CCNA (ROUTING AND SWITCHING)

HUB

- Hubs do not have intelligence to find out best path for data packets.
- Pretty much repeat signal on one end to another.

BRIDGE

- A bridge maintains a MAC address table for both LAN segments it is connected to.
- Bridge looks at the destination of the packet before forwarding unlike a hub. It
- Restrict transmission on other LAN segment if destination is not found.

SWITCH

- A switch when compared to bridge has multiple ports**.**
- Switches can perform error checking before forwarding data.
- Usually large networks use switches instead of hubs to connect computers within the same subnet.

ROUTER

- A router, like a switch **f**orwards packets based on IP address.
- It is used to connect different devices.

REPEATER:

- A network device used to regenerate or replicate a signal. Repeaters are used in
- Transmission systems to regenerate analog or digital signals distorted by
- Transmission loss.

HALF-DUPLEX

- Half-duplex devices let you send and receive, but only one-way at a time.
- If you've ever used a walkie-talkie, then you know what half-duplex conversations sound like.
- You have to push the TALK button to send your message. But as long as you are holding the TALK key, you can't hear what anyone else is saying.
- You must release the button to receive.

- One side can talk at a time.
- Once one side has finished transmitting its data, the other side can respond.
- Only one node can talk at a time. If both try to talk at the same time, a collision will occur on the network.

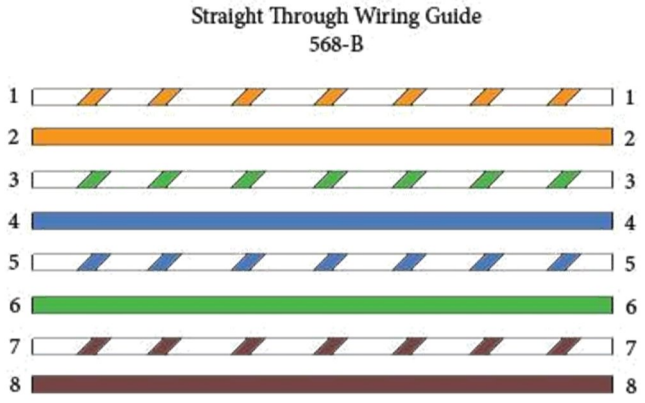
FULL- DUPLEX

- On the other hand, full-duplex is used to describe communication where both sides are able to send and receive data at the same time.
- In these cases, there is no danger of a collision and therefore the transfer of data is completed much faster.

OR

- Actually, full duplex is nothing new.
- In fact, you already know exactly what it sounds like.
- Your corded or cordless phones are full-duplex devices letting you and your caller speaks simultaneously without any dropouts in either one of your voices.

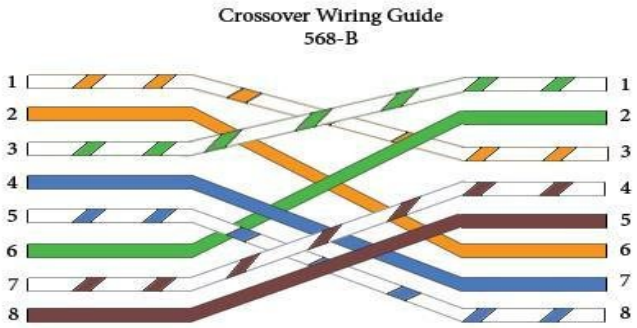
STRAIGHT THROUGH CABLE



White Orange	**White Orange**
Orange	**Orange**
Green White	**Green White**
Blue	**Blue**

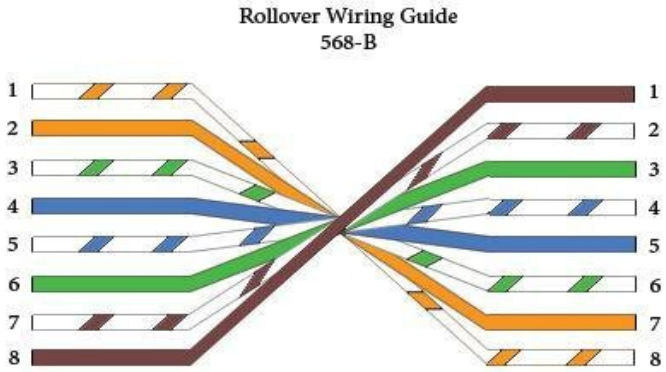
White Blue	**White Blue**
Green	**Green**
White Brown	**White Brown**
Brown	**Brown**

CROSSOVER CABLE

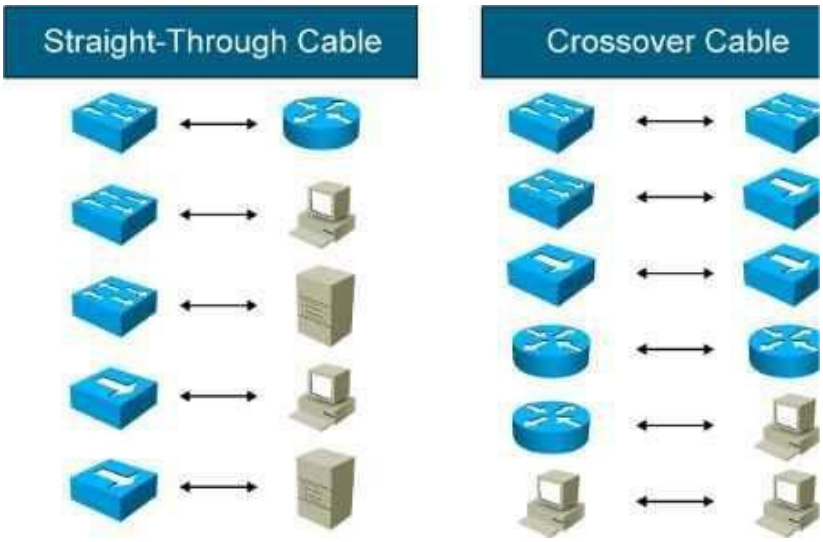


White orange	**White Green**
Orange	**Green**
White Green	**White Orange**
Blue	**Blue**
White Blue	**White Blue**
Green	**Orange**
White Brown	**White Brown**
Brown	**Brown**

ROLLOVER CABLE



- Rollover cables are most commonly used to connect to a devices console port to make programming changes to the device.
- Unlike crossover and straight-wired cables, rollover cables are not intended to carry data but instead create an interface with the device.

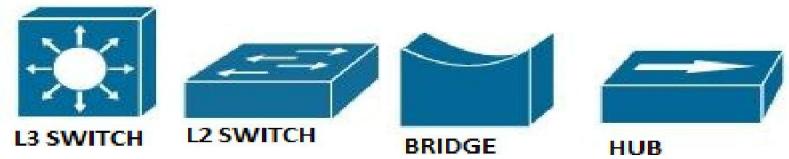


UNICAST • One sender • One receiver •

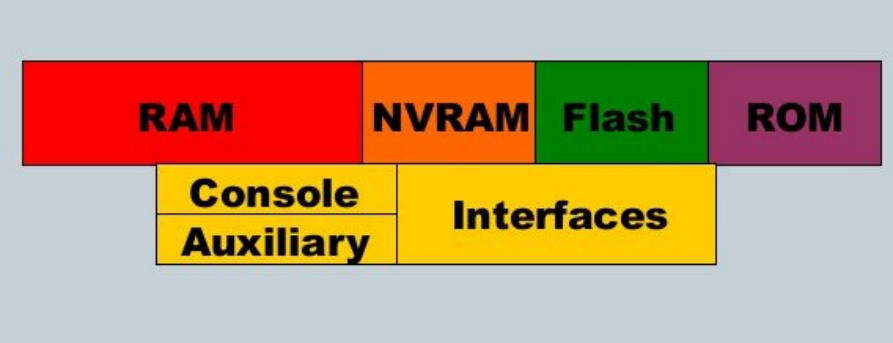
BROADCAST • One sender • All receive

MULTICAST • One sender • N receivers

ANYCAST •One sender • One receiver on a group



INTERNAL COMPONENTS OF ROUTER



RAM : „

- Temporary storage for router config files.
- RAM content is lost on power down „
- It stores routing tables, ARP cache, Fast switching cache, Packet buffering, Packet hold queue.

NVRAM :

- Non-volatile RAM „
- Stores backup/startup configuration files „
- Content is not lost when router is powered down or restarted.

FLASH :

- EEPROM (Electronically Erasable Programmable Read-Only Memory) „
- Holds the Cisco IOS „
- Allows updating of software without replacing the Flash chip „
- Store multiple versions of IOS.

ROM :

- Contains POST (Power on Self Test) „
- A bootstrap program (loads the Cisco IOS)

INTERFACE:

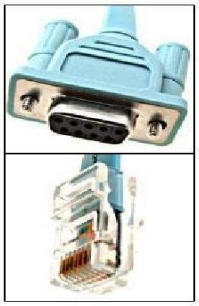
- Network connections through which packets enter and exit the router „
- Attached to the motherboard or as separate modules.

Cisco Catalyst 2950: This is a layer2 switch that does **everything** you need for CCNA.

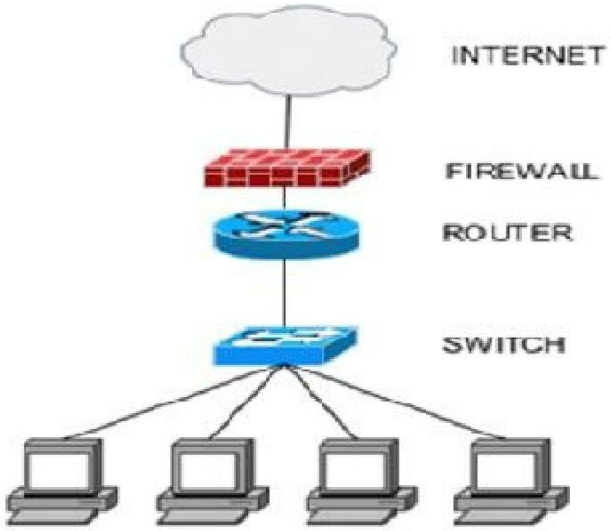
Cisco Catalyst 3550: It offers pretty much the same features as the 2950 but it also supports routing which we require for CCNP

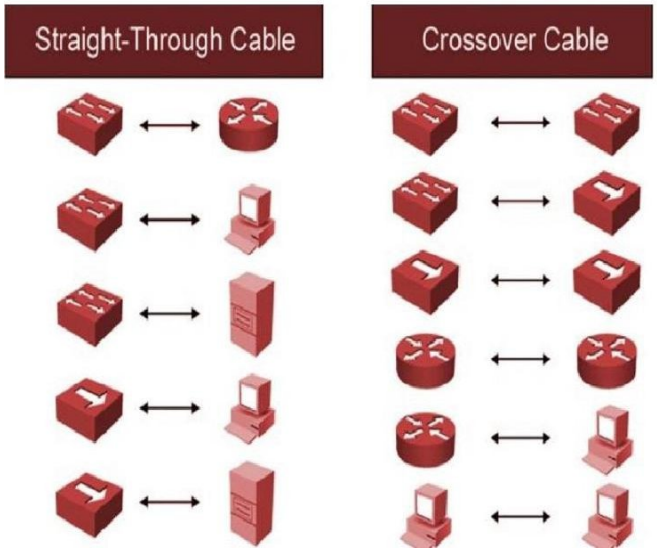
- The Cisco Catalyst 2960 is the successor of the Cisco Catalyst 2950, it's a great Layer 2 switch but more expensive.
- The Cisco Catalyst 3560 is the successor of the Cisco Catalyst 3550, it also offers Routing features but it's quite more expensive…around $300 on eBay.
- The Cisco Catalyst 3750 is also a switch that can do routing but it's very Expensive

Below you see the blue Cisco console cable. It probably comes with the switch but make Sure you have at least one. You'll need this to configure your switches.



- IF your computer doesn't have any serial ports to connect your blue Cisco console cable
- You need to get one of these. It's a USB to serial port converter.





Command Modes

User EXEC : Begin a session with your router.

Router>

Privileged EXEC: Enter the enable command while in user EXEC mode.

Router#

Global configuration: Enter the configure command while in privileged EXEC mode.

Router (config) #

Interface configuration: Enter the interface command (with a specific interface) while in the global configuration mode.

Router (config-if)

Router configuration: Enter your router command, followed by the appropriate keyword, while in global configuration mode.

Router (config-router) #

Line configuration: Specify a line with the line vty command while in the global configuration mode.

Router (config-line) #

Saving Configuration

- You need to enter the copy running-config startup-config command to save your configuration changes to nonvolatile random-access memory (NVRAM) so that they are not lost if there is a system reload or power outage.

Router# copy running-config startup-config

IP ADDRESS

- An IP address is a unique global address for a network interface.
- IP addresses are displayed in dotted decimal notation, and appear as four numbers separated by dots.
- Each number of an IP address is made from eight individual bits known as octet.
- Each octet can create number value from 0 to 255.

- An IP address would be 32 bits long in binary divided into the two components, network component and host component.

IP addresses are broken into the two components:

Network component: - Defines network segment of device.
Host component: - Defines the specific device on a particular network segment

IP Classes in decimal notation

Class A	(1-126)
Class B	(128-191)
Class C	(192-223)
Class D	(224-239)
Class E	(240-254)

- 0 [Zero] is reserved and represents all IP addresses.
- 127 is a reserved address and are used for testing, like a loop back on an interface.
- 255 is a reserved address and are used for broadcasting purposes.

Subnet mask

- Subnet mask is a 32 bits long address used to distinguish between network address and host address in IP address.
- Subnet mask is always used with IP address. Subnet mask has only one purpose, to indentify which part of an IP address is network address and which part is host address.

IP Class	Default Subnet	Network bits	Host bits	Total hosts	Valid hosts
A	255.0.0.0	First 8 bits	Last 24 bits	16, 777, 216	16, 777, 214
B	255.255.0.0	First 16 bits	Last 16 bits	65,536	65,534
C	255.255.255.0	First 24 bits	Last 8 bits	256	254

Private IP Addressing

The Internet Assigned Numbers Authority (IANA) has reserved a number of IPv4 network ranges as private.

10.0.0.0 – 10.255.255.255 (10.0.0.0/8)

172.16.0.0 – 172.31.255.255 (172.16.0.0/12).

192.168.0.0 – 192.168.255.255

SUBNETTING

- Sub netting is a process of dividing large network into the smaller networks based on layer 3 IP address.
- Every computer on network has an IP address that represents its location on network.

Advantage of Sub netting

- Sub netting breaks large network in smaller networks and smaller networks are easier to manage.
- Sub netting reduces network traffic by removing collision and broadcast traffic, that overall improve performance.
- Sub netting allows you to apply network security polices at the interconnection between subnets.
- Sub netting allows you to save money by reducing requirement for IP range.

Base position	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Decimal value	128	64	32	16	8	4	2	1

CIDR	**Decimal**
/25	128
/26	192
/27	224
/28	240
/29	248
/30	252

EXAMPLE: /25

CIDR /25 has subnet mask 255.255.255.128 and 128 is 10000000 in binary. We used one host bit in network address.

N = 1 [Number of host bit used in network]

H = 7 [Remaining host bits]

Total subnets (2^N) :- $2^1 = 2$

Block size (256 - subnet mask) :- 256 - 128 = 128

Valid subnets (Count blocks from 0) :- 0,128

Total hosts (2^H) :- $2^7 = 128$

Valid hosts per subnet (Total host - 2) :- 128 - 2 = 126

Subnets	Subnet 1	Subnet 2
Network ID	0	128
First host	1	129
Last host	126	254
Broadcast ID	127	255

ROUTING

- Routing is the process of moving packets across a network from one host to another.
- It is usually performed by dedicated devices called routers.

TYPES OF ROUTING

- STATIC
- DYNAMIC
- DEFAULT

DYNAMIC ROUTING

Function(s) of Dynamic Routing Protocols

– Dynamically share information between routers.

– Automatically update routing table when topology changes.

– Determine best path to a destination.

The purpose of a dynamic routing protocol is to:

– Discover remote networks

– Maintaining up-to-date routing information

– Choosing the best path to destination networks

– Ability to find a new best path if the current path is no longer available

Advantages of dynamic over static routing

– It can backup multiple interfaces/networks on a router

– Easy to configure

– No extra resources are needed

– More secure

Disadvantages of static routing

– Network changes require manual reconfiguration

– Does not scale well in large topologies.

Dynamic routing protocols are grouped according to characteristics.

Examples include:

– RIP

– EIGRP

– OSPF

Comparison of Distance Vector & Link State Routing Protocols

– Distance vector

• Routes are advertised as vectors of distance & direction.

• Incomplete view of network

• Topology

• Generally, periodic updates.

– Link state

• complete view of network

• Topology is created.

• Updates are not periodic.

STATIC ROUTE

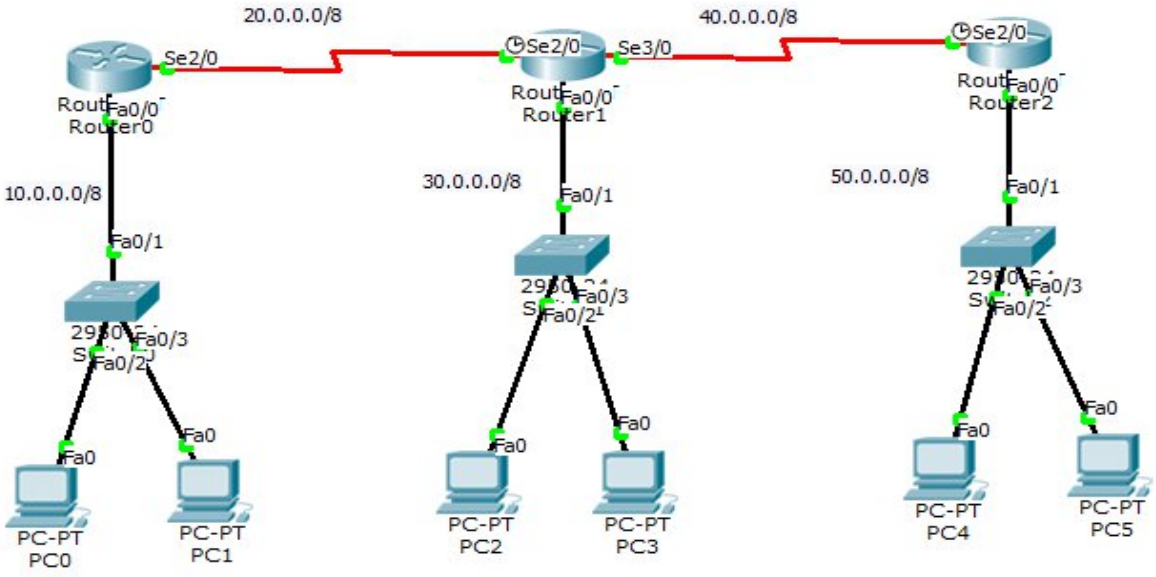
DEFINITION

- Uses a route that a network administrator enters into the router manually.
- Static routes are user-defined route that specify the path that packets moving between source to destination.
- The administrator must manually update his static route entry whenever an internetwork topology changes require an update .

SYNTAX FOR CONFIGURING STATIC ROUTE

The commands to add a static route are as follows:

```
Router> enable
Router# configure terminal
Router (config) # ip route <destination n/w> <subnet mask> <default
gateway>
```



FOR ROUTER 1,

```
Router> enable
Router# configure t
Router(config)# ip route 30.0.0.0 255.0.0.0 20.0.0.2
Router(config)# ip route 40.0.0.0 255.0.0.0 20.0.0.2
Router(config)# ip route 50.0.0.0 255.0.0.0 20.0.0.2
```

FOR ROUTER 2,

```
Router> enable
Router# configure t
Router(config)# ip route 10.0.0.0 255.0.0.0 20.0.0.1
Router(config)# ip route 50.0.0.0 255.0.0.0 40.0.0.2
```

FOR ROUTER 3,

```
Router> enable
Router# configure t
Router(config)# ip route 10.0.0.0 255.0.0.0 40.0.0.1
Router(config)# ip route 20.0.0.0 255.0.0.0 40.0.0.1
Router(config)# ip route 30.0.0.0 255.0.0.0 40.0.0.1
```

OUTPUT

ADVANTAGES

- Static routes are supported on all routing devices and all routers.
- They are easy to predict and understand in small networks.

DISADVANTAGES

- Static routes do not dynamically adapt to network topology changes or equipment failures.
- Static routing does not scale well in large networks.
- Administrator must update all routers.

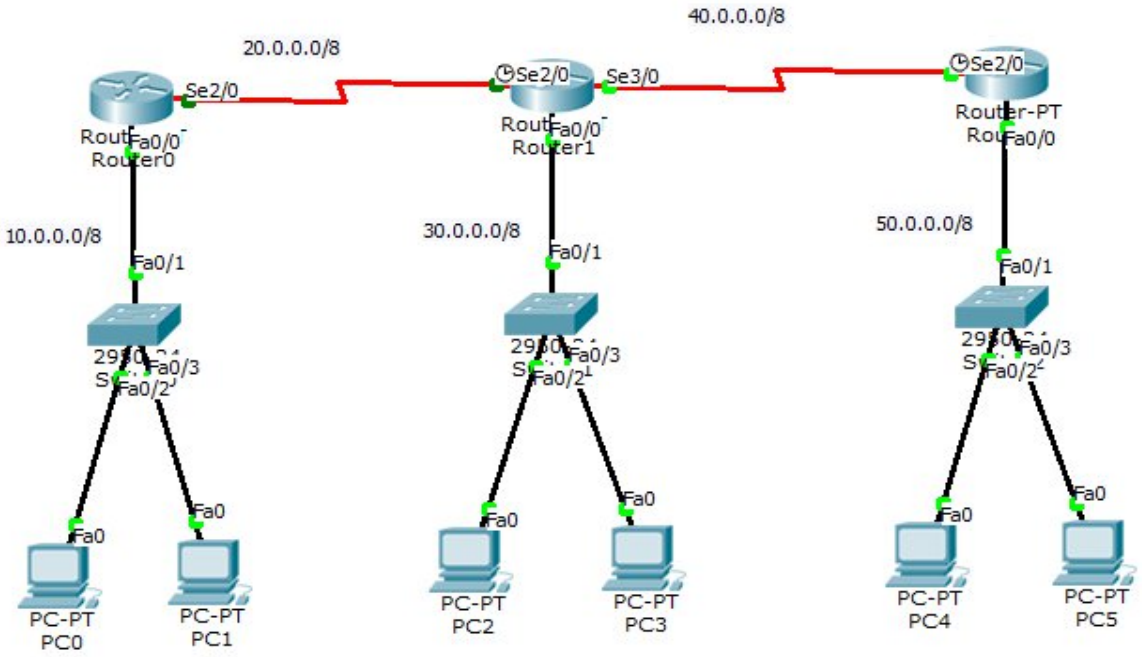
DEFAULT ROUTING

DEFINITION

- A default route allows traffic to be forwarded, even without a specific route to a particular network.
- The default route is identified by all zeros in both the network and subnet mask (0.0.0.0 0.0.0.0).

SYNTAX FOR CONFIGURING DEFAULT ROUTE

```
Router> enable
Router# configure terminal
Router(config)# ip route 0.0.0.0 0.0.0.0 <exit-interface>
```



OUTPUT

```
Router#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

C    10.0.0.0/8 is directly connected, FastEthernet0/0
C    20.0.0.0/8 is directly connected, Serial2/0
S*   0.0.0.0/0 is directly connected, Serial2/0
```

ROUTING INFORMATION PROTOCOL (RIP)

PROPERTIES

- Open standard
- Classful protocol
- It is a distance-vector, interior gateway protocol (IGP) used by routers to exchange routing information.
- RIP uses hop count to determine the best path between two locations.
- Hop count is the number of routers the packet must go through till it reaches the destination network.
- The maximum allowable number of hops a packet can traverse in an IP network implementing RIP is 0-15 hops.
- Its Advertisement Distance is 120.
- It uses Bellman-ford algorithm.

VERSIONS OF RIP

1. RIP V1
    - Classful routing protocol
    - It is a Distance vector routing protocol.
    - It does not support VLSM.
    - It supports maximum metric value of 0- 15.
    - Broadcast ip address 255.255.255.255.
    - It does not support authentication.
    -

2. RIP V2.
    - Classless routing protocol
    - It is a Distance vector routing protocol.
    - It supports VLSM.
    - It support maximum metric value of 0-15.
    - It allows periodic updates.
    - Multicast address: 224.0.0.9.
    - It supports authentication. (Plain text, MD5).

CLASSFUL PROTOCOL :

Routing Protocol that do not send subnet mask information when a route update is sent out. All devices in the network must use the same subnet mask. Classful routing allows FLSM. E.g.: RIP V1

CLASSLESS PROTOCOL:

Routing that sends subnet mask information in the routing updates. Classless routing allows VLSM (Variable Length Subnet Masking) E.g.: RIP V2, EIGRP, & OSPF.

RIP TIMERS

RIP has four basic timers:

- **Update Timer (default 30 seconds**) – indicates how often the router will send out a routing table update.
- **Invalid Timer (default 180 seconds)** – indicates how long a route will remain in a routing table before being marked as invalid, if no new updates are heard about this route.
- **Hold-down Timer (default 180 seconds) -** RIP will not accept any new updates for routes in a hold-down state, until the hold-down timer expires.
- **Flush Timer (default 240 seconds)** – indicates how long a route can remain in a routing table before being flushed, if no new updates are heard about this route.

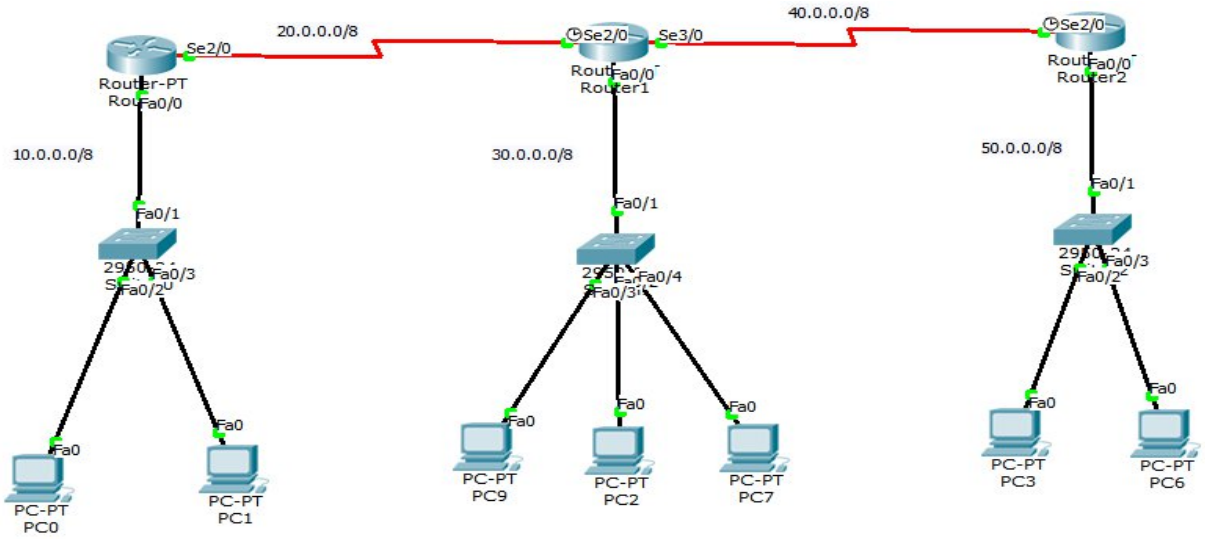
SYNTAX FOR CONFIGURING RIP

RIP V1

```
Router> enable
Router# configure t
Router (config) #routers rip
Router (config) # network <dc> or <known network>
```

RIP V2

```
Router> enable
Router# configure t
Router (config) #routers rip
Router (config) # network <dc> or <known network>
Router (config)# version 2
```



OUTPUT

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, FastEthernet0/0
C    20.0.0.0/8 is directly connected, Serial2/0
R    30.0.0.0/8 [120/1] via 20.0.0.2, 00:00:22, Serial2/0
R    40.0.0.0/8 [120/1] via 20.0.0.2, 00:00:22, Serial2/0
R    50.0.0.0/8 [120/2] via 20.0.0.2, 00:00:22, Serial2/0
Router#
```

ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL (EIGRP)

PROPERTIES

EIGRP is a Cisco-proprietary **Hybrid routing protocol**, incorporating features of both Distance-Vector and Link-State routing protocols.

- EIGRP uses **Diffusing Update Algorithm** (DUAL) to determine the best path among all "feasible" paths.
- EIGRP will form neighbor relationships with adjacent routers in the same Autonomous System (AS).
- EIGRP traffic is either sent as unicasts, or as multicasts on address 224.0.0.10.
- EIGRP is a classless protocol, and thus supports VLSMs.
- Administrative distance= 90.
- It is used for larger networks.
- Fast convergence.
- Auto- summarization.
- It supports Equal / Unequal cost Load balancing
- Protocol number : 88
- Triggered updates
- It supports Authentication (MD5).
- Timer :
    - Hello – 5seconds
    - Hold –down – 15 seconds

EIGRP handles three types of Tables :

- **Neighbor table** – list of all neighboring routers. Neighbors must belong to the same Autonomous System.
- **Topology table** – list of all routes in the Autonomous System.
- **Routing table** – contains the best route for each known network.

EIGRP Packet Types

• **Hello packets** - EIGRP forms neighbor relationships, called adjacencies, with other routers in the same AS by exchanging Hello packets. Only after an adjacency is formed can routers share routing information. EIGRP Hellos are sent **every 5 seconds**.

• **Update packets** – Update packets are sent between neighbors to build the topology and routing tables.

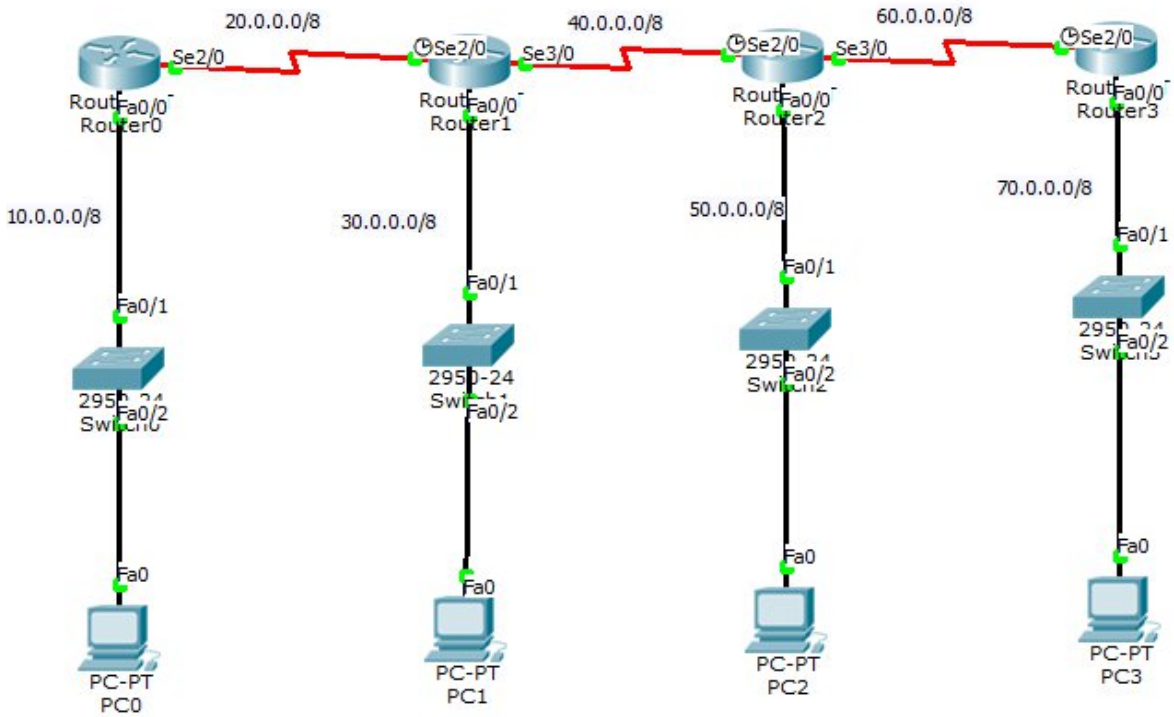
• **Query packets** – Query packets are sent by a router when a Successor route fails, and there are no Feasible Successors in the topology table.

• **Reply packets** – Reply packets are sent in response to Query packets, assuming the responding router has an alternative route.

• **Acknowledgement packets** - Acknowledgment packets (also known as ACK's) are simply Hello packets with no data, other than an acknowledgment number.

SYNTAX FOR CONFIGURING EIGRP

```
Router> enable
Router# configure t
Router(config)# router eigrp <AS NUMBER>
Router(config)# network <dc> or <known network>
```



FOR ROUTER 1,

```
Router> enable
Router# configure t
Router(config)# router eigrp 100
Router(config)# network 10.0.0.0
Router(config)# network 20.0.0.0
```

FOR ROUTER 2,

```
Router> enable
Router# configure t
Router(config)# router eigrp 100
Router(config)# network 20.0.0.0
Router(config)# network 30.0.0.0
Router(config)# network 40.0.0.0
```

FOR ROUTER 3,

```
Router(config)# router eigrp 100
Router(config)# network 40.0.0.0
Router(config)# network 50.0.0.0
Router(config)# network 60.0.0.0
```

FOR ROUTER 4,

```
Router(config)# router eigrp 100
Router(config)# network 60.0.0.0
Router(config)# network 70.0.0.0
```

OUTPUT

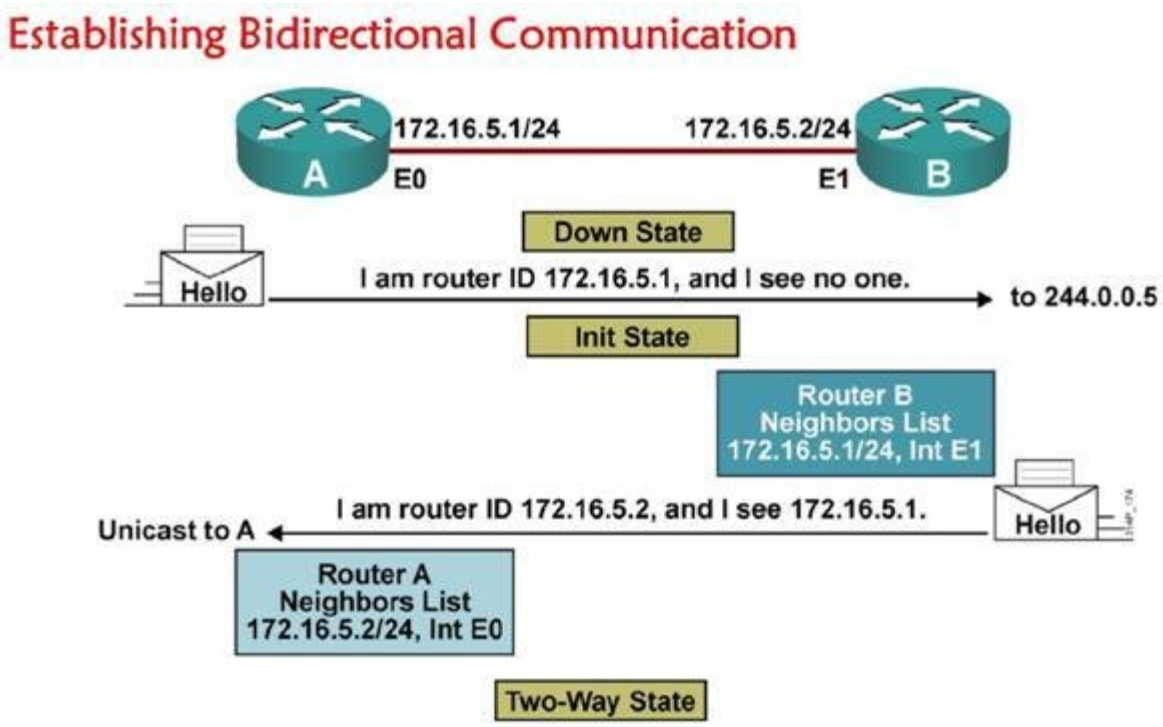
```
Router#SHow IP ROUte
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, FastEthernet0/0
C    20.0.0.0/8 is directly connected, Serial2/0
D    30.0.0.0/8 [90/20514560] via 20.0.0.2, 00:06:02, Serial2/0
D    40.0.0.0/8 [90/21024000] via 20.0.0.2, 00:06:02, Serial2/0
D    50.0.0.0/8 [90/21026560] via 20.0.0.2, 00:06:00, Serial2/0
D    60.0.0.0/8 [90/21536000] via 20.0.0.2, 00:06:00, Serial2/0
D    70.0.0.0/8 [90/21538560] via 20.0.0.2, 00:06:00, Serial2/0
Router#
```

OPEN SHORTEST PATH FIRST (OSPF)

PROPERTIES

OSPF is a standardized Link-State routing protocol, designed to scale efficiently to support larger networks.

- Open Standard
- It uses the SPF (shortest path first) algorithm, developed by Dijkstra, to provide a loop-free topology.
- Fast convergence.
- It supports Equal cost load balancing.
- Administrative distance= 110
- Protocol number = 89
- Classless protocol
- It supports authentication (plain text, MD5).
- OSPF traffic is multicast either to address 224.0.0.5 or 224.0.0.6.
- OSPF employs a hierarchical network design using Areas.
- OSPF will form neighbor relationships with adjacent routers in the same Area.
- OSPF supports only IP routing.



OSPF PACKETS

- HELLO : Discover neighbors and builds adjacency
- DBD : Checks for database synchronization between routers
- LSR : Requests specific link state records from router to router
- LSU : Sends specifically requested link state records
- LSACK : Acknowledges other packet types

OSPF ROUTER STATES:

- Down
- Init
- Two way
- Ex-start
- Exchange
- Loading
- Full

OSPF TIMER

- **Hello interval (10 sec):** This defines how often we send the hello packet.
- **Dead interval (40 sec):** This defines how long we should wait for hello packets before we declare the neighbor dead.

OSPF maintains three separate tables:

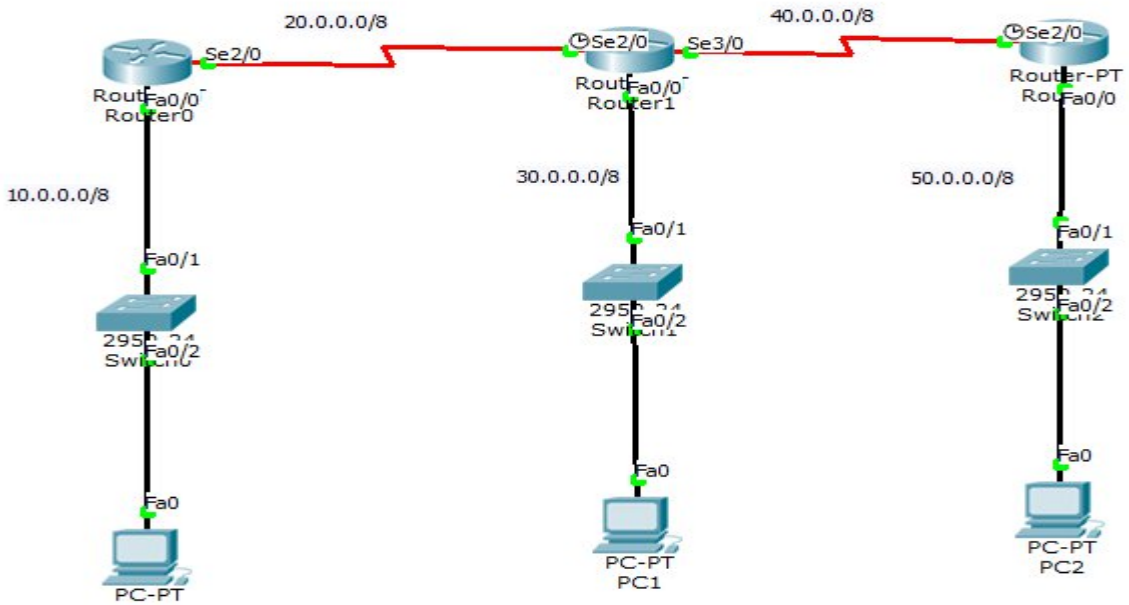
• **A neighbor table** – contains a list of all neighboring routers.

• **A topology table** – contains a list of all possible routes to all known networks within an area.

• **A routing table** – contains the best route for each known network.

SYNTAX FOR CONFIGURING OSPF

```
Router> enable
Router# configure t
Router (config) # router ospf <process id >
Router (config) # network <known port > < wildcard mask> <area id >
```



OUTPUT

```
Router#SHow ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, FastEthernet0/0
C    20.0.0.0/8 is directly connected, Serial2/0
O    30.0.0.0/8 [110/65] via 20.0.0.2, 00:10:42, Serial2/0
O    40.0.0.0/8 [110/128] via 20.0.0.2, 00:10:42, Serial2/0
O    50.0.0.0/8 [110/129] via 20.0.0.2, 00:10:42, Serial2/0
Router#
```

ADMINISTRATIVE DISTANCE

- Administrative Distance (AD) is a value that routers use in order to select the best path when there are two or more different routes to the same destination from two different routing protocols.
- Administrative Distance (AD) is a numeric value which can range from 0 to 255.

CONNECTED	0
STATIC	1
RIP	120
EIGRP	90
OSPF	110
EXTERNAL EIGRP	170

INTERNET OPERATING SYSTEM BACKUP (IOS)

PROPERTIES

- Cisco IOS is stored in flash memory of device.
- Data stored in Flash memory remains safe even in powered off stage.
- IOS is the most critical part of any Cisco device.
- You should always take Backup of IOS to deal with any unwanted situations.

How to take backup of Cisco IOS

You can use any supporting file transfer protocol for backup such as FTP, TFTP .

TFTP Protocol

- TFTP is the most lightweight authentication less protocol.
- It does not implement any security measurements such as login or access control mechanism.
- TFTP can only read and write files from TFTP server. It cannot list, delete or rename files or directories
- TFTP is originally designed for LAN (Local Area Network).
- TFTP use UDP as transport protocol.
- Transfer request is always initiated on port 69.

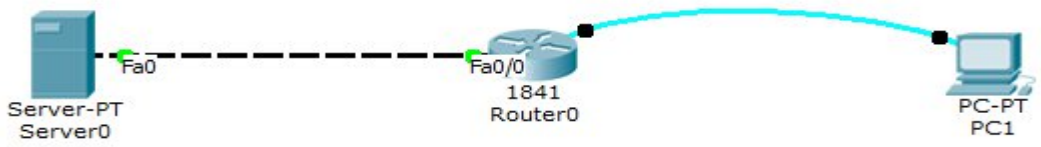
BACKUP :

Step 1 : Open Packet Tracer and click **End devices**. From End devices drag and drop **Server** and **PC-PT** in workspace.

Step 2: Click **Router**. From available Routers drag and drop a 1841 series router in workspace.

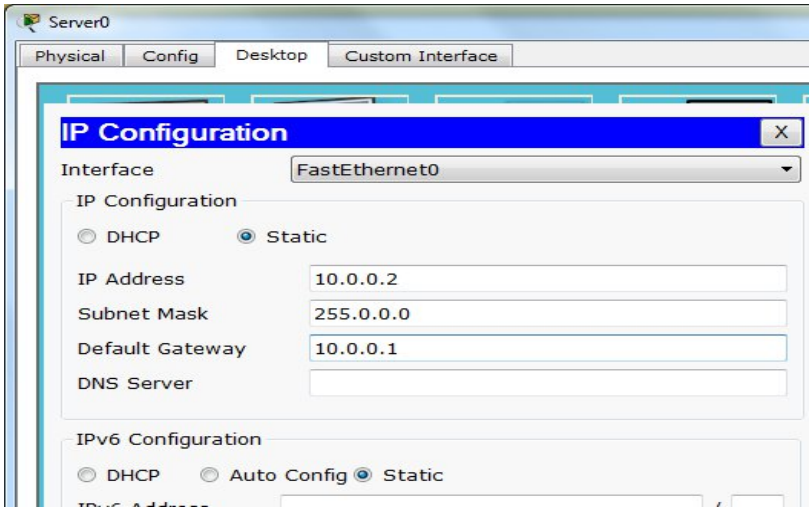
Step 3: Click **Connections**. Connect Server's Fast Ethernet 0 with Router's FastEthernet0/0 via cross cable and Router's console with PC-PT's RS232 via console cable.

Step 4: Configure Router's interface FastEthernet0/0 with IP address 10.0.0.1.

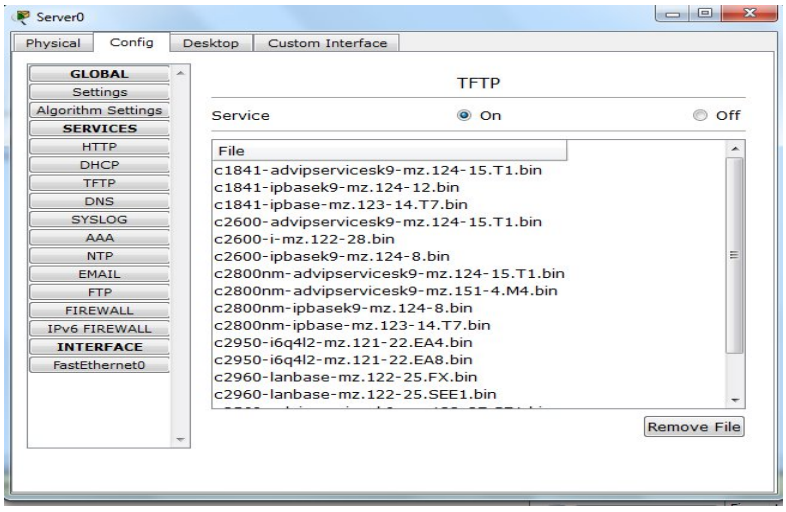



```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/0        10.0.0.1        YES manual up                    up

FastEthernet0/1        unassigned      YES unset  administratively down down

Vlan1                  unassigned      YES unset  administratively down down
Router#
```

Step 5: Configure IP address on Server



Step 6: By default TFTP service is running on Server. To verify it click on Config menu tab and expend the Services left menu item.



Step 7: Click **PC-PT** and click **Desktop** menu and click **Terminal** and accept default Settings. Now we are connected with Router.

Step 8: We need to supply the name of IOS that you can find with **show flash** command.

```
Router#show flash:

System flash directory:
File  Length   Name/status
  3   33591768 c1841-advipservicesk9-mz.124-15.T1.bin
  2   28282    sigdef-category.xml
  1   227537   sigdef-default.xml
[33847587 bytes used, 30168797 available, 64016384 total]
63488K bytes of processor board System flash (Read/Write)
```

- **Copy flash tftp** command is used to copy IOS from Flash to TFTP server. It takes three parameters.
    - **Source filename**: **-** Name of IOS files that need to be copied.
    - **Address or name of remote host**: **-** IP address of TFTP Server.
    - **Destination filename**: **-** Name of file used at destination to store the source file.

```
Router#copy flash: tftp
Source filename []? c1841-advipservicesk9-mz.124-15.T1.bin
Address or name of remote host []? 10.0.0.2
Destination filename [c1841-advipservicesk9-mz.124-15.T1.bin]?

Writing c1841-advipservicesk9-mz.124-15.T1.bin....!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 33591768 bytes]

33591768 bytes copied in 3.685 secs (9115000 bytes/sec)
Router#
```

Step 9: We have successfully taken the backup of IOS on TFTP Server.

DELETE

Step 1: From privileged mode use **delete** command to delete IOS file from flash.

Step 2: Press Enter when asked to confirm the delete operation.

Step 3: During the boot process router copy and decompress the IOS file in RAM. Router will work as it is until we reload it. Enter **reload** command in privileged mode to reload the router.

```
Router#delete flash:c1841-advipservicesk9-mz.124-15.T1.bin
Delete filename [c1841-advipservicesk9-mz.124-15.T1.bin]?
Delete flash:/c1841-advipservicesk9-mz.124-15.T1.bin? [confirm]

Router#sh
Router#show fl
Router#show flash:

System flash directory:
File  Length   Name/status
  2   28282    sigdef-category.xml
  1   227537   sigdef-default.xml
[255819 bytes used, 63760565 available, 64016384 total]
63488K bytes of processor board System flash (Read/Write)
```

Step 4: As expected Router entered in ROMMON mode. ROMMON mode is used for disaster recovery.

```
Router#reload
Proceed with reload? [confirm]
System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)
Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.

Boot process failed...

The system is unable to boot automatically.  The BOOT
environment variable needs to be set to a bootable
image.
rommon 1 >
```

How to restore IOS from ROMMON mode

- ROMMON Mode allows us to restore IOS from TFTP Server in Flash.
- ROMMON mode has only couple of commands to work with.
- You can list all available commands by entering?

```
rommon 1 >
rommon 1 > ?
boot                boot up an external process
confreg             configuration register utility
dir                 list files in file system
help                monitor builtin command help
reset               system reset
set                 display the monitor variables
tftpdnld            tftp image download
unset               unset a monitor variable
rommon 2 >
```

- **tftpdnld** command needs following variable to be set, before it can download the file.

```
usage: tftpdnld
  Use this command for disaster recovery only to recover an image via TFTP.
  Monitor variables are used to set up parameters for the transfer.
  (Syntax: "VARIABLE_NAME=value" and use "set" to show current variables.)
  "ctrl-c" or "break" stops the transfer before flash erase begins.

  The following variables are REQUIRED to be set for tftpdnld:
           IP_ADDRESS: The IP address for this unit
        IP_SUBNET_MASK: The subnet mask for this unit
       DEFAULT_GATEWAY: The default gateway for this unit
           TFTP_SERVER: The IP address of the server to fetch from
             TFTP_FILE: The filename to fetch

  The following variables are OPTIONAL:
          TFTP_VERBOSE: Print setting. 0=quiet, 1=progress(default), 2=verbose
      TFTP_RETRY_COUNT: Retry count for ARP and TFTP (default=7)
          TFTP_TIMEOUT: Overall timeout of operation in seconds (default=7200)
         TFTP_CHECKSUM: Perform checksum test on image, 0=no, 1=yes (default=1)
         FE_SPEED_MODE: 0=10/hdx, 1=10/fdx, 2=100/hdx, 3=100/fdx, 4=Auto(deflt)
```

- **IP_ADDRESS**:- Temporary IP address assigned to the router.
- **IP_SUBNET_MASK**:- Must match with the subnet of TFTP Server.
- **DEFAULT_GATEWAY**:- For this process it would be IP Address of TFTP Server.
- **TFTP_SERVER**:- IP address of TFTP Server.
- **TFTP_FILE**:- Exact name of IOS file. Name is case sensitive.
- **TFTP_CHECKSUM**:- This prevents checksum errors with earlier version of boot ROMs.

```
rommon 3 > IP_ADDRESS=10.0.0.10
rommon 4 > IP_SUBNET_MASK=255.0.0.0
rommon 5 > DEFAULT_GATEWAY=10.0.0.2
rommon 6 > TFTP_SERVER=10.0.0.2
rommon 7 > TFTP_FILE=c1841-advipservicesk9-mz.124-15.T1.bin
rommon 8 > TFTP_CHECKSUM=0
rommon 9 > tftpdnld

           IP_ADDRESS: 10.0.0.10
        IP_SUBNET_MASK: 255.0.0.0
       DEFAULT_GATEWAY: 10.0.0.2
           TFTP_SERVER: 10.0.0.2
             TFTP_FILE: c1841-advipservicesk9-mz.124-15.T1.bin
Invoke this command for disaster recovery only.
WARNING: all existing data in all partitions on flash will be lost!

Do you wish to continue? y/n:  [n]:  y
```

RESET:

```
program flash location 0x61fb0000
program flash location 0x61fc0000
program flash location 0x61fd0000
program flash location 0x61fe0000
program flash location 0x61ff0000
program flash location 0x62000000

rommon 10 > reset
System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)
Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.

Self decompressing the image :
##################################
```

PASSWORD SETTING AND BREAKING .

Protecting Passwords with Enable Password and Enable Secret

- To provide an additional layer of security, particularly for passwords that cross the network or are stored
  on a TFTP server, you can use either the **enable password** or **enable secret** commands.
- We recommend that you use the **enable secret** command because it uses an improved encryption algorithm.
- Use the **enable password** command only if you boot an older image of the Cisco IOS software.

Router(config)# **enable password**

- Establishes a password for a privilege command mode.

Router(config)# **enable secret**

- Specifies a secret password, saved using a non-reversible encryption method. (If enable password and enable secret are both set, users must enter the enable secret password.)

Setting or Changing a Line Password

Router(config)# line console 0

Router (config-line)# password Cisco

Router (config-line)# login

Router (config-line)#exit

- Establishes a new password or change an existing password for the privileged command level.

TELNET PASSWORD

Router(config)# line vty 0 4

Router (config-line)# password Cisco

Router (config-line)# login

Router (config-line)#exit

Encrypting Passwords

- Encryption prevents the password from being readable in the configuration file.

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

- The **service password-encryption** command is primarily useful for keeping unauthorized individuals from viewing your password in your configuration file.

PASSWORD BREAKING OR RECOVERY

Step 1:- Restart the router by pressing the power button on and off

```
System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
cisco 2811 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory
Self decompressing the image :
#################################
```

Step 2:- Before the self decompressing you should press Ctrl + break (pause break), a new option will be opened as shown below

```
System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
cisco 2811 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory
Self decompressing the image :
########################
monitor: command "boot" aborted due to user interrupt
rommon 1 >
```

Step 3:- Now we are at Rom mode as it shows rom prompt in the screen.

```
rommon 1 > confreg 0x2142
rommon 2 > reset
System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
cisco 2811 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory
Self decompressing the image :
################################
```

Step 4:- The router will restart automatically once again and will ask Continue with configuration dialog? [Yes/no]: no and press enter

```
Continue with configuration dialog? [yes/no]: no
Press RETURN to get started!
Router>
```

Step 5:- Enter into privilege mode and copy the start up configuration

Step 6:- At Present you haven't saved the settings before restart make it all into default

```
Router(config)# config-register 0x2102
Router(config)# exit
Router# copy running-config startup-config
Destination filename [startup-config]?
Building configuration…
[OK]
Router# reload
```

ACCESS CONTROL LISTS (ACL)

- Access control lists (ACLs) can be used for two purposes on Cisco devices:
  - To filter traffic
  - To identify traffic
- Access lists are a set of rules or commands.
- Each rule or line in an access-list provides a condition, either permit or deny.

Types of Access Lists

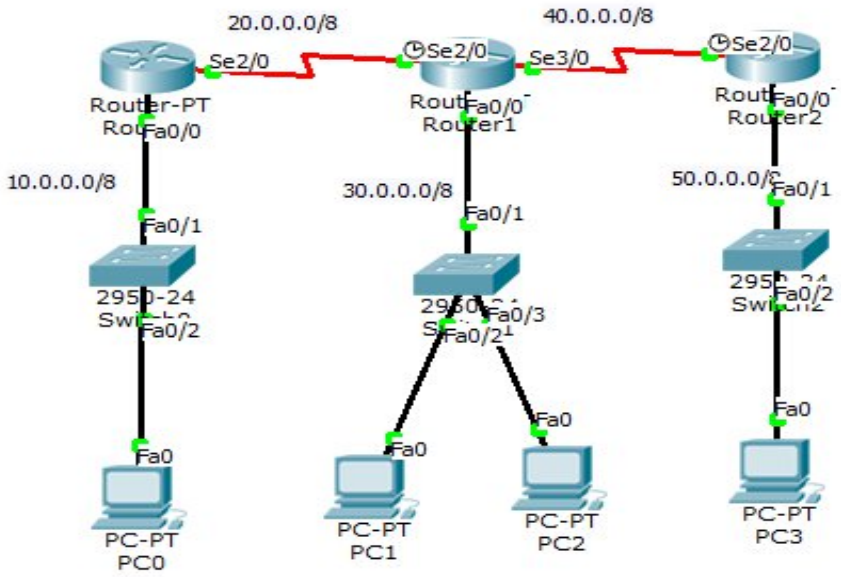
- Standard IP ACL
- Extended IP ACL

- **Standard** – Permits or denies packets based on source IP address. Valid standard ACL IDs are 1 – 99 or a string.

- **Extended –** Permits or denies packets based on source and destination IP address. Valid extended ACL IDs are a number from 100 – 199 or a string.

Standard IP Access List

Standard IP access-lists are based upon the source host or network IP address, and should be placed closest to the destination network.



PARTICULAR PC

access-list [1-99] [permit | deny] host [source address]

In order to block particular host 30.0.0.2 from accessing the 50.0.0.0 network, we would create the following access-list on Router. (Destination router)

```
Router(config)#access-list 20 deny host 30.0.0.2
Router(config)#access-list 20 permit any
Router(config)#int f0/0
Router(config-if)#ip access-group 20 out
Router(config-if)#
```

To view all IP access lists configured on the router

Router# show ip access-list

PARTICULAR NETWORK

access-list [1-99] [permit | deny] host [source address] [wildcard mask]

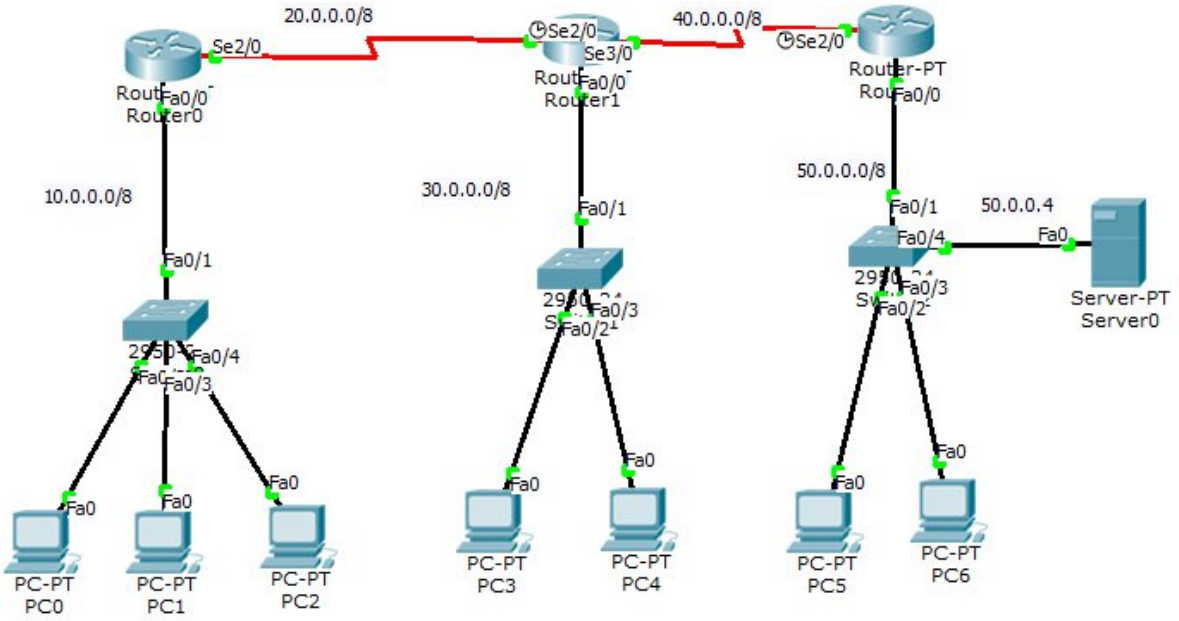
In order to block particular network 30.0.0.0 from accessing the 50.0.0.0 network, we would create the following access-list on Router. (Destination router)

```
Router(config-if)#access-list 10 deny 30.0.0.0 0.255.255.255
Router(config)#access-list 10 permit any
Router(config)#int f0/0
Router(config-if)#ip access-group 10 out
```

EXTENDED IP ACCESS LIST

- Extended IP access-lists block based upon the source IP address, destination IP address, and TCP or UDP port number.
- Extended access-lists should be placed closest to the source network.

access-list [100-199] [permit | deny] [protocol] [source address] [destination address] [port no]




```
Router(config-if)#access-list 110 deny tcp host 10.0.0.2 host 50.0.0.4 eq 80 est
ablished
Router(config)#access-list 110 permit ip any any
Router(config)#int f0/0
Router(config-if)#ip access-group 110 in
Router(config-if)#
```

NETWORK ADDRESS TRANSLATION (NAT)

Private Network

- Private IP network is an IP network that is not directly connected to the Internet.
- Generally, private networks use addresses from the following experimental address ranges (non-routable addresses):

    - 10.0.0.0 – 10.255.255.255
    - 172.16.0.0 – 172.31.255.255
    - 192.168.0.0 – 192.168.255.255

DEFINITION

- A **public address** can be routed on the Internet. Thus, devices that must be Internet-accessible must be configured with (or reachable by) public addresses.

- A **private address** is intended for internal use within a home or organization, and can be freely used by anyone. However, private addresses can never be routed on the Internet.

NAT allows a host configured with a private address to be stamped with a public address, thus allowing that host to communicate across the Internet.

Types of NAT

NAT can be implemented using one of three methods:

Static NAT – performs a static one-to-one translation between two addresses, or between a port on one address to a port on another address.

Dynamic NAT – utilizes a pool of global addresses to dynamically translate the outbound traffic of clients behind a NAT-enabled device.

NAT Overload or Port Address Translation (PAT) – translates the outbound traffic of clients to unique port numbers off of a single global address.

NAT Terminology

Specific terms are used to identify the various NAT addresses:

• **Inside Local** – the specific IP address assigned to an inside host behind a NAT-enabled device (usually a private address).

• **Inside Global** – the address that identifies an inside host to the outside world (usually a public address). Essentially, this is the dynamically or statically-assigned public address assigned to a private host.

• **Outside Global** – the address assigned to an outside host (usually a public address).

• **Outside Local** – the address that identifies an outside host to the inside network.

SYNTAX FOR CONFIGURING STATIC NAT

The first step to configure Static NAT is to identify the inside (usually private) and outside (usually public) interfaces:

Router (config)# int e0/0

Router (config-if)# ip nat inside

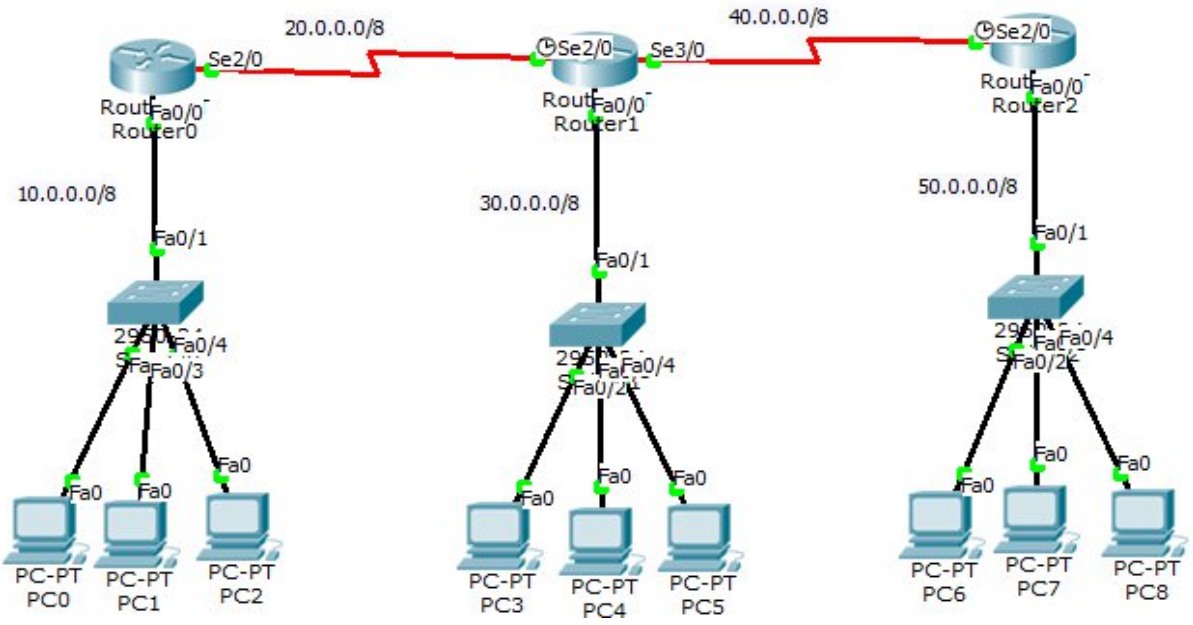
Router(config)# int s0/0

Router(config-if)# ip nat outside

To statically map a public address to a private address, the syntax is as follows:

Router (config)# ip nat inside source static <private address><global public address>

This command performs a static translation of the source address 172.16.1.1 (located on the inside of the network), to the outside address of 158.80.1.40.



OUTPUT

```
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 200.200.200.1:1   10.0.0.2:1         50.0.0.4:1         50.0.0.4:1
icmp 200.200.200.1:2   10.0.0.2:2         30.0.0.3:2         30.0.0.3:2
icmp 200.200.200.1:2   10.0.0.2:2         30.0.0.4:2         30.0.0.4:2
---  200.200.200.1     10.0.0.2           ---                ---
```

SYNTAX FOR CONFIGURING DYNAMIC NAT

When configuring Dynamic NAT, the inside and outside interfaces must first be identified:

Router (config)# int e0/0

Router (config-if)# ip nat inside

Router (config)# int s0/0

Router (config-if)# ip nat outside

Router (config)# access-list <1-99> permit <private address> <wildcard mask>

Router (config)# ip nat pool <name> <beginning ip address><ending ip address> netmask

Router (config) # ip nat inside source list <1-99> pool <name>

OUTPUT

```
Router#
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 20.0.0.1:3        10.0.0.2:3         50.0.0.2:3         50.0.0.2:3
icmp 20.0.0.1:4        10.0.0.2:4         30.0.0.2:4         30.0.0.2:4
icmp 20.0.0.1:5        10.0.0.2:5         30.0.0.2:5         30.0.0.2:5
icmp 20.0.0.1:6        10.0.0.2:6         30.0.0.2:6         30.0.0.2:6
icmp 20.0.0.2:3        10.0.0.3:3         50.0.0.3:3         50.0.0.3:3
icmp 20.0.0.2:4        10.0.0.3:4         30.0.0.2:4         30.0.0.2:4
icmp 20.0.0.2:5        10.0.0.3:5         30.0.0.2:5         30.0.0.2:5
icmp 20.0.0.3:10       10.0.0.4:10        50.0.0.3:10        50.0.0.3:10
icmp 20.0.0.3:13       10.0.0.4:13        50.0.0.3:13        50.0.0.3:13
icmp 20.0.0.3:3        10.0.0.4:3         30.0.0.2:3         30.0.0.2:3
icmp 20.0.0.3:4        10.0.0.4:4         30.0.0.3:4         30.0.0.3:4
icmp 20.0.0.3:8        10.0.0.4:8         50.0.0.4:8         50.0.0.4:8
```

SYNTAX FOR CONFIGURING NAT OVERLOAD

Router (config)# int e0/0

Router (config-if)# ip nat inside

Router (config)# int s0/0

Router (config-if)# ip nat outside

Router (config)# access-list <1-99> permit <private address> <wildcard mask>

Router (config)# ip nat pool <name> <beginning ip address><ending ip address> netmask

Router (config) # ip nat inside source list <1-99> pool <name> overload.

OUTPUT

```
Router#
Router#
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 20.0.0.3:16       10.0.0.2:16        50.0.0.3:16        50.0.0.3:16
icmp 20.0.0.3:17       10.0.0.2:17        50.0.0.3:17        50.0.0.3:17
icmp 20.0.0.3:7        10.0.0.2:7         50.0.0.2:7         50.0.0.2:7
icmp 20.0.0.3:8        10.0.0.2:8         30.0.0.2:8         30.0.0.2:8
icmp 20.0.0.3:9        10.0.0.2:9         30.0.0.3:9         30.0.0.3:9
icmp 20.0.0.3:15       10.0.0.3:15        50.0.0.3:15        50.0.0.3:15
icmp 20.0.0.3:10       10.0.0.4:10        50.0.0.4:10        50.0.0.4:10
icmp 20.0.0.3:11       10.0.0.4:11        50.0.0.4:11        50.0.0.4:11
icmp 20.0.0.3:12       10.0.0.4:12        50.0.0.4:12        50.0.0.4:12
icmp 20.0.0.3:3        10.0.0.4:3         30.0.0.2:3         30.0.0.2:3
icmp 20.0.0.3:5        10.0.0.4:5         30.0.0.2:5         30.0.0.2:5
```

DESIGNATED ROUTER (DR) AND BACKUP DESIGNATED ROUTER (BDR)

- If a link off of Router (10.0.0.0) were to fail, it would flood this information to all neighbors.
- Each neighbor, in turn, would then flood that same information to all other neighbors.
- This is a waste of bandwidth and processor load.
- To prevent this, OSPF will elect a Designated Router (DR) for each multi-access networks, accessed via multicast address 224.0.0.6.
- For redundancy purposes, a Backup Designated Router (BDR) is also elected.
- OSPF routers will form adjacencies with the DR and BDR.
- If a change occurs to a link, the update is forwarded only to the DR, which then forwards it to all other routers.

OSPF ELECTION PROCESS

STEP 1: Router with highest priority becomes the DR. By default, the entire routers have priority of 1.

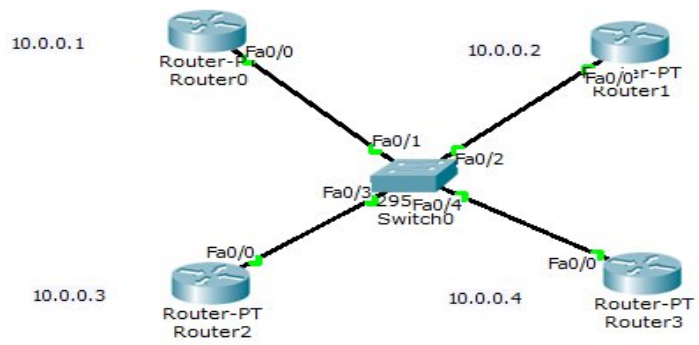
STEP 2: It there is a tie, router will consider the highest router –id (not ip address) becomes the DR.

STEP 3: Highest loopback

STEP 4: Highest physical address

- If DR fails or shutdown, then BDR becomes the DR and new BDR is elected.
- If priority is 0, it will never become DR or BDR.

HIGHEST PHYSICAL ADDRESS

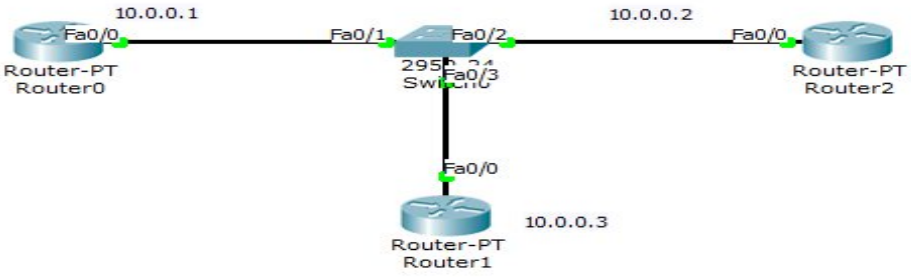


Router> enable
Router# configure t
Router(config)# router ospf <process id >
Router(config)# network <dc> or <known port > < wildcard mask> <area id >

OUTPUT

```
Router#show ip ospf nei
Router#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.0.0.3          1   FULL/BDR        00:00:34    10.0.0.3        FastEthernet0/
0
10.0.0.2          1   2WAY/DROTHER    00:00:35    10.0.0.2        FastEthernet0/
0
10.0.0.4          1   FULL/DR         00:00:31    10.0.0.4        FastEthernet0/
0
```

HIGHEST PRIORITY

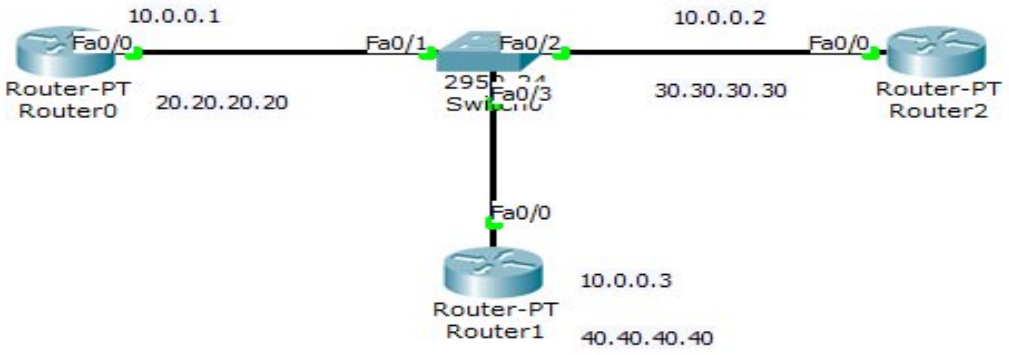


```
Router> enable
Router# configure t
Router(config)# int f0/0
Router(config)#ip ospf priority <1-255>
```

OUTPUT

```
Router#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.0.0.2        200   FULL/DR         00:00:37    10.0.0.2        FastEthernet0/
0
10.0.0.1        100   FULL/BDR        00:00:39    10.0.0.1        FastEthernet0/
0
```

HIGHEST ROUTER –ID

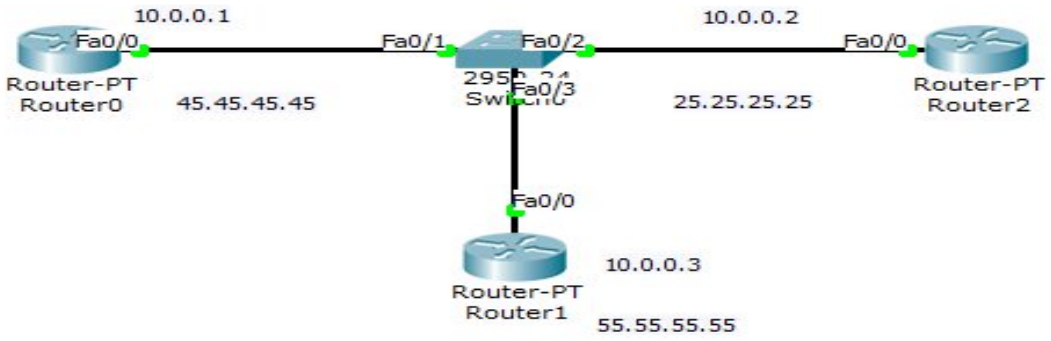


Router# configure t
Router(config)# router ospf <process-id>
Router(config)#router –id <A.B.C.D>

OUTPUT

```
Router#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
40.40.40.40       1   FULL/DR         00:00:31    10.0.0.3        FastEthernet0/
0
30.30.30.30       1   FULL/BDR        00:00:33    10.0.0.2        FastEthernet0/
0
```

HIGHEST LOOPBACK ADDRESS




```
Router(config)# int LO 1
Router(config)# ip address 45.45.45.45 <subnet mask>
Router(config-if) # exit
Router(config)# router ospf <process-id>
Router(config)# network <dc> 0.0.0.0 area 0
```

OUTPUT

```
Router#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
55.55.55.55       1   FULL/DR         00:00:37    10.0.0.3        FastEthernet0/
0
25.25.25.25       1   FULL/BDR        00:00:39    10.0.0.2        FastEthernet0/
0
```

TROUBLE SHOOTING COMMANDS

- Show ip ospf neighbor
- Clear ip ospf process.

SWITCHING

ETHERCHANNEL

- A network will often span across multiple switches.
- Trunk ports are usually used to connect switches together.

There are two issues with using only a single physical port for the trunk connection:

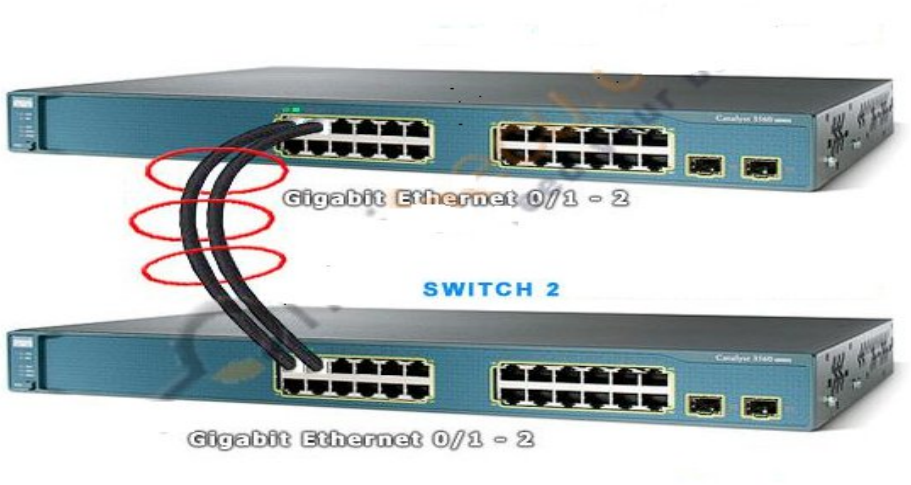
- The port represents a single point of failure. If the port goes down, the trunk connection is lost.
- The port represents a traffic bottleneck.

It allows groping of several physical Ethernet links to create one logical Ethernet links for the purpose of fault-tolerance.

- PaGP (Port aggregation protocol)
- LACP (Link aggregation control protocol)
- Cisco's implementation of port aggregation is called Ether Channel.
- Ether Channel supports Fast, Gigabit, and 10 Gigabit Ethernet ports.

A maximum of 8 active ports are supported in a single Ether Channel.

- Fast Ethernet – 1600 Mbps
- Gigabit Ethernet – 16 Gbps
- 10 Gigabit Ethernet – 160 Gbps



Ether Channel – Manual Configuration

There are two methods of configuring an Ether Channel:

- Manually
- Dynamically, using an aggregation protocol.

To manually configure two ports to join an Ether Channel:

Switch (config) # interface range gi2/23 – 24
Switch (config-if) # channel-group 1 mode desirable
Switch (config-if) # channel protocol pagp

- The channel-group number identifies the Ether Channel on the local switch.
- This number does not need to match on both switches.

Ether Channel – Dynamic Configuration

Cisco switches support two dynamic aggregation protocols:

• PAgP (Port Aggregation Protocol) – Cisco proprietary aggregating protocol.

• LACP (Link Aggregation Control Protocol) – IEEE standardized aggregation protocol.

Ether Channel - PAgP

PAgP is a Cisco-proprietary aggregation protocol, and supports two modes:

• Desirable – actively attempts to form a channel

• Auto – waits for the remote switch to initiate the channel.

A PAgP channel will form in the following configurations:

	DESIRABLE	AUTO
DESIRABLE	YES	YES
AUTO	YES	NO

- A channel will not form if both sides are set to auto.

To create an Ether Channel using PAgP negotiation:

Switch (config) # interface range gi2/23 – 24
Switch (config-if) # channel-protocol pagp
Switch (config-if) # channel-group 1 mode desirable

```
Switch#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

1      Po1(SU)           PAgP   Fa0/1(P) Fa0/2(D) Fa0/3(D) Fa0/4(D)
Switch#
```

Ether Channel – LACP

LACP is an IEEE standard aggregation protocol, and supports two modes:

• Active – actively attempts to form a channel

• Passive – waits for the remote switch to initiate the channel.

	ACTIVE	PASSIVE
ACTIVE	YES	YES
PASSIVE	YES	NO

To create an Ether Channel using LACP negotiation:

Switch (config) # interface range gi2/23 – 24
Switch (config-if) # channel-protocol lacp
Switch (config-if) # channel-group 1 mode active

```
Switch#SHow ETHERchannel SUMMary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

2      Po2(SU)           LACP   Fa0/1(P) Fa0/2(D) Fa0/3(D) Fa0/4(D) Fa0/5(D) Fa0
/6(D) Fa0/7(D) Fa0/8(D)
```

Troubleshooting

To view status information on all configured Ether Channels:

Switch# show ether channel summary.

SPANNING TREE PROTOCOL

Switching Loops

- When a switching loop is introduced into the network, a destructive broadcast storm will develop within second.
- A storm occurs when broadcasts are endlessly forwarded through the loop.

PROPERTIES

Spanning Tree Protocol (STP) was developed to prevent the broadcast storms caused by switching loops.

STP was originally defined in IEEE 802.1D.

STP will identify if there are any loops, and then disable or block as many ports as necessary to eliminate all loops in the topology.

STP switches exchange Bridge Protocol Data Units (BPDU's) to build the topology database.

BPDU's are forwarded out all ports every two second.

Building the STP topology:

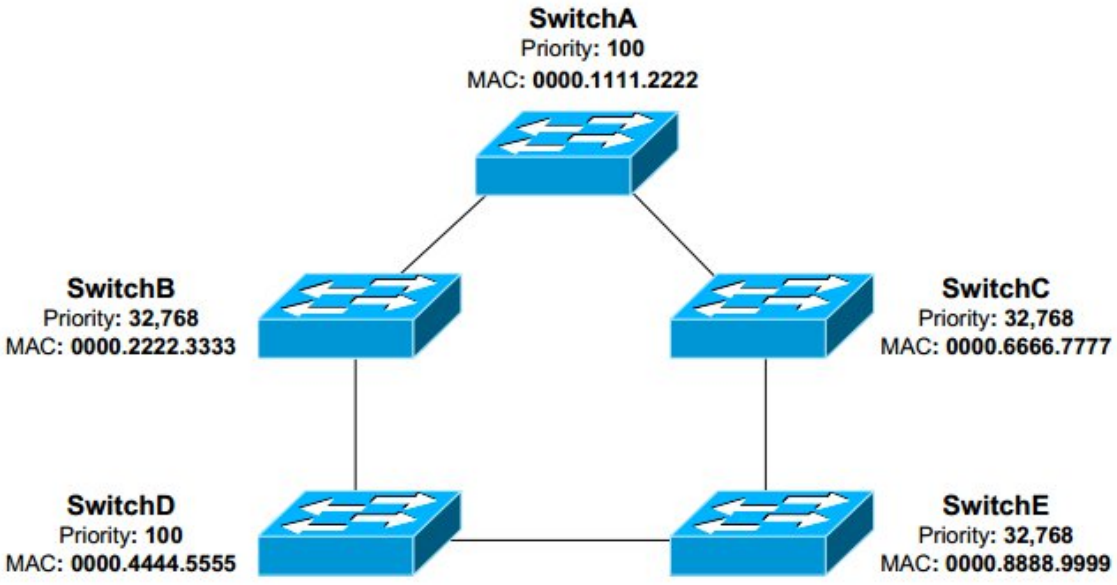
- A Root Bridge is elected
- Root ports are identified
- Designated ports are identified
- Ports are placed in a blocking state as required, to eliminate loops.

Electing an STP Root Bridge

A Root Bridge is elected based on its Bridge ID, comprised of two components.

- 16-bit Bridge priority
- 48-bit MAC address. The default priority is 32,768, and the lowest priority wins

If there is a tie in priority, the lowest MAC address is used as the tie-breaker.

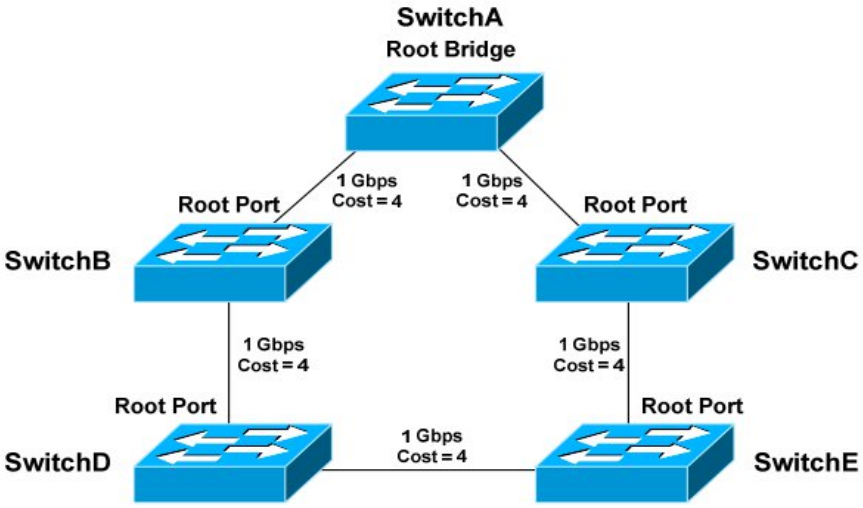


- Switches exchange BPDU's to perform the election process, and the lowest Bridge ID determines the Root Bridge:
- Switch B, Switch C, and Switch E have the default priority of 32,768.
- Switch A and Switch D are tied with a lower priority of 100.
- Switch A has the lowest MAC address, and will be elected the Root Bridge.

Identifying Root Ports

- The second step in the STP convergence process is to identify root ports.
- The root port of each switch has the lowest root path cost to get to the Root Bridge.
- Each switch can only have *one* root port.
- The *higher* the bandwidth, the *lower* the path cost:

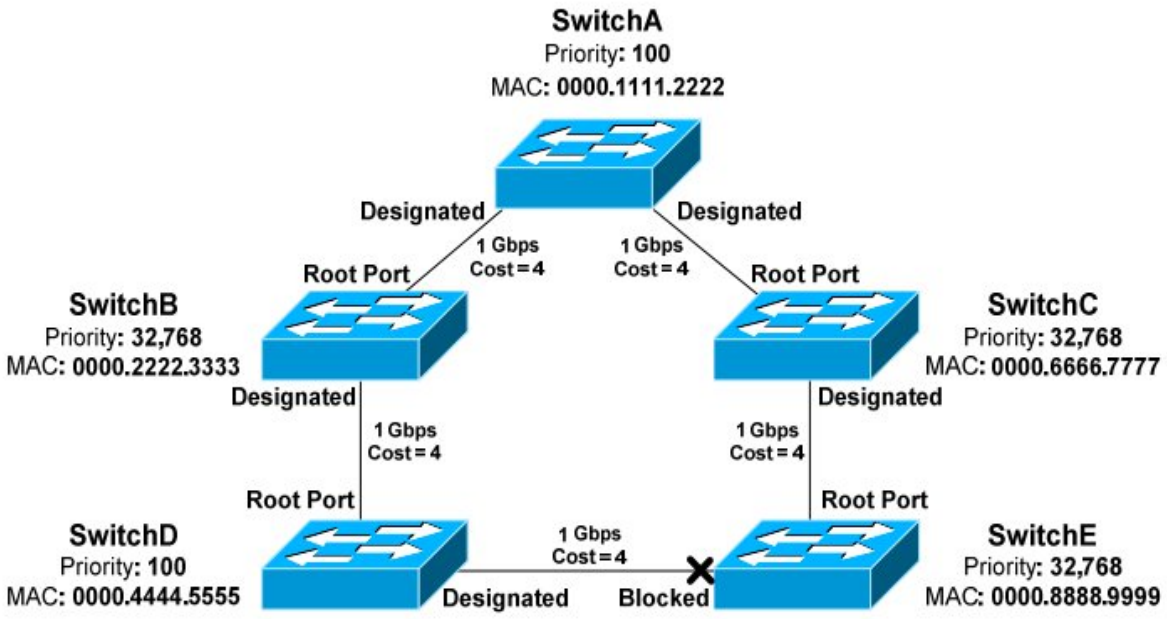
Bandwidth	*Cost*
4 Mbps	250
10 Mbps	100
16 Mbps	62
45 Mbps	39
100 Mbps	19
155 Mbps	14
1 Gbps	4
10 Gbps	2



Identifying Designated Ports

- A single designated port is identified for each network segment.
- This port is responsible for forwarding BPDUs and frames to that segment.
- If two ports are eligible to become the designated port, then there is a loop.
- One of the ports will be placed in a blocking state to eliminate the loop.

.



- Ports on the Root Bridge are never placed in a blocking state.
- One of the ports must be elected as the designated port, and the other must be placed in a blocking state.
- In the above example, there is a tie in cumulative path cost. Both SwitchD and SwitchE have a path cost of 12 to reach the Root Bridge on that segment.

STP Port States

- Blocking
- Listening
- Learning
- Forwarding

Initially, a switch port will start in a blocking state:

- A blocking port will not forward frames.

A port will then transition from a blocking to a listening state:

- A listening port will not forward frames or learn MAC addresses.
- A listening port will send and listen for BPDUs, to participate in the election of the Root Bridge, root ports, and designated ports.
- If a listening port is not elected as a root or a designated Port; it will transition back to a blocking state.

If a listening port is elected as a root or designated port, it will transition to a learning state:

- Learning port cannot forward frames quite yet.

Finally, a learning port will transition to a forwarding state:

- Root and designated ports will eventually transition to a forwarding state.

Technically, there is a fifth port state – disabled.

A port in a disabled state has been administratively shutdown.

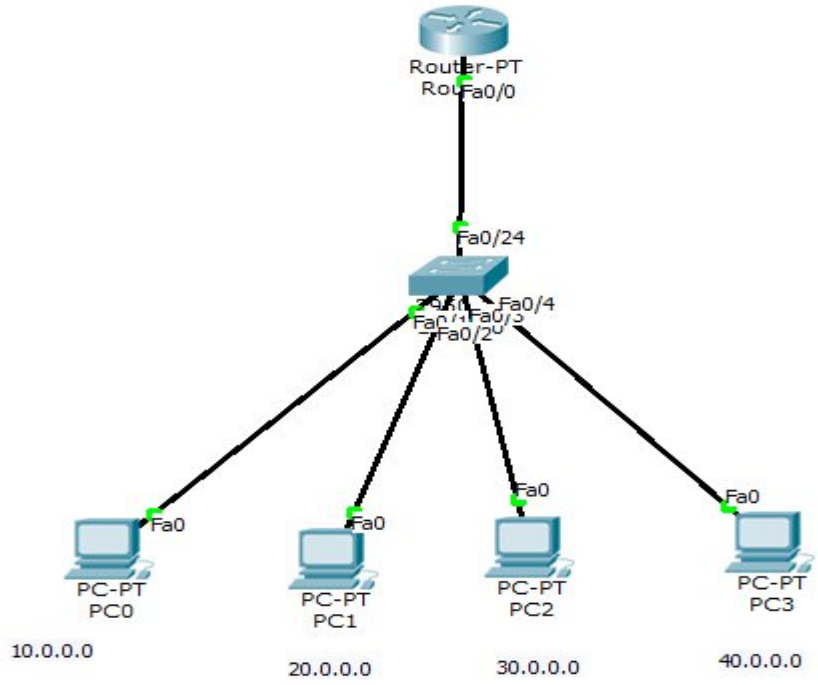
```
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    1
              Address     0060.47CB.56A6
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15

  Bridge ID   Priority    1  (priority 0 sys-id-ext 1)
              Address     0060.47CB.56A6
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/1            Desg FWD 19        128.1    P2p
```

VLAN AND INTER-VLAN

Each VLAN represents a unique broadcast domain:

• Traffic between devices within the same VLAN is switched.

• Traffic between devices in different VLANs requires a Layer-3 device to communicate.



STEP 1: SWITCH PORT TRUNK

```
Switch(config)#
Switch(config)#INT F0/24
Switch(config-if)#SWITCHPORT MODE TRUNK
Switch(config-if)#SWITCHPORT TRUNK ALLOWED VLAN ALL
Switch(config-if)#EXIT
```

STEP 2: CREATING DOMAIN AND SERVER

Switch # vlan database
Switch # vtp domain tcs
Switch # vtp server

STEP 3: CREATING VLAN

```
Switch#CONF T
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#VLAN 10
Switch(config-vlan)#NAME ACCOUNTS
Switch(config-vlan)#EXIT
Switch(config)#VLAN 20
Switch(config-vlan)#NAME CASH
Switch(config-vlan)#EXIT
Switch(config)#VLAN 30
Switch(config-vlan)#NAME IT
Switch(config-vlan)#EXIT
Switch(config)#VLAN 40
Switch(config-vlan)#NAME FINANCE
Switch(config-vlan)#EXIT
```

STEP 4: ENCAPSULATION

Router (config) #INT F0/0.1
Router (config-subif) #Encapsulation DOT1Q 10
Router (config-subif) #IP Address 10.0.0.1 255.0.0.0
Router (config-subif) #EXIT

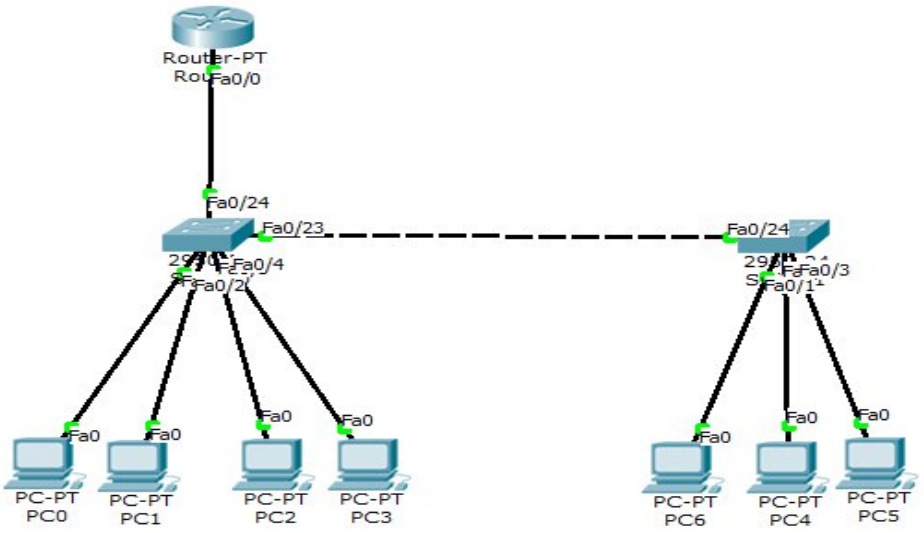
Router (config) #INT F0/0.2
Router (config-subif) #Encapsulation DOT1Q 20
Router (config-subif) #IP Address 20.0.0.1 255.0.0.0
Router (config-subif) #EXIT

Router (config) #INT F0/0.3
Router (config-subif) #Encapsulation DOT1Q 30
Router (config-subif) #IP Address 30.0.0.1 255.0.0.0
Router (config-subif) #EXIT

STEP 5: SWITCHPORT ACCESS

```
Switch(config)#INT F0/1
Switch(config-if)#SWITCHPORT ACCESS VLAN 10
Switch(config-if)#EXIT
Switch(config)#INT F0/2
Switch(config-if)#SWITCHPORT ACCESS VLAN 20
Switch(config-if)#EXIT
Switch(config)#INT F0/3
Switch(config-if)#SWITCHPORT ACCESS VLAN 30
Switch(config-if)#EXIT
Switch(config)#INT F0/4
Switch(config-if)#SWITCHPORT ACCESS VLAN 40
Switch(config-if)#EXIT
```

INTER- VLAN



SWITCH 1

Switch (config) #INT F0/23
Switch (config-if) #SWITCHPORT MODE TRUNK
Switch (config-if) #SWITCHPORT TRUNK Allowed VLan ALL

SWITCH 2

```
Switch(config)#
Switch(config)#INT F0/24
Switch(config-if)#SWITCHPORT MODE TRUNK
Switch(config-if)#SWITCHPORT TRUNK ALLOWED VLAN ALL
Switch(config-if)#EXIT
```

TROUBLE-SHOOT COMMAND

- Switch# show vlan
- Switch # show vtp

HOT STANDBY ROUTING PROTOCOL (HSRP)

Cisco supports two protocols to provide transparent Layer-3 redundancy:

• Hot Standby Router Protocol (HSRP)

• Virtual Router Redundancy Protocol (VRRP)

Hot Standby Router Protocol (HSRP)

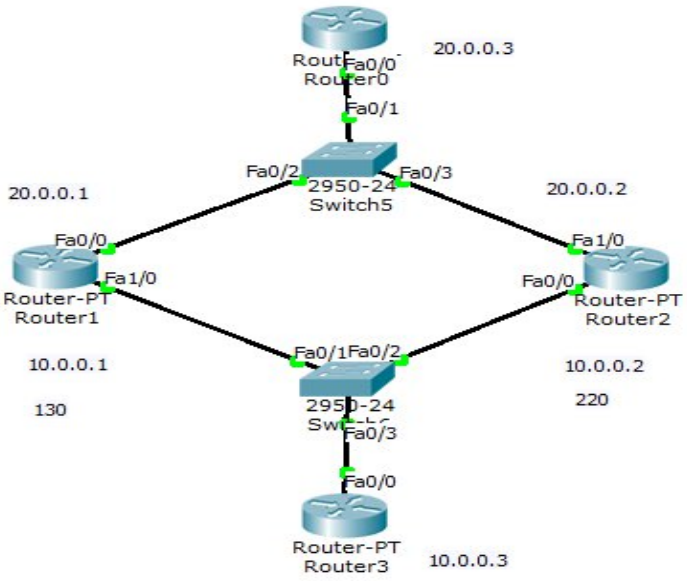
- Cisco developed the proprietary Hot Standby Router Protocol (HSRP) to allow multiple routers or multilayer switches as a single gateway.
- This is accomplished by assigning a virtual IP and MAC address to all routers participating in an HSRP group.
- Routers within the same HSRP group must be assigned the same group number, which can range from 0 to 255.

HSRP routers are elected to specific roles:

• Active Router – router currently serving as the gateway.

• Standby Router – backup router to the Active Router.

- Only one active and one standby router are allowed per HSRP group.
- The role of an HSRP router is dictated by its priority. The priority can range from 0 – 255, with a default of 100. A higher priority is preferred.



- Thus, the router with the highest priority is elected the active router.
- The router with the second highest priority becomes the standby router
- If all priorities are equal, whichever router has the highest IP Address on its HSRP interface is elected the active router.

SYNTAX FOR CONFIGURING HSRP

ROUTER 2, 3

Router (config) #INT F0/0

Router (config-if) #Standby 1 IP 10.0.0.254

Router (config-if) #Standby 1PRIority 200

The standby 1 command specifies the HSRP group the interface belongs to.

Output

```
Router#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Fa0/0       1    220   Active   local           10.0.0.1        10.0.0.254
Router#
```

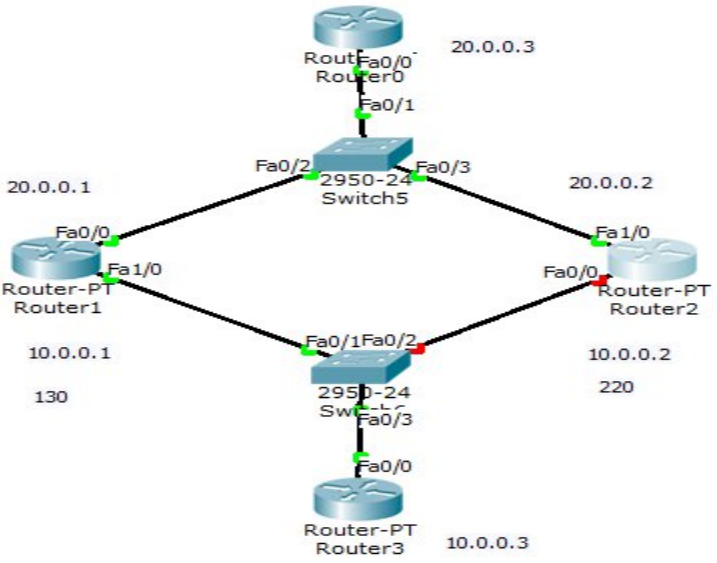
PREEMPT

Router (config-if) #standby 1 preempt

- The preempt parameter will allow a router to forcibly assume the role of active router, if it has the highest priority.

```
Router#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Fa0/0       1    220 P Active   local           10.0.0.1        10.0.0.254
```

- If the interface is assumed to be shutdown,




```
Router#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Fa0/0       1    220 P Init     unknown         unknown         10.0.0.254

Router#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Fa1/0       1    130   Active   local           unknown         10.0.0.254
```

Once the interface is up,

```
Router#
%HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Standby -> Active

Router#
Router#
Router#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Fa0/0       1    220 P Active   local           unknown         10.0.0.254
```

TROUBLE SHOOT COMMAND

- Router # show standby brief.

Virtual Router Redundancy Protocol (VRRP)

- The Virtual Router Redundancy Protocol (VRRP) is an industry-standard Layer-3 redundancy protocol, originally defined in RFC 2338.
- VRRP is nearly identical to HSRP, with some notable exceptions:
- The router with the highest priority becomes the master router.
- All other routers become backup routers.
- The virtual MAC address is the reserved 0000.5e00.01xx, with xx representing the hexadecimal group number.
- Hello packets are sent every 1 second, by default, and sent to multicast address 224.0.0.18.
- VRRP will preempt by default.

SYNTAX

Router (config) #INT F0/0

Router (config-if) # vrrp1 IP 10.0.0.254

Router (config-if) # vrrp 1PRIority 200

- As with HSRP, the default VRRP priority is 100, and a higher priority is preferred.
- Unlike HSRP, preemption is enabled by default.

To manually disable preempt:

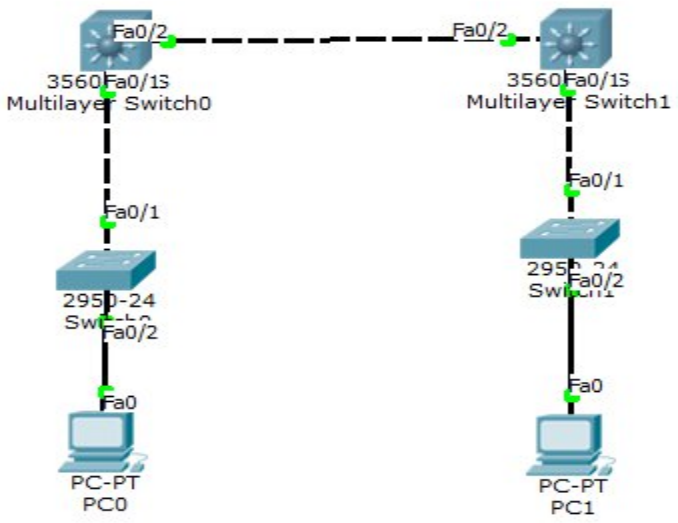
Switch (config-if) # no vrrp 1 preempt

To view the status of each VRRP group:

Switch# show vrrp

MULTI LAYER SWITCHING

- It supports both Layer-2 and Layer-3 forwarding.



Layer-2 forwarding, usually referred to as switching, involves decisions based on frame or data-link headers.

Layer-3 forwarding, usually referred to as routing, involves decisions based on packet or network headers.

A multilayer switch supports two port types:

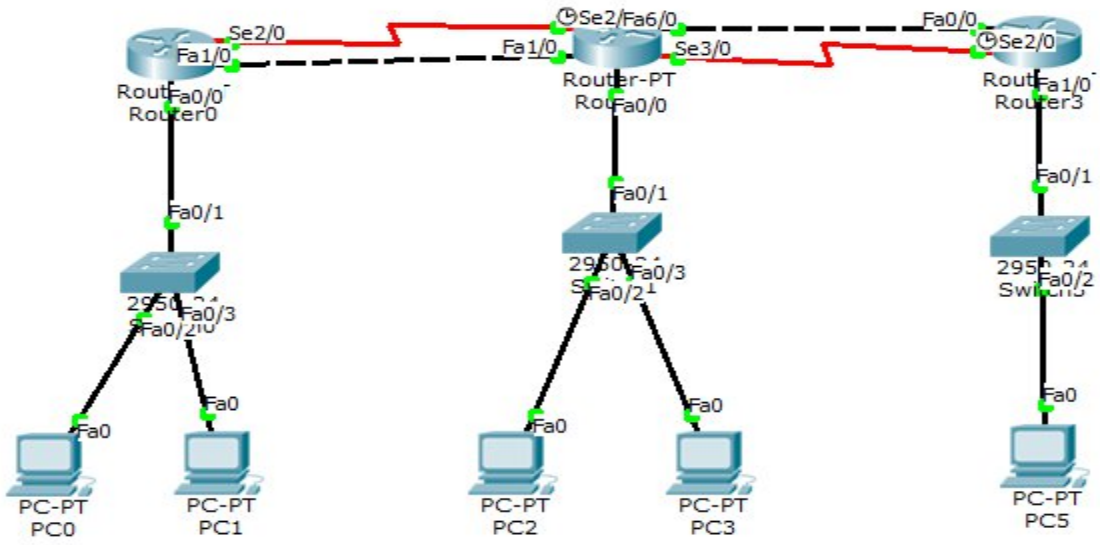
- Layer-2 or switch ports
- Layer-3 or routed ports

- A switch port can either be an access or trunk port. By default on Cisco switches, all interfaces are switch ports.
- A routed port behaves exactly like a physical router interface, and is not associated with a VLAN.
- The no switch port command configures an interface as a routed port, allowing an IP address to be assigned:

Switch (config) # interface gi1/20
Switch (config-if) # no switch port
Switch (config-if) # exit
Switch (config) # interface gi1/20
Switch (config-if) # ip address 10.101.101.1 255.255.255.0

FLOATIC – STATIC ROUTING

- Floating static routes are static routes that are configured on the networking device but not used unless the dynamic route to a network is lost.
- When a dynamic route to a network is lost the networking device will install an alternative static route to the same network if such a route exists.
- A floating static route is often used as a backup route to a dynamic routing protocol.



Output:

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, FastEthernet0/0
C    20.0.0.0/8 is directly connected, Serial2/0
S    30.0.0.0/8 [1/0] via 40.0.0.2
                [1/0] via 20.0.0.2
C    40.0.0.0/8 is directly connected, FastEthernet1/0
S    50.0.0.0/8 [1/0] via 40.0.0.2
                [1/0] via 20.0.0.2
S    60.0.0.0/8 [1/0] via 40.0.0.2
                [1/0] via 20.0.0.2
S    70.0.0.0/8 [1/0] via 40.0.0.2
                [1/0] via 20.0.0.2
```

PASSIVE INTERFACE ON ROUTING PROTOCOLS

- The passive-interface command will prevent updates from being sent out of the interface, but we still receive updates on this interface.
- We can configure all interfaces to be passive using the passive-interface default command, and then individually use the no passive-interface command on the interfaces.

RIP

For RIP, the passive-inter-face command will prevent the inter-face from sending out routing updates but will allow the interface to receive updates.

Router (config) #routers rip

Router (config-router) # network 10.4.0.0

Router (config-router) # network 10.2.0.0

Router (config-router) # passive-interface s0

EIGRP.

With EIGRP running on a network, the passive-interface command stops both outgoing and incoming routing updates, since the effect of the command causes the **router** to stop sending and receiving hello packets over an interface.

RouterC (config) # router eigrp 10

RouterC (config-router) # network 10.4.0.0

RouterC (config-router) # network 10.2.0.0

RouterC (config-router) # passive-interface s0

OSPF

RouterC(config)# router ospf 1

RouterC(config-router)# network 10.4.0.0 0.0.255.255 area 0

RouterC(config-router)# network 10.2.0.0 0.0.255.255 area 0

RouterC(config-router)# passive-interface s0

PORT SECURITY

- Port Security adds an additional layer of security to the switching network.
- The MAC address of a host generally does not change.
- If a specific host will always remain connected to a specific switch port, then the switch can filter all other MAC addresses on that port using Port Security.
- To enable Port Security on an interface:

```
Switch(config)# interface gi1/10
Switch(config-if)# switch port port-security
Switch(config-if)# switch port mode access
Switch(config-if)# switch port access vlan 1
```

- By default, Port Security will allow only one MAC on an interface.
- To adjust the maximum number of allowed VLANs, up to 1024:

Switch(config-if)# *switchport port-security maximum 2*

- To statically map the allowed MAC addresses on an interface:

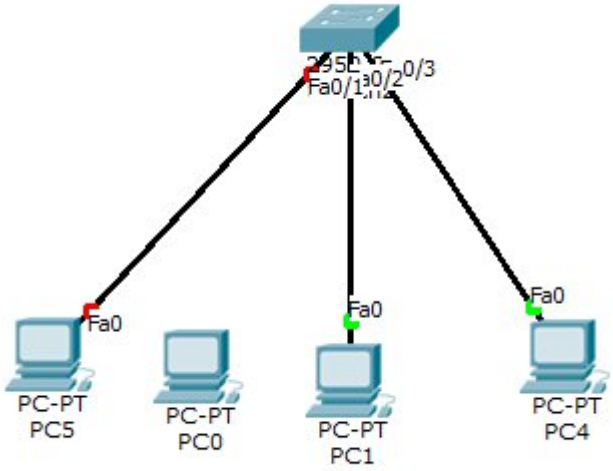
```
Switch(config-if)# switchport port-security mac-address 0001.1111.2222
Switch(config-if)# switchport port-security mac-address 0001.3333.5555
```

- Only hosts configured with the above two MAC addresses will be allowed to send traffic through this port.
- Port Security refers to dynamically learned MAC addresses as sticky addresses.

Switch (config-if) # switchport port-security mac-address sticky

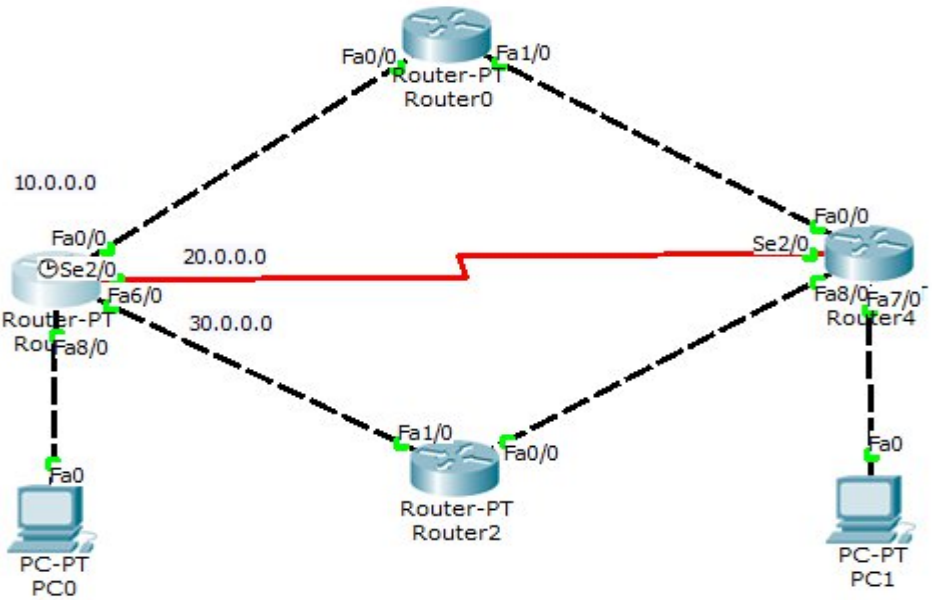
- A violation occurs if an unauthorized MAC address attempts to forward traffic through a port.
- Shutdown – If a violation occurs, the interface is placed in an err disable state.
- To configure the desired Port Security violation action:

Switch(config-if)# switchport port-security violation shutdown



Switch(config)#int f0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 1
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security violation shutdown

EIGRP EQUAL AND UNEQUAL COST LOAD BALANCING



OUTPUT

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, FastEthernet0/0
C    30.0.0.0/8 is directly connected, FastEthernet6/0
D    40.0.0.0/8 [90/30720] via 10.0.0.2, 00:02:57, FastEthernet0/0
D    60.0.0.0/8 [90/30720] via 30.0.0.2, 00:02:57, FastEthernet6/0
C    70.0.0.0/8 is directly connected, FastEthernet8/0
D    80.0.0.0/8 [90/33280] via 10.0.0.2, 00:02:57, FastEthernet0/0
                [90/33280] via 30.0.0.2, 00:02:57, FastEthernet6/0
C    90.0.0.0/8 is directly connected, Serial2/0
```

```
Router#SHow IP ROUte
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, FastEthernet0/0
C    30.0.0.0/8 is directly connected, FastEthernet6/0
D    40.0.0.0/8 [90/30720] via 10.0.0.2, 00:06:44, FastEthernet0/0
D    60.0.0.0/8 [90/30720] via 30.0.0.2, 00:06:44, FastEthernet6/0
C    70.0.0.0/8 is directly connected, FastEthernet8/0
D    80.0.0.0/8 [90/33280] via 10.0.0.2, 00:06:44, FastEthernet0/0
                [90/33280] via 30.0.0.2, 00:06:44, FastEthernet6/0
```

TYPES OF PROTOCOLS

- In order for computers to communicate with one another, standard methods of information transfer and processing have been devised.
- These are referred to as "protocols" and some of the more common ones such as TCP, IP, UDP, POP, SMTP, HTTP, and FTP.

INTERNET PROTOCOL (IP)

The Internet Protocol (IP) is a network-layer (Layer 3) protocol that contains addressing information and some control information that enables packets to be routed.

IP has two primary responsibilities:

- Providing connectionless, best-effort delivery of datagram through an internetwork.
- Providing fragmentation and reassembly of datagram to support data links with different maximum-transmission unit (MTU) sizes.

Internet Control Message Protocol (ICMP)

- The Internet Control Message Protocol (ICMP) is a network-layer Internet protocol that provides message packets to report errors and other information regarding IP packet processing back to the source.
- ICMP is documented in RFC 792.
- ICMPs generate several kinds of useful messages, including Destination Unreachable, Echo Request and Reply, Redirect, Time Exceeded, and Router Advertisement.

Transmission Control Protocol (TCP)

- The TCP provides reliable transmission of data in an IP environment.
- TCP corresponds to the transport layer (Layer 4) of the OSI reference model.
- TCP offers reliability by providing connection-oriented, end-to-end reliable packet delivery through an internetwork.

User Datagram Protocol (UDP)

- The User Datagram Protocol (UDP) is a connectionless transport-layer protocol (Layer 4) that belongs to the Internet protocol family.
- UDP is basically an interface between IP and upper-layer processes.
- UDP is the transport protocol for several well-known application-layer protocols, including Network File System (NFS), Simple Network Management Protocol (SNMP), Domain Name System (DNS), and Trivial File Transfer Protocol (TFTP).

File Transfer Protocol (FTP)—Moves files between devices.

Simple Network-Management Protocol (SNMP)—primarily reports anomalous network conditions and sets network threshold values.

Telnet—serves as a terminal emulation protocol.

Network File System (NFS), **External Data Representation (XDR), and Remote Procedure Call (RPC)—**Work together to enable transparent access to remote network resources.

Simple Mail Transfer Protocol (SMTP)—Provides electronic mail services.

Domain Name System (DNS)—translates the names of network nodes into network addresses.

PING, TRACE ROUTE

- **Ping**
  - measure the time for a packet to travel to a remote host and back
  - The server sends back an acknowledgment when the packet arrives
- **Trace route**
  - List the router hops between the client host and a remote host.
  - The IP address and domain name (if there is one) of each router is returned to the client.

How data travels.

Each computer on the trace route is identified by its IP address, which is the nine-digit number separated by periods that identifies that computer's unique network connection.

Here are a few details regarding a trace route:

- The journey from one computer to another is known as a hop.
- The amount of time it takes to make a hop is measured in milliseconds.
- The information that travels along the trace route is known as a packet.

TROUBLE SHOOTING COMMANDS

Show running-configuration

The show running-config command shows the router, switch, or firewall's current configuration.

Copy running-configuration startup-configuration

This command will save the configuration that is currently being modified (in RAM), also known as the running-configuration, to the nonvolatile RAM (NVRAM). If the power is lost, the NVRAM will preserve this configuration.

Show interface

The show interface command displays the status of the router's interfaces.

- Interface status (up/down)
- Protocol status on the interface
- Utilization
- Errors
- MTU

This command is essential for troubleshooting a router or switch

Show ip interface

The show ip interface command provides tons of useful information about the configuration and status of the IP protocol and its services, on all interfaces.

No shutdown

The no shutdown command enables an interface (brings it up). This command must be used in interface configuration mode. It is useful for new interfaces and for troubleshooting

Show ip route

The show ip route command is used to show the router's routing table. This is the list of all networks that the router can reach, their metric (the router's preference for them), and how to get there.

Show version

The show version command gives you the router's configuration register (essentially, the router's firmware settings for booting up), the last time the router was booted, the version of the IOS, the name of the IOS file, the model of the router, and the router's amount of RAM and Flash.

Debug

The debug command has many options and does not work by itself. It provides detailed debugging output on a certain application, protocol, or service.

IOS INSTALLATION ON ROUTER

Requirements

You'll need:

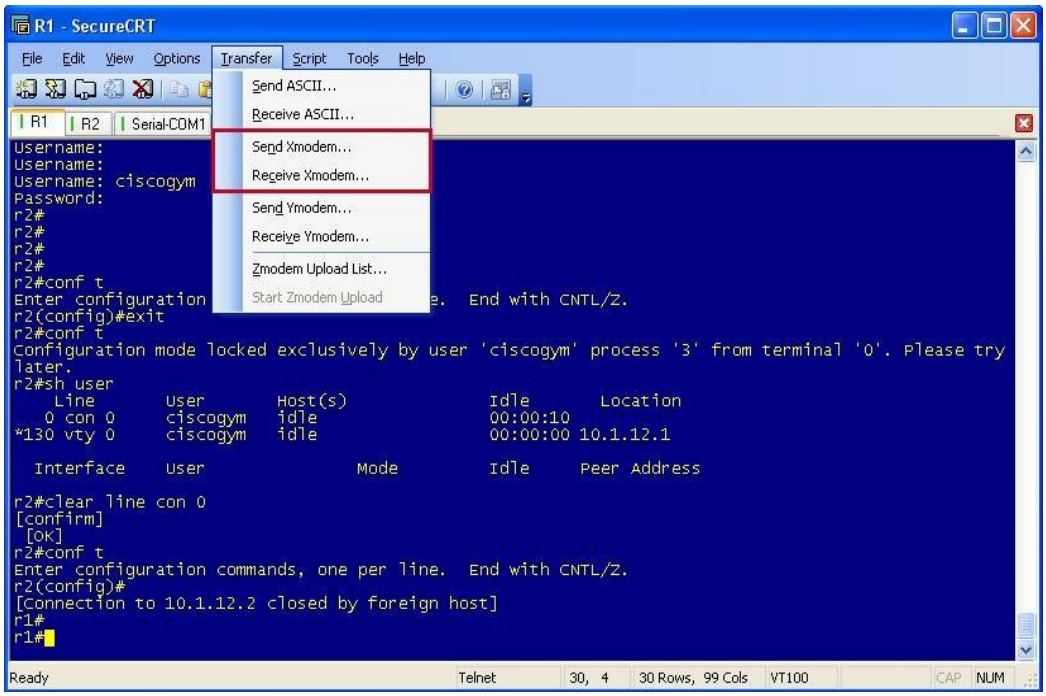
A terminal emulator which supports XMODEM (or YMODEM) transfers.

- SecureCRT(shown),
- HyperTerminal
- Tera Term Pro all support XMODEM.

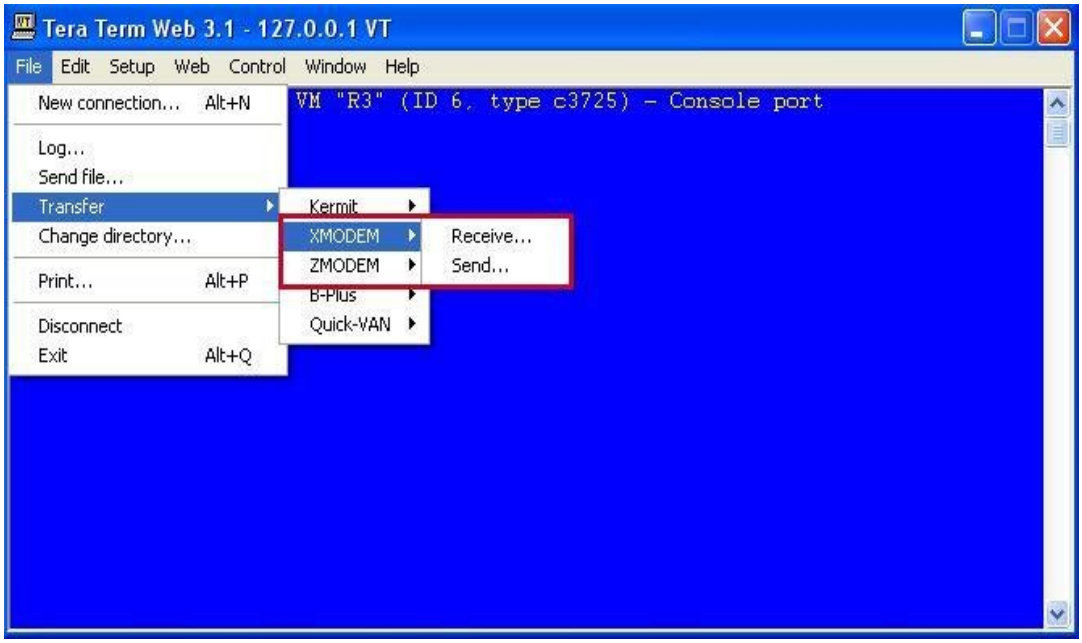
Access to the console port of the Cisco device.

A PC with the files you want to transfer.

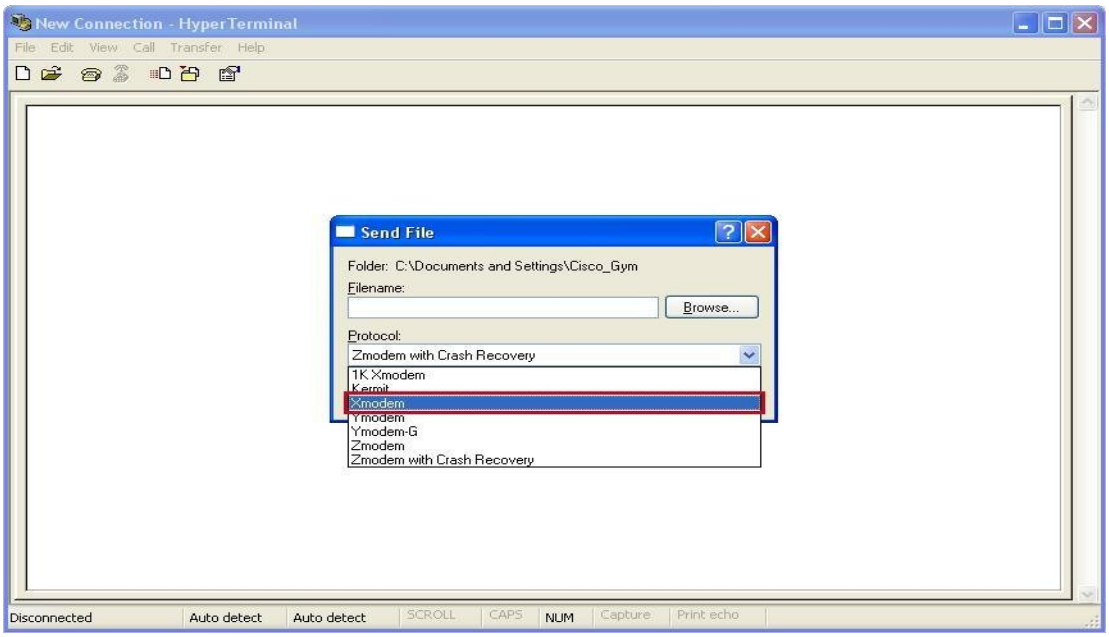
SECURECRT



TERA TEAM



HYPER TERMINAL



Setting the console port speed

By default the console port's speed is 9600 baud:

2610#sh line con 0 | i Baud

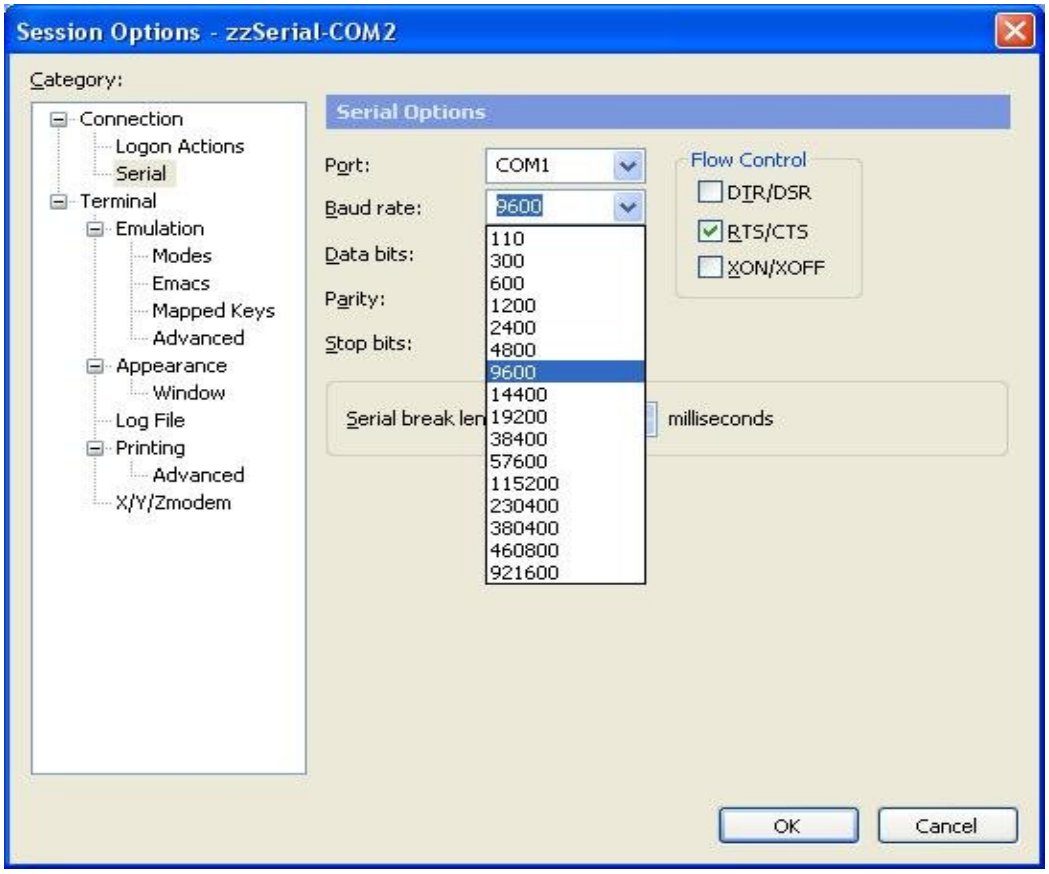
Baud rate (TX/RX) is **9600/9600**, no parity, 2 stop bits, 8 data bits

You can change this with the 'speed' command under the console line:

2610(config) #line con 0
2610(config-line) #speed?
<0-4294967295> Transmit and receive speeds
2610(config-line) #speed 115200

A good speed to set is 115200. This is the max speed on a lot of Cisco devices.

Match speed on your terminal emulator



COPY XMODEM

2610#copy xmodem: flash:2:

Destination filename []? C2600-imz.123-26.bin Erase flash:2: before copying? [confirm]n
Begin the Xmodem or Xmodem-1K transfers now...
CCCCCCCC
Starting xmodem transfer. Press Ctrl+C to cancel.
Transferring c2600-i-mz.123-26.bin...
0% 6 KB 0 KB/s 02:48:08 ETA 0 Errors

XMODEM with ROMMON

Use the **xmodem** ROM monitor command to download a new system image to your router from a local personal computer (such as a PC, Mac, or UNIX workstation), or a remote computer over a modem connection, to the router's console port.

Rommon > xmodem -c new-ios-image.