Experiment #2

Basic Router Configurations

Learning Objectives

- Cable a network according to the Topology Diagram.
- Erase the startup configuration and reload a router to the default state.
- Perform basic configuration tasks on a router.
- Configure and activate interfaces.
- Configure RIP routing on all routers.
- Verify RIP routing using **`show`** and **`debug`** commands.
- Gather information about RIP processing using the **`debug ip rip`** command.

Theoretical Background

Router is a computer, just like any other computer including a PC. Routers have many of the same hardware and software components that are found in other computers including:

- CPU
- RAM
- ROM
- Operating System

Typical users may be unaware of the presence of numerous routers in their own network or in the Internet. Users expect to be able to access web pages, send e-mails, and download files - whether the server they are accessing is on their own network or on another network half-way around the world. However, networking professionals know it is the router that is responsible for forwarding packets from network-to-network, from the original source to the final destination.

A router connects multiple networks. This means that it has multiple interfaces that each belong to a different IP network. When a router receives an IP packet on one interface, it determines which interface to use to forward the packet onto its destination. The interface that the router uses to forward the packet may be the network of the final destination of the packet (the network with the destination IP address of this packet), or it may be a network connected to another router that is used to reach the destination network.

Each network that a router connects to typically requires a separate interface. These interfaces are used to connect a combination of both Local Area Networks (LANs) and Wide Area Networks (WANs). LANs are commonly Ethernet networks that contain devices such as PCs, printers, and servers. WANs are used to connect networks over a large geographical area. For example, a WAN connection is commonly used to connect a LAN to the Internet Service Provider (ISP) network.

The primary responsibility of a router is to direct packets destined for local and remote networks by:

- Determining the best path to send packets
- Forwarding packets toward their destination

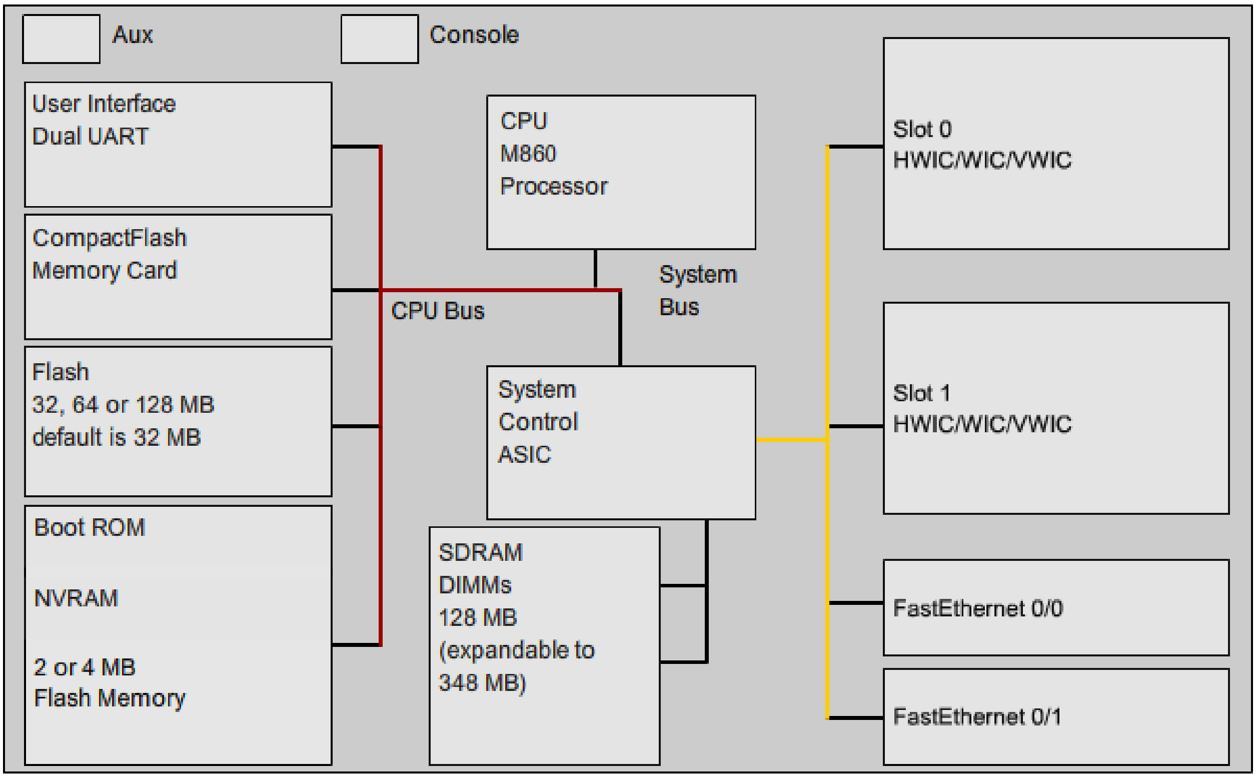
The router uses its routing table to determine the best path to forward the packet. When the router receives a packet, it examines its destination IP address and searches for the best match with a network address in the router's routing table. The routing table also includes the interface to be used to forward the packet. Once a match is found, the router encapsulates the IP packet into the data link frame of the outgoing or exit interface, and the packet is then forwarded toward its destination.

It is very likely that a router will receive a packet that is encapsulated in one type of data link frame, such as an Ethernet frame and when forwarding the packet, the router will encapsulate it in a different type of data link frame, such as Point-to-Point Protocol (PPP). The data link encapsulation depends on the type of interface on the router and the type of medium it connects to. The different data link technologies that a router connects to can include LAN technologies, such as Ethernet, and WAN serial connections, such as T1 connection using PPP, Frame Relay, and Asynchronous Transfer Mode (ATM).

PPP is used over many types of physical networks including serial cable, phone line, trunk line, cellular telephone, specialized radio links, and fiber optic links such as SONET. Most Internet service providers (ISPs) use PPP for customer dial-up access to the Internet. Two encapsulated forms of PPP, Point-to-Point Protocol over Ethernet (PPPoE) and Point-to-Point Protocol over ATM (PPPoA),

Router Components and their Functions

Hardware Components of a Router



Logical diagram of the Internal Components of a Cisco 1841 router

1- CPU

The CPU executes operating system instructions, such as system initialization, routing functions, and switching functions.

2- RAM

RAM stores the instructions and data needed to be executed by the CPU. RAM is used to store these components:

- Operating System: The Cisco IOS (Internetwork Operating System) is copied into RAM during bootup.
- Running Configuration File: This is the configuration file that stores the configuration commands that the router IOS is currently using. With few exceptions, all commands configured on the router are stored in the running configuration file, known as running-config.
- IP Routing Table: This file stores information about directly connected and remote networks. It is used to determine the best path to forward the packet.
- ARP Cache: This cache contains the IPv4 address to MAC address mappings, similar to the ARP cache on a PC. The ARP cache is used on routers that have LAN interfaces such as Ethernet interfaces.
- Packet Buffer: Packets are temporarily stored in a buffer when received on an interface or before they exit an interface.

RAM is volatile memory and loses its content when the router is powered down or restarted. However, the router also contains permanent storage areas, such as ROM, flash and NVRAM.

3- ROM

ROM is a form of permanent storage. Cisco devices use ROM to store:

- The bootstrap instructions
- Basic diagnostic software
- Scaled-down version of IOS

ROM uses firmware, which is software that is embedded inside the integrated circuit. Firmware includes the software that does not normally need to be modified or upgraded, such as the bootup instructions. Many of these features, including ROM monitor software, will be discussed in a later course. ROM does not lose its contents when the router loses power or is restarted.

4- Flash Memory

Flash memory is nonvolatile computer memory that can be electrically stored and erased. Flash is used as permanent storage for the operating system, Cisco IOS. In most models of Cisco routers, the IOS is permanently stored in flash memory and copied into RAM during the bootup process, where it is then executed by the CPU. Some older models of Cisco routers run the IOS directly from flash. Flash consists of SIMMs or PCMCIA cards, which can be upgraded to increase the amount of flash memory.

Flash memory does not lose its contents when the router loses power or is restarted.

5- NVRAM

NVRAM (Nonvolatile RAM) does not lose its information when power is turned off. This is in contrast to the most common forms of RAM, such as DRAM, that requires continual power to maintain its information. NVRAM is used by the Cisco IOS as permanent storage for the startup configuration file (startup-config). All configuration changes are stored in the running-config file in RAM, and with few exceptions, are implemented immediately by the IOS. To save those changes in case the router is restarted or loses power, the running-config must be copied to NVRAM, where it is stored as the startup-config file. NVRAM retains its contents even when the router reloads or is powered off.

ROM, RAM, NVRAM, and flash are discussed in the following section which introduces the IOS and the bootup process. They are also discussed in more detail in a later course relative to managing the IOS.

Routing Table

A routing table is a data file in **RAM** that is used to store route information about directly connected and remote networks. The routing table contains network/next hop associations. These associations tell a router that a particular destination can be optimally reached by sending the packet to a specific router that represents the "next hop" on the way to the final destination. The next hop association can also be the outgoing or exit interface to the final destination.

The network/exit-interface association can also represent the destination network address of the IP packet. This association occurs on the router's directly connected networks.

<u>A directly connected network</u>

is a network that is directly attached to one of the router interfaces. When a router interface is configured with an IP address and subnet mask, the interface becomes a host on that attached network. The network address and subnet mask of the interface, along with the interface type and number, are entered into the routing table as a directly connected network. When a router forwards a packet to a host, such as a web server, that host is on the same network as a router's directly connected network.

<u>A remote network is a network</u>

that is not directly connected to the router. In other words, a remote network is a network that can only be reached by sending the packet to another router. Remote networks are added to the routing table using either a dynamic routing protocol or by configuring static routes. Dynamic routes are routes to remote networks that were learned automatically by the router, using a dynamic routing protocol. Static routes are routes to networks that a network administrator manually configured.

Routing Table Principles

1. Every router makes its decision alone, based on the information it has in its own routing table.
2. The fact that one router has certain information in its routing table does not mean that other routers have the same information. Because routers do not necessarily have the same information in their routing tables, packets can traverse the network in one direction, using one path, and return via another path. This is called asymmetric routing. Asymmetric routing is more common in the Internet, which uses the BGP routing protocol.

3. Routing information about a path from one network to another does not provide routing information about the reverse, or return, path.

Routing types:

1- Static Routing

A static route includes the network address and subnet mask of the remote network, along with the IP address of the next-hop router or exit interface. Static routes are denoted with the code S in the routing table. Static routes should be used in the following cases:

- A network consists of only a few routers. Using a dynamic routing protocol in such a case does not present any substantial benefit. On the contrary, dynamic routing may add more administrative overhead.
- A network is connected to the Internet only through a single ISP. There is no need to use a dynamic routing protocol across this link because the ISP represents the only exit point to the Internet.
- A large network is configured in a hub-and-spoke topology. A hub-and-spoke topology consists of a central location (the hub) and multiple branch locations (spokes), with each spoke having only one connection to the hub. Using dynamic routing would be unnecessary because each branch has only one path to a given destination-through the central location.

2- Dynamic Routing

Remote networks can also be added to the routing table by using a dynamic routing protocol. Dynamic routing protocols are used by routers to share information about the reachability and status of remote networks. Dynamic routing protocols perform several activities, including:

- *Network discovery*
- *Updating and maintaining routing tables*

Automatic Network Discovery

Network discovery is the ability of a routing protocol to share information about the networks that it knows with other routers that are also using the same routing protocol. Instead of configuring static routes to remote networks on every router, a dynamic routing protocol allows the routers to automatically learn about these networks from other routers. These networks - and the best path to each network - are added to the router's routing table and denoted as a network learned by a specific dynamic routing protocol.

Maintaining Routing Tables

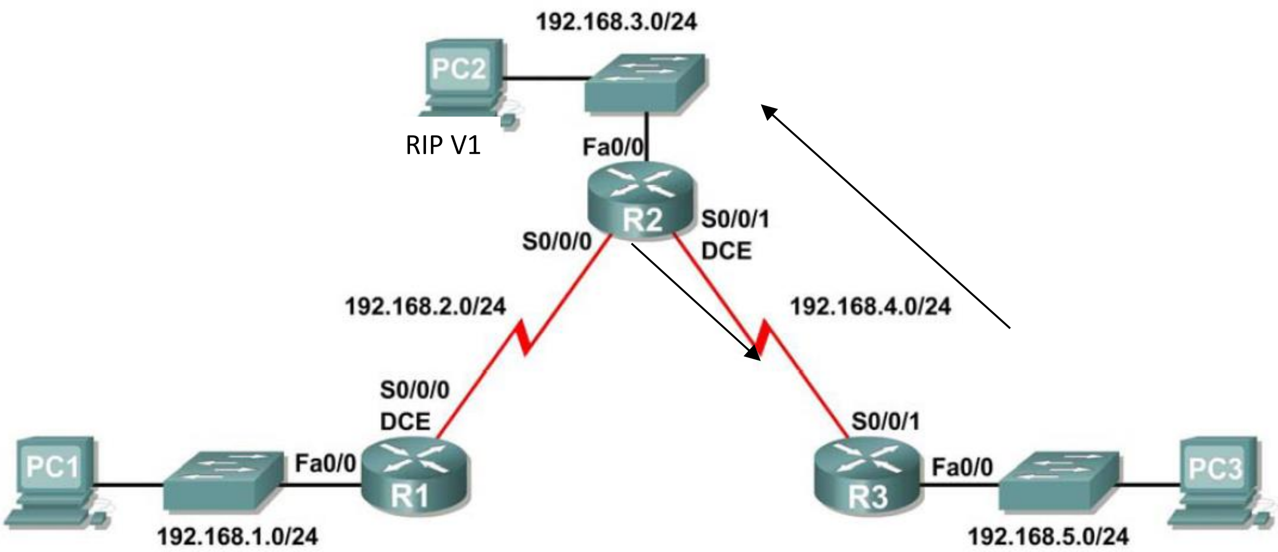
After the initial network discovery, dynamic routing protocols update and maintain the networks in their routing tables. Dynamic routing protocols not only make a best path determination to various networks, they will also determine a new best path if the initial path becomes unusable (or if the topology changes). For these reasons, dynamic routing protocols have an advantage over static routes. Routers that use dynamic routing protocols automatically share routing information with other routers and compensate for any topology changes without involving the network administrator.

IP Routing Protocols

There are several dynamic routing protocols for IP. Here are some of the more common dynamic routing protocols for routing IP packets:

- RIP (Routing Information Protocol)
- IGRP (Interior Gateway Routing Protocol)
- EIGRP (Enhanced Interior Gateway Routing Protocol)
- OSPF (Open Shortest Path First)
- IS-IS (Intermediate System-to-Intermediate System)
- BGP (Border Gateway Protocol)

Topology Diagram



Addressing Table

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
	S0/0/1	192.168.4.2	255.255.255.0	N/A
R3	Fa0/0	192.168.5.1	255.255.255.0	N/A
	S0/0/1	192.168.4.1	255.255.255.0	N/A
PC1	NIC	192.168.1.10	255.255.255.0	192.168.1.1
PC2	NIC	192.168.3.10	255.255.255.0	192.168.3.1
PC3	NIC	192.168.5.10	255.255.255.0	192.168.5.1

Task 1: Prepare the Network.

Step 1: Cable a network that is similar to the one in the Topology Diagram.

Step 2: Clear any existing configurations on the routers.

Task 2: Perform Basic Router Configurations.

Perform basic configuration of the R1, R2, and R3 routers according to the following guidelines:

1. Configure the router hostname.
2. Disable DNS lookup.
3. Configure an EXEC mode password.
4. Configure a message-of-the-day banner.
5. Configure a password for console connections.
6. Configure a password for VTY connections.

Task 3: Configure and Activate Serial and Ethernet Addresses.

Step 1: Configure interfaces on R1, R2, and R3.

Configure the interfaces on the R1, R2, and R3 routers with the IP addresses from the table under the Topology Diagram.

Step 2: Verify IP addressing and interfaces.
Use the `show ip interface brief` command to verify that the IP addressing is correct and that the interfaces are active.
When you have finished, be sure to save the running configuration to the NVRAM of the router.

Step 3: Configure Ethernet interfaces of PC1, PC2, and PC3.
Configure the Ethernet interfaces of PC1, PC2, and PC3 with the IP addresses and default gateways from the table under the Topology Diagram.

Step 4: Test the PC configuration by pinging the default gateway from the PC.

Task 4: Configure RIP.

Step 1: Enable dynamic routing.
To enable a dynamic routing protocol, enter global configuration mode and use the `router` command.
Enter `router ?` at the global configuration prompt to a see a list of available routing protocols on your router.
To enable RIP, enter the command `router rip` in global configuration mode.

```
R1(config)#router rip
R1(config-router)#
```

Step 2: Enter classful network addresses.
Once you are in routing configuration mode, enter the classful network address for each directly connected network, using the `network` command.

```
R1(config-router)#network 192.168.1.0
R1(config-router)#network 192.168.2.0
R1(config-router)#
```

The `network` command:
• Enables RIP on all interfaces that belong to this network. These interfaces will now both send and receive RIP updates.
• Advertises this network in RIP routing updates sent to other routers every 30 seconds. When you are finished with the RIP configuration, return to privileged EXEC mode and save the current configuration to NVRAM.

```
R1(config-router)#end
%SYS-5-CONFIG_I: Configured from console by console
R1#copy run start
```

Step 3: Configure RIP on the R2 router using the `router rip` and `network` commands.

```
R2(config)#router rip
R2(config-router)#network 192.168.2.0
R2(config-router)#network 192.168.3.0
R2(config-router)#network 192.168.4.0
R2(config-router)#end
%SYS-5-CONFIG_I: Configured from console by console
R2#copy run start
```

When you are finished with the RIP configuration, return to privileged EXEC mode and save the current configuration to NVRAM.

Step 4: Configure RIP on the R3 router using the `router rip` and `network` commands.

```
R3(config)#router rip
R3(config-router)#network 192.168.4.0
R3(config-router)#network 192.168.5.0
R3(config-router)#end
%SYS-5-CONFIG_I: Configured from console by console
R3# copy run start
```

When you are finished with the RIP configuration, return to privileged EXEC mode and save the current configuration to NVRAM.

Task 5: Verify RIP Routing.

Step 1: Use the `show ip route` command to verify that each router has all of the networks in the topology entered in the routing table.

Routes learned through RIP are coded with an **R** in the routing table. If the tables are not converged as shown here, troubleshoot your configuration. Did you verify that the configured interfaces are active? Did you configure RIP correctly? Return to Task 3 and Task 4 to review the steps necessary to achieve convergence.

```
R1#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 192.168.1.0/24 is directly connected, FastEthernet0/0
C 192.168.2.0/24 is directly connected, Serial0/0/0
R 192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:04, Serial0/0/0
R 192.168.4.0/24 [120/1] via 192.168.2.2, 00:00:04, Serial0/0/0
R 192.168.5.0/24 [120/2] via 192.168.2.2, 00:00:04, Serial0/0/0
R1#
```

```
R2#show ip route
<Output omitted>
R 192.168.1.0/24 [120/1] via 192.168.2.1, 00:00:22, Serial0/0/0
C 192.168.2.0/24 is directly connected, Serial0/0/0
C 192.168.3.0/24 is directly connected, FastEthernet0/0
C 192.168.4.0/24 is directly connected, Serial0/0/1
R 192.168.5.0/24 [120/1] via 192.168.4.1, 00:00:23, Serial0/0/1
R2#
```

```
R3#show ip route
<Output omitted>
R 192.168.1.0/24 [120/2] via 192.168.4.2, 00:00:18, Serial0/0/1
R 192.168.2.0/24 [120/1] via 192.168.4.2, 00:00:18, Serial0/0/1
R 192.168.3.0/24 [120/1] via 192.168.4.2, 00:00:18, Serial0/0/1
C 192.168.4.0/24 is directly connected, Serial0/0/1
C 192.168.5.0/24 is directly connected, FastEthernet0/0
R3#
```

Step 2: Use the `show ip protocols` command to view information about the routing processes.

The **`show ip protocols`** command can be used to view information about the routing processes that are occurring on the router. This output can be used to verify most RIP parameters to confirm that:

- RIP routing is configured
- The correct interfaces send and receive RIP updates
- The router advertises the correct networks
- RIP neighbors are sending updates

```
R1#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 16 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
```

```
Default version control: send version 1, receive any version
Interface Send Recv Triggered RIP Key-chain
FastEthernet0/0   1 2 1
Serial0/0/0       1 2 1
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
192.168.1.0
192.168.2.0
Passive Interface(s):
Routing Information Sources:
Gateway Distance Last Update
192.168.2.2 120
Distance: (default is 120)
R1#
```

R1 is indeed configured with RIP. R1 is sending and receiving RIP updates on FastEthernet0/0 and Serial0/0/0. R1 is advertising networks 192.168.1.0 and 192.168.2.0. R1 has one routing information source. R2 is sending R1 updates.

Step 3: Use the `debug ip rip` command to view the RIP messages being sent and received.

Rip updates are sent every 30 seconds so you may have to wait for debug information to be displayed.

```
R1#debug ip rip
R1#RIP: received v1 update from 192.168.2.2 on Serial0/0/0
192.168.3.0 in 1 hops
192.168.4.0 in 1 hops
192.168.5.0 in 2 hops
RIP: sending v1 update to 255.255.255.255 via FastEthernet0/0 (192.168.1.1)
RIP: build update entries
network 192.168.2.0 metric 1
network 192.168.3.0 metric 2
network 192.168.4.0 metric 2
network 192.168.5.0 metric 3
RIP: sending v1 update to 255.255.255.255 via Serial0/0/0 (192.168.2.1)
RIP: build update entries
network 192.168.1.0 metric 1
```

The debug output shows that R1 receives an update from R2. Notice how this update includes all the networks that R1 does not already have in its routing table. Because the FastEthernet0/0 interface belongs to the 192.168.1.0 network configured under RIP, R1 builds an update to send out that interface.
The update includes all networks known to R1 except the network of the interface. Finally, R1 builds an update to send to R2. Because of split horizon, R1 only includes the 192.168.1.0 network in the update.

Step 4: Discontinue the debug output with the `undebug all` command.

```
R1#undebug all
All possible debugging has been turned off
```