NETWORK ROUTING AND COMMUNICATION ALGORITHM

Atadjanova Nozima[1], Khudoyorkhon Jamolov[2], Kamola Ahmadova[3], Javliev Shakhzod[4]
[1]TATU senior teacher
[2,3,4]TATU assistant

https://doi.org/10.5281/zenodo.7517416

Abstract. *Analysis of network routing and communication algorithms. Analyze physical and logical topologies Analyze network speed and analysis of cost indicators.*

Key word: *topology, networks, applications, security, switch, routers, Cisco devices, system software, router rip, protocols.*

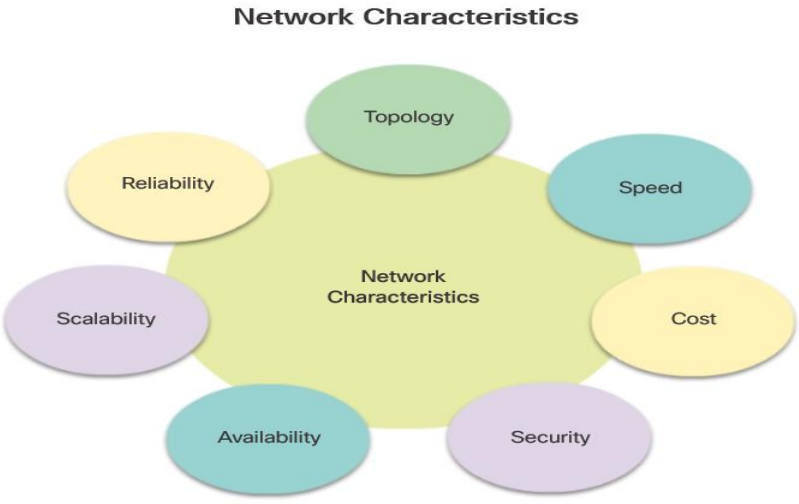
Characteristics of a Network

Networks have had a significant impact on our lives. They have changed the way we live, work, and play.

Networks allow us to communicate, collaborate, and interact in ways we never did before. We use the network in a variety of ways, including web applications, IP telephony, video conferencing, interactive gaming, electronic commerce, education, and more.

As shown in the figure, there are many key structures and performance-related characteristics referred to when discussing networks:

- **Topology** - There are physical and logical topologies. The physical topology is the arrangement of the cables, network devices, and end systems. It describes how the network devices are actually interconnected with wires and cables. The logical topology is the path over which the data is transferred in a network. It describes how the network devices appear connected to network users.
- **Speed** - Speed is a measure of the data rate in bits per second (b/s) of a given link in the network.

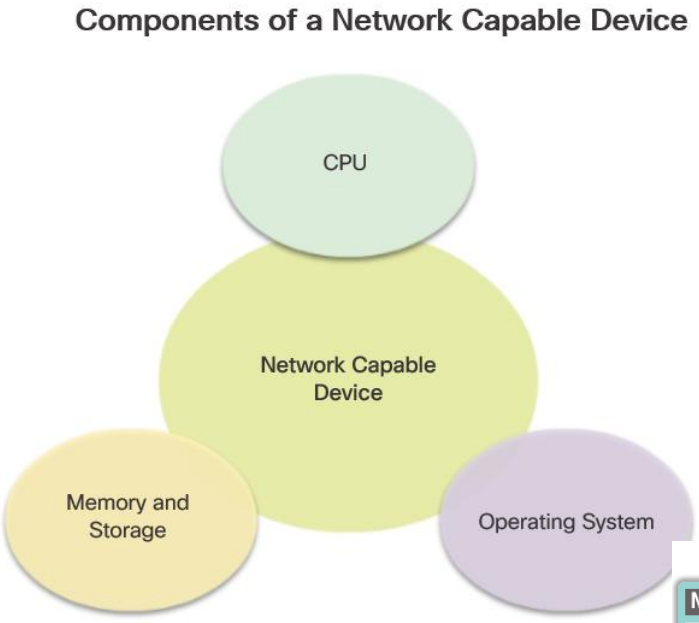


- **Cost** - Cost indicates the general expense for purchasing of network components, and installation and main-tenance of the network.
- **Security** - Security indicates how protected the network is, including the information that is transmitted over the network. The subject of security is important, and techniques and practices are constantly evolving. Consider security whenever actions are taken that affect the network.
- **Availability** - Availability is the likelihood that the network is available for use when it is required.

- **Scalability** - Scalability indicates how easily the network can accommodate more users and data transmission requirements. If a network design is optimized to only meet current requirements, it can be very difficult and expensive to meet new needs when the network grows.
- **Reliability** - Reliability indicates the dependability of the components that make up the network, such as the routers, switches, PCs, and servers. Reliability is often measured as a probability of failure or as the mean time between failures (MTBF).

Routers Are Computers

Most network capable devices (e.g.., computers, tablets, and smartphones) require the following components to operate, as shown in Figure 1:



- Central processing unit (CPU)
- Operating system (OS)
- Memory and storage (RAM, ROM, NVRAM, Flash, hard drive)

A router is essentially a specialized computer. It requires a CPU and memory to temporarily and permanently store data to execute operating system instructions, such as system initialization, routing functions, and switching functions.

Note: Cisco devices use the Cisco Internetwork Operating System (IOS) as the system software.

Router memory is classified as volatile or non-volatile. Volatile memory loses its content when the power is turned off, while non-volatile memory does not lose its content when the power is turned off.

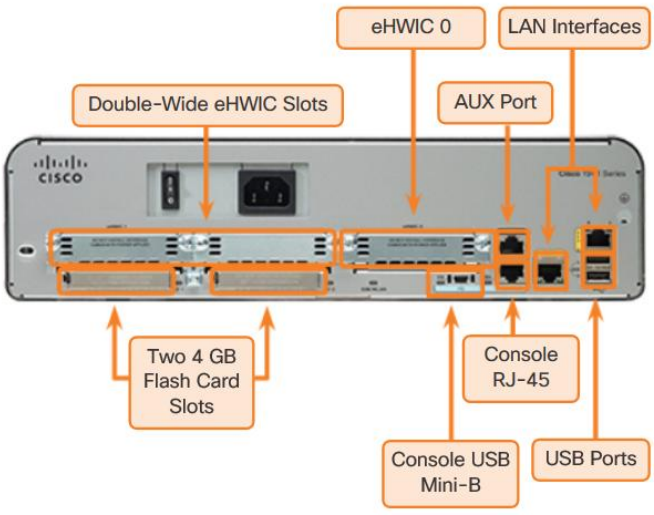
The table in Figure 2 summarizes the types of router memory, the volatility, and examples of what is stored in each.

Router Memory

Memory	Description
Random Access Memory (RAM)	Volatile memory that provides temporary storage for various applications and processes including: • Running IOS • Running configuration file • IP routing and ARP tables • Packet buffer
Read-Only Memory (ROM)	Non-volatile memory that provides permanent storage for: • Bootup instructions • Basic diagnostic software • Limited IOS in case the router cannot load the full featured IOS
Non-Volatile Random Access Memory	Non-volatile memory that provides permanent storage for the: • Startup configuration file

Unlike a computer, a router does not have video adapters or sound card adapters. Instead, routers have specialized ports and network interface cards to interconnect devices to other networks. Figure 3 identifies some of these ports and interfaces.

Back Panel of a Router

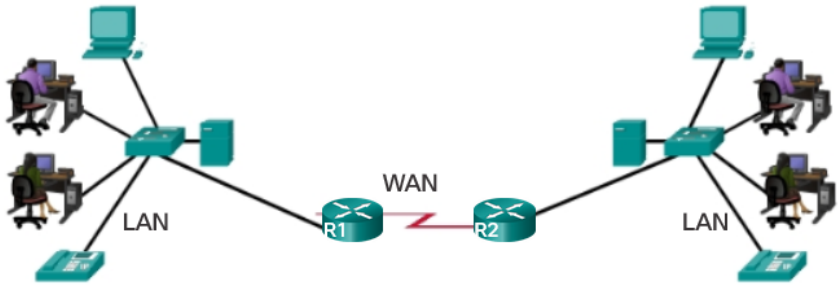


Routers Interconnect Networks

Most users are unaware of the presence of numerous routers on their own network or on the Internet. Users expect to

be able to access web pages, send emails, and download music, regardless of whether the server accessed is on their own network or on another network. Networking professionals know that 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, which 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 to the destination. The interface that the router uses to forward the packet may be the final destination, or it may be a network connected to another router that is used to reach the destination network.



R1 and R2 are responsible for receiving the packet on one network and forwarding the packet out another network toward 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.

Packet Forwarding Mechanisms

Routers support three packet-forwarding mechanisms:

- **Process switching** - An older packet forwarding mechanism still available for Cisco routers. When a packet arrives on an interface, it is forwarded to the control plane where the CPU matches the destination address with an entry in its routing table, and then determines the exit interface and forwards the packet. It is important to understand that the router does this for every packet, even if the destination is the same for a stream of packets. This process-switching mechanism is very slow and rarely implemented in modern networks.
- **Fast switching** - This is a common packet forwarding mechanism which uses a fast-switching cache to store next-hop information. When a packet arrives on an interface, it is forwarded to the control plane where the CPU searches for a match in the fast-switching cache. If it is not there, it is process-switched and forwarded to the exit interface. The flow information for the packet is also stored in the fast-switching cache. If another packet going to the same destination arrives on an interface, the next-hop information in the cache is re-used without CPU intervention.
- **Cisco Express Forwarding (CEF)** - CEF is the most recent and preferred Cisco IOS packet-forwarding mechanism. Like fast switching, CEF builds a Forwarding Information Base (FIB), and an adjacency table. However, the table entries are not packet-triggered like fast switching but change-triggered such as when something changes in the network topology. Therefore, when a network has converged, the FIB and adjacency tables contain all the information a router would have to consider when forwarding a packet. The FIB contains pre-computed reverse lookups, next hop information for routes including the interface and Layer 2

information. Cisco Express Forwarding is the fastest forwarding mechanism and the preferred choice on Cisco routers.

Figures 5 to 7 illustrate the differences between the three packet-forwarding mechanisms. Assume that a traffic flow consisting of five packets are all going to the same destination. As shown in Figure 1, with process switching, each packet must be processed by the CPU individually. Contrast this with fast switching, as shown in Figure 6. With fast switching, notice how only the first packet of a flow is process-switched and added to the fast-switching cache. The next four packets are quickly processed based on the information in the fast-switching cache. Finally, in Figure 7, CEF builds the FIB and adjacency tables, after the network has converged. All five packets are quickly processed in the data plane.

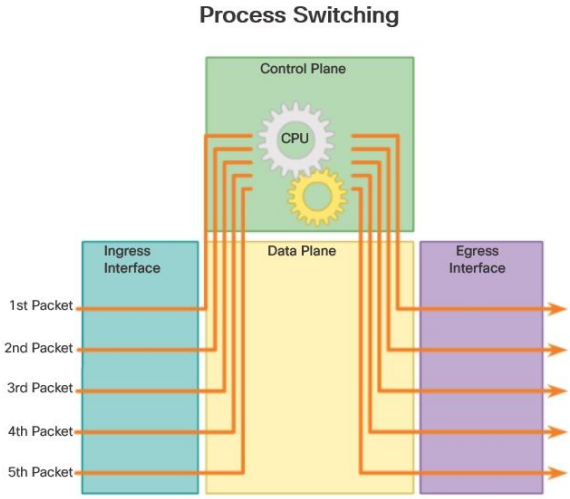


Figure 5

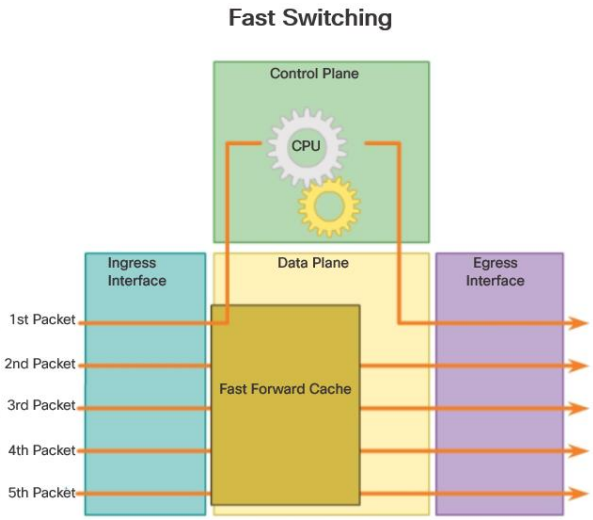


Figure 6

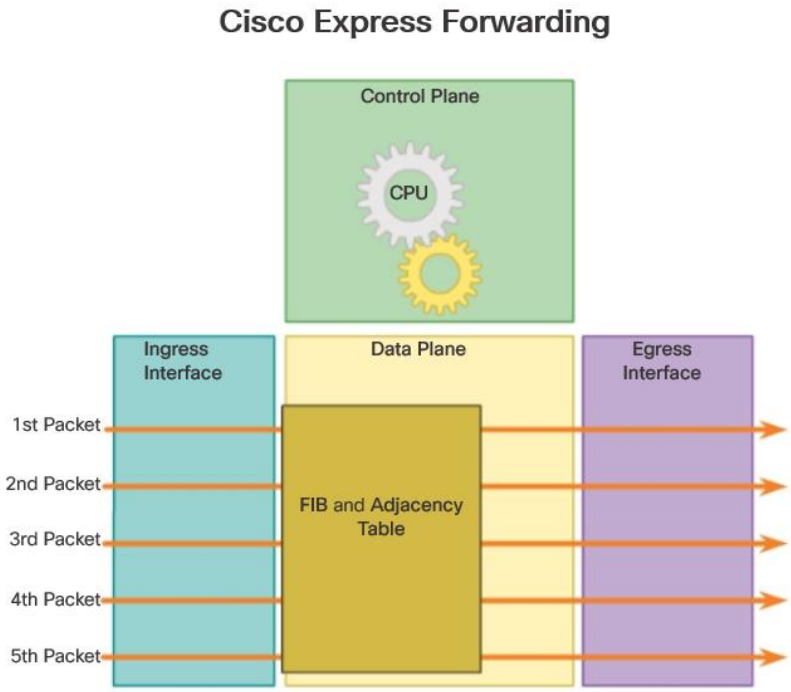


Figure 7

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

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

- Fast switching solves a problem by doing math long hand one time and remembering the answer for subsequent identical problems.
- CEF solves every possible problem ahead of time in a spreadsheet.

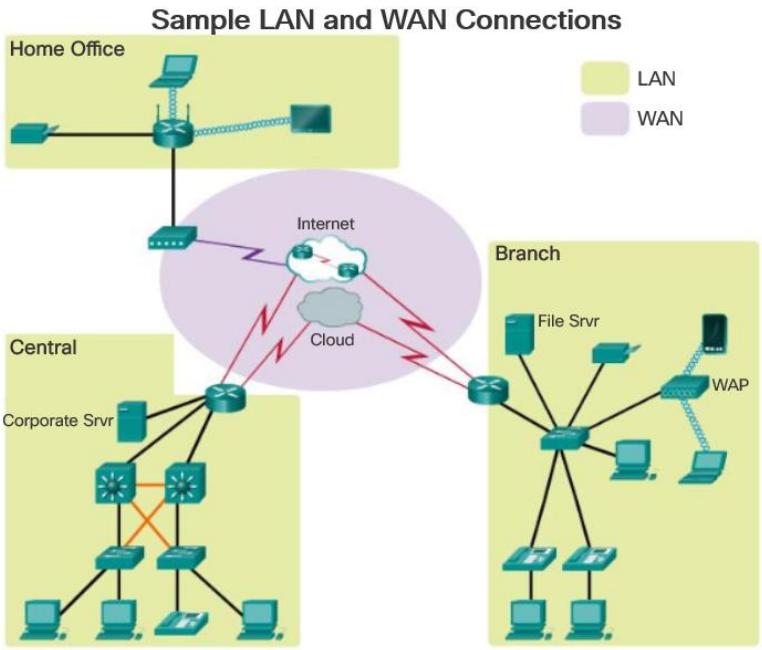
Connect to a Network

Network devices and end users typically connect to a network using a wired Ethernet or wireless connection. Refer to the figure as a sample reference topology. The LANs in the figure serve as an example of how users and network devices could connect to networks.

Home Office devices can connect as follows:

- Laptops and tablets connect wirelessly to a home router.
- A network printer connects using an Ethernet cable to the switch port on the home router.
- The home router connects to the service provider cable modem using an Ethernet cable.
- The cable modem connects to the Internet service provider (ISP) network.

The Branch site devices connect as follows:



- Corporate resources (i.e., file servers and printers) connect to Layer 2 switches using Ethernet cables.
- Desktop PCs and voice over IP (VoIP) phones connect to Layer 2 switches using Ethernet cables.
- Laptops and smartphones connect wirelessly to wireless access points (WAPs).
- The WAPs connect to switches using Ethernet cables.
- Layer 2 switches connect to an Ethernet interface on the edge router using Ethernet cables. An edge router is a device that sits at the edge or boundary of a network and routes between that network and another, such as between a LAN and a WAN.
- The edge router connects to a WAN service provider (SP).
- The edge router also connects to an ISP for backup purposes.

The Central site devices connect as follows:

- Desktop PCs and VoIP phones connect to Layer 2 switches using Ethernet cables.
- Layer 2 switches connect redundantly to multilayer Layer 3 switches using Ethernet fiber-optic cables (orange connections).
- Layer 3 multilayer switches connect to an Ethernet interface on the edge router using Ethernet cables.
- The corporate website server is connected using an Ethernet cable to the edge router interface.
- The edge router connects to a WAN SP.

- The edge router also connects to an ISP for backup purposes.

In the Branch and Central LANs, hosts are connected either directly or indirectly (via WAPs) to the network infrastructure using a Layer 2 switch.

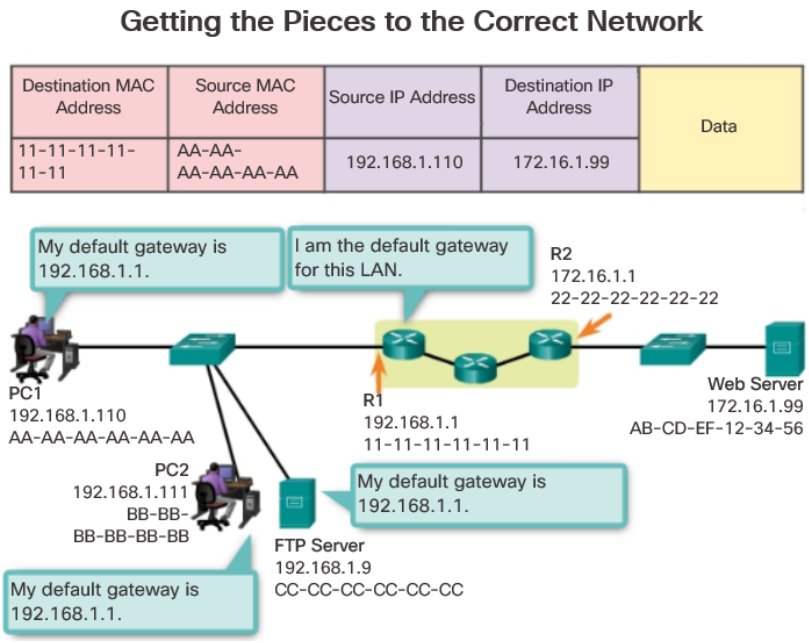
Default Gateways

To enable network access, devices must be configured with IP address information to identify the appropriate:

- **IP address** - Identifies a unique host on a local network.
- **Subnet mask** - Identifies with which network subnet the host can communicate.
- **Default gateway** - Identifies the IP address of the router to send a packet to when the destination is not on the same local network subnet.

When a host sends a packet to a device that is on the same IP network, the packet is simply forwarded out of the host interface to the destination device.

When a host sends a packet to a device on a different IP network, then the packet is forwarded to the default gateway, because a host device cannot communicate directly with devices outside of the local network. The default gateway is the destination that routes traffic from the local network to devices on remote networks. It is often used to connect a local network to the Internet.



The default gateway is usually the address of the interface on the router connected to the local network. The router maintains routing table entries of all connected networks as well as entries of remote networks, and determines the best path to reach those destinations.

For example, if PC1 sends a packet to the Web Server located at 176.16.1.99, it would discover that the Web Server is not on the local network and it, therefore, must send the packet to the Media Access Control (MAC) address of its default gateway. The Packet protocol data unit (PDU) in the figure identifies the source and destination IP and MAC addresses.

Static Routing

ip route Command

Static routes are configured using the **ip route** global configuration command. The basic syntax for the command is shown in the figure.

The following parameters are required to configure static routing:

- *network-address* - Destination network address of the remote network to be added to the routing table, often this is referred to as the prefix.

- *subnet-mask* - Subnet mask, or just mask, of the remote network to be added to the routing table. The subnet mask can be modified to summarize a group of networks.

One or both of the following parameters must also be used:

- *ip-address* - The IP address of the connecting router to use to forward the packet to the remote destination network. Commonly referred to as the next hop.
- *exit-intf* - The outgoing interface to use to forward the packet to the next hop.

The *distance* parameter is used to create a floating static route by setting an administrative distance that is higher than a dynamically learned route.

ip route Command Syntax

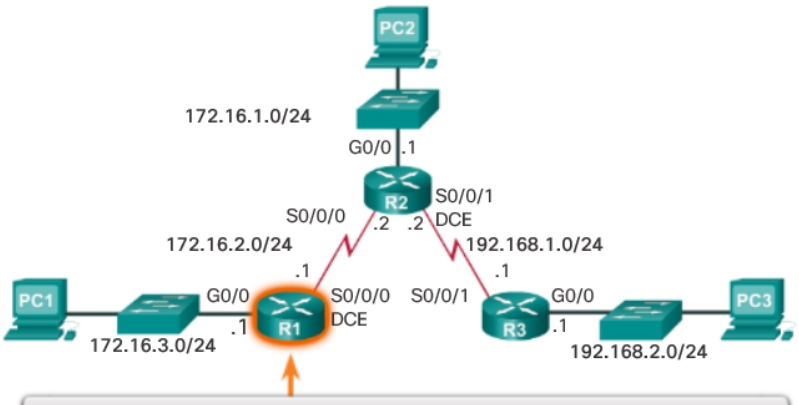
```
Router(config)# ip route network-address subnet-mask
{ip-address | exit-intf}
```

Parameter	Description
network-address	Destination network address of the remote network to be added to the routing table
subnet-mask	• Subnet mask of the remote network to be added to the routing table. • The subnet mask can be modified to summarize a group of networks.
ip-address	• Commonly referred to as the next-hop router's IP address. • Typically used when connecting to a broadcast media (i.e., Ethernet). • Commonly creates a recursive lookup

Verify a Default Static Route

In the figure, the **show ip route static** command output displays the contents of the static routes in the routing table. Note the asterisk (*)next to the route with code 'S'. As displayed in the Codes table in the figure, the asterisk indicates that this static route is a candidate default route, which is why it is selected as the Gateway of Last Resort.

Verifying the Routing Table of R1




```
R1# show ip route static
Codes: L - local, C - connected, S - static, 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, i - IS-IS,
       su - IS-IS summary, L1 - IS-IS level-1,
```

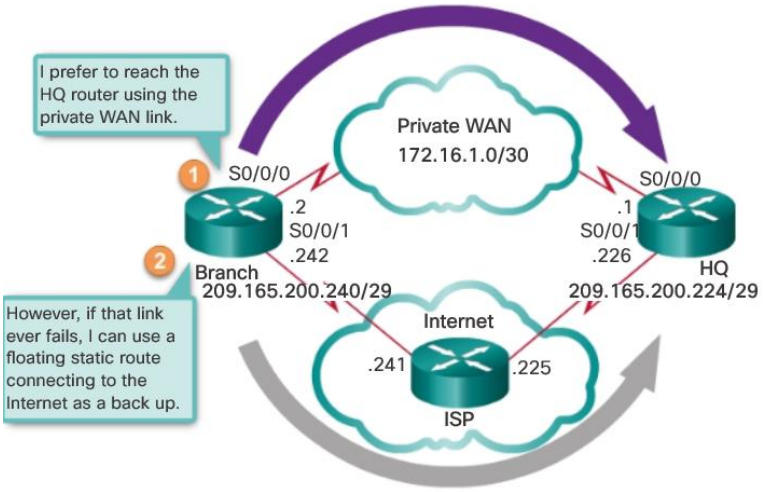
The key to this configuration is the /0 mask. The subnet mask in a routing table determines how many bits must match between the destination IP address of the packet and the route in the routing table. A binary 1 indicates that the bits must match. A binary 0 indicates that the bits do not have to match. A /0 mask in this route entry indicates that none of the bits are required to match. The default static route matches all packets for which a more specific match does not exist.

Floating Static Routes

Floating static routes are static routes that have an administrative distance greater than the administrative distance of another static route or dynamic routes. They are very useful when providing a backup to a primary link, as shown in the figure.

By default, static routes have an administrative distance of 1, making them preferable to routes learned from dynamic routing protocols. For example, the administrative distances of some common dynamic routing protocols are:

- EIGRP = 90
- IGRP = 100
- OSPF = 110
- IS-IS = 115
- RIP = 120



The administrative distance of a static route can be increased to make the route less desirable than that of another static route or a route learned through a dynamic routing protocol. In this way, the static route "floats" and is not used when the route with the better administrative distance is active. However, if the preferred route is lost, the floating static route can take over, and traffic can be sent through this alternate route.

Dynamic Routing

Router RIP Configuration Mode

Although RIP is rarely used in modern networks, it is useful as a foundation for understanding basic network routing. This section provides a brief overview of how to configure basic RIP settings and how to verify RIPv2.

Refer to the reference topology in Figure 8 and the addressing table in Figure 9. In this scenario, all routers have been configured with basic management features and all interfaces identified in the reference topology are configured and enabled. There are no static routes configured and no routing protocols enabled; therefore, remote network access is currently impossible. RIPv1 is used as the dynamic routing protocol. To enable RIP, use the **router rip** command, as shown in Figure 10. This command does not directly start the RIP process. Instead, it provides access to the router configuration mode where the RIP routing settings are configured. When enabling RIP, the default version is RIPv1.

To disable and eliminate RIP, use the **no router rip** global configuration command. This command stops the RIP process and erases all existing RIP configurations.

Figure 11 displays the various RIP commands that can be configured. The highlighted keywords are covered in this section.

Reference Topology

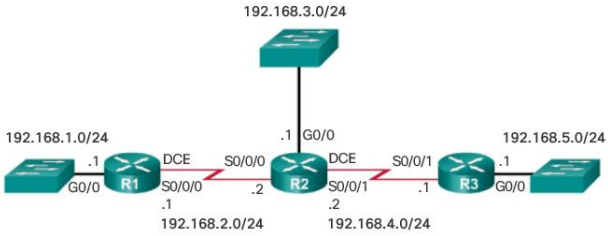


Figure 8

Addressing Table

Device	Interface	IP Address	Subnet Mask
R1	G0/0	192.168.1.1	255.255.255.0
	S0/0/0	192.168.2.1	255.255.255.0
R2	G0/0	192.168.3.1	255.255.255.0
	S0/0/0	192.168.2.2	255.255.255.0
	S0/0/1	192.168.4.2	255.255.255.0
R3	G0/0	192.168.5.1	255.255.255.0
	S0/0/1	192.168.4.1	255.255.255.0

Figure 9

Entering Routing Configuration Mode

```
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# router rip
R1(config-router)#
```

Figure 10

RIP Configuration Options

```
R1(config-router)# ?
Router configuration commands:
 address-family          Enter Address Family command mode
 auto-summary            Enable automatic network
                         number summarization
 default                 Set a command to its defaults
 default-information     Control distribution of
                         default information
 default-metric          Set metric of redistributed
                         routes
 distance                Define an administrative
                         distance
 distribute-list         Filter networks in routing
                         updates
 exit                    Exit from routing protocol
                         configuration mode
 flash-update-threshold  Specify flash update
                         threshold in second
 help                    Description of the
                         interactive help system
 input-queue             Specify input queue depth
 maximum-paths           Forward packets over multiple
                         paths
```

Figure 11

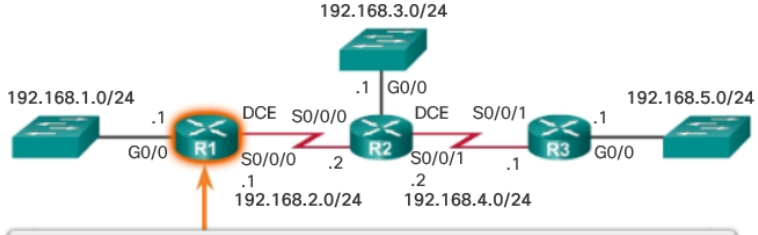
Advertise Networks

By entering the RIP router configuration mode, the router is instructed to run RIPv1. But the router still needs to know which local interfaces it should use for communication with other routers, as well as which locally connected networks it should advertise to those routers.

To enable RIP routing for a network, use the **network** *network-address* router configuration mode command. Enter the classful network address for each directly connected network. This command:

- Enables RIP on all interfaces that belong to a specific network. Associated interfaces now both send and receive RIP updates.
- Advertises the specified network in RIP routing updates sent to other routers every 30 seconds.

Advertising the R1 Networks




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

Note: RIPv1 is a classful routing protocol for IPv4. Therefore, if a subnet address is entered, the IOS automatically converts it to the classful network address. For example, entering the **network 192.168.1.32** command would automatically be converted to **network 192.168.1.0** in the running configuration

file. The IOS does not give an error message, but instead corrects the input and enters the classful network address.

The **network** command is used to advertise the R1 directly connected networks.

Verify RIP Routing

The **show ip protocols** command displays the IPv4 routing protocol settings currently configured on the router. This output displayed in Figure 1 confirms most RIP parameters including:

1. RIP routing is configured and running on router R1.
2. The values of various timers; for example, the next routing update, is sent by R1 in 16 seconds.
3. The version of RIP configured is currently RIPv1.
4. R1 is currently summarizing at the classful network boundary.
5. The classful networks are advertised by R1. These are the networks that R1 includes in its RIP updates.
6. The RIP neighbors are listed, including their next-hop IP address, the associated AD that R2 uses for updates sent by this neighbor, and when the last update was received from this neighbor.

Verifying RIP Settings on R1

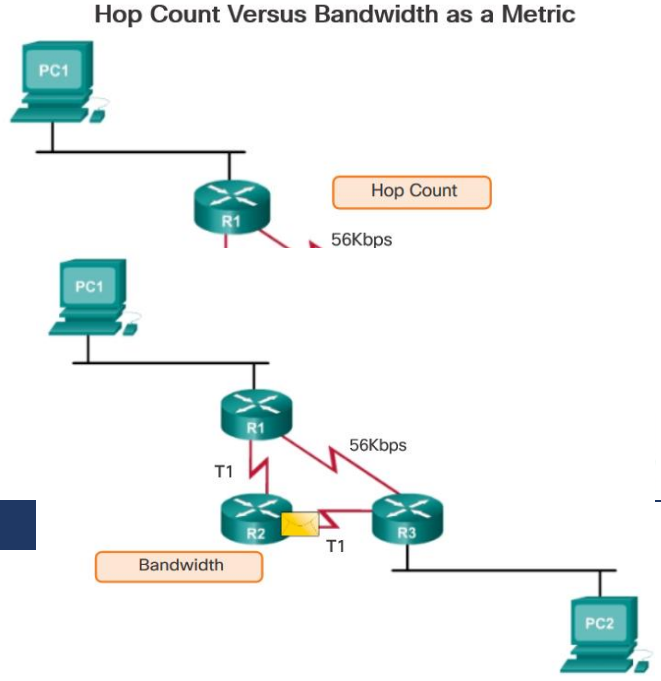
```
R1# show ip protocols
*** IP Routing is NSF aware ***

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

  Default version control: send version 1, receive any version
    Interface              Send  Recv  Triggered RIP  Key-chain
    GigabitEthernet0/0     1     1 2
    Serial0/0/0            1     1 2

  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    192.168.1.0
    192.168.2.0

  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.2.2          120      00:00:15
  Distance: (default is 120)

R1#
```

Best Path

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

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

Dynamic routing protocols typically use their own rules and metrics to build and update routing tables. The



routing algorithm generates a value, or a metric, for each path through the network. Metrics can be based on either a single characteristic or several characteristics of a path. Some routing protocols can base route selection on multiple metrics, combining them into a single metric.

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

- **Routing Information Protocol (RIP)** - Hop count
- **Open Shortest Path First (OSPF)** - Cisco's cost based on cumulative bandwidth from source to destination
- **Enhanced Interior Gateway Routing Protocol (EIGRP)** - Bandwidth, delay, load, reliability

REFERENCES

1. Bishop, M. Computer Security. Reading, MA: Addison-Wesley, 2003.
2. Couch, L. Digital and Analog Communication Systems. Upper Saddle River, NJ: Prentice Hall, 2000.
3. Forouzan, B. Local Area Networks. New York, NY: McGraw-Hill, 2003
4. Halsall, F. Multimedia Communication. Reading, MA: Addison-Wesley, 2001.
5. Stallings, W. DataAnd Computer Communications. Upper Saddle River, NJ: Prentice Hall, 2004.
6. Н.Олифер, В.Олифер: Компьютерные сети 2016.г