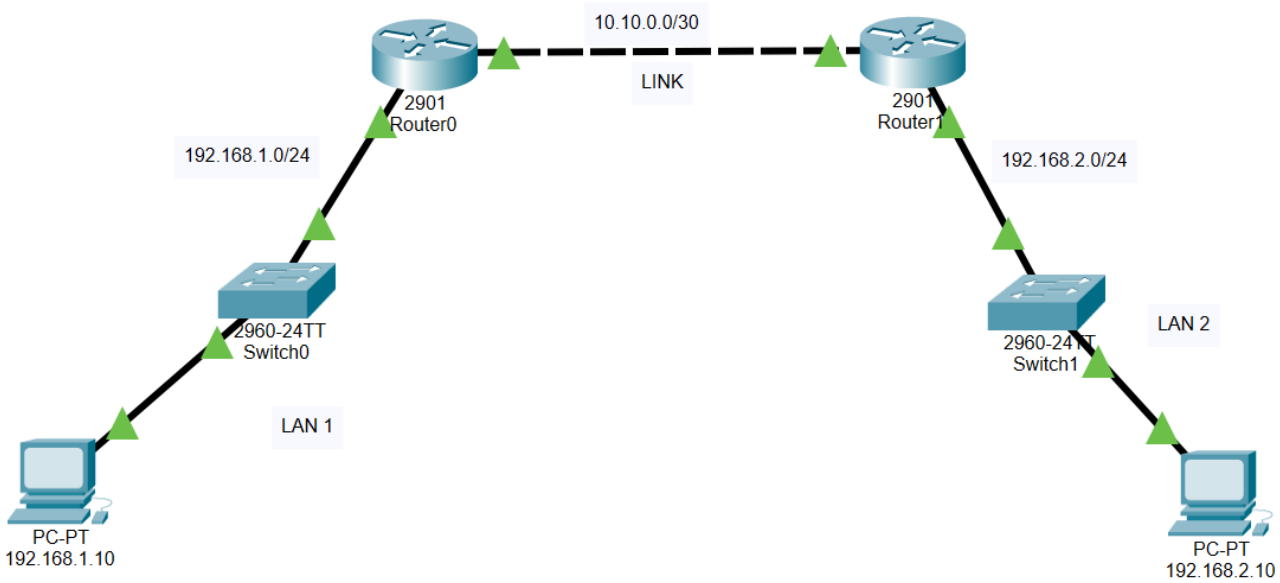
The main advantage of RIP is that its bandwidth utilization is very high and it updates every 30 seconds. However, a maximum of 16 routers can be composed, as it supports only 15 hop counts.

RIPv2 routing protocol

RIPv2 stands for hybrid routing protocol version 2. It is a distance-vector routing protocol defined in RFC 1723 and has the characteristics of link-state routing protocols. It is a classless routing protocol which means it involves the subnet mask having the network addresses in the routing updates.

ii. RIPv1 Configuration

Network diagram below has 3 different network LAN 1: 192.168.1.0/24, LAN 2: 192.168.2.0/24 and LINK between routers: 10.10.0.0/30



Step1: Configuring the interface on Router0 and on Router1, and Assign the IP address on the connected PC

a. **Router0**

```
Router>en
Router#config t
Router(config)#hostname Router0
Router0(config)#interf g0/1
Router0(config-if)#ip address 10.10.0.2 255.255.255.252  // First interface
Router0(config-if)#no shutdown
Router0(config-if)#exit

Router0(config)#inter g0/0  //Second interface
Router0(config-if)#ip address192.168.1.1 255.255.255.0
Router0(config-if)#no shutdown
```

b. Router1

```
Router>en
Router#config t
Router(config)#hostname Router1
Router1(config)#interf g0/1
Router1(config-if)#ip address 10.10.0.1 255.255.255.252  // First interface
Router1(config-if)#no shutdown
Router1(config-if)#exit

Router1(config)#inter g0/0  //Second interface
Router1(config-if)#ip address 192.168.2.1 255.255.255.0
Router1(config-if)#no shutdown
```

Step2: Configuration of RIPv1 on Router0

```
Router0(config)#router RIP
Router0(config-router)#network 192.168.1.0
Router0(config-router)#network 10.10.0.0
Router0(config-router)#end
Router0#copy running-config startup-config // Saving configuration
```

Step3: Configuration of RIPv1 on Router1

```
Router1(config)#router rip
Router1(config-router)#network 10.10.0.0
Router1(config-router)#network 192.168.2.0
Router1(config-router)#exit
Router1(config)#exit
Router1#copy running-config startup-config // Saving configuration
```

iii. RIPv1 Summary

The characteristics of RIPv1 follow:

- Distance-vector protocol.
- Uses UDP port 520.
- Classful protocol (no support for VLSM or CIDR).
- **Metric** is router hop count.
- Maximum hop count is 15; unreachable routes have a metric of 16.
- Periodic route updates broadcast every 30 seconds.
- 25 routes per RIP message.
- Implements split horizon with poison reverse.

- Implements triggered updates.
- No support for authentication.
- Administrative distance for RIP is 120.
- Used in small, flat networks or at the edge of larger networks.

iv. RIPv1 Verification

Router0#show ip route // verification of available routes
Router0#show ip protocols
Router0#show ip RIP database

v. RIPv1 Troubleshooting

Most of the RIP troubleshooting issues are about missing routing information.

Here are a number of things that could go wrong with RIP:

- **Wrong network command(s):** the network command is used to tell RIP what networks to advertise but also where to send RIP routing updates to. Wrong (or missing) network commands will cause issues.
- **Interface shut**: A network on an interface that is in shutdown will not be advertised.
- **Passive interface:** An interface that has been configured as passive will not send any RIP updates.
- **Version mismatch:** RIP has two versions, both routers should use the same version.
- **Max hop count:** When the hop count is 16, the network is considered unreachable.
- **Route Filtering:** Filters might prevent RIP updates from being sent or received.
- **Authentication:** Both RIP routers should have the same authentication parameters.
- **Split horizon:** Networks that are learned on an interface are not advertised out of the same interface.
- **Auto-summarization:** Causes issues with dis-contiguous networks.

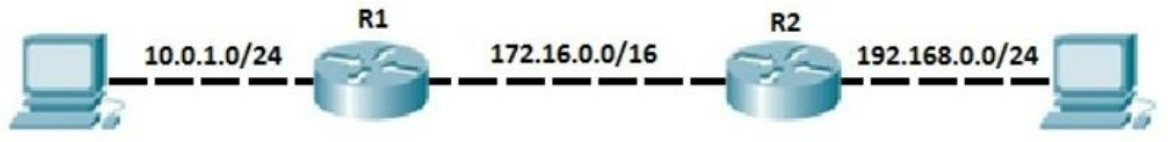
vi. Processing RIP Updates

This protocol advertises the specified network in RIP updates every 30 seconds. RIPv1 does not send the subnet mask in the update.

CONFIGURING RIPV2 ROUTING PROTOCOL

Configuring RIPv2 is a pretty straightforward process. Only three steps are required:

- ✓ Enabling RIP by using the ***router rip*** global configuration command
- ✓ Instructing the router to use RIPv2 by typing the ***version 2*** command
- ✓ Telling RIP which networks to advertise by using one or more ***network*** commands.



So, the configuration on R1 should look like this:

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 10.0.0.0
R1(config-router)#network 172.16.0.0
```

The configuration on R2 looks similar, but with a different network number for the directly connected subnet:

```
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 192.168.0.0
R2(config-router)#network 172.16.0.0
```

You can verify that router R1 has a route to R2's directly connected subnet by typing the ***show IP route or show IP protocols*** command:

```
Router#show ip route
Router# show ip protocols
```

- **IGRP (Interior Gateway Routing Protocol) routing protocol**

i. IGRP operations

Characteristics

- ✓ The Interior Gateway Routing Protocol (IGRP) is a distance-vector routing protocol created by Cisco.
- ✓ In addition to bandwidth, delay (by default), reliability, load, and MTU are all measured in the IGRP protocol.

- ✓ It transmits updates every 90 seconds, with a hold-down time of 280 seconds between each broadcasting session.
- ✓ When network changes occur, triggered updates are utilized to accelerate the convergence process.
- ✓ The IGRP router command needs the inclusion of an AS number.
- ✓ For routers to communicate routing information, they must be in the same Associated System Number (AS).
- ✓ The maximum number of hops allowed by IGRP is 255. It has a default value of 100 and is often changed to 50 or less.
- ✓ The IGRP Administrative Distance value is 100.

The following formula is used to calculate the composite metric of IGRP.

Metric = [K1 * Bandwidth + (K2 * Bandwidth)/ (256-Load) + K3*Delay] * [K5/(Reliability + K4)]

The default constant values are K1 = K3 = 1 and K2 = K4 = K5 = 0.

Note: IGRP is not supported in modern networking equipment

ii. IGRP Verification

R1# show IP route or
R#show IP protocols

iii. IGRP Troubleshooting

- Autonomous system number should be the same.

- **EIGRP routing protocol**

Enhanced **I**nterior **G**ateway **R**outing **P**rotocol (EIGRP) is referred to as a hybrid routing protocol because it has the characteristics of both distance-vector and link-state protocols but now Cisco refers it as an advanced distance vector protocol.

EIGRP is a classless routing protocol, meaning that it sends the subnet mask of its interfaces in routing updates, which use a complex metric based on **bandwidth, load, reliability, MTU and delay**. By default, EIGRP uses only bandwidth and delay.

The main features of EIGRP:

- ✓ Support **VLSM and dis-contiguous** networks
- ✓ **Use Reliable Transport Protocol** (RTP) for the delivery and reception of EIGRP packets

- ✓ Use the best path selection **Diffusing Update Algorithm (DUAL)**, guaranteeing loop-free paths and backup paths throughout the routing domain
- ✓ **Discover neighboring devices using periodic Hello messages** to discover and monitor connection status with its neighbors
- ✓ Exchange the full routing table at startup and send **partial* triggered updates** thereafter (not full updates like distance-vector protocols) and the triggered updates are only sent to routers that need the information. This behavior is different from the link-state protocol in which an update will be sent to all the link-state routers within that area. For example, EIGRP will send updates when a new link comes up or a link becomes unavailable
- ✓ **Supports multiple protocols**: EIGRP can exchange routes for IPv4, IPv6, AppleTalk and IPX/SPX networks
- ✓ **Load balancing**: EIGRP supports unequal metric load balancing, which allows administrators to better distribute traffic flow in their networks.

EIGRP use five types of packets to communicate:

- ✓ **Hello:** used to identify neighbors. They are sent as periodic multicasts
- ✓ **Update:** used to advertise routes, only sent as multicasts when something is changed
- ✓ **Ack:** acknowledges receipt of an update. In fact, Ack is Hello packet without data. It is always unicast and uses UDP.
- ✓ **Query:** used to find alternate paths when all paths to a destination have failed
- ✓ **Reply:** is sent in response to query packets to instruct the originator not to recompute the route because feasible successors exist. Reply packets are always unicast to the originator of the query

These packets are sent over TCP.

After hearing "Hello" from R1, R2 will respond with another "Hello" packet.

R2 will also send its routing table to R1 by "Update" packets. Remember that R2 will send its complete routing table for the first time.

R1 confirms it has received the Update packet by an "ACK" message.

R1 will also send to R2 all of its routing table for the first time

R2 sends a message saying it has received R1's routing table.

I. Configuring EIGRP for IPv4

- **EIGRP Network topology**

The topology table is where EIGRP stores the information for up to six alternate routes to a particular network.

EIGRP uses three tables:

- ✓ **The neighbor table,**
- ✓ **The topology table**, and
- ✓ **The IP routing table.**

The neighbor table keeps state information regarding neighbors, and is displayed using the **show ip eigrp neighbors** command.

Based on the contents of the **topology table**, each router chooses its best routes and installs these routes in its respective **IP routing table**.

- **Autonomous System Number**

An autonomous system (AS) is a network or a collection of networks that are all managed and supervised by a single entity or organization.

Autonomous System Number (ASN) is a globally unique identifier that defines a group of one or more IP prefixes run by one or more network operators that maintain a single, clearly-defined routing policy. All routers in the same network must use the same AS number.

- **Router EIGRP Commands (IPv4)**

Router(config)#router eigrp 1	Syntax: **router eigrp** <AS number> 1 is the Autonomous System (AS) number. It can be from 1 to 65535.
Router(config-router)#network 192.168.1.0 0.0.0.255	Router will turn on EIGRP 1 process on all the interfaces belonging to 192.168.1.0/24 network. `Router(config-router)# network network_address [wildcard_mask]`

- **Passive interface**

Passive EIGRP interfaces do not send out or process EIGRP hellos, which prevents EIGRP from forming adjacencies on that interface.

To configure an EIGRP interface as passive, you use the command **passive-interface interface-id** under the EIGRP process for classic configuration.

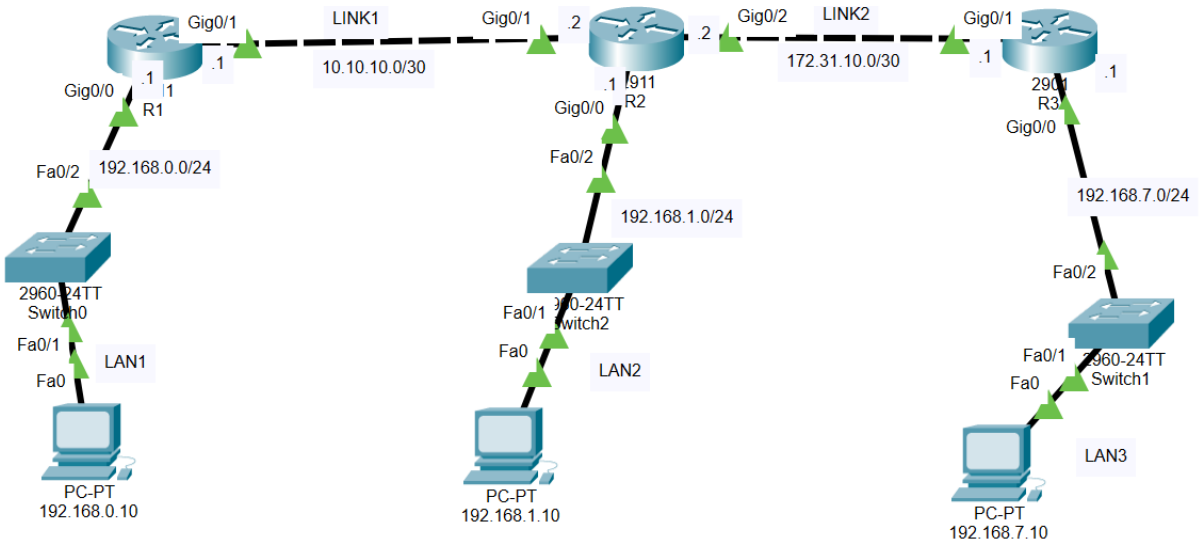
For example:

```
Router# config t
Router(config)#router OSPF 1
Router(config-router)#passive-interface G0/0
Router(config-router)#end
```

The **EIGRP term "active**" refers to a route for which a router is currently using the Query process to find a loop-free alternative route

EXAMPLE:

The following diagram has 5 different networks: LAN1-192.168.0.0/24, LAN2-198.168.1.0/24, LAN3-192.168.7.0/24, LINK1 which interconnect R1 and R2-10.10.10.0/30 and LINK2 which interconnect R2 and R3: 172.31.10.0/30



Step1: Configuring the interfaces on R1, R2, and R3

b. Configurin g interface on R1

```
Router>enable
Router#configure terminal
Router(config)#hostname R1
R1(config)#interface G0/0
R1(config-if)#ip address 192.168.0.1 255.255.255.0
R1(config-if)#no shutdown

R1(config-if)#exit
R1(config)#interface G0/1
R1(config-if)#ip address 10.10.10.1 255.255.255.252
R1(config-if)#no shutdown
```

c. Configuring interface on R2

```
Router>enable
Router#configure terminal
```

```
Router(config)#hostname R2
R2(config)#interface g0/1
R2(config-if)#ip address 10.10.10.2 255.255.255.252
R2(config-if)#no shutdown

R2(config-if)#exit
R2(config)#interface g0/0
R2(config-if)#ip address 192.168.1.1 255.255.255.0
R2(config-if)#no shutdown


R2(config-if)#exit
R2(config)#interface G0/2
R2(config-if)#ip address 172.31.10.2 255.255.255.252
R2(config-if)#no shutdown
```

d. Configuring interface on R3

```
Router>en
Router#configure terminal
Router(config)#hostname R3
R3(config)#interface g0/1
R3(config-if)#ip address 172.31.10.1 255.255.255.252
R3(config-if)#no shutdown

R3(config-if)#exit
R3(config)#interface g0/0
R3(config-if)#ip address 192.168.7.1 255.255.255.0
R3(config-if)#no shutdown
```

Step2: Configuring the EIGRP on R1, R2, and R3

a. Configure the EIGRP on R1

```
R1(config)#router EIGRP 1
R1(config-router)#network 192.168.0.0  0.0.0.255
R1(config-router)#network 10.10.10.0    0.0.0.3
R1(config-router)#exit
R1(config)#
```

b. Configure the EIGRP on R2

```
R2(config)#router eigrp 1
R2(config-router)#network 10.10.10.0   0.0.0.3
R2(config-router)#network 172.31.10.0 0.0.0.3
R2(config-router)#network 192.168.1.0 0.0.0.255
R2(config-router)#exit
```

c. Configure the EIGRP on R3

```
R3(config)#router egrp 1
R3(config-router)#network 172.31.10.0  0.0.0.3
R3(config-router)#network 192.168.7.0  0.0.0.255
```

R3(config-router)#exit

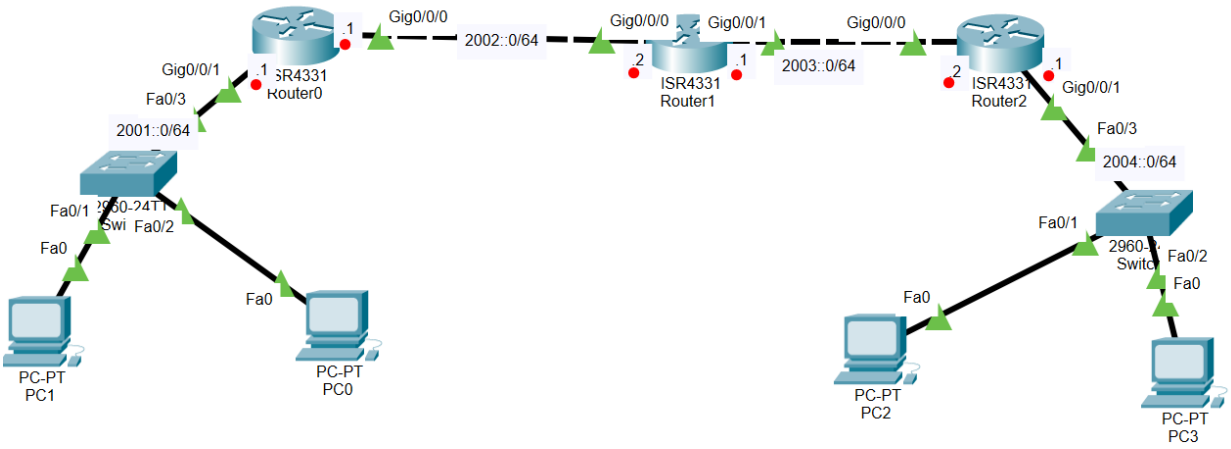
- **Verifying EIGRP**
  - show ip eigrp
  - show ip eigrp neighbors
  - show ip eigrp neighbors details
  - show ip eigrp interfaces
  - show ip route

Troubleshooting EIGRP issues

The autonomous system number should be the same, and make sure the wild mask is well configured.

I. Configuring EIGRP for IPv6

- **EIGRP Network topology**



Note: Autonomous **S**ystem **N**umber**:** should be the same for all connecter routers.

Router EIGRP Commands (IPv6)

Step1: Configure IPv6 addresses on PCs and router interfaces

ROUTER1:

```
Router>enable
Router# config  t
Router(config)#hostname R1
R1(config)#ipv6 unicast-routing
R1(config)#interface G0/0/0
R1(config-if)#ipv6 address 2001::1/64
R1(config-if)#no shut
R1(config-if)#
R1(config-if)#interface G0/0/1
R1(config-if)#ipv6 enable
```

```
R1(config-if)#ipv6 address 2002::1/64
R1(config-if)#no shut
```

ROUTER2:

```
Router>enable
Router# config  t
Router(config)#hostname R2
R2(config)#ipv6 unicast-routing
R2(config)#interface G0/0/0
R2(config-if)#ipv6 address 2002::2/64
R2(config-if)#no shut
R2(config-if)#
R2(config-if)#interface G0/0/1
R2(config-if)#ipv6 enable
R2(config-if)#ipv6 address 2003::1/64
R2(config-if)#no shut
```

ROUTER3:

```
Router>enable
Router# config  t
Router(config)#hostname R3
R3(config)#ipv6 unicast-routing
R3(config)#interface G0/0/0
R3(config-if)#ipv6 enable
R3(config-if)#ipv6 address 2003::2/64
R3(config-if)#no shut
R3(config-if)#
R3(config-if)#interface G0/0/1
R3(config-if)#ipv6 enable
R3(config-if)#ipv6 address 2004::1/64
R3(config-if)#no shut
```

Step2: configure EIGRPv6 on the routers

ROUTER1

```
R1#config t
R1(config)#ipv6 router eigrp 10 // configure the EIGRP with autonomous system number of 10
R1(config-rtr)#eigrp router-id 1.1.1.1
R1(config-rtr)#no sh
R1(config-rtr)#exit

R1(config)#interface g0/0/0
R1(config-if)#ipv6 eigrp 10  //assigning the routing protocol to the interface
R1(config-if)#no sh

R1(config-if)#interface g0/0/1
R1(config-if)#ipv6 eigrp 10 //assigning the routing protocol to the interface
R1(config-if)#exit
R1(config)#
```

Router 2:

```
R2#config t
R2(config)#ipv6 router eigrp 10 // configure the EIGRP with autonomous system number of 10
```

R2(config-rtr)#eigrp router-id 2.2.2.2
R2(config-rtr)#no sh
R2(config-rtr)#exit

R2(config)#interface g0/0/0
R2(config-if)#ipv6 eigrp 10 //assigning the routing protocol to the interface
R2(config-if)#no sh

R2(config-if)#interface g0/0/1
R2(config-if)#ipv6 eigrp 10 //assigning the routing protocol to the interface
R2(config-if)#exit
R2(config)#

Router 3:

R3#config t
R3(config)#ipv6 router eigrp 10 // configure the EIGRP with autonomous system number of 10
R3(config-rtr)#eigrp router-id 3.3.3.3
R3(config-rtr)#no sh
R3(config-rtr)#exit

R3(config)#interface g0/0/0
R3(config-if)#ipv6 eigrp 10 //assigning the routing protocol to the interface
R3(config-if)#no sh

R3(config-if)#interface g0/0/1
R3(config-if)#ipv6 eigrp 10 //assigning the routing protocol to the interface
R3(config-if)#exit
R3(config)#

- **Verifying EIGRP**

For verification of configured routing protocols you can use the following commands:

1. **show ipv6 route**

```
Router#show ipv6 route
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
C   2001::/64 [0/0]
     via GigabitEthernet0/0/1, directly connected
L   2001::1/128 [0/0]
     via GigabitEthernet0/0/1, receive
C   2002::/64 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   2002::1/128 [0/0]
     via GigabitEthernet0/0/0, receive
D   2003::/64 [90/3072]
     via FE80::201:63FF:FE35:8E01, GigabitEthernet0/0/0
D   2004::/64 [90/5632]
     via FE80::201:63FF:FE35:8E01, GigabitEthernet0/0/0
L   FF00::/8 [0/0]
     via Null0, receive
```

2. **show ipv6 eigrp neighbor**
3. **show ipv6 protocols**
    - **Troubleshooting EIGRP issues**

- Issue the show ip eigrp interface command to verify
- Check whether all routers have same Autonomous system number

- Check the IP configurations

OSPFv2 (Single OSPF) routing protocol

OSPF is one of the most popular link state routing protocols. It is an open standard, so it can be run on routers from different vendors.

OSPF supports **key features** such as:

- IPv4 and IPv6 routing
- Classless routing
- Equal cost load balancing

OSPF has a default administrative distance of 110. It uses cost as the parameter for determining route metric. It uses the multicast address of 224.0.0.5 and 224.0.0.6 for communication between OSPF-enabled neighbors.

OSPF routers store routing and topology information in three tables.

- **Neighbor table**-which stores information about OSPF neighbors.
- **Topology table**-stores topology structure of the network.
- **Routing table**-stores the best routes

OSPF areas

An area is simply a logical grouping of adjacent networks and routers. All routers in the same area have the same topology table and don't know about routers in other areas. The main benefits of using areas in an OSPF network are:

- Routing tables on the routers are reduced.
- Routing updates are reduced.

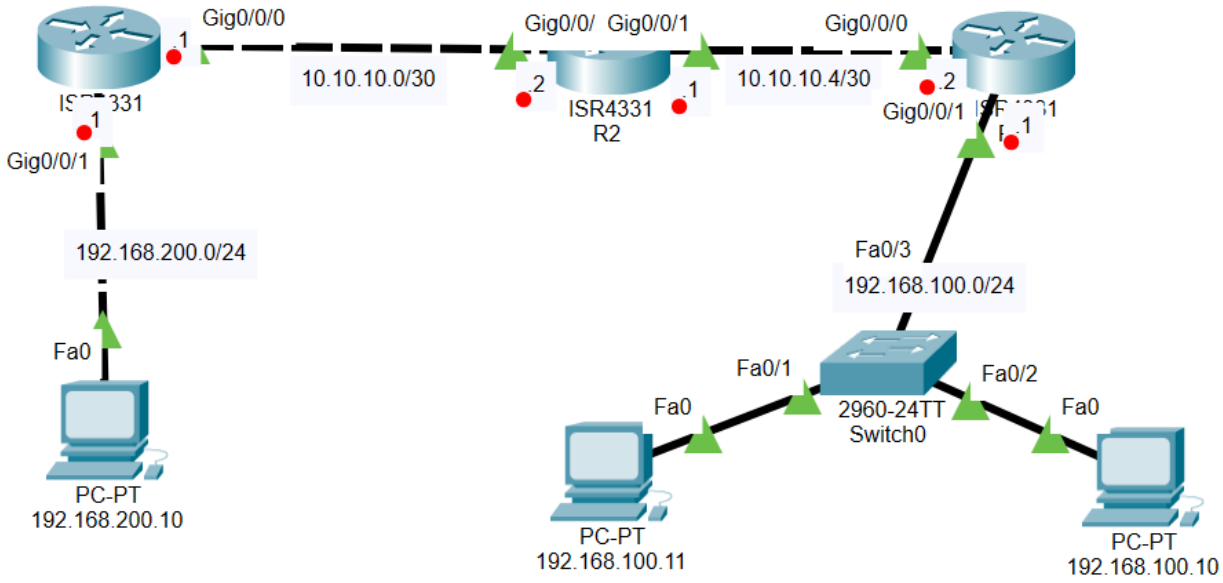
Each area in an OSPF network must be connected to the **backbone area** (also known as **area 0**). All routers inside an area must have the **same area ID**.

A router that has interfaces in more than one area (for example area 0 and area 1) is known as an Area Border Router (**ABR**). A router that connects an OSPF network to other routing networks (for example, to an EIGRP network) is called an Autonomous System Border Router (**ASBR**).

Configure OSPF on the routers:
The configuration is pretty simple and requires only two major steps:
1. Enable OSPF on a router using the *router ospf PROCESS_ID* in the global configuration mode.

2.Define on which interfaces OSPF will run and what networks will be advertised using *network IP_ADDRESS WILCARD_MASK AREA* command in the OSPF configuration mode.

OSPF Network topology



Step1: Configure IP addresses on PCs and router interfaces

ROUTER1:

Router>en
Router#conf t
Router(config)#hostname R1
R1(config)#interface G0/0/0
R1(config-if)#ip address 192.168.200.1 255.255.255.0
R1(config-if)#no sh

R1(config-if)#interface g0/0/1
R1(config-if)#ip address 10.10.10.1 255.255.255.252
R1(config-if)#no sh

ROUTER2:

Router>en
Router#config t
Router(config)#hostname R2
R2(config)#interface g0/0/0
R2(config-if)#ip address 10.10.10.2 255.255.255.252
R2(config-if)#no sh

R2(config-if)#
R2(config-if)#interface g0/0/1
R2(config-if)#ip address 10.10.10.5 255.255.255.252
R2(config-if)#no sh

ROUTER3:

```
Router>en
Router# config t
Router(config)# hostname R3
R3(config)#interface g0/0/0
R3(config-if)#ip address 10.10.10.6 255.255.255.252
R3(config-if)#no sh
R3(config-if)#

R3(config-if)#interface g0/0/1
R3(config-if)#ip address 192.168.100.1 255.255.255.0
R3(config-if)#no sh
```

STEP2: Configure OSPF on the routers

Router 1:

```
R1#config t
R1(config)#router OSPF 20
R1(config-router)#network 10.10.10.0       0.0.0.3 area 0
R1(config-router)#network 192.168.200.0 0.0.0.255 area 0
R1(config-router)#
```

Router2:

```
R2>en
R2#config t
R2(config)#router OSPF 20
R2(config-router)#network 10.10.10.0 0.0.0.3 area 0
R2(config-router)#network 10.10.10.4 0.0.0.3 area 0
R2(config-router)#
```

Router3:

```
R3#config t
R3(config)#router OSPF 20
R3(config-router)#network 10.10.10.4          0.0.0.3 area 0
R3(config-router)#network 192.168.100.0     0.0.0.255 area 0
R3(config-router)#no sh
```

Verifying OSPF

- show ip ospf neighbor

```
R2#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.100.1     1   FULL/BDR        00:00:35    10.10.10.6      GigabitEthernet0/0/1
R2#
```

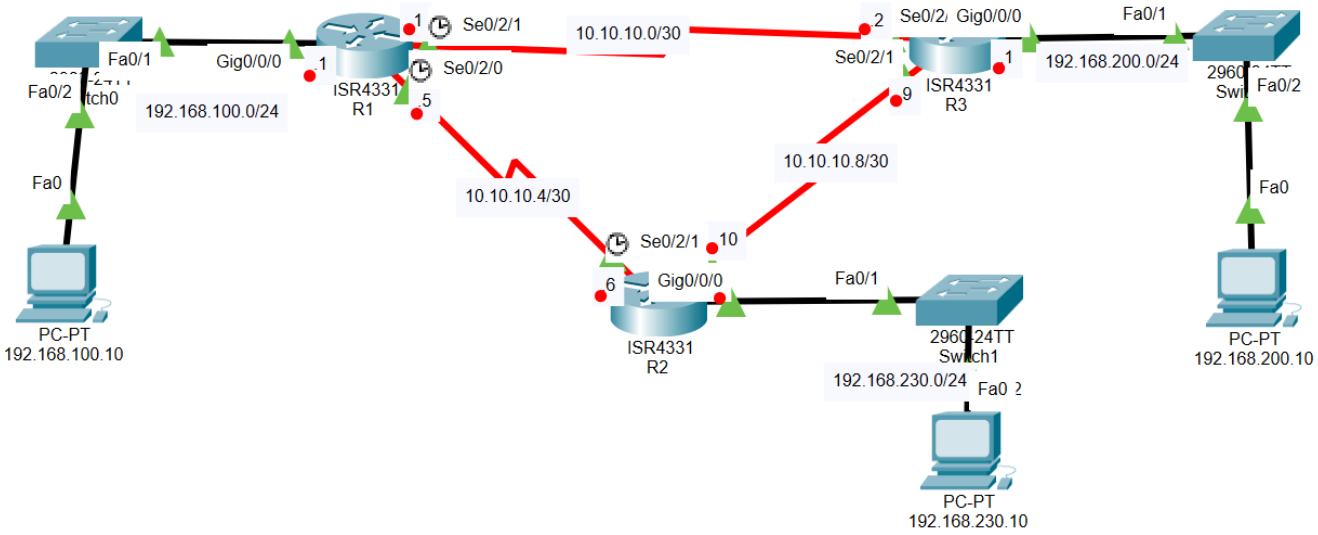
- show ip route ospf
- show ip ospf neighbors detail

- show ip ospf database
- show ip ospf interface

Troubleshooting OSPF issues

- Make sure that all routers are in the same area
- No error on network configuration commands

Configure OSPFv2 in a Single Area



Step1: Assigning IP addresses on router and PCs' interfaces

ROUTER1:

Router>en
Router#config t
Router(config)#hostname R1 //change the router name
R1(config)#interface g0/0/0
R1(config-if)#ip address 192.168.100.1 255.255.255.0 //assigning the IP on interface
R1(config-if)#no sh
R1(config-if)#exit

R1(config)#interface s0/2/1
R1(config-if)#ip address 10.10.10.1 255.255.255.252
R1(config-if)#clock rate 64000
R1(config-if)#no sh

R1(config-if)#interface s0/2/0
R1(config-if)#ip address 10.10.10.5 255.255.255.252
R1(config-if)#clock rate 64000
R1(config-if)#no sh

```
R1(config)#interface loopback 0     //configure the Loopback address on Router 1
R1(config-if)#ip address 1.1.1.1 255.255.255.255
R1(config-if)#
```

ROUTER2:

```
Router>en
Router#conf t
Router(config)#hostname R2
R2(config)#interface s0/2/1
R2(config-if)#ip address 10.10.10.10 255.255.255.252
R2(config-if)#clock rate 64000
R2(config-if)#no sh

R2(config-if)#interface s0/2/0
R2(config-if)#ip address 10.10.10.6 255.255.255.252
R2(config-if)#no sh

R2(config-if)#interface g0/0/0
R2(config-if)#ip address 192.168.230.1 255.255.255.0
R2(config-if)#no sh

R2(config)#interface loopback 0     //configure the Loopback address on Router 1
R2(config-if)#ip address 2.2.2.2 255.255.255.255
R2(config-if)#
```

ROUTER3:

```
Router>en
Router#config t
Router(config)#hostname R3
R3(config)#interface s0/2/1
R3(config-if)#ip address 10.10.10.9 255.255.255.252
R3(config-if)#no sh

R3(config-if)#interface s0/2/0
R3(config-if)#ip address 10.10.10.2 255.255.255.252
R3(config-if)#no sh
R3(config-if)#interface g0/0/0
R3(config-if)#ip address 192.168.200.1 255.255.255.0
R3(config-if)#no sh
```

STEP2: CONFIGURE THE OSPF on routers

ROUTER1:

```
R1#conf t
R1(config)#router OSPF 10
R1(config-router)#router-id 1.1.1.1
```

```
R1(config-router)#network 10.10.10.0 0.0.0.3 area 0
R1(config-router)#network 10.10.10.4 0.0.0.3 area 0
R1(config-router)#network 192.168.100.0 0.0.0.255 area 0
R1(config-router)#end
```

ROUTER2:

```
R2(config)#
R2(config)#router OSPF 10
R2(config-router)#router-id 2.2.2.2
R2(config-router)#network 192.168.203.0 0.0.0.255 area 0
R2(config-router)#network 10.10.10.4 0.0.0.3 area 0
R2(config-router)#network 10.10.10.8 0.0.0.3 area 0
R2(config-router)#
```

ROUTER3:

```
R3(config)#
R3(config)#router OSPF 10
R3(config-router)#router-id 3.3.3.3
R3(config-router)#network 10.10.10.8 0.0.0.3 area 0
R3(config-router)#network 10.10.10.0 0.0.0.3 area 0
R3(config-router)#network 192.168.200.0 0.0.0.255 area 0
R3(config-router)# end
R3#write
```

Factor to choosing Dynamic routing protocol

- Scalability
- Vendor interoperability
- Familiarity
- Convergence

Convergence time: Amount of time a dynamic routing protocol takes to reroute around a network failure

- Summarization: A routing protocol feature that allows multiple routes to be represented by a single summary route

- 10.0.0.0/24
- 10.0.1.0/24
- 10.0.2.0/24
- 10.0.3.0/24 => summary 10.0.0.0/22

4. Apply HSRP (Hot standby router protocol)

The Hot Standby Router Protocol (HSRP) is an IP routing redundancy protocol designed to allow for transparent failover at the first-hop IP router. HSRP provides high network availability because it routes IP traffic from hosts on networks without relying on the availability of any single router.

HSRP (Hot Standby Router Protocol) is a member of the FHRP (First Host Redundant protocol) family. It works only on Cisco routers.

FHRP family are HSRP (Hot Standby Router Protocol), VRRP (Virtual Router Redundancy Protocol), and GLBP (Gateway Load Balancing Protocol).

HSRP States

HSRP consists of 6 states:

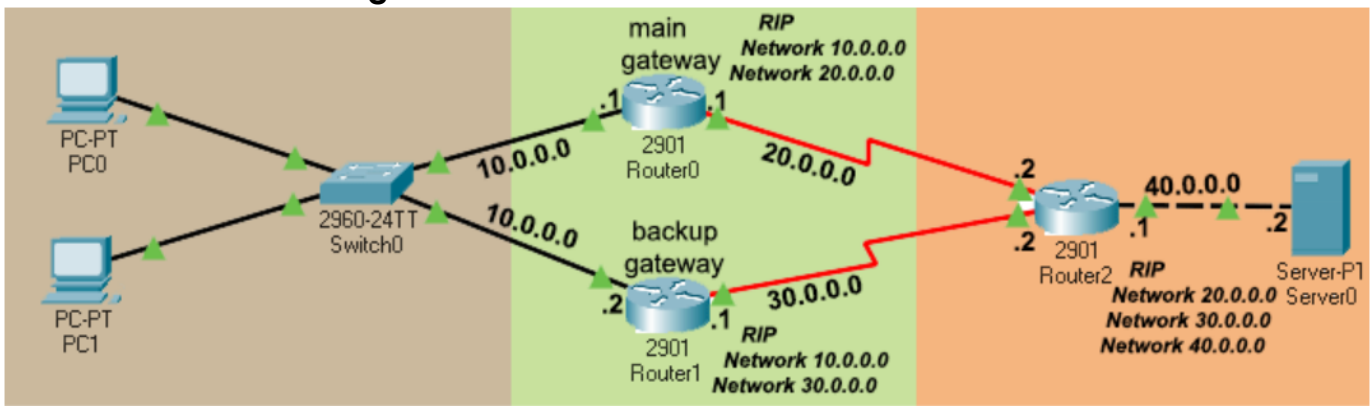
State	Description
Initial	This is the beginning state. It indicates HSRP is not running. It happens when the configuration changes or the interface is first turned on
Learn	The router has not determined the virtual IP address and has not yet seen an authenticated hello message from the active router. In this state, the router still waits to hear from the active router.
Listen	The router knows both IP and MAC address of the virtual router but it is not the active or standby router. For example, if there are 3 routers in HSRP group, the router which is not in active or standby state will remain in listen state.
Speak	The router sends periodic HSRP hellos and participates in the election of the active or standby router.
Standby	In this state, the router monitors hellos from the active router and it will take the active state when the current active router fails (no packets heard from active router)
Active	The router forwards packets that are sent to the HSRP group. The router also sends periodic hello messages

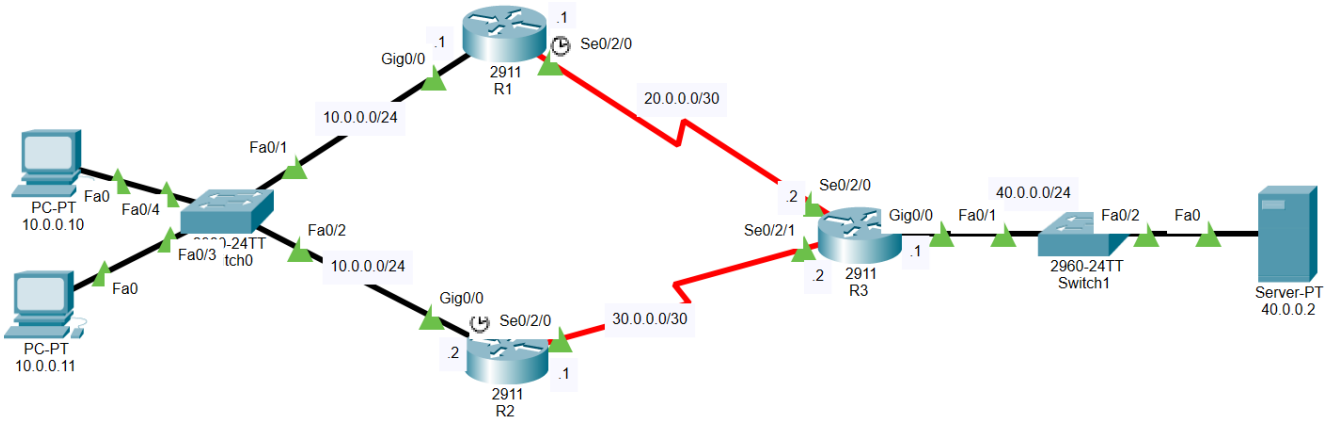
Hot Standby Router Protocol (HSRP) has 2-versions:

version 1: The messages are multicast at 224.0.0.2 and use the UDP port 1985. This version allows group numbers ranging from 0 to 255.

version 2 The messages are multicast at 224.0.0.102 and use the UDP port 1985. This version allows group numbers ranging from 0 to 4095.

Consider the below diagram:





ROUTER 1 Configuration:

Interface configuration:

Router>en
Router#conf t
Router(config)#hostname R1
R1(config)#interface s0/2/0
R1(config-if)#ip address 20.0.0.1 255.255.255.252
R1(config-if)#clock rate 64000
R1(config-if)#no sh
R1(config-if)#interface g0/0
R1(config-if)#ip address 10.0.0.1 255.255.255.0
R1(config-if)#no sh
RIP CONFIGURATION
R1#config t
R1(config)#router RIP
R1(config-router)#version 2
R1(config-router)#network 10.0.0.0
R1(config-router)#network 20.0.0.0
R1(config-router)#exit
R1(config)#do write

ROUTER 2 CONFIGURATION:

```
Router>en
Router#config t
Router(config)#hostname R2
R2(config)#interface g0/0
R2(config-if)#ip address 10.0.0.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#interface s0/2/0
R2(config-if)#ip address 30.0.0.1 255.255.255.252
R2(config-if)#no sh
R2(config-if)#clock rate 64000
R2(config-if)#exit
```

RIP configuration:

```
R2>en
R2#config t
R2(config)#router RIP
R2(config-router)#version 2
R2(config-router)#network 30.0.0.0
R2(config-router)#network 10.0.0.0
R2(config-router)#exit
R2(config)#
```

ROUTER 3 CONFIGURATION:

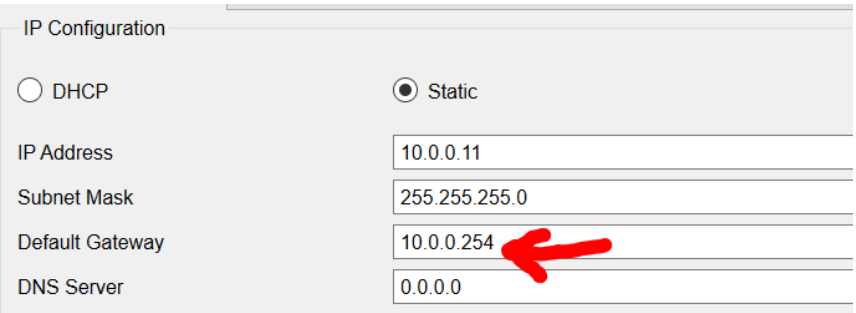
```
Router>en
Router#config t
Router(config)#hostname R3  //renaming the router
R3(config)#interface s0/2/0
R3(config-if)#ip address 20.0.0.2 255.255.255.252
R3(config-if)#no sh
R3(config-if)#interface s0/2/1
R3(config-if)#ip address 30.0.0.2 255.255.255.252
R3(config-if)#no sh
R3(config-if)#interface g0/0
R3(config-if)#ip address 40.0.0.1 255.255.255.0
R3(config-if)#no sh
R3(config-if)#
```

RIP Configuration:

```
R3#config t
R3(config)#router RIP
R3(config-router)#version 2
R3(config-router)#network 40.0.0.0
R3(config-router)#network 20.0.0.0
R3(config-router)#network 30.0.0.0
R3(config-router)#exit
R3(config)#
```

R3# copy running-config startup-config // For saving the provided configuration

PCs CONFIGURATION:



On the Gateway address, we put a virtual address which is not on either R1 or R2.

HSRP configuration

Router(config-if)#standby group-id **ip** ip-address

The group-id is the group number of HSRP. The IP address is a virtual IP address that you want to use as the default gateway IP address.

CONFIGURE HSRP on ROUTER 1:

R1>enable
R1#config t
R1(config)#interface g0/0
R1(config-if)#standby 10 ip 10.0.0.254
R1(config-if)#standby 10 preempt
R1(config-if)#standby 10 priority 110
//R2(config-if)# standby 10 authentication md5 key-string mypassword
R1(config-if)#exit
R1(config)#

CONFIGURE HSRP on ROUTER 2:

R2>en
R2#config t
R2(config)#interface g0/0
R2(config-if)#standby 10 ip 10.0.0.254
R2(config-if)#standby 10 preempt
R2(config-if)# standby 10 authentication md5 key-string mypassword
R2(config-if)#exit

Note:

- **The "preempt"** command allows a router with a higher priority to take over as the active router if it becomes available.
- **The "authentication"** command enables authentication using the MD5 algorithm and a shared password.

HSRP Verification:

R1# show standby

```
R1#show standby
GigabitEthernet0/0 - Group 10
  State is Active
    13 state changes, last state change 01:15:52
  Virtual IP address is 10.0.0.254
  Active virtual MAC address is 0000.0C07.AC0A
    Local virtual MAC address is 0000.0C07.AC0A (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.898 secs
  Preemption enabled
  Active router is local
  Standby router is unknown, priority 100 (expires in 27360043 sec)
  Priority 110 (configured 110)
  Group name is hsrp-Gig0/0-10 (default)
```

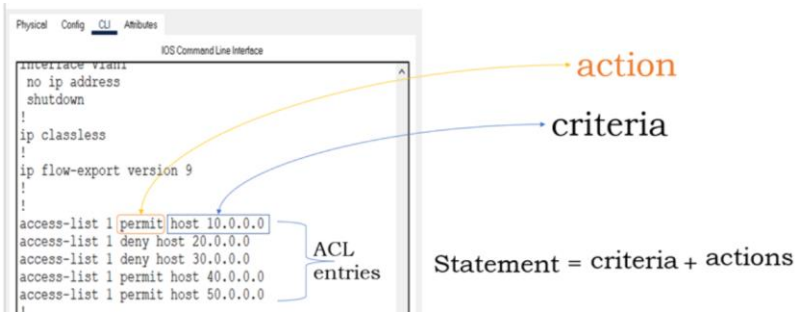
R1#show standby brief

```
R1#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig0/0      10   110 P Active   local           unknown         10.0.0.254
```

LEARNING OUTCOME 4: CONFIGURE ACCESS CONTROL LIST (ACL)

Access control lists (ACL) is a set of rules or filters that define how traffic is allowed or denied through a network device such as a router, switch, or firewall.

An access list is a list of statements. An ACL statement consists of **criteria** and **actions**. **The criteria** define the pattern to be matched and **the actions** define the functions that must be performed when the pattern is matched.



An ACL is used to control access to network resources by permitting or denying traffic based on criteria such as:

- Source IP address
- Destination IP address

- Source port number
- Destination port number
- Protocol (TCP, UDP, ICMP, etc.)
- Time of day
- Type of service (TOS)

The advantages of using access control lists include:

- Better protection of internet-facing servers.
- More control of access through entry points.
- More control of access to and traffic between internal networks.
- More granular control of user and group permissions.
- Better protection from spoofing and denial of service attacks.
- Improved network performance and manageability.

Normally ACLs reside in a firewall router or in a router connecting two internal networks.

You can set up ACLs to control traffic at Layer 2, Layer 3, or Layer 4. MAC ACLs operate on Layer 2. IP ACLs operate on Layers 3 and 4.

Limitations

The following limitations apply to ACLs. These limitations are platform dependent.

- Maximum of 100 ACLs.
- Maximum rules per ACL is 8-10.
- The system supports ACLs set up for inbound traffic only.
- You can configure mirror or redirect attributes for a given ACL rule, but not both.
- The system does not support MAC ACLs and IP ACLs on the same interface.
- A hardware platform may support a limited number of counter resources, so it may not be possible to log every ACL rule.

Types of Internet protocol Access Control lists (IP ACL):

1. Standard access control list

These ACLs permit or deny packets based only on the source IPv4 address, it uses range number 1-99, its extended number is ranging from:1300-1999

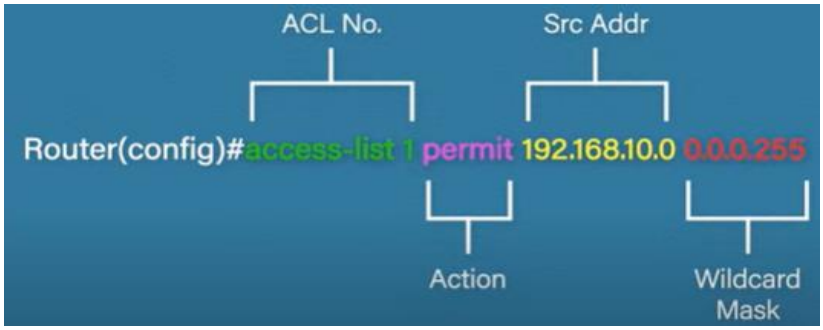
Note:

- Standard ACL are applied closest to the destination.
- At the end of each ACL, there is an **implicit deny** this means deny everything

Steps of configuring the Standard Access Control List:

1. Create an access list ranging from 1-99
2. Apply the access list to the interface (inbound or outbound)

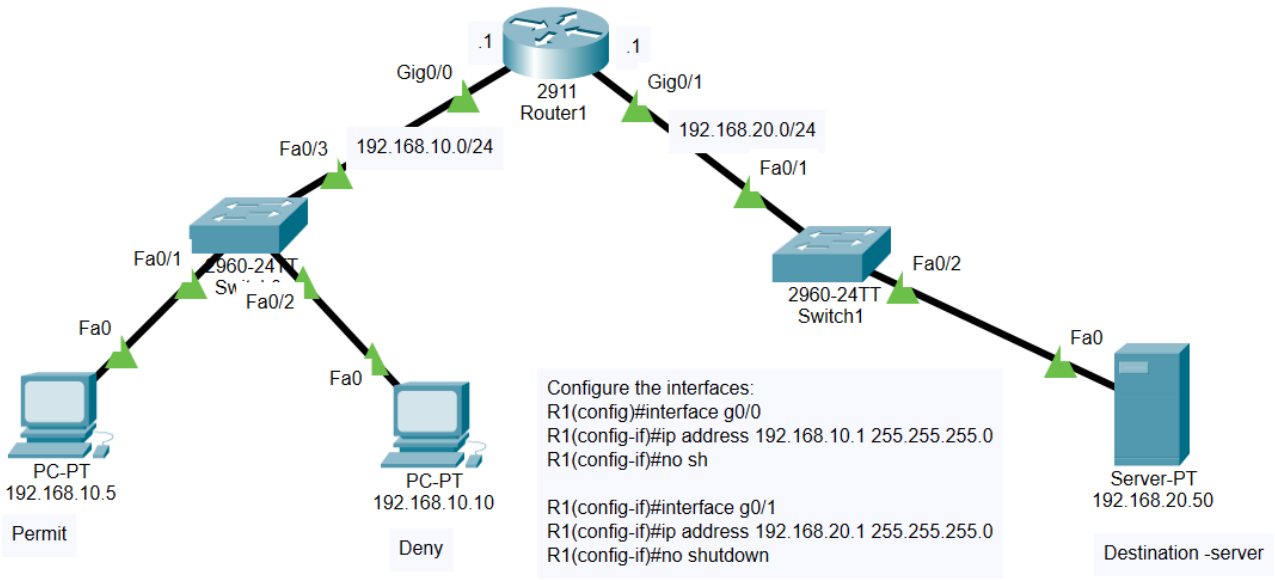
Example 1: Create an access control list that will allow traffic from any host on the 192.168.10.0/24 network.



Router(config)#*access-list 1 permit 192.168.10.0 0.0.0.255*
Router(config)#*interface fa 0/0*
Router(config-if)#*ip access-group 1 in* *//Applying the ACL to the interface*

In this example, ACL 10 permits the host on the source network 192.168.10.0/24. Because of the implied "deny any" at the end, all traffic except for traffic coming from the 192.168.10.0/24 network is blocked with this ACL.

Example2: Consider the network diagram below with two networks 192.168.10.0/24 (PC1: 192.168.10.5 and PC2: 192.168.10.10) and 192.168.20.0/24 (Server: 192.168.20.50)



Question: Create the standard access control list which will deny PC: 192.168.10.10 to access the server and Permit PC: 192.168.10.5 to access the server.

R1#conf t
R1(config)#access-list 10 deny 192.168.10.10 0.0.0.0 //ACL 10 for deny 192.168.10.10
R1(config)#access-list 10 permit any // ACL 10 for allowing another remaining host
R1(config)#interface g0/0
R1(config-if)#ip access-group 10 in //Applying the ACL 10 to the interface
The above ACL can be written also as:
R1(config)#access-list 10 deny host 192.168.10.10 //use 'HOST' keyword instead of 'WILDMASK'
R1(config)#access-list 10 permit any

Note:

- **Once there is a match, the access list is exited**
- **More specific statements should be at the top**
- **More general statements should be at the at the bottom**
- **At the end of every ACL there is "Implicit deny" 'deny any'**

Example:
R1(config)#access-list 10 permit any
R1(config)# access-list 10 deny 192.168.10.10 0.0.0.0 // This will never be executed

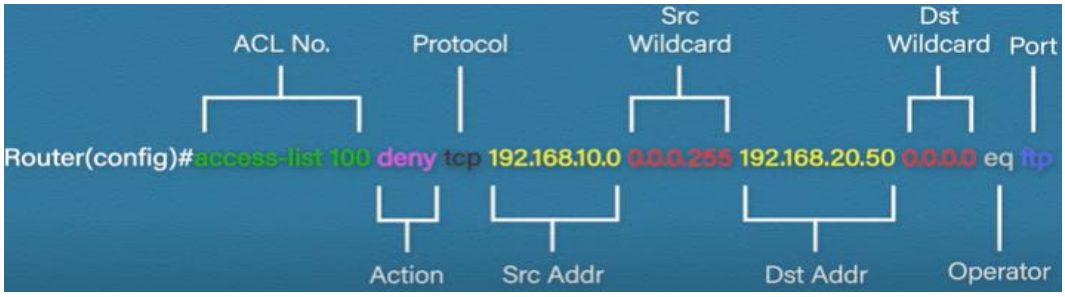
2. Extended ACL

These ACLs permit or deny packets based on the source IPv4 address and destination IPv4 address, protocol type, source and destination TCP or UDP ports, and more.

It uses ranging number from **100-199.** Its expanded ranging number is from **2000-2699**

Note: Extended ACL are applied closest to the source

Example: Create an Extended ACL (100) the deny TCP traffics from any host in 192.168.10.0/24 network to access the ftp resources from 192.168.20.50 server.

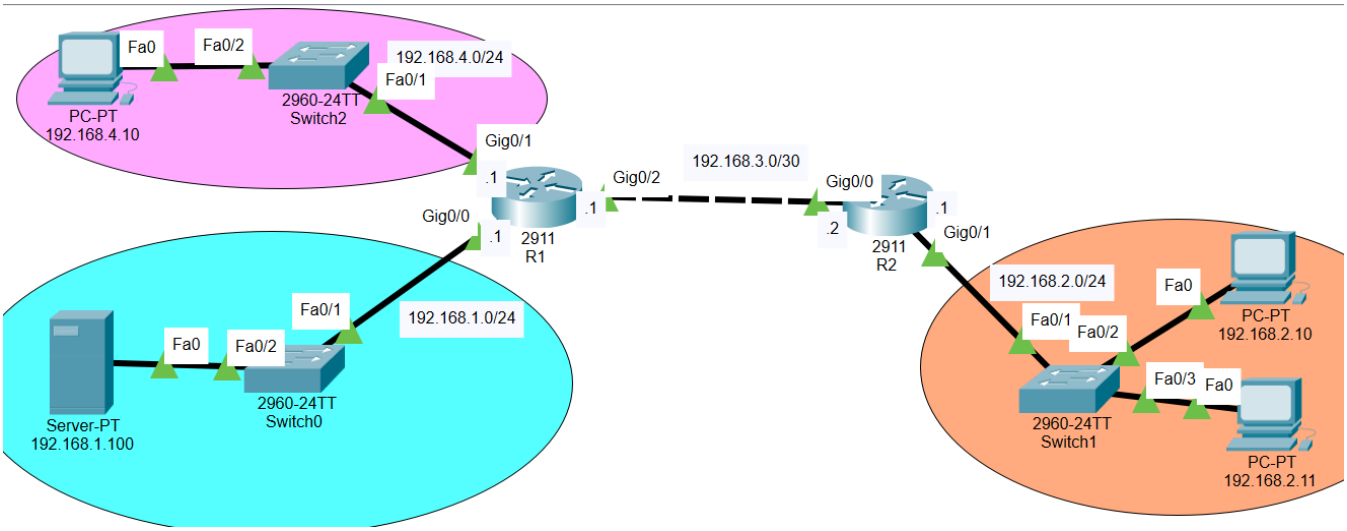


Example 2: Create an Extended ACL (100) the permit TCP traffics from any host in 192.168.10.0/24 network to access the HTTP resources from 192.168.20.50 server.

R1(config)#*access-list 100 permit tcp 192.168.10.0 0.0.0.255 192.168.20.50 0.0.0.0 eq 80 (www)*
R1(config)#*interface fa 0/0*
R1(config-if)#*ip access-group 100 in*

Example: Consider the below network diagram which has 4 different networks: 192.168.1.0/24, 192.168.3.0/30,192.168.4.0/24 and 192.168.2.0/24

- Configure the static route or RIP or EIGRP to enable the communication among all networks.



a. Create an ACL that permits all hosts in LAN 192.168.2.0/24 to access the webpage (HTTP) on the server: 192.168.1.100 and continue to have access to LAN: 192.168.4.0/24

STEP1: CONFIGURE THE INTERFACES

Configure the interface on R1	Configure the interface on R2
Router>en Router#config t Router(config)#hostname R1 R1(config)#interface g0/1 R1(config-if)#ip address 192.168.4.1 255.255.255.0 R1(config-if)#no sh R1(config-if)#interface g0/2 R1(config-if)#ip address 192.168.3.1 255.255.255.252 R1(config-if)#no sh R1(config-if)#interface g0/0 R1(config-if)#ip address 192.168.1.1 255.255.255.0 R1(config-if)#no sh	Router>en Router#config t Router(config)#hostname R2 R2(config)#interface g0/0 R2(config-if)#ip address 192.168.3.2 255.255.255.252 R2(config-if)#no sh R2(config-if)#interface g0/1 R2(config-if)#ip address 192.168.2.1 255.255.255.0 R2(config-if)#no sh

STEP2: CONFIGURE Static route on both routes

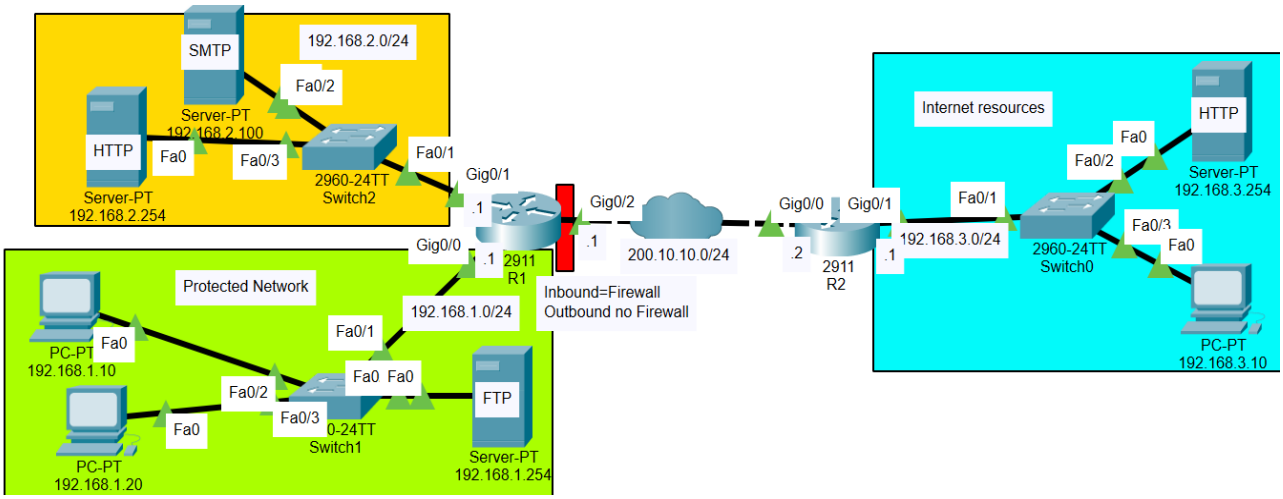
Configure the static route on R1	Configure the static route on R2
R1#conf t R1(config)#ip route 192.168.2.0 255.255.255.0 192.168.3.2 R1(config)#end	R2(config)#ip route 192.168.4.0 255.255.255.0 192.168.3.1 R2(config)#ip route 192.168.1.0 255.255.255.0 192.168.3.1 R2(config)#end

- ✓ **Create an ACL that permits all hosts in LAN 192.168.2.0/24 to access the webpage (HTTP, https) on the server: 192.168.1.100 and continue to have access to LAN: 192.168.4.0/24**

```
R2(config)#access-list 100 permit tcp 192.168.2.0 0.0.0.255 host 192.168.1.100 eq 80
R2(config)#access-list 100 permit tcp 192.168.2.0 0.0.0.255 host 192.168.1.100 eq 443
R2(config)#access-list 100 permit ip 192.168.2.0 0.0.0.255 192.168.4.0 0.0.0.255
R2(config)#interface g0/1
R2(config-if)#ip access-group 100 in
R2(config-if)#exit
```

Example2: TCP established ACLs (Traffics generated within the network)

Consider the network diagram below:



Create an ACL, that permits 192.168.3.0/24 network to access HTTP and SMTP server located in 192.168.2.0/24 network, permits protected network (192.168.1.0/24) to access HTTP server located in 192.168.3.0/24 network.

Step1: Configure the interfaces

Configure the interfaces on R1	**Configure the interface on R2**

Router>en Router#config t Router(config)#hostname R R(config)#interface G0/0 R(config-if)#ip address 192.168.1.1 255.255.255.0 R(config-if)#no sh R(config-if)#interface g0/1 R(config-if)#ip address 192.168.2.1 255.255.255.0 R(config-if)#no sh R(config-if)#interface g0/2 R(config-if)#ip address 200.10.10.1 255.255.255.0 R(config-if)#no sh	Router>en Router#conf t Router(config)#hostname R2 R2(config)#interface g0/0 R2(config-if)#ip address 200.10.10.2 255.255.255.0 R2(config-if)#no sh R2(config-if)#interface g0/1 R2(config-if)#ip address 192.168.3.1 255.255.255.0 R2(config-if)#no sh

Step 2: Configure the routing protocol

Configure static route on R1	Configure static route on R2
R#config t R(config)#ip route 192.168.3.0 255.255.255.0 200.10.10.2 R(config)#	R2#config t R2(config)#ip route 192.168.2.0 255.255.255.0 200.10.10.1 R2(config)#ip route 192.168.1.0 255.255.255.0 200.10.10.1 R2(config)#

Step 3: Creating the access control list

The ACL is created on R1 and applied on the interface g0/2 inbound

```
R#config t
R(config)#access-list 100 permit tcp any 192.168.2.0 0.0.0.255 eq 80
R(config)#access-list 100 permit tcp any 192.168.2.0 0.0.0.255 eq 443
R(config)#access-list 100 permit tcp any 192.168.2.0 0.0.0.255 eq 25
R(config)#access-list 100 permit tcp any eq 80 192.168.1.0 0.0.0.255 established // Allowing protected network to access the external http server
R(config)#access-list 100 permit tcp any eq 443 192.168.1.0 0.0.0.255 established // Allowing https traffics
R(config)#interface g0/2
R(config-if)#ip access-group 100 in
```

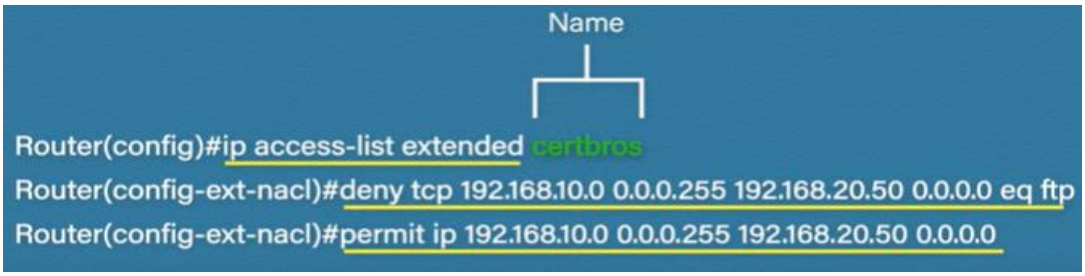
3. Named Access control list

Allows standard and extended ACLS to be given names instead of numbers making them easier to manage.

Using named ACLs is the preferred method when configuring ACLs. You can name standard and extended ACLs to provide information about the purpose of each ACL.

The following are the general rules to follow for named ACLs:

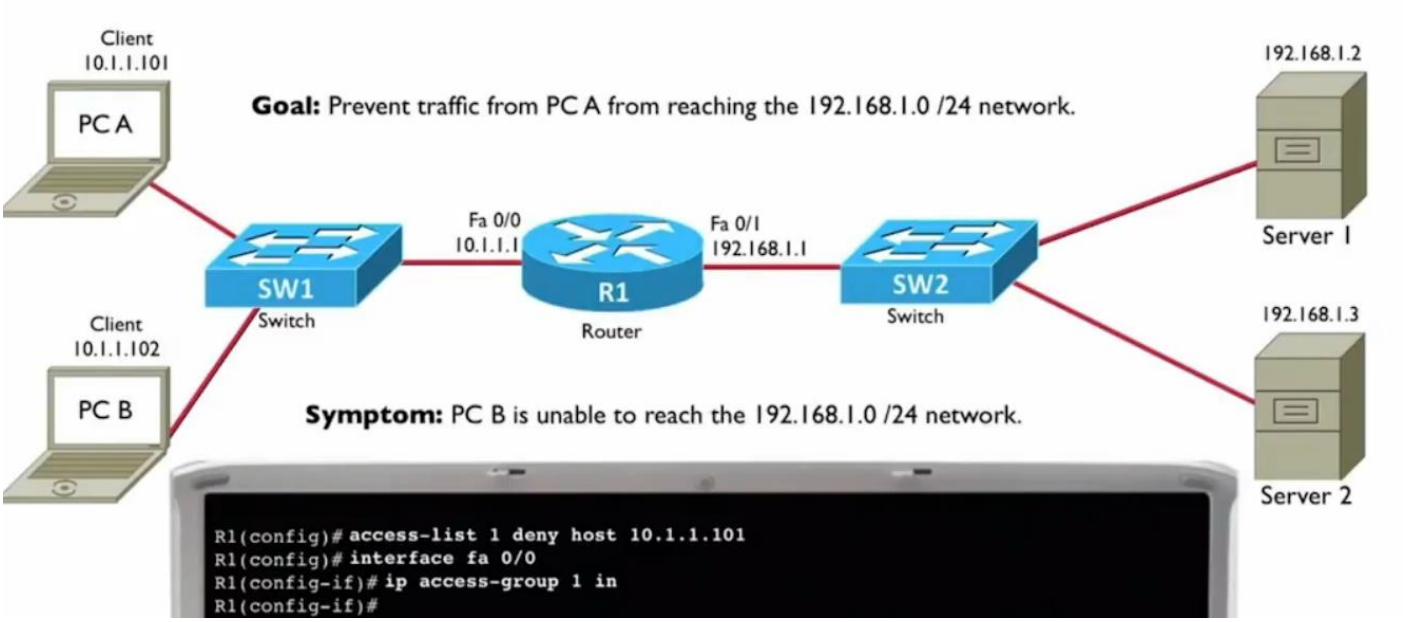
- Assign a name to identify the purpose of the ACL.
- Names can contain alphanumeric characters.
- Names cannot contain spaces or punctuation.
- It is suggested that a name be written in CAPITAL LETTERS.
- Entries can be added or deleted within an ACL.



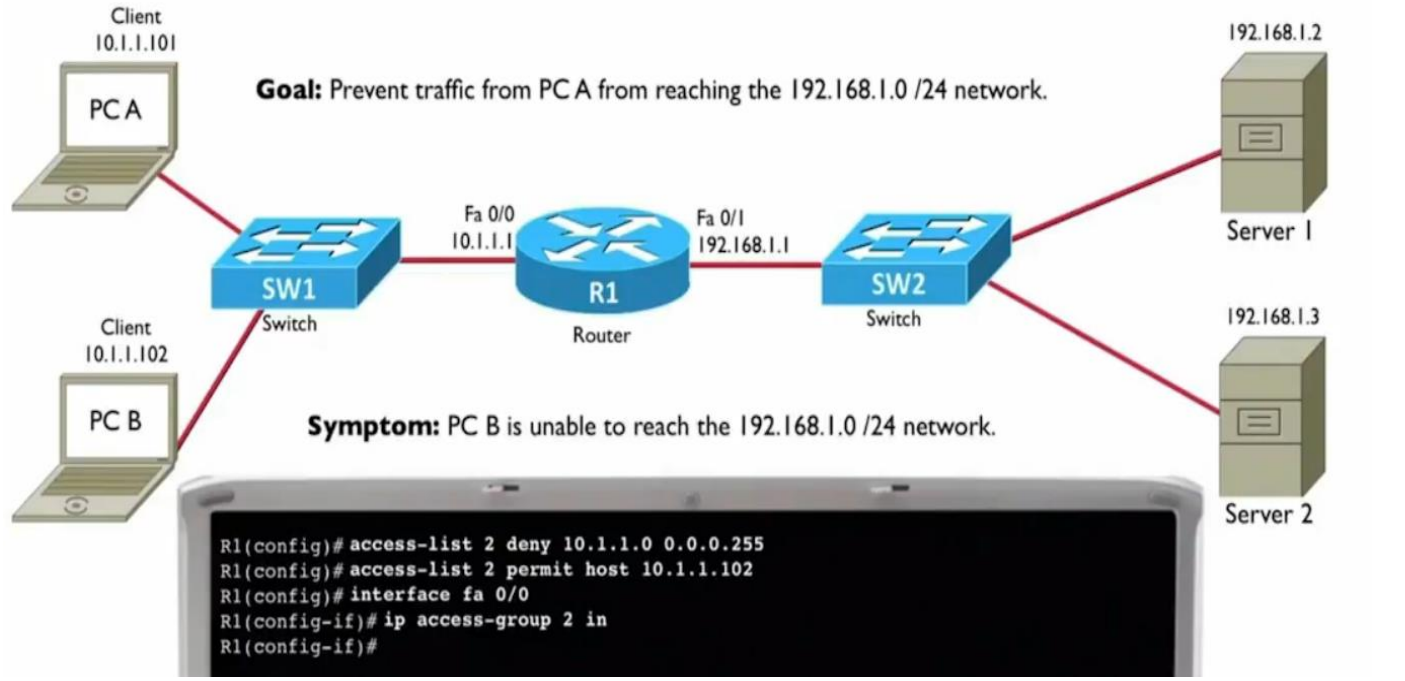
Example: Create a named ACL that filter(permit) all FTP traffics and denies other traffics.

R1(config)# **ip access-list extended FTP-FILTER**
R1(config-ext-nacl)# **permit tcp 192.168.10.0 0.0.0.255 any eq ftp**
R1(config-ext-nacl)# **permit tcp 192.168.10.0 0.0.0.255 any eq ftp-data**
R1(config-ext-nacl)#exit
R1(config)#interface g0/0
R1(config-if)#ip access-group FTP-FILTER in //apply ACL to the interface
Note: Sequence number is followed during the execution of configured ACLS. It is possible to add new entry with in-between sequence number

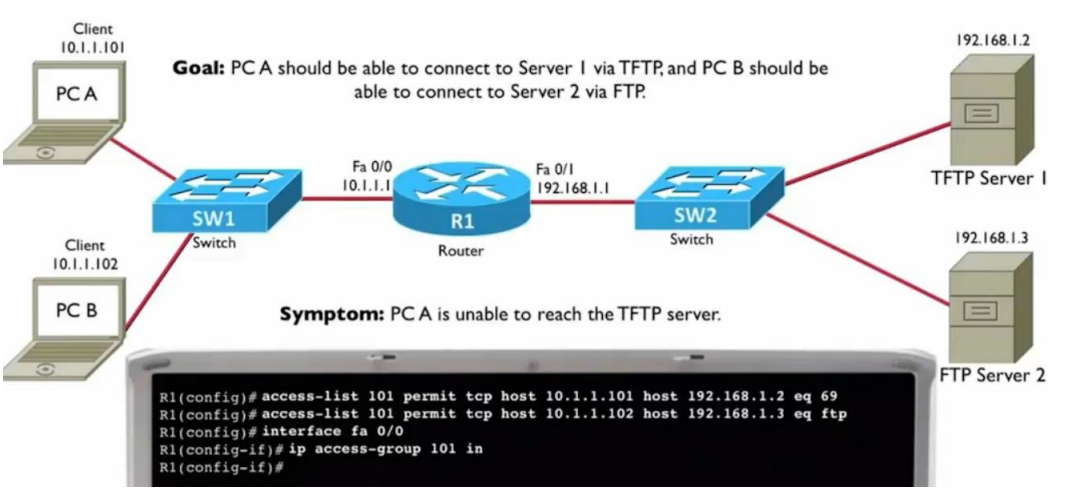
Troubleshooting ACLS
1. ACL troubleshooting exercise (Implicitly deny)



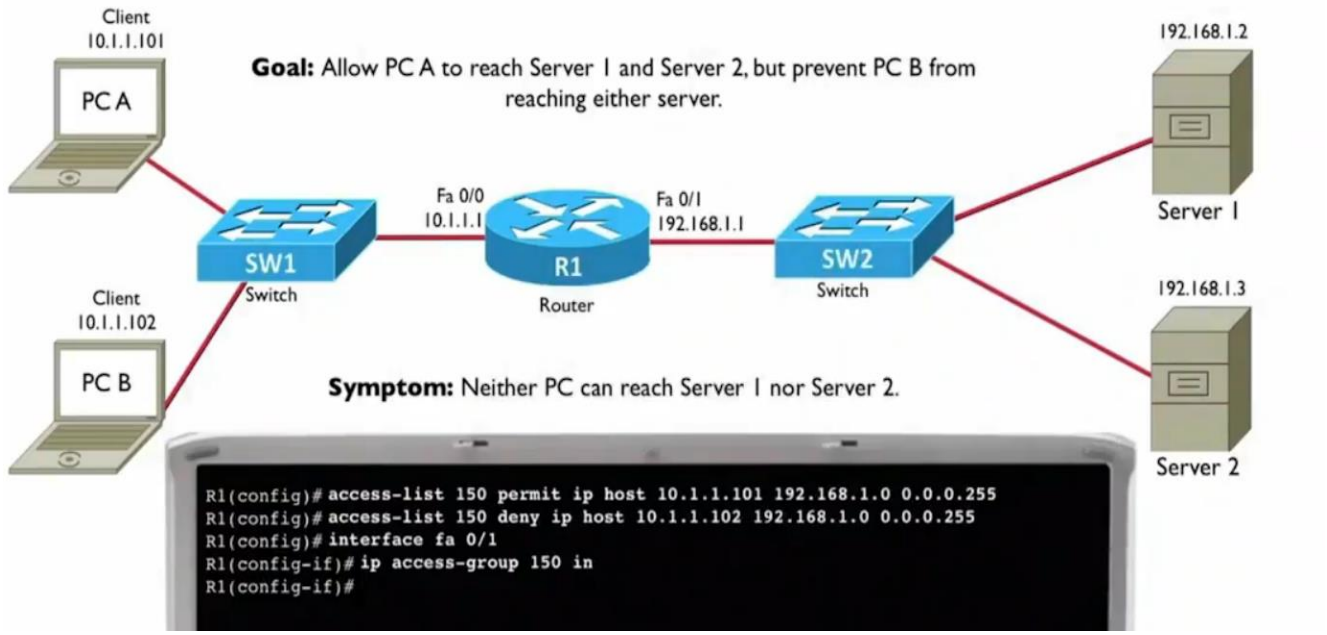
2. ACL troubleshooting exercise (All network is denied)



3. ACL troubleshooting exercise (Improper type of protocol => TFTP is UDP not TCP)



4. ACL troubleshooting exercise (ISSUE ON THE INTERFACE) (we can change the interface or set it as outbound)



References: https://www.certificationkits.com/cisco-access-list-ccna/

LEARNING OUTCOME 5: IMPLEMENT ROUTER SECURITY

1. **Router access security**

i. **Limiting password length on Cisco router**

Router# config t

Router(config)#security passwords min-length 9
Router(config)#

ii. Setting password to protect Privileged Mode

Router# config t
Router(config)#enable password cisco12345
Router(config-line)#

iii. Setting password to protect Console Port

Router# config t
Router(config)#line console 0
Router(config-line)#password cisco12345 // secret Cisco12345
Router(config-line)#login

iv. Setting password to protect Auxiliary (AUX Port) Port

Router# config t
Router(config)#line aux 0
Router(config-line)#password cisco12345 // secret Cisco12345
Router(config-line)#login

v. Setting password to protect VTY Ports (Telnet Ports)

There are 5 VTY virtual ports, which are named 0, 1, 2, 3, and 4. You can use the shortcut 0 4 (a zero, a space, and 4) to set all 5 passwords at the same time:

Router# config t
Router(config)#line vty 0 4
Router(config-line)#password cisco12345
Router(config-line)#login
Router(config-line)#transport input telnet

vi. Encrypting Passwords

Router# config t
Router(config)#service password-encryption

Note:

- This Password-encryption provide "**password 7"** encryption algorithm which is easier to be cracked online through: https://www.ifm.net.nz/cookbooks/passwordcracker.html
- The best way of encrypting password is to use "**secret**" which encrypts by using "**md5**" encryption algorithm.

vii. Setting the banner message

Router# config t
Router(config)# banner motd $Only Authorized users are allowed…"$

viii. Setting the execution timeout

Router# config t
Router(config)#line console 0 // or line vty 0 4 or Line aux 0
Router(config-line)#exec-timeout 5 0 // Five Minutes and zero seconds

Note: The default execution timeout is 10 minutes.

ix. Setting username and password

Router# config t
Router(config)#username admin privilege 15 secret Admin@123

Note: Activate to login using username and password

Router(config)#line console 0 // or Line vty 0 4
Router(config-line)#login local

x. Configuring the SSH access to the router

Router(config)# hostname R1
R1(config)# ip domain-name rca.rw
R1(config)# username Username secret Password12 //Setting username and password
R1(config)# crypto key generate rsa modulus 1024 //Encryption method
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh //Allowing the SSH only for remoting the router
R1(config-line)#exit
R1(config)# ip SSH version 2
R1(config)# end

Verification of configured settings:

Router# show run | s line (S: section)
Router# show run | b line (b: begin)
Router# show run | i password (i: include)

xi. Blocking someone who fails 5 times to login to the router within 2 minutes and keeping logs. (Enable router to watch for login attacks)

R1(config)#
R1(config)# login block-for 180 attempts 5 within 120
R1(config)# login on-success log
R1(config)# login on-failure log every 2 // for every 2 login failure, keep log

Verification command:

Router# show login

2. Standards ports and protocols

- **Ports 20 and 21:** File Transfer Protocol (FTP). FTP is for transferring files between a client and a server.
- **Port 22:** Secure Shell (SSH). SSH is one of many tunneling protocols that create secure network connections.
- **Telnet 23**
- **Port 25:** Simple Mail Transfer Protocol (SMTP). SMTP is used for email.
- **Port 53:** Domain Name System (DNS). DNS is an essential process for the modern Internet; it matches human-readable domain names to machine-

readable IP addresses, enabling users to load websites and applications without memorizing a long list of IP addresses. It is a UDP protocol.

- **Port 80:** Hypertext Transfer Protocol (HTTP). HTTP is the protocol that makes the World Wide Web possible.
- **Port 123:** Network Time Protocol (NTP). NTP allows computer clocks to sync with each other, a process that is essential for encryption. UDP protocol.
- **Port 179:** Border Gateway Protocol (BGP). BGP is essential for establishing efficient routes between the large networks that make up the Internet (these large networks are called autonomous systems). Autonomous systems use BGP to broadcast which IP addresses they control.
- **Port 443:** HTTP Secure (HTTPS). HTTPS is the secure and encrypted version of HTTP. All HTTPS web traffic goes to port 443. Network services that use HTTPS for encryption, such as DNS over HTTPS, also connect at this port.
- **Port 500:** Internet Security Association and Key Management Protocol (ISAKMP), which is part of the process of setting up secure IPsec connections.
- **Port 587:** Modern, secure SMTP that uses encryption.
- **Port 3389:** Remote Desktop Protocol (RDP). RDP enables users to remotely connect to their desktop computers from another device.
- **Port 143:** Internet Message Access Protocol (IMAP), management of electronic mail messages on a server. It is a TCP protocol

References:

https://www.networkworld.com/article/2283765/chapter-9--eigrp.html?page=2

https://www.computernetworkingnotes.com/ccna-study-guide/hot-standby-router-protocol-explained.html

https://www.ciscopress.com/articles/article.asp?p=3089353&seqNum=7#:~:text=There%20are%20two%20types%20of,or%20UDP%20ports%2C%20and%20more.

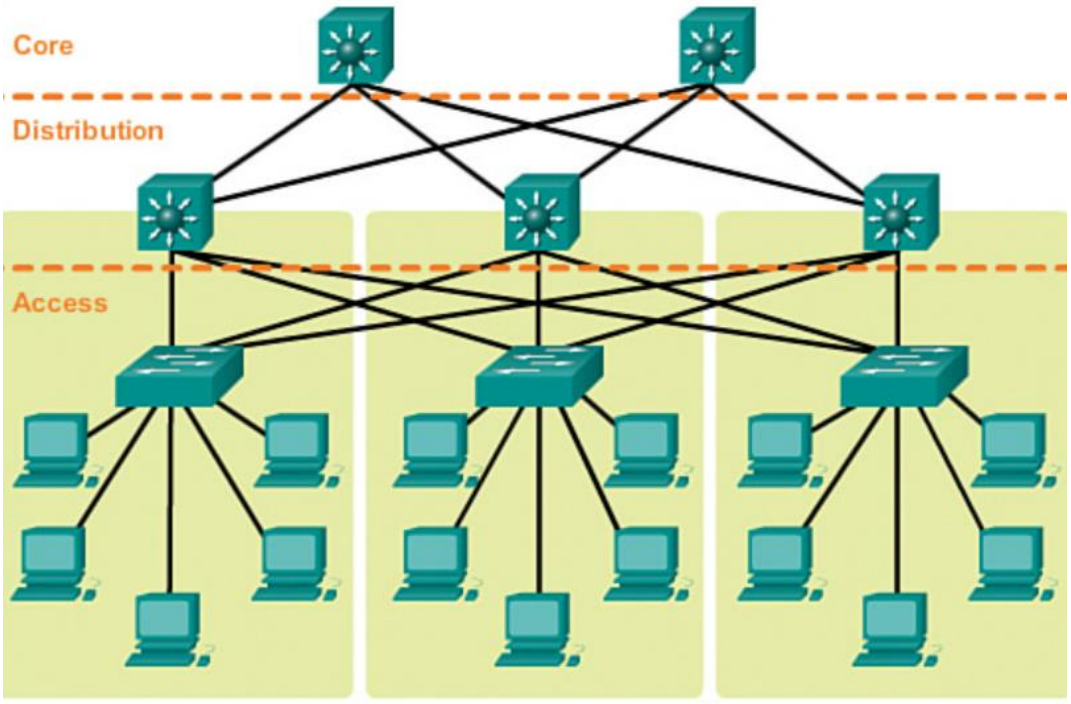
Learning Unit 2: CONFIGURE VLANs, VTP and STP

LO 1: CONFIGURE VLANS

1. **The hierarchical network models**

   The Hierarchical Network Model consists of 3 layers: the Core, Distribution, and Access layers. It is used to provide structure to campus networks.
   A typical enterprise hierarchical LAN, campus network design includes the following three layers:

   - **Access layer:** Provides workgroup/user access to the network
   - **Distribution layer:** Provides policy-based connectivity and controls the boundary between the access and core layers
   - **Core layer:** Provides fast transport between distribution switches within the enterprise campus



Three separate broadcast domains

Benefits of a hierarchical network:

- Scalability
- Redundancy
- Performance
- Security
- Manageability
- Maintainability

2. **Structured Engineering Principles**

Regardless of network size or requirements, a critical factor for the successful implementation of any network design is to follow good structured engineering principles. These principles include:

- **Hierarchy**: A hierarchical network model is a useful high-level tool for designing a reliable network infrastructure. It breaks the complex problem of network design into smaller and more manageable areas.
- **Modularity**: By separating the various functions that exist on a network into modules, the network is easier to design. Cisco has identified several modules, including the enterprise campus, services block, data center, and Internet edge.
- **Resiliency**: The network must remain available for use under both normal and abnormal conditions. **Normal conditions** include normal or expected traffic flows and traffic patterns, as well as scheduled events such as maintenance. **Abnormal conditions** include hardware or software failures, extreme traffic loads, unusual traffic patterns, denial-of-service (DoS) events, whether intentional or unintentional and other unplanned events.
- **Flexibility**: The ability to modify portions of the network, add new services, or increase capacity without going through a major forklift upgrade (i.e., replacing major hardware devices).

3. **Switching as a general concept**

   Network switching is the process of channeling data received from any number of input ports to another designated port that will transmit the data to its desired destination.

   The fundamental concept of switching refers to a device making a decision based on two criteria:

   - Ingress port
   - Destination address

   The term ingress is used to describe where a frame enters the device on a port. **The term egress** is used to describe frames leaving the device from a particular port.

   When a switch makes a decision, it is based on the ingress port and the destination address of the message.

4. **Switch MAC address table**

   The MAC address table is where the switch stores information about the other Ethernet interfaces to which it is connected on a network. The table enables the switch to send outgoing data (Ethernet frames) on the specific port required to reach its destination, instead of broadcasting the data on all ports (flooding).

To display the MAC table, enter the show mac-address command in privilege exec mode.

Switch#show mac-address-table

5. **Switching domains**

In computer networking, a **switch domain** refers to a group of switches that are connected together and operate as a single logical unit. Switch domains are often used to create high-performance networks with high availability and redundancy.

Collusion domain is a group of network devices that are connected to the same physical segment or Ethernet switch and can potentially interfere with each other when transmitting data.

Collisions can significantly reduce network performance and can lead to network congestion and downtime.

To reduce the number of collisions in a network, it is important to minimize the size of the collision domain. This can be done in several ways, including:

- **Segmenting the network**: This involves dividing the network into smaller segments or VLANs to reduce the number of devices on each segment or VLAN. This can be done using routers, switches, or firewalls.
- **Using network devices with collision detection and avoidance features**: This includes devices such as switches and routers, which have the ability to detect and avoid collisions by using techniques such as CSMA/CD (Carrier Sense Multiple Access with Collision Detection).
- **Implementing full-duplex communication**: Full-duplex communication allows data to be transmitted and received simultaneously, which can help reduce collisions in the network.
- **Using network devices with higher bandwidth**

By reducing the size of the collision domain, network administrators can improve network performance and reliability, reduce network downtime, and ensure that data is transmitted efficiently and reliably.

Alleviating Network congestion:

Network congestion occurs when the amount of traffic on a network exceeds the network's capacity to handle it. This can result in slower network speeds, packet loss, and increased latency.

To alleviate network congestion, here are some strategies that can be used:

1. **Upgrade network equipment:** Upgrading network equipment, such as routers and switches, can increase the capacity and speed of the network.
2. **Optimize network settings:** Tweaking network settings, such as MTU (maximum transmission unit), can improve network performance and reduce congestion.
3. **Implement Quality of Service (QoS):** QoS is a set of technologies that prioritize different types of network traffic. This allows more important traffic, such as voice and video, to be prioritized over less important traffic, such as email and web browsing.
4. **Implement traffic shaping:** Traffic shaping limits the amount of bandwidth that different types of traffic can use. This can help prevent one type of traffic from monopolizing the network and causing congestion.
5. **Reduce unnecessary network traffic:** This can be done by limiting access to certain websites or applications, and by implementing policies that restrict the use of certain types of traffic.
6. **Load balancing**: Load balancing distributes network traffic evenly across multiple network devices, which can help prevent congestion.
7. **Implement caching:** Caching stores frequently accessed data locally, which reduces the amount of traffic on the network and improves network performance.

Following are some important characteristics of switches that contribute to alleviating network congestion:

- **High port density** - Switches have high-port densities: 24- and 48-port switches are often just 1 rack unit (1.75 inches) in height and operate at speeds of 100 Mb/s, 1 Gb/s, and 10 Gb/s. Large enterprise switches may support many hundreds of ports.

- **Large frame buffers** - The ability to store more received frames before having to start dropping them is useful, particularly when there may be congested ports to servers or other parts of the network.
- **Port speed** - Depending on the cost of a switch, it may be possible to support a mixture of speeds. Ports of 100 Mb/s, and 1 or 10 Gb/s are common (100 Gb/s is also possible).
- **Fast internal switching** - Having fast internal forwarding capabilities allows high performance. The method that is used may be a fast internal bus or shared memory, which affects the overall performance of the switch.
- **Low per-port cost** - Switches provide high-port density at a lower cost. For this reason, LAN switches can accommodate network designs featuring fewer users per segment, therefore, increasing the average available bandwidth per user.

6. **Key elements of ethernet /802.3 networks**
    - ✓ **Media Access control in ethernet**
        - Carrier sense Multiple access collusion detection (CSMA/CD)
    - ✓ **Ethernet communications**
        - Unicast communication
        - Multicast communication
        - Broadcast communication
    - ✓ **Preamble and start frame Delimiter fields**
    - ✓ **Destination MAC**
        - Address field
        - Source MAC address field
        - Length /type field
        - Data and pad fields
        - Frame check sequence field
    - ✓ **Duplex settings**
        - Half duplex
        - Full duplex
    - ✓ **Switch port settings**
        - Auto option setting
        - Full option setting
        - Half option setting
    - ✓ **MAC addressing and switch MAC address tables**
        - MAC addressing
        - Switch MAC address table

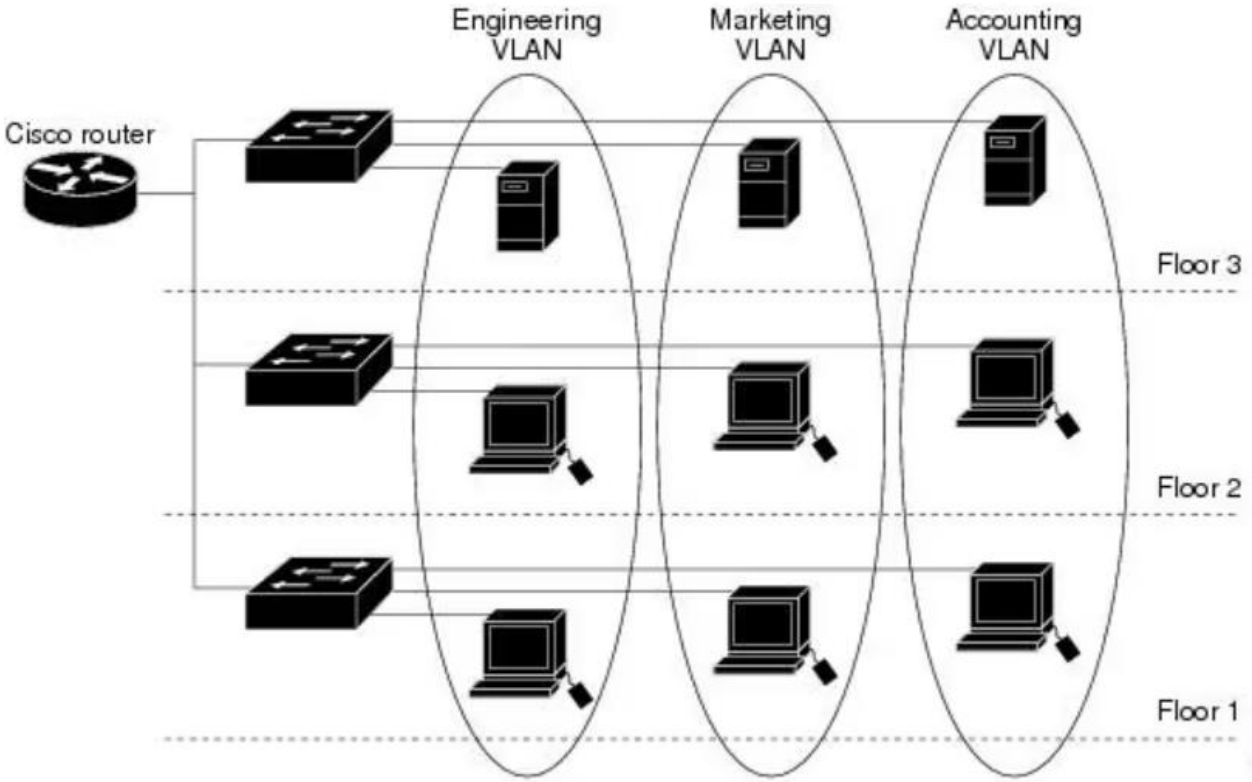
7. **Design consideration for Ethernet /802.3 Networks**
    - Bandwidth and throughput
    - Collusion domains
    - Broadcast domains
    - Network latency
    - Network congestion
    - LAN segmentation
8. **Configuration of VLANS**

    A VLAN (Virtual Local Area Network) is a logical grouping of devices on a computer network that allows network administrators to segment the network and improve network performance and security.
    VLANs are used to group devices based on common requirements such as department, function, or location, regardless of their physical location on the network.

    Each VLAN acts as a separate network segment, with its own set of network addresses, traffic flow and security policies. Devices on different VLANs cannot communicate with each other unless a routing device, such as a router or layer 3 switch, is used to connect them.

    Benefits of VLANs include:

    1. **Improved network security:** By separating devices into different VLANs, network administrators can apply different security policies and controls to each VLAN based on their individual security requirements.
    2. **Improved network performance**: By reducing the size of broadcast domains, VLANs can help improve network performance by reducing network traffic and congestion.
    3. **Improved network management:** By grouping devices based on common requirements, VLANs make it easier for network administrators to manage the network and troubleshoot network issues.
    4. **Scalability:** VLANs can be used to scale networks by creating multiple smaller broadcast domains, which can be managed more efficiently than a single large network.



✓ CREATION OF VLANS

DETAILED STEPS for Creating a VLAN

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters configuration mode.

Step 2	**vlan** {*vlan-id* | *vlan-range*}
	Example:
	`switch(config)# vlan 5`
	`switch(config-vlan)#`
		Places you into the VLAN configuration sub-mode. If the VLAN does not exist, the system creates the specified VLAN and then enters the VLAN configuration sub-mode.

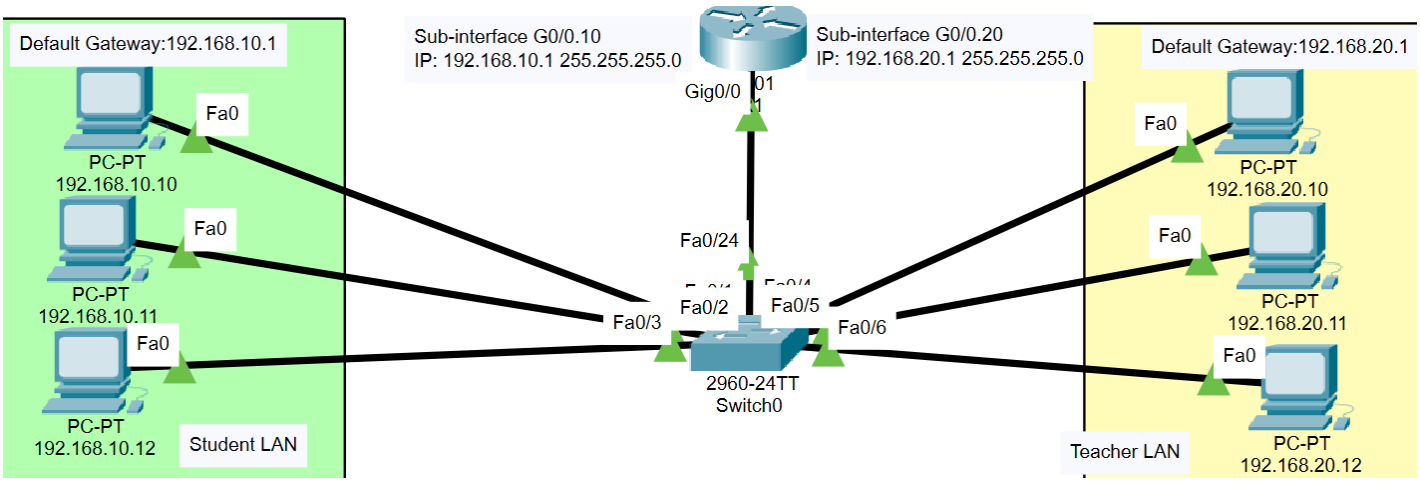
Step 3	**name** *vlan-name* **Example:** `switch(config-vlan)# name accounting`	Names the VLAN. You can enter up to 32 alphanumeric characters to name the VLAN. You cannot change the name of VLAN1 or the internally allocated VLANs.

Step 4	**state** {**active** | **suspend**} **Example:** `switch(config-vlan)# state active`	Sets the state of the VLAN to active or suspend. While the VLAN state is suspended, the ports associated with this VLAN become inactive, and that VLAN does not pass any traffic. The default state is active. You cannot suspend the state for the default VLAN or VLANs 1006 to 4094.
Step 5	**no shutdown** **Example:** `switch(config-vlan)# no shutdown`	Enables the VLAN. The default value is no shutdown (or enabled). You cannot shut down the default VLAN, VLAN1, or VLANs 1006 to 4094.

Step 6	**exit**
	Example:
	`switch(config-vlan)# exit`
	`switch(config)#`
		Exits the VLAN configuration sub-mode.

Step 7	**show vlan** **Example:** `switch# show vlan`	(Optional) (Verification of configured VLAN information) Displays information and status of VLANs.
Step 8	**show vtp status** **Example:** `switch# show vtp status`	(Optional) Displays information and status of VLAN Trunking Protocols (VTPs).
Step 9	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional)-saving the configuration Copies the running configuration to the startup configuration.

✓ ASSIGNING SWITCH PORTS TO VLANS



Step1: Configure the interfaces on both Pcs as shown on the above diagram

Step2: Configure Student-VLAN and Teacher-VLAN on the Switch

```
Switch>en
Switch#conf t
Switch(config)#vlan 10
Switch(config-vlan)#name student
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name teacher
Switch(config-vlan)#exit
```

Step3: Assign switch ports to VLANs

Switch port mode:

A switch port can be in one of two modes: **access** and **trunk**. There are two ways a switch port can settle down into one of these two modes: static and dynamic.

1. **Access Port:**

- Access port is a connection on a switch that transmits data to and from a specific VLAN.
- It is used to connect switches to host devices such as desktops, laptops, printers etc., only available in access link.
- It sends and receives Ethernet frames in untagged form from access VLAN.
- It can only be member of single VLAN i.e. the access VLAN, and discards all frames that are not classified to the access VLAN.

2. **Trunk Port:**

- Trunk port is a connection on a switch that transmits data to and from multiple VLANs.
- It is used to connect switches to other switches, routers and servers available in trunk link.
- Frames are marked with unique identifying tags when they move between switches so that they can be directed to their designated VLANs.
- It can manage traffic for numerous VLANs at the same time.

VLAN 10

```
Switch(config)#interface range fa0/1-3  //You can use interface range or single interface
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#exit
```

VLAN 20

```
Switch(config)#interface range fa0/4-6
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#exit
```

Step4: Verification of VLAN configuration

Switch#show VLAN or

Switch#show interfaces switchport

✓ CONFIGURATION OF TRUNKS

A trunk port is a port that carries data from multiple local area networks or virtual local area networks (VLANs) across a single interconnect between network switches or routers.

Step1: Configure trunk port on the switch

```
Switch(config)#int fa0/24
Switch(config-if)#switchport mode trunk

Switch(config-if)#switchport trunk allow VLAN 1-99 //allow all VLANs
```

Step2: Configure the sub-interface on the router

Sub-interfaces divide the parent interface into two or more virtual interfaces on which you can assign unique Layer 3 parameters such as IP addresses and dynamic routing protocols.

```
Router#conf t
Router(config)#interface g0/0
Router(config-if)#no sh
```

Configure Sub-interface for VLAN 10

```
Router#conf t
Router(config)#interface g0/0.10
Router(config-if)#encapsulation dot1Q 10 // dot1Q : IEEE 802.1Q Virtual LAN, 10 is VLAN ID
Router(config-if)#ip address 192.168.10.1 255.255.255.0
Router(config-if)#
```

Configure Sub-interface for VLAN 20

```
Router(config)#interface g0/0.20
Router(config-if)#encapsulation dot1Q 20 //
Router(config-if)#ip address 192.168.20.1 255.255.255.0
Router(config-if)#
```

Types of VLANs

There are 5 main types of VLANs depending on the type of network they carry:

1. **Default VLAN –** When the switch initially starts up, all switch ports become a member of the default VLAN (generally all switches have a default VLAN named **VLAN 1**), which makes them all part of the same broadcast domain. Using default VLAN allows any network device connected to any of the switch ports to connect with other devices on other switch ports. One unique feature of Default VLAN is that it can't be renamed or deleted.

2. **Data VLAN –** Data VLAN is used to divide the whole network into 2 groups. One group of users and other groups of devices. This VLAN also known as a user VLAN, the data VLAN is used only for user-generated data. This VLAN carries data only. It is not used for carrying management traffic or voice.

3. **Voice VLAN –** Voice VLAN is configured to carry voice traffic. Voice VLANs are mostly given high transmission priority over other types of network traffic. To ensure voice-over IP (VoIP) quality (delay of less than 150 milliseconds (ms) across the network), we must have separate voice VLAN as this will preserve bandwidth for other applications.

4. **Management VLAN –** A management VLAN is configured to access the management capabilities of a switch (traffic-like system logging, and monitoring). VLAN 1 is the management VLAN by default (VLAN 1 would be a bad choice for the management VLAN). Any switch VLAN could be

defined as the management VLAN if the admin has not configured a unique VLAN to serve as the management VLAN. This VLAN ensures that bandwidth for management will be available even when user traffic is high. You must configure the IP address and gateway for the management VLAN

5. **Native VLAN –** This VLAN identifies traffic coming from each end of a trunk link. A native VLAN is allocated only to an 802.1Q trunk port. The 802.1Q trunk port places untagged traffic (traffic that does not come from any VLAN) on the native VLAN. It is best to configure the native VLAN as an unused VLAN.

   Note:

   - It is common practice to separate voice and management traffic from data traffic.
   - The computer will be in **data VLAN, and the IP phone will be in the voice VLAN.**

VLAN Ranges			
VLANs	**Range**	**Usage**	**Propagated by VTP**
0, 4095	Reserved	For system use only. You cannot see or use these VLANs.	—
1	Normal	Cisco default. You can use this VLAN but you cannot delete it.	Yes
2-1001	Normal	For Ethernet VLANs; you can create, use, and delete these VLANs.	Yes
1002-1005	Normal	Cisco defaults for FDDI and Token Ring. You cannot delete VLANs 1002-1005.	Yes
1006-4094	Extended	For Ethernet VLANs only.	No

References: https://www.educba.com/vlan-tagged-vs-untagged/

Learning Outcome 2: Configure STP

1. **INTRODUCTION TO STP**

   STP (Spanning Tree Protocol) is a networking protocol that prevents loops in a layer 2 network by selectively blocking redundant paths.

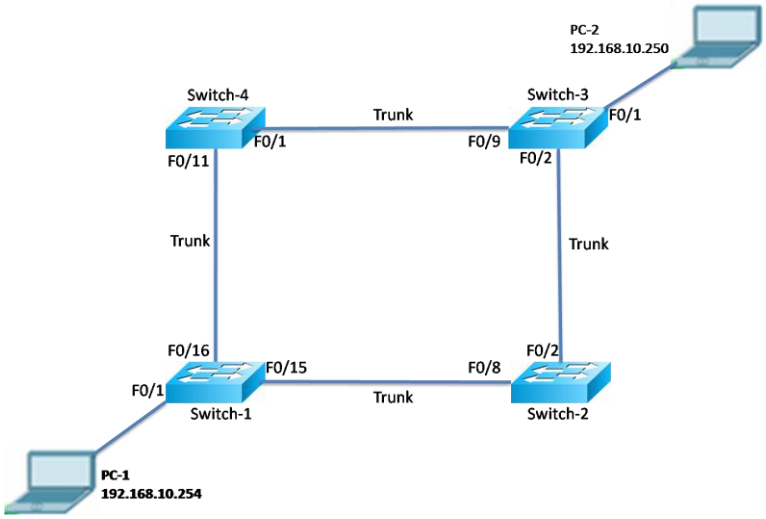
   By properly configuring STP, you can help ensure that your network is free from loops and is able to provide reliable and efficient communication between devices.

2. **REDUNDANCY**

   ✓ **Examine a redundant design**

   A redundant link is an additional link between two switches. A redundant link is usually created for backup purposes.

   The biggest disadvantage of a redundant link is that it creates a loop between switches. If a loop exists between two switches, they do not work properly.



3. **STP operation**

   ✓ All switches of the STP domain, first elect a root bridge. The root bridge acts as a point of reference for all other switches in the network. All ports of the root bridge remain in the forwarding mode.

   ✓ Once the root bridge is elected, all remaining switches select a single port that has the shortest path cost to reach the root bridge and marked it as the root port.

   ✓ After selecting the root port, switches determine a single designated port for each connection.

   ✓ If multiple ports are connected with the same switch or LAN segment, the switch select only one port that has the lowest path cost and marks it as the designated port.

- ✓ Once the root port and designated ports are selected, the switch blocks all remaining ports to remove any possible or existing loop from the network.

4. **Spanning Tree Algorithm**

   The STA(**Spanning Tree Algorithm**) algorithm first creates a topology database then it finds and disables the redundant links. Once redundant links are disabled, only the STP-chosen links remain active. If a new link is added or an existing link is removed, the STP re-runs the STA algorithm and re-adjusts all links to reflect the change.

5. **STP BPDU**

   BPDUs (Bridge Protocol Data Units) are multicast frames that switches used to share information about themselves and their connections.

   Types of BPDU

   - Configuration BPDU (Hello BPDU)
   - Topology change BPDU (TCN BPDU): learn which switch is connected with which switches
   - Topology change Acknowledgement (TCA BPDU): to learn whether any layer 2 switching loop exists in the learned topology or not.

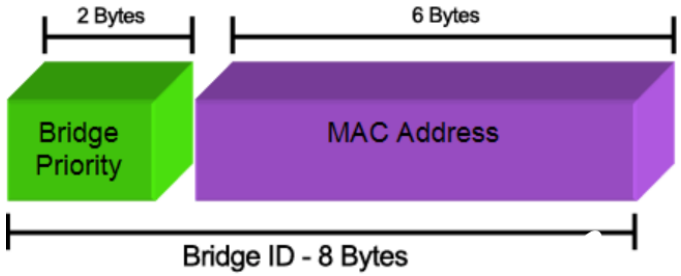
   Reasons for Topology Change:

   Spanning Tree Protocol activated network can encounter topology change due to the following reasons:

   - Link failure
   - Switch failure
   - Port transitioning to the forwarding state

6. **Bride ID**

   Bridge ID or BID is the identity of every switch that they are part of a network. It is an 8 bytes field that is divided into two parts. The first part is a 2-byte Bridge Priority field (which can be configured) while the second part is the 6-byte MAC address of the switch.



7. **Port roles**

   - ✓ **Root Port**

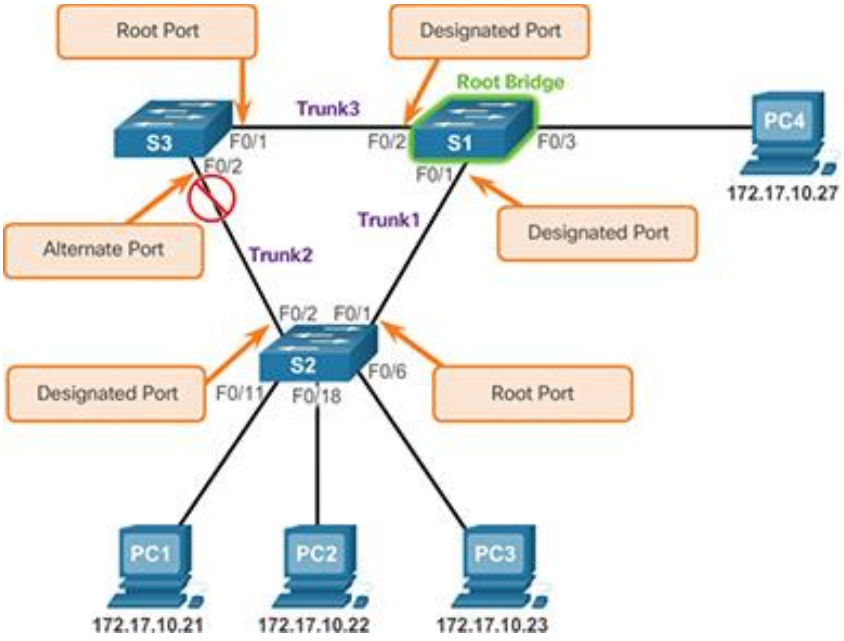
The Root port is the port that directly connects to the Root Bridge, or has the shortest path to the Root Bridge. The shortest path is the path that has the lowest path cost value. Remember that, a switch can go through many other switches to get to the root bridge. So it's not always the shortest path but it is the fastest path.

- ✓ **Designated Ports**

A designated port is the port that has the lowest port cost value to get on a given network, compared to other ports on that segment. STP marks the designated ports as the forwarding ports. Forwarding ports are used to forward the frames.

- ✓ **Non-Designated Ports**

A non-designated port is a port that has a higher port cost than the designated port. STP marks the non-designated port as the blocking port. **Blocking ports** are used to remove loops.



8. **STP port states and BPDU timers**
   - **Disabled** - The port in this state does not participate in the STP operation (it is shut down).
   - **Blocking** - The port does NOT forward any Ethernet frames, does NOT accept any Ethernet frames (discards arriving frames), does NOT learn any MAC addresses. However, the port **DOES** process **BPDU frames** received from neighbor switches. If the port transitions to this state (blocking), it can stay blocked for **20 seconds by default (max_age)**.

- **Listening** - The port in this state **CAN send and receive the BPDU frames**. However, the port in this state does NOT learn any MAC addresses and does NOT forward or process incoming frames either. All Ethernet frames are being discarded. The computation of loop-free topology takes place in this state. If the port transitions to this state (listening), it can stay in this state for **15 seconds by default (forward_delay)**.
- **Learning** - The port will not forward any Ethernet frames yet. It will be learning MAC addresses from the frames arriving at the port in order to populate the MAC address table. This helps avoid too much flooding when the port transition to the forwarding state. If the port transitions to this state (learning), it can stay in this state for **15 seconds by default (forward_delay)**.
- **Forwarding** - The port in this state will forward all Ethernet frames as per switch operation. Also, the port will process all incoming Ethernet frames and will actively learn MAC addresses from the arriving traffic.

9. STP Modes

There are different modes of STP that are used depending on the requirements and topology of the network.

a. **STP (Spanning Tree Protocol):** The original version of the protocol that allows for a single active path in the network, with backup paths in case of failure.
b. **RSTP (Rapid Spanning Tree Protocol):** This protocol is an improvement over STP and provides faster convergence times in case of a topology change. It is backward-compatible with STP.
c. **MSTP (Multiple Spanning Tree Protocol):** This protocol allows for the creation of multiple logical spanning trees on a single physical network, which can be useful in large and complex networks.
d. **PVST (Per VLAN Spanning Tree):** This protocol allows for the creation of a separate spanning tree for each VLAN, allowing for more efficient use of network resources.
e. **RPVST (Rapid PVST):** This protocol is similar to PVST+ but provides faster convergence times in case of a topology change.

10. Electing roots bridge

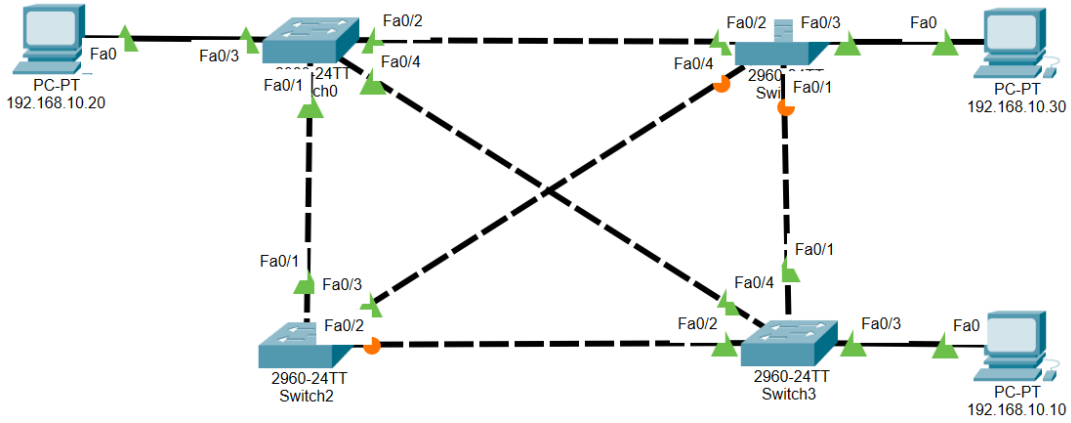
A Root Bridge is the starting point of the STP network topology. To elect a Root Bridge from all switches of the network, STP uses two parameters; a variable known as **bridge priority** and the **MAC addresses** of participating switches. A switch that has the lowest bridge priority value, is elected as the root bridge. If the bridge priority value is the same in all switches, the switch which has the lowest MAC address is elected as the Root Bridge.

By default, the **bridge priority value** is set to **32768** in all Cisco switches. Unless you change this value, a switch that has the lowest MAC address is elected as the Root Bridge.
The selection process of the Root Bridge happens each time when a **network change occurs** like a **new switch is added** to the network topology or an **existing switch is removed** or the **current Root Bridge is failed**. If other switches of the network do not receive BPDUs from the Root Bridge within 20 seconds, they assume that the Root Bridge has failed. If the current Root Bridge fails, the remaining switches automatically start the election process to choose a new Root Bridge again.

11. Non-root bridge

Except for the Root Bridge, all remaining switches of the network are considered as Non-Root Bridges. Non-Root Bridges receive updates from the Root Bridge and update their STP databases relatively.

12. Configuration of STP bridges IDs



Verification of spanning tree protocol

Switch#show spanning-tree

Changing Spanning tree priority number (Changing bridge priority)

Switch#config t
Switch(config)#spanning-tree vlan 1 priority <num>
Or
Switch(config)#spanning-tree vlan 1 root primary
Or
Switch(config)#spanning-tree vlan 1 root secondary

Changing STP mode

```
Switch#conf t
Switch(config)#spanning-tree mode ?
        pvst Per-Vlan spanning tree mode
        rapid-pvst Per-Vlan rapid spanning tree mode
Switch(config)#spanning-tree mode rapid-pvst
Switch(config)#
```

Note: By default, Per-VLAN Spanning tree mode is enabled for most CISCO switches

Difference between Rapid STP and standard STP

S.NO	STP	RSTP
1.	Its IEEE standard is 802.1D.	Its IEEE standard is 802.1W.
2.	In STP only the root bridge sends BPDU (Bridge protocol data unit) and it is transferred by others.	In RSTP all bridges can forward BPDUs.
3.	STP has three port roles (i.e., Root Port, Designated Port, Blocked Port).	RSTP has four-port roles (i.e., Root Port, Designated Port, Alternate Port, Backup Port).
4.	STP has five port states (i.e., Forwarding, Learning, Listening, Blocking, Disabled).	RSTP has three port states (i.e., Forwarding, Learning, Discarding).
5.	It doesn't have any link type.	It has Two link types i.e., Shared link and Point to point link.
6.	STP provides slower network convergence in response.	RSTP provides significantly faster network convergence.
7.	Flag bits used in STP are Bit 0 for TCN (Topology Change Notification) and Bit 7 for TCA (Topology Change Acknowledgement).	Flag bits used in RSTP are Bit 0 for TCN, Bit 1 for Proposal, Bit 2 and 3 for Port role, Bit 4 for Learning, Bit 5 for forwarding, Bit 6 for Agreement, and Bit 7 for TCN.

LEARNING OUTCOME 3: CONFIGURE VTP

1. VTP BENEFITS

VLAN Trunk Protocol (VTP) is a Cisco proprietary protocol used to share VLAN configuration across the network. Cisco created this protocol to share and synchronize their VLAN information throughout the network.

The main goal of VTP is to manage all configured VLANs across the network.

It is very easier to add or remove or rename a VLAN while you have a small network, for example, a network of 3 switches. But for a large network of 50 or 100 switches, this process could be more tedious and difficult. We might make a mistake in the VLAN configuration. We might forget to add VLAN on one of the switches, or we may assign the wrong VLAN number. Vice versa we may forget to remove VLAN on one of the switches while removing VLANs.

Advantages of VTP:

- It allows you to track and monitoring of VLANs accurately.
- Plug-and-play configuration when adding new VLANs.
- VLAN configuration consistency across the network.
- Accurate tracking and monitoring of VLANs.
- Provide dynamic reporting of added VLANs across a network.
- Offers simplify the management of the VLAN database across multiple switches.
- VLAN management on switches like adding, deleting, and renaming VLANs.
- Configurations are consistent and have fewer errors
- Reduce VLAN management.

2. VTP COMPONENTS (VTP domain, VTP Pruning, VTP Advertisements)

a. VTP domain

VTP domain is a group of switches that share same VLAN information. A switch can have a single domain. VTP domain limits the extent to which configuration change are propagated in the network if an error occurs.

b. VTP advertisement

This VTP mode uses a hierarchy of advertisements to synchronize and distribute VLAN configurations in the network. This component distributes VTP domain name and VLAN configuration changes to VTP-enabled switches.

VTP Message types: Summary advertisements, subset advertisement and advertisement requests

Request advertisements are sent when:

- The VTP domain name has been changed.
- A summary advertisement comes with a higher configuration revision number.
- A subset advertisement message is missed.
- When the switch has been reset.

Summary Advertisement:

This type of advertisement component contains the VTP domain name, the current revision number, and other VTP configuration details.

- A VTP Server sends it every 5 minutes.
- Notify VTP enables switches of the current VTP configuration revision number.
- They are sent immediately after a configuration change.

c. VTP Pruning:

This component prevents unnecessary flooding of broadcast information from one VLAN across all trunks in the VTP domain. By default, VLANs 2-1001 are pruning eligible.

It works by preventing VLAN traffic from being forwarded over a trunk link if the traffic is destined for a VLAN that is not present on the other end of the link.

S1(config-if)#switchport trunk pruning vlan 10,20,30

There are two modes of VTP pruning in Cisco switches:

1. **VTP pruning enabled**: When VTP pruning is enabled on a switch, it sends VTP pruning messages to its neighboring switches to inform them of which VLANs are active on the switch. This helps to prevent unnecessary traffic on trunk links.
2. **VTP pruning disabled:** This mode disables VTP pruning on a switch. When VTP pruning is disabled, the switch will forward all VLAN traffic

over trunk links, regardless of whether the VLAN is active on the other end of the link.

d. VTP Modes

- **VTP server mode**
- **VTP client mode**
- **VTP transparent mode**

VTP Server Mode

VTP Server can add, modify, and delete VLANs. It will propagate a VTP message containing all the changes from all of its trunk ports. If server receives a VTP message, it will incorporate the change and forward the message from all remaining trunk ports.

VTP Transparent Mode

VTP Transparent switch can also make change in VLANs but it will not propagate these changes to other switches. If transparent switch receives a VTP message, it will not incorporate the change and forward the message as it receives, from all remaining trunk ports.

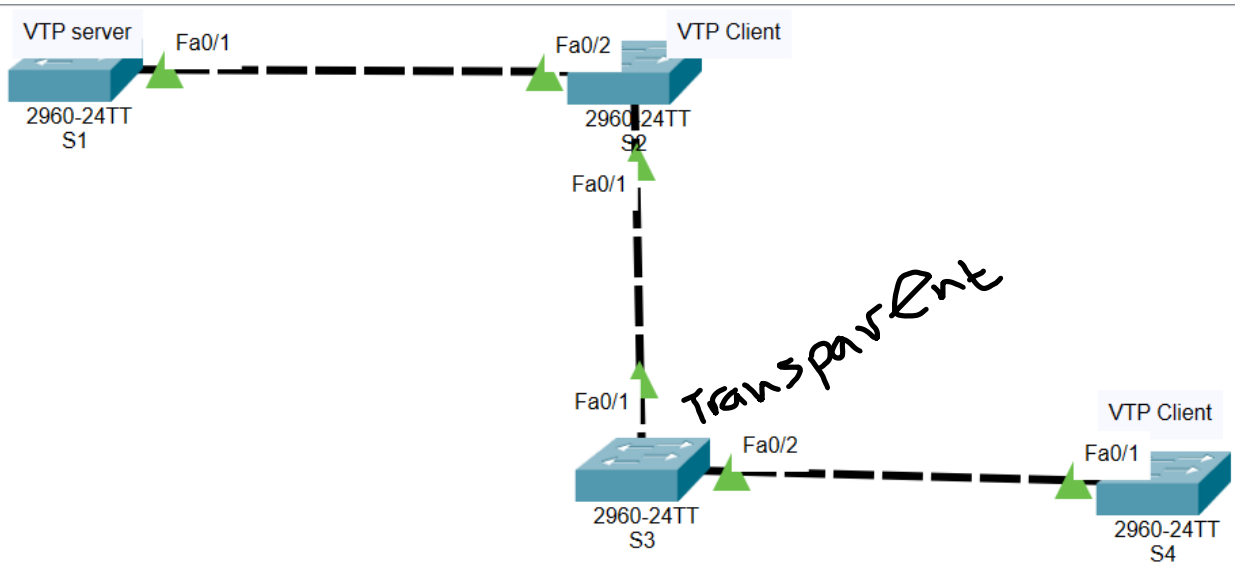
VTP Client Mode

VTP client switch cannot change the VLAN configurations itself. It can only update its VLAN configuration through the VTP messages that it receive from VTP server. When it receives a VTP message, it incorporates with the change and then forwards it from remaining trunk ports.

VTP Configuration Guidelines

Here are some important causes of the VTP failure:

- You need to check for incompatible VTP versions and password related issues.
- Incorrect name of VTP mode
- All switches are set to VTP client mode.



Configure the VTP server

Switch>EN
Switch#conf t
Switch(config)#hostname S1 //Changing the switch hostname
S1(config)#VTP mode server //configure VTP SERVER.
S1(config)#VTP domain rca.ac.rw //Changing VTP domain name from NULL to rca.ac.rw
S1(config)#VTP password rca@123 // Setting device VLAN database password to rca@123
S1(config)#

Configure 3 VLANs (Student, Teacher and staff) on VTP server

S1>en
S1#conf t
S1(config)#vlan 10
S1(config-vlan)#name student
S1(config-vlan)#vlan 20
S1(config-vlan)#name teacher
S1(config-vlan)#vlan 30
S1(config-vlan)#name staff
S1(config-vlan)#

Verification of Configured on VTP server

S1>en
S1#show vlan

Verification of VTP server status

S1>en
S1#show vtp status

Configure the VTP Client

Switch>EN
Switch#conf t
Switch(config)#hostname S2 //Changing the switch hostname
S2(config)#VTP mode client//configure VTP Client.
S2(config)#VTP domain rca.ac.rw //Changing VTP domain name from NULL to rca.ac.rw
S2(config)#VTP password rca@123 // Setting device VLAN database password to rca@123
S2(config)#

Configure the VTP transparent

Switch>EN
Switch#conf t
Switch(config)#hostname S3 //Changing the switch hostname
S3(config)#VTP mode transparent //configure VTP transparent
S3(config)#VTP domain rca.ac.rw //Changing VTP domain name from NULL to rca.ac.rw
S3(config)#VTP password rca@123 // Setting device VLAN database password to rca@123
S3(config)#

Configure trunk port to all switch

SWITCH 1:
S1(config)#interface fa0/1
S1(config-if)# switchport mode trunk
S1(config-if)#switchport trunk allowed VLAN 1-99
S1(config-if)#exit
SWITCH 2:
S2(config)#interface fa0/1
S2(config-if)# switchport mode trunk
S2(config-if)#switchport trunk allowed VLAN 1-99
S2(config-if)#exit

SWITCH 3:
S3(config)#interface fa0/2
S3(config-if)# switchport mode trunk
S3(config-if)#switchport trunk allowed VLAN 1-99
S3(config-if)#exit

Verification of VTP configuration

Switch#show vtp counters
Switch#show vtp status
Switch#show vtp password

3. VTP Versions

Three types of VTP versions are V1, V2, and V3.

The first two versions are similar except that V2 adds support for token ring VLANs.

Question: How to check VTP version?

```
Cisco-Switch#show vtp status
```

4. VTP traps generation

VTP traps are a mechanism used by Cisco devices to notify network administrators of changes to the VLAN configuration.

When a change occurs to the VLAN configuration, such as the creation, deletion, or modification of a VLAN, the VTP server sends a VTP update message to all of its VTP clients. In turn, the clients update their VLAN databases accordingly. However, sometimes it is necessary to notify administrators immediately of these changes, rather than waiting for the next VTP update message.

- **VTP Domain name propagation**

The **VTP domain name** is a unique name that identifies the VTP domain to which a switch belongs. All switches in the same VTP domain must have the same VTP domain name. If switches have different VTP domain names, they will not be able to communicate with each other using VTP.

- **VTP frame structure VTP revision number**

VTP frames are used to exchange VLAN information between switches in the same VTP domain.

The VTP frame structure consists of four fields:

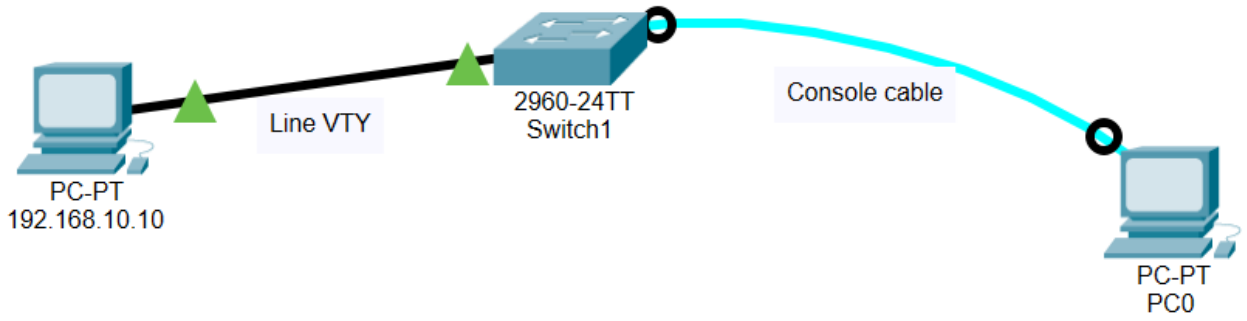
1. **VTP header:** This field contains information about the VTP frame, including the VTP domain name, the type of VTP message (advertisement, join, or summary), and the length of the VTP message.
2. **Management domain name**: This field contains the name of the VTP domain.

3. **Configuration revision number**: This field is used to keep track of the most recent VLAN configuration changes in the VTP domain. The VTP revision number is incremented whenever a VLAN is added, deleted, or modified. When a switch receives a VTP advertisement with a higher revision number than its own, it updates its VLAN database with the new information.
4. **VLAN information:** This field contains information about the VLANs in the VTP domain, including the VLAN ID, the VLAN name, and the VLAN type (Ethernet, FDDI, Token Ring, etc.). The VLAN information is carried in TLVs (Type-Length-Value) format

Questions: https://ipwithease.com/vtp-30-interview-questions/

LEARNING OUTCOME 4: CONFIGURE SWITCH SECURITY

Reference: https://www.networkstraining.com/basic-cisco-switch-configuration/



1. Configure console access

The console port is used to connect a computer directly to a router or switch and manage the router or switch since there is no display device for a router or switch.

	Description	Commands
1.	Enter global configuration mode	switch# config t
2.	Changing switch name	switch(config)#hostname switch1
3.	Enter Console configuration mode	switch1(config)# line console 0
4.	Setting the password	switch1(config-line)# password strongconsolepass
5.	Enabling the provided password to be used for login	switch1(config-line)# login
6.	Exiting line configuration mode	switch1(config-line)# exit

2. Configure virtual terminal access

	Description	Commands
.	Enter global configuration mode	Switch1# config t
•	Enter Console configuration mode	switch1(config)# line vty 0 15
•	Setting the password	switch1(config-line)# password strongconsolepass

• Enabling the provided password to be used for login	switch1(config-line)# login
• Exiting line configuration mode	switch1(config-line)# exit

3. **Configure Privilege EXE Mode password (enable secret password)**
   switch1(config)# enable secret somestrongpass

4. **Configure Encrypted Passwords**
   Switch1# config t
   Switch1(config)#security passwords min-length 9 //Setting the password minimum length
   Switch1(config)#service password-encryption //Enable password encryption
   Switch1(config)#exit

5. **Configure a login MOTD Banner**
   Switch1(config)#banner motd $Only Authorized people are allowed$
6. **Assign IP address to the switch for management**
   !**Management IP is assigned to Vlan 1 by default**

   switch1(config)# interface vlan 1
   switch1(config-if)# ip address 10.1.1.200 255.255.255.0
   switch1(config-if)# exit
   switch1(config)#

7. **Telnet and SSH**
   a. Enabling Telnet
   switch1(config)# line vty 0 15
   switch1(config-line)# password strongtelnetpass
   switch1(config-line)# login
   switch1(config-line)#transport input telnet
   switch1(config-line)# exit
   switch1(config)#
   Define which IP addresses are allowed to access the switch via Telnet

   switch1(config)# ip access-list standard TELNET-ACCESS
   switch1(config-std-nacl)# permit 10.1.1.100
   switch1(config-std-nacl)# permit 10.1.1.101
   switch1(config-std-nacl)# exit

!Apply the access list to Telnet VTY Lines

switch1(config)# line vty 0 15
switch1(config-line)# access-class TELNET-ACCESS in
switch1(config-line)# exit
switch1(config)#

b. SSH configuration

Switch(config)#username rca privilege 15 secret rca123
Switch(config)#hostname switch1
Switch1(config)#ip domain-name rca
Switch1(config)#crypto key generate rsa general-keys modulus 1024
switch1(config)#line vty 0 15
switch1(config-line)#login local
switch1(config-line)#transport input ssh
switch1(config-line)#exit
switch1(config)#

8. Disable unneeded ports on the switch

! Assume that we have a 48-port switch and we don't need ports 25 to 48
switch1(config)# interface range fa 0/25-48
switch1(config-if-range)# shutdown
switch1(config-if-range)# exit
switch1(config)#

9. Some Useful "Show" Commands

switch1# show run (Displays the current running configuration)
switch1# show interfaces (Displays the configuration of all interfaces and the status of each one)
switch1# show vlan (Displays all vlan numbers, names, ports associated with each vlan etc)
switch1# show interface status (Displays status of interfaces, speed, duplex etc)
switch1# show mac address-table (Displays current MAC address table and which MAC address is learned on each interface)

10. Common security attacks and countermeasures

i. MAC address attacks
ii. VLAN hopping
iii. ARP attacks
iv. DHCP attacks
v. General attacks
vi. Port security

LEARNING UNIT 3: IMPLEMENT INTER-VLAN ROUTING

Reference: https://www.comparitech.com/net-admin/inter-vlan-routing-configuration/

A VLAN is a broadcast domain, which means computers on separate VLANs are unable to communicate without the intervention of a routing device.

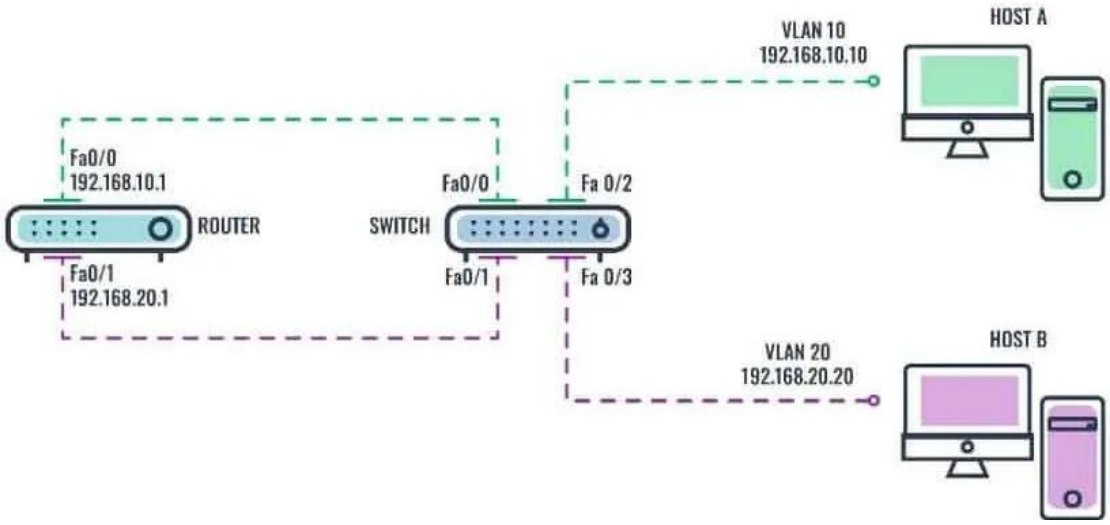
Whenever hosts in one VLAN need to communicate with hosts in another VLAN, the traffic must be routed through a routing device. This process is known **as inter-VLAN routing**. To successfully exchange information between VLANs, you need a **router** or a **Layer 3 switch**.

L O 1: CONFIGURE TRADITIONAL INTER-VLAN ROUTING

This method of inter-VLAN routing relies on a router with multiple physical interfaces. Each interface is usually connected to the switch, one for each VLAN.

The switch ports connected to the router are placed in access mode and each router interface can then accept traffic from the VLAN associated with the switch interface that it is connected to, and traffic can be routed to the other VLANs connected to the other interfaces.

This means that each of the routers' interface IP addresses would then become the default gateway address for each host in each VLAN.



Device	Interface	VLAN ID	IP Address	Subnet Mask	Default Gateway
Router	Fa0/0	VLAN 10	192.168.10.1	255.255.255.0	N/A
	Fa0/1	VLAN 20	192.168.20.1	255.255.255.0	N/A
Host A	NIC	VLAN 10	192.168.10.10	255.255.255.0	192.168.10.1
Host B	NIC	VLAN 20	192.168.20.20	255.255.255.0	192.168.20.1

Step 1: Create VLANs (VLANs 10 and 20) on the switch

Description	Command
Enter global configuration mode	Switch# conf t
Create VLAN 10	Switch(config)# vlan 10
Give a name to VLAN 10	Switch(config-vlan)# name Admin-dept
Create VLAN 20	Switch(config-vlan)# vlan 20
Give a name to VLAN 20	Switch(config-vlan)# name Finance-dept
Exit the VLAN config. mode	Switch(config-vlan)# exit
Check if the VLANs were created	Switch # show vlan brief

Step 2: Assign the VLANs to switch port

Description	Command
Enter global configuration mode	Switch# conf t
Enter interface config. mode for fa0/2	Switch(config)# interface fa0/2
Set the port to access mode	Switch(config-if)#switchport mode access
Assign VLAN 10 to interface fa0/2	Switch(config-if)#switchport access vlan 10
Exit the interface	Switch(config-if)# exit
Enter interface configuration for fa0/3	Switch(config)# interface fa0/3
Set the port to access mode	Switch(config-if)#switchport mode access
Assign VLAN 20 to interface fa0/3	Switch(config-if)#switchport access vlan 20
Exit the interface	Switch(config-if)# exit

Now at this stage, when you try to ping between Host A and Host B, the ping fails because the two PCs are on separate networks, and the router is not yet configured for inter-VLAN routing, so they cannot communicate with one another. Our next step is to configure inter-VLAN routing to enable communication between the VLANs.

Step 3: Configure the IP addresses on the router

Description	Command
Enter global configuration mode	Router# conf t
Enter interface config. mode for fa0/0	Router(config)# interface fa0/0
Configure IP address and subnet mask	Router(config-if)#ip address 192.168.10.1 255.255.255.0
Activate the interface	Router(config-if)#no shutdown
Exit the interface	Router(config-if)#exit
Enter interface config. mode for fa0/1	Router(config)# interface fa0/1
Configure IP address and subnet mask	Router(config-if)# ip address 192.168.20.1 255.255.255.0
Activate the interface	Router(config-if)#no shutdown

Exit the interface	Router(config-if)# exit
Save configuration	Router# copy running-config startup-config

Now at this juncture, if you try to ping between Host A and Host B, it will be successful because the two VLANs are now interconnected through the router.

L O 2: CONFIGURE ROUTER ON-A-STICK INTER-VLAN ROUTING

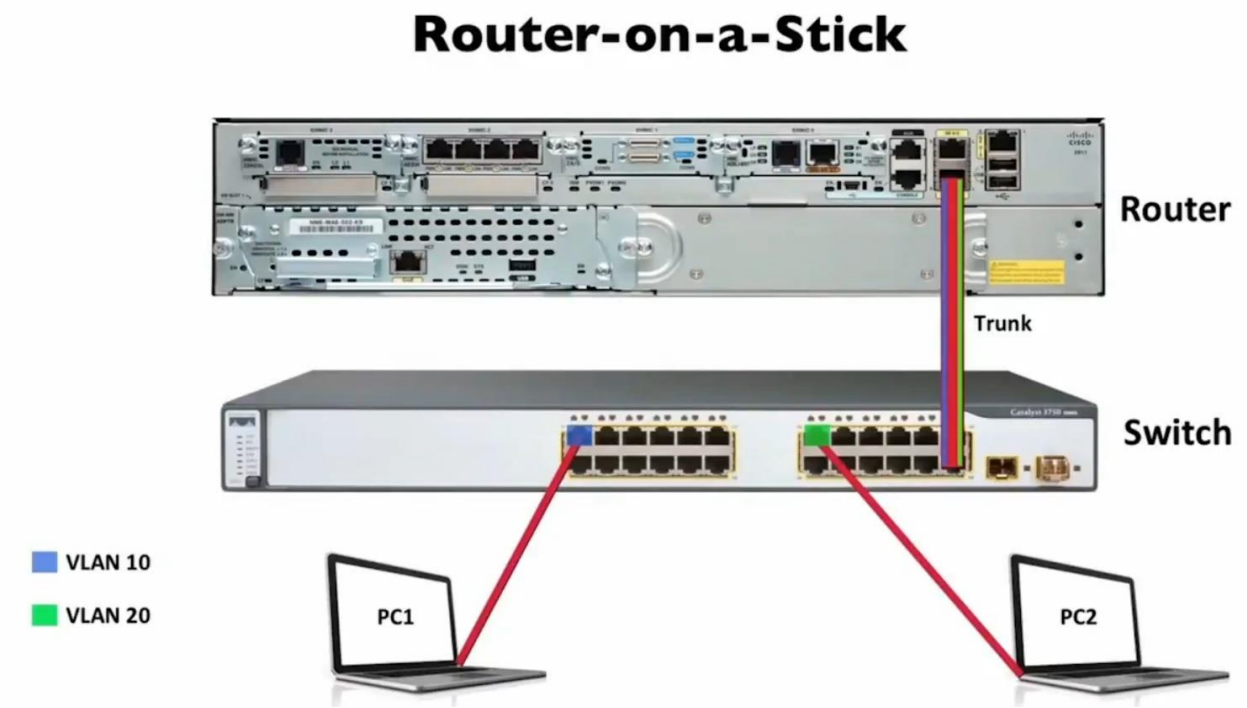
A router-on-a-stick is a method of inter-VLAN routing in which the router is connected to the switch using a single physical interface to allow traffic from multiple VLANs.

In this configuration, a **single physical interface** on the router is connected to a switch port configured as a **trunk port** that carries traffic for multiple VLANs.

The router uses **sub-interfaces**, which are logical interfaces that are created on the physical interface and assigned to different VLANs.

Each sub-interface is configured with an IP address that corresponds to the IP subnet of the corresponding VLAN. The router performs inter-VLAN routing by forwarding traffic between the sub-interfaces and their associated VLANs.

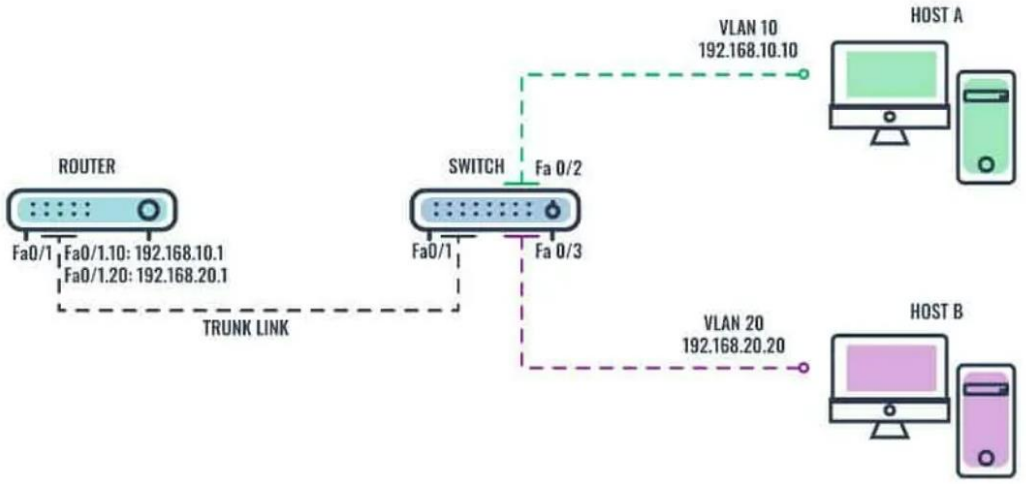
IEEE 802.1Q (**Dot1q**) protocol—which defines a system of VLAN tagging for Ethernet frames, is used to provide multi-vendor VLAN support.



How does it work?

Let's take a look at the diagram shown in Figure below. If Host A on VLAN 10, wants to send a message to Host B on VLAN 20, the steps it would take are as follows:

1. Host A sends its unicast traffic to the switch.
2. The switch then tags the unicast traffic as originating on VLAN 10 and forwards it out its trunk link to the router.
3. The router accepts the tagged unicast traffic on VLAN 10 and routes it to VLAN 20 using its configured sub-interfaces.
4. The unicast traffic is tagged with VLAN 20 as it is sent out the router interface to the switch.
5. The switch removes the VLAN tag of the unicast frame and forwards the frame directly to Host B on port Fa0/3.



To configure router-on-a-stick inter-VLAN routing on a Cisco device, in accordance with the diagram shown in Figure above:

Device	Interface	VLAN ID	IP Address	Subnet Mask	Default Gateway
Router	Fa0/1.10	VLAN 10	192.168.10.1	255.255.255.0	N/A
	Fa0/1.20	VLAN 20	192.168.20.1	255.255.255.0	N/A
Host A	NIC	VLAN 10	192.168.10.10	255.255.255.0	192.168.10.1
Host B	NIC	VLAN 20	192.168.20.20	255.255.255.0	192.168.20.1

Step 1: Create VLANs (VLANs 10 and 20) on the switch

Description	Command
Enter global configuration mode	Switch# conf t
Create VLAN 10	Switch(config)# vlan 10
Give a name to VLAN 10	Switch(config-vlan)# name Admin-dept
Create VLAN 20	Switch(config-vlan)# vlan 20
Give a name to VLAN 20	Switch(config-vlan)# name Finance-dept
Exit the VLAN config. mode	Switch(config-vlan)# exit
Check if the VLANs were created	Switch # show vlan brief

Step 2: Assign the VLANs to switch ports

Description	Command
Enter global configuration mode	Switch#conf t
Enter the interface configuration mode for fa0/2	Switch(config)# interface fa0/2
Set the port to access mode	Switch(config-if)#switchport mode access
Assign VLAN 10 to interface fa0/2	Switch(config-if)#switchport access vlan 10
Exit the interface	Switch(config-if)# exit
Enter interface configuration for fa0/3	Switch(config)# interface fa0/3
Set the port to access mode	Switch(config-if)#switchport mode access
Assign VLAN 20 to interface fa0/3	Switch(config-if)#switchport access vlan 20
Exit the interface	Switch(config-if)# exit
Enter interface configuration for fa0/1	Switch(config)# interface fa0/1
Set the port to trunk mode	Switch(config-if)#switchport mode trunk
Exit the interface	Switch(config-if)# exit
Save configuration	Switch# copy running-config startup-config

Step 3: Configure the IP addresses on the router

Description	Command
Enter global configuration mode	Router# conf t
Enter sub-interface config. mode for fa0/1.10	Router(config)# interface fa0/1.10
Set encapsulation type to 802.1Q and assign VLAN 10 to the virtual interface	Router(config-subif)# encapsulation dot1Q 10
Configure IP address and subnet mask	Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Exit the sub-interface	Router(config-subif)#exit
Enter sub-interface config. mode for fa0/1.20	Router(config)# interface fa0/1.20
Set the encapsulation type to 802.1Q and assign VLAN 20 to the virtual interface.	Router(config-subif)# encapsulation dot1Q 20
Configure IP address and subnet mask	Router(config-subif)# ip address 192.168.20.1 255.255.255.0
Exit the sub-interface	Router(config-subif)#exit
Enter interface config. mode for fa0/1	Router(config)# interface fa0/1
Activate the physical interface	Router(config-if)# no shutdown
Save configuration	Router# copy running-config startup-config
Verify configuration	Router #show ip route

A ping between Host A and Host B will be successful because the two VLANs are now interconnected through the router.

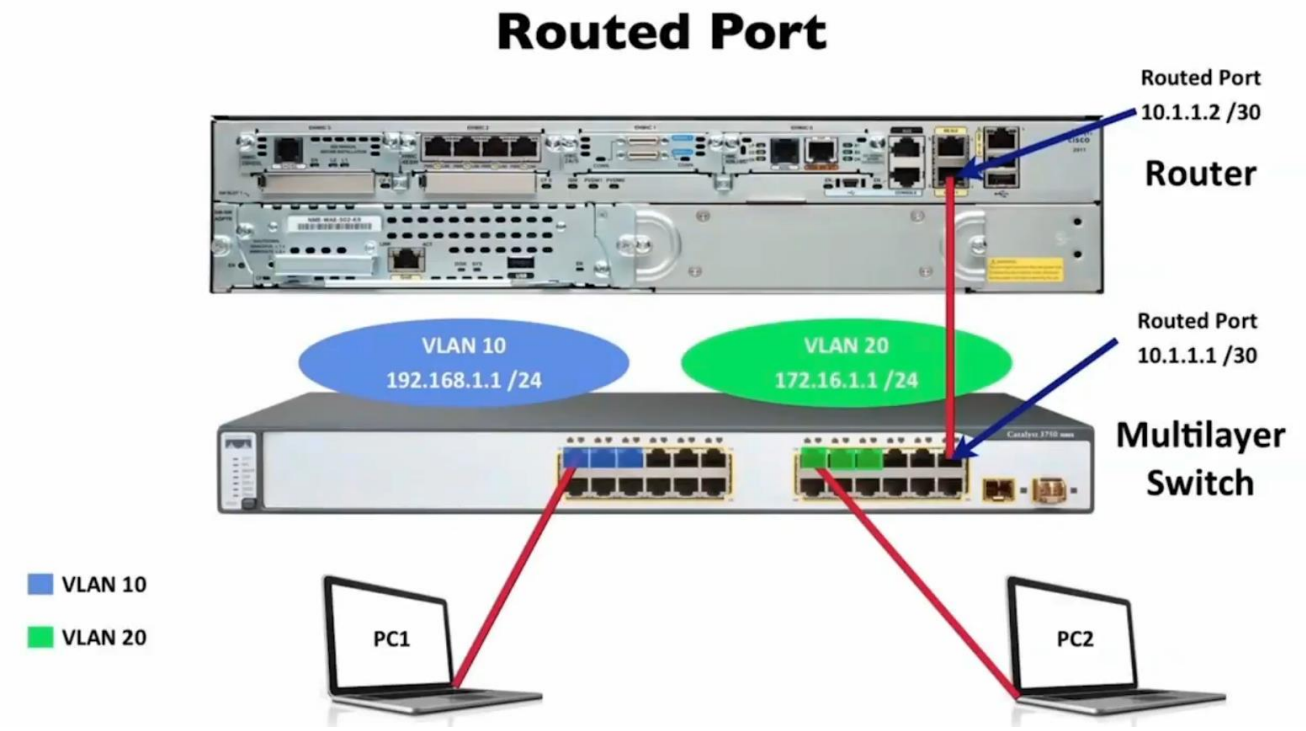
The router-on-a-stick method of inter-VLAN routing also has some **limitations**, such as scalability and latency issues. To overcome these issues, Cisco developed a better alternative: The Multilayer Switch Inter-VLAN Routing.

L O 3: IMPLEMENT LAYER 3 SWITCHING INTER-VLAN ROUTING

Multilayer Switch Inter-VLAN Routing is a method of inter-VLAN routing in which a different kind of switch known as a multilayer switch is used to perform routing functions.

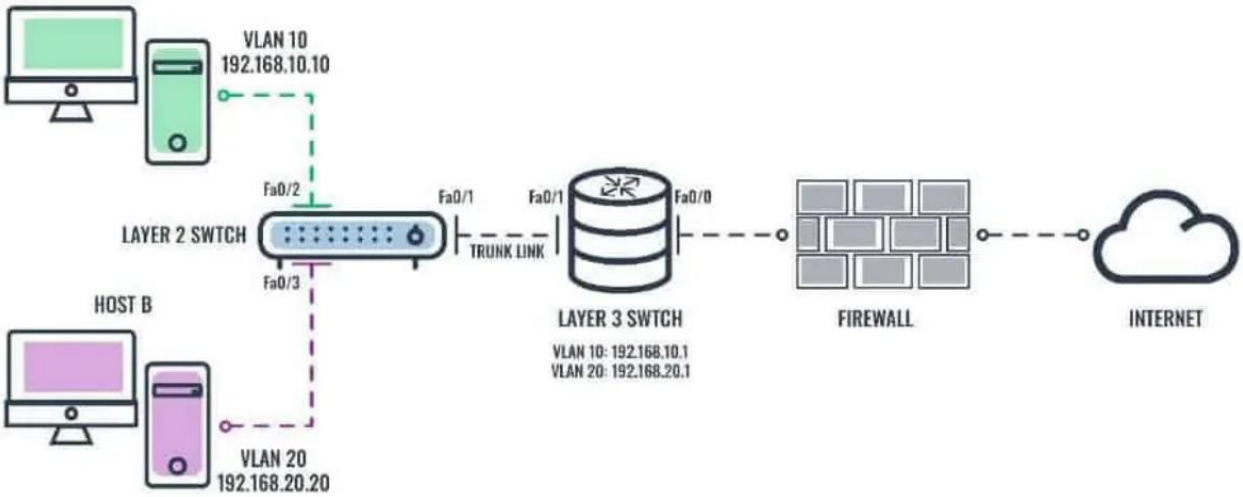
A multilayer switch is a hybrid device that combines the functions of a switch with a router, which enables it to operate on both Layer 2 (L2) and Layer 3 (L3) of the OSI model, hence the name multilayer. Unlike the router-on-a-stick inter-VLAN routing method, a multilayer switch inter-VLAN routing does not require a dedicated router-everything happens inside the switch.

To enable a multilayer switch to perform routing functions, logical (virtual) interfaces known as **Switch Virtual Interface** (SVI) are used, one for each VLAN. Each SVI is configured for different subnets corresponding to their assigned VLAN to facilitate logical routing.



How does it work?

When the multilayer switch receives a packet in a VLAN intended at the Layer 2 switch, the multilayer switch performs routing. Let's take a look at the diagram shown in the Figure below:



If Host A in VLAN 10, wants to send a message to Host B in VLAN 20, the steps it would take are as follows:

1. Host A sends its unicast traffic to the directly connected L2 switch.
2. L2 switch tags the unicast traffic as originating on VLAN 10 and forwards it to the L3 switch via the trunk link.
3. The L3 switch removes the VLAN tag and forwards the unicast traffic internally to the VLAN 10 virtual interface.
4. The L3 switch internally routes the unicast traffic to its VLAN 20 virtual interface and then retags the traffic, which it then forwards back to the L2 switch via the trunk link.
5. L2 switch removes the VLAN tag of the unicast frame and forwards the frame directly to Host B on port fa0/3.

To configure multi-layer switch inter-VLAN routing on a Cisco device, in accordance with the diagram shown in the Figure above, use the IP addresses shown in a Table and follow the steps below:

Device	**Interface**	**VLAN ID**	**IP Address**	**Subnet Mask**	**Default Gateway**
L3 Switch	Fa0/0	N/A	192.0.0.1	255.255.255.0	192.0.0.2
	SVI 10	VLAN 10	192.168.10.1	255.255.255.0	N/A
	SVI 20	VLAN 20	192.168.20.1	255.255.255.0	N/A
Host A	NIC	VLAN 10	192.168.10.10	255.255.255.0	192.168.10.1
Host B	NIC	VLAN 20	192.168.20.20	255.255.255.0	192.168.20.1

Table: IP address detail for above Figure

Step 1: Create VLANs (VLANs 10 and 20) on the L2 switch

Description	Command
Enter global configuration mode	L2-Switch# conf t
Create VLAN 10	L2-Switch(config)# vlan 10
Give a name to VLAN 10	L2-Switch(config-vlan)# name Admin-dept
Create VLAN 20	L2-Switch(config-vlan)# vlan 20
Give a name to VLAN 20	L2-Switch(config-vlan)# name Finance-dept
Exit the VLAN config mode	L2-Switch(config-vlan)# exit
Check if the VLANs were created	L2-Switch#show vlan brief

Step 2: Assign the VLANs to the L2 switch ports

Description	Command
Enter global configuration mode	L2-Switch# conf t
Enter interface config. mode for fa0/2	L2-Switch(config)# interface fa0/2
Set the port to access mode	L2-Switch(config-if)#switchport mode access
Assign VLAN 10 to interface fa0/2	L2-Switch(config-if)#switchport access vlan 10
Exit the interface	L2-Switch(config-if)# exit
Enter interface configuration for fa0/3	L2-Switch(config)# interface fa0/3
Set the port to access mode	L2-Switch(config-if)#switchport mode access
Assign VLAN 20 to interface fa0/3	L2-Switch(config-if)#switchport access vlan 20
Exit the interface	L2-Switch(config-if)# exit
Enter interface configuration for fa0/1	L2-Switch(config)# interface fa0/1
Set the port to trunk mode	L2-Switch(config-if)# switchport mode trunk
Exit the interface	L2-Switch(config-if)# exit
Save all configuration	L2-Switch# copy running-config startup-config

Step 3: Enable L3 routing and create VLANs (VLANs 10 and 20) on the L3 switch

Description	Command
Enter global configuration mode	L2-Switch#conf t
Enable L3 routing	L3-Switch(config) # ip routing
Create VLAN 10	L3-Switch(config)#vlan 10
Give a name to VLAN 10	L3-Switch(config-vlan)# name Admin-dept
Create VLAN 20	L3-Switch(config-vlan)# vlan 20
Give a name to VLAN 20	L3-Switch(config-vlan)# name Finance-dept
Exit the VLAN config mode	L3-Switch(config-vlan)# exit
Enter interface configuration for fa0/1	L3-Switch(config)# interface fa0/1
Set the encapsulation type to 802.1Q on the interface	L3-Switch(config-if)# switchport trunk encapsulation dot1q
Set the port to trunk mode	L3-Switch(config-if)#switchport mode trunk
Exit the interface	L3-Switch(config-if)# exit
Save all configuration	L3-Switch)# copy running-config startup-config

Step 4: Configure Switch VLAN Interfaces (SVI)

Description	Command
Enter global configuration mode	L3-Switch# conf t
Create a virtual interface for VLAN 10	L3-Switch(config)# interface vlan10
Configure a static route to reach VLAN 10	L3-Switch(config-if)# ip address 192.168.10.1 255.255.255.0
Activate interface	L3-Switch(config-if)# no shut
Exit the interface	L3-Switch(config-if)# exit

Create a virtual interface for VLAN 20	L3-Switch(config)# interface vlan20
Configure a static route to reach VLAN 20	L3-Switch(config-if)# ip address 192.168.20.1 255.255.255.0
Activate interface	L3-Switch(config-if)# no shut
Exit the interface	L3-Switch(config-if)# exit

Step 5: Configure a routed port for connecting to the firewall on the L3 switch

Description	**Command**
Enter global configuration mode	L3-Switch# conf t
Enter interface configuration for fa0/0	L3-Switch(config)# interface fa0/0
Interface description	L3-Switch(config-if)# description to Internet Firewall
Creates an L3 port on the switch's physical port	L3-Switch(config-if)# no switchport
Configure IP address	L3-Switch(config-if)# ip address 192.0.0.1 255.255.255.252
Configure the default route toward the firewall	L3-Switch(config)# ip route 0.0.0.0 0.0.0.0 192.0.0.2
Exit the interface	L3-Switch(config-if)# exit
Save all configuration	L3-Switch)# copy running-config startup-config

Learning Unit 4: CONFIGURE WIRELESS NETWORK

LO4.1 Systematic Implementation of SOHO and Enterprise wireless network

(Group discussion on the use of wireless and its applications, Wireless infrastructure components and WLAN deployment solutions, Practical configuration of Wireless network devices)

1. **WLANs Standards**

WLAN (Wireless Local Area Network) standards are a set of specifications developed by the IEEE (Institute of Electrical and Electronics Engineers) for wireless communication between devices. These standards specify the frequency bands, data rates, modulation techniques, security protocols, and other parameters that govern wireless communication.

The most widely used WLAN standards (802.11 WLAN technologies) are:

a. **IEEE 802.11a**: This standard operates in the 5 GHz frequency band and supports data rates up to 54 Mbps.
b. **IEEE 802.11b:** This standard operates in the 2.4 GHz frequency band and supports data rates up to 11 Mbps.
c. **IEEE 802.11g**: This standard operates in the 2.4 GHz frequency band and supports data rates up to 54 Mbps.
d. **IEEE 802.11n:** This standard operates in both the 2.4 GHz and 5 GHz frequency bands and supports data rates up to 600 Mbps.
e. **IEEE 802.11ac:** This standard operates in the 5 GHz frequency band and supports data rates up to 7 Gbps.
f. **IEEE 802.11ax** (also known as Wi-Fi 6): This standard operates in both the 2.4 GHz and 5 GHz frequency bands and supports data rates up to 9.6 Gbps.

Benefits of Wireless

- ✓ **Mobility:** Wireless technology allows devices to be used without the need for cables or fixed connections, enabling people to work and communicate on the go, which increases productivity and convenience.
- ✓ **Flexibility:** Wireless networks can be easily configured and reconfigured to meet changing business needs or adapt to new technologies, making wireless technology more adaptable and scalable than wired networks.
- ✓ **Cost-effectiveness:** Wireless technology eliminates the need for expensive cabling and infrastructure, making it more cost-effective than wired networks. Wireless networks are also easier and less expensive to maintain and upgrade.

- ✓ **Improved collaboration:** Wireless technology allows people to work together and share information more easily, regardless of their location, which enhances collaboration and teamwork, leading to better business outcomes.
- ✓ **Increased efficiency**: Wireless technology can increase operational efficiency by enabling real-time data collection and analysis, as well as remote monitoring and control of equipment and systems.
- ✓ **Access to information:** Wireless technology provides access to information and resources from anywhere, making it easier to stay informed and make informed decisions.
- ✓ **Convenience:** Wireless technology eliminates the need for physical connections, which reduces clutter and simplifies the setup process.
- ✓ **Improved user experience:** Wireless technology provides a more seamless and convenient user experience, making it easier to connect devices and access data.

2. **Wireless technologies**

Wireless technologies refer to any communication system that uses wireless signals to transmit and receive data over the airwaves. These technologies are widely used in various applications, including mobile communications, internet connectivity, and sensor networks

Some of the most common wireless technologies are:

1. **Wi-Fi:** This technology uses radio waves to connect devices to the internet or to each other without the need for cables. Wi-Fi is widely used in homes, offices, and public places such as coffee shops and airports.
2. **Bluetooth:** This technology is used for short-range wireless communication between devices, such as smartphones, tablets, and headphones. Bluetooth operates in the 2.4 GHz frequency band and supports data rates up to 24 Mbps.
3. **Zigbee:** This technology is designed for low-power, low-data-rate wireless communication between sensors, smart meters, and other devices in the Internet of Things (IoT) ecosystem. Zigbee operates in the 2.4 GHz frequency band and supports data rates up to 250 kbps.
4. **NFC (Near Field Communication):** This technology is used for short-range wireless communication between devices, such as smartphones and contactless payment terminals. NFC operates in the 13.56 MHz frequency band and supports data rates up to 424 kbps.
5. **Cellular:** This technology uses radio waves to provide wireless voice and data communication over long distances. Cellular networks are used by mobile phone operators to provide mobile services to users.

6. **Satellite:** This technology uses orbiting satellites to provide wireless communication services over large geographic areas. Satellite communication is commonly used for broadcasting, remote sensing, and military applications

3. **Wireless infrastructure components**
   - ✓ Wireless NICs
   - ✓ Wireless Home router
   - ✓ Wireless Access points
   - ✓ Wireless antennas
4. **Small wireless deployment solutions**

   Small wireless deployment solutions typically involve the implementation of a wireless network in a small office, home office (SOHO), or small business environment.

   Here are some common solutions for small wireless deployments:

   1. **Wireless routers:** Wireless routers are devices that provide wireless connectivity to multiple devices within a small area, such as a home or small office. They typically offer a range of up to 100 feet and support multiple wireless standards, including Wi-Fi, Bluetooth, and Zigbee.
   2. **Wireless access points:** Wireless access points (WAPs) are devices that extend the range of an existing wired network by providing wireless connectivity to devices within a small area. They are typically used in larger homes or small businesses and can support multiple wireless standards.
   3. **Wireless range extenders:** Wireless range extenders are devices that amplify the signal of an existing wireless network to extend its range. They are typically used in homes or small offices where the wireless signal is weak or inconsistent.
   4. **Mesh networks:** Mesh networks are wireless networks that consist of multiple wireless access points that communicate with each other to provide seamless coverage throughout a larger area. They are typically used in larger homes or small businesses and can provide better coverage and performance than traditional wireless networks.
   5. **Mobile hotspots:** Mobile hotspots are devices that provide wireless connectivity to devices on the go, such as laptops or tablets. They typically use cellular networks to provide internet access and can be used in a variety of settings, including business trips, remote work, or outdoor events.

5. **Wireless topology mode**

Wireless topology mode refers to the way in which wireless devices are connected to each other to form a wireless network.

There are three main wireless topology modes:

1. **Ad hoc mode:** In ad hoc mode, wireless devices connect directly to each other without the need for an access point (AP) or any other network infrastructure. Ad hoc mode is useful for creating a small, temporary network, such as for sharing files or playing multiplayer games.
2. **Infrastructure mode:** In infrastructure mode, wireless devices connect to a central access point (AP) or wireless router that acts as a hub for the network. The AP is connected to a wired network, such as an Ethernet network or the internet, and serves as a bridge between the wireless devices and the wired network.
3. **Mesh mode:** In mesh mode, wireless devices are connected to each other in a mesh network, in which each device can act as a router for other devices. This creates a decentralized network that is more resilient and flexible than traditional infrastructure mode networks and can provide coverage over a wider area.

The choice of wireless topology mode will depend on the specific needs and requirements of the wireless network. **Ad hoc mode** is useful for small, temporary networks, while **infrastructure mode** is suitable for larger, more permanent networks that require access to a wired network or the internet. **Mesh mode** is useful for large-scale, outdoor, or industrial networks where coverage and resilience are critical.

6. **RF fundamental**

   RF (Radio Frequency) fundamentals refer to the basic principles and concepts involved in the transmission, reception, and processing of radio waves.

   Here are some key fundamentals:

   - **Radio Waves:** RF signals are carried by electromagnetic waves that travel through the air at the speed of light. These waves have a specific frequency, wavelength, and amplitude that determine their properties.
   - **Frequency:** Frequency is the number of cycles per second of an electromagnetic wave, measured in Hertz (Hz). RF signals typically operate at frequencies between 3 kHz and 300 GHz.
   - **Modulation:** Modulation is the process of varying the amplitude, frequency, or phase of a carrier wave to transmit information. Common

modulation techniques include amplitude modulation (AM), frequency modulation (FM), and phase modulation (PM).

- **Antennas:** Antennas are devices used to transmit or receive RF signals. They are designed to radiate or receive electromagnetic waves efficiently and with minimal loss.
- **Transmission lines:** Transmission lines are used to transfer RF signals from one point to another. They are designed to minimize signal loss and distortion.
- **Filters:** Filters are used to remove unwanted signals and noise from an RF signal. They can be designed to block specific frequencies or pass certain frequency ranges.
- **Amplifiers**: Amplifiers are used to increase the power of an RF signal. They can be designed to provide gain at specific frequencies or across a wide range of frequencies.
- **Mixers:** Mixers are used to combine two or more RF signals to create a new signal. They can also be used to convert the frequency of a signal.
- **Oscillators:** Oscillators are used to generate RF signals. They can be designed to operate at specific frequencies or to provide a tunable frequency range.
- **Demodulation:** Demodulation is the process of extracting the original information from a modulated RF signal. It is the opposite process of modulation and involves detecting changes in the amplitude, frequency, or phase of the carrier wave.

7. Application of wireless

Wireless technology has become an essential part of modern society, and it is used in a wide range of applications across many industries.

Some of the most common applications of wireless technology:

- **Mobile communication**: Wireless technology enables mobile communication through mobile phones, tablets, laptops, and other mobile devices.
- **Internet connectivity:** Wireless technology allows users to access the internet wirelessly through Wi-Fi, cellular data, and other wireless networks.
- **Smart homes:** Wireless technology is used in smart homes to connect devices such as security systems, smart thermostats, and other home automation devices.
- **Healthcare:** Wireless technology is used in healthcare for patient monitoring, telemedicine, and remote diagnosis.

- **Transportation:** Wireless technology is used in transportation for vehicle-to-vehicle communication, navigation, and tracking.
- **Industrial automation:** Wireless technology is used in industrial automation for remote control, monitoring, and data acquisition.
- **Entertainment:** Wireless technology is used in entertainment for streaming audio and video content to wireless speakers, headphones, and other devices.
- **Retail:** Wireless technology is used in retail for inventory management, point-of-sale systems, and customer analytics.

8. Wireless network operations

✓ 802.11 frame structure

Overview of the frame structure:

- **Frame control field**: This field includes information about the type of frame (management, control, or data), as well as information about the frame's transmission and reception.
- **Duration field:** This field indicates the duration of time that the wireless medium will be occupied for the transmission of the current frame and any subsequent frames.
- **MAC address fields:** This field includes the MAC addresses of the source and destination devices.
- **Sequence control field:** This field includes a sequence number that is used to ensure that frames are received in the correct order.
- **Frame body:** This field includes the actual data being transmitted.
- **Frame check sequence (FCS) field:** This field is used to check the integrity of the transmitted frame.

✓ 802.11 frame structure control frames

Control frames serve several important functions, such as managing access to the wireless medium, negotiating data rates, and handling errors.

Common types of control frames and their functions:

1. **Request to Send** (RTS): The RTS frame is used by a device to request permission to transmit data to another device. The RTS frame includes the duration of time the requesting device intends to transmit and the destination MAC address.
2. **Clear to Send** (CTS): The CTS frame is sent by the destination device in response to an RTS frame, granting permission for the requesting device to

transmit data. The CTS frame also includes the duration of time the destination device intends to occupy the wireless medium.

3. **Acknowledgement** (ACK): The ACK frame is used to acknowledge the receipt of a data frame. The sending device waits for an ACK frame before sending the next frame, ensuring that frames are received correctly.
4. **Power Save Poll** (PS-Poll): The PS-Poll frame is used by a wireless station in power-saving mode to request buffered frames from an access point.
5. **Beacon:** The Beacon frame is sent periodically by an access point to advertise the presence of a wireless network and provide information about the network's capabilities.

- ✓ **Wireless frame types**

Most common types of frames used in wireless communication:

1. **Data Frames:** Data frames are used to carry data between wireless devices in a wireless local area network (WLAN). They contain the actual data being transmitted, along with control information such as the source and destination MAC addresses, sequence numbers, and error-checking codes.
2. **Control Frames**: Control frames are used to manage access to the wireless medium, negotiate data rates, and handle errors in the wireless network. They include frames such as Request to Send (RTS), Clear to Send (CTS), and Acknowledgement (ACK) frames.
3. **Management Frames**: Management frames are used to manage and control the wireless network itself, rather than transmitting data. They include frames such as Beacon, Probe Request, and Probe Response frames, which are used for network discovery and management.
4. **Null Data Frames**: Null data frames are used to reserve the wireless medium when no actual data is being transmitted. They are sent periodically by wireless devices to prevent other devices from transmitting on the same channel.
5. **Association and Disassociation Frames:** Association and disassociation frames are used to connect and disconnect wireless devices from the wireless network. They include frames such as Association Request, Association Response, Disassociation, and Reassociation frames.

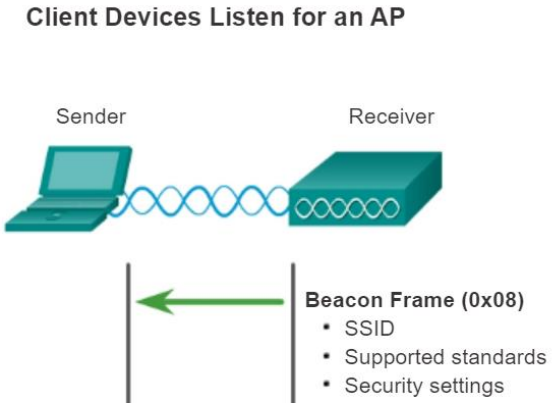
- ✓ **CSMA/CA**

CSMA/CA stands for Carrier Sense Multiple Access with Collision Avoidance. It is a protocol used in wireless communication to avoid collisions between wireless devices transmitting on the same channel.

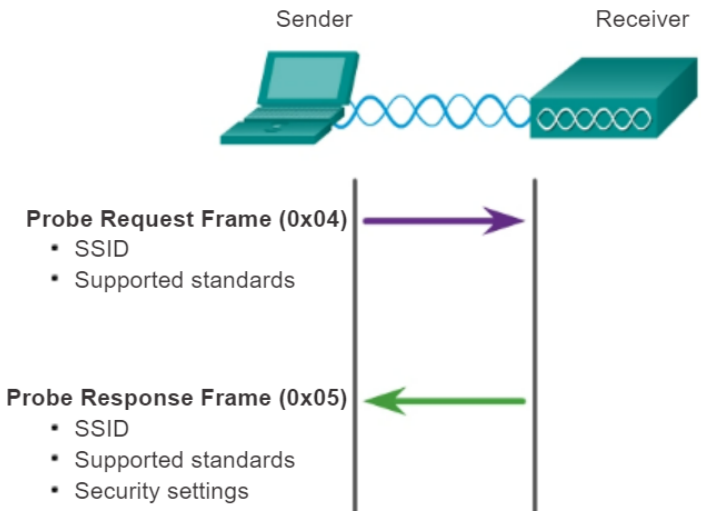
✓ **Discovering Aps**

Wireless devices must discover and connect to an AP or wireless router. Wireless clients connect to the AP using a scanning (probing) process. This process can be:

- **Passive mode**: The AP openly advertises its service periodically, but continually sends **broadcast beacon frames** containing the SSID, supported standards, and security settings. The primary purpose of the beacon is to allow wireless clients to learn which networks and APs are available in a given area, thereby allowing them to choose which network and AP to use.



- **Active mode** - Wireless clients must know the name of the SSID. The wireless client initiates the process by broadcasting a probe request frame on multiple channels. The probe request includes the SSID name and standards supported. Active mode may be required if an AP or wireless router is configured to not broadcast beacon frames.



9. **Channel management**
   In wireless communication, channels refer to the frequencies on which data is transmitted between wireless devices.
   Effective channel management is critical to ensuring reliable and efficient wireless communication.
10. **Installing, configuring, and managing the WLANs devices**
    - **a.** Access points
    - **b.** Enterprise WLAN switches and controllers
    - **c.** Remote office WLAN switches and controllers
    - **d.** Power over Ethernet injectors and switches
    - **e.** WLAN bridges
    - **f.** Residential WLAN gateways
    - **g.** Enterprise encryption gateways
    - **h.** WLAN mesh routers
11. **Installing, configuring, and managing WLANs Client devices**
    a. PC CARDS
    b. USB, Compact Flash, and SD devices
    c. PCI and Mini-PCI cards Wireless presentation gateways

LO 4.2 Apply security technology

1. identifying and preventing WLAN security attacks

- ✓ Eavesdropping
- ✓ Hijacking
- ✓ Man-in-the-Middle
- ✓ Denial of Service (DOS)
- ✓ Management interface exploits
- ✓ Encryption cracking

- ✓ Authentication cracking
- ✓ MAC spoofing
- ✓ Peer-to-peer attacks
- ✓ Social engineering

LO 4.3 Test of wireless connectivity and security arrangements

Wireless LAN Testing Considerations

- ✓ Signal coverage testing
- ✓ Performance testing
- ✓ In-motion testing
- ✓ Security vulnerability testing
- ✓ Acceptance/verification testing
- ✓ Simulation testing
- ✓ Prototype testing
- ✓ Pilot testing
- ✓ Test documentation

Troubleshooting wireless station connection to AP

- ✓ Can any wireless stations connect to the AP?
- ✓ Troubleshooting wireless stations
- ✓ Wireless network detected
- ✓ Signal interference
- ✓ Site survey
- ✓ Station status
- ✓ Using correct SSID
- ✓ Station configuration
- ✓ Correct security settings
- ✓ TCP/IP protocol installed and configured

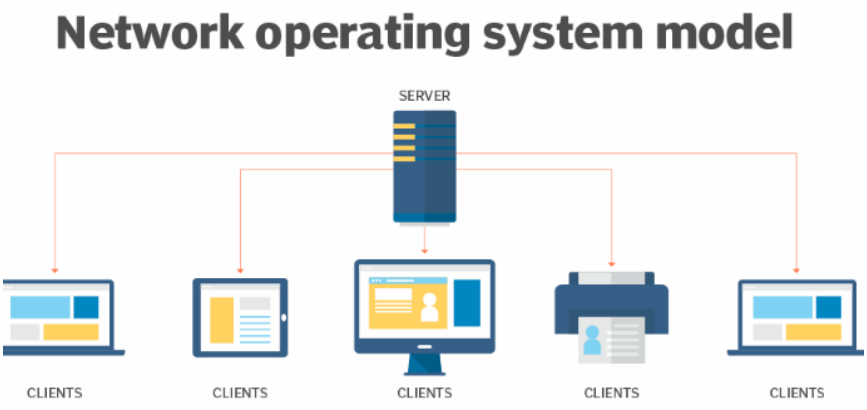
LU 5: Installation, configuration and Management of Network Operating system

LO1: Describe server operation system

What is a network operating system (NOS)?

A network operating system (NOS) is a computer operating system (OS) that's designed primarily to support workstations, PCs and, in some instances, older terminals that are connected on a local area network (LAN). The software behind a NOS enables multiple devices within a network to communicate and share resources with each other.

A NOS coordinates the activities of multiple computers across a network. This can include such devices as PCs, printers, file servers and databases connected to a local network. The role of the NOS is to provide basic network services and features that support multiple input requests simultaneously in a multiuser environment.



Common features of network operating systems

Features of network operating systems are typically associated with user administration, system maintenance and resource management functionality. These include the following:

- Basic support for OSes, including protocol and processor support, hardware detection and multiprocessing
- Printer and application sharing.
- Common file system and database sharing.
- Network security capabilities, such as user authentication and access control.
- Directory services.

- Backup and web services.
- Internetworking.

Considerations when selecting a server operating system

Some considerations when selecting a server operating system include:

- Compatibility with existing hardware and software,
- Level of technical expertise required for administration,
- Security features,
- Licensing and cost, and
- Availability of support and updates.

Some examples of network operating systems:

- **Windows Server**: Microsoft's Windows Server is a popular network operating system used in many organizations. It provides a wide range of networking features and services, such as Active Directory for user and resource management, DNS services, file and print sharing, and remote access capabilities.
- **Linux:** Linux distributions like Ubuntu Server, CentOS, and Red Hat Enterprise Linux (RHEL) are widely used as network operating systems. Linux offers robust networking capabilities, excellent performance, and extensive customization options. It also supports various networking protocols and services, making it suitable for a wide range of network infrastructures.
- **macOS Server:** Apple's macOS Server is a network operating system designed specifically for Mac-based networks. It provides features like file sharing, user and device management, VPN services, and Time Machine backups. However, Apple has deprecated many server features in recent versions, and macOS Server is now more focused on management tools rather than providing a full network operating system.
- **FreeBSD:** FreeBSD is a Unix-like operating system known for its stability and security. It can be used as a network operating system due to its robust networking stack and features like TCP/IP networking, firewalling, packet filtering, and network services like DNS, DHCP, and NFS.
- **Novell NetWare:** Although less prevalent today, NetWare was a popular network operating system in the past. It provided advanced file and print services, directory services, and reliable networking capabilities. However, Novell has shifted its focus to other products, and NetWare has lost significant market share over the years.

- **IBM AIX:** AIX is IBM's Unix-based operating system designed for IBM Power Systems. It offers a range of networking features and services, including TCP/IP stack, file and printer sharing, and security features. AIX is primarily used in enterprise environments and supports high availability and clustering options.
- **Solaris:** Solaris is a Unix-based operating system developed by Oracle Corporation. It provides comprehensive networking capabilities and features like TCP/IP, IPsec, virtualization support, and network services such as NFS, DNS, and DHCP.