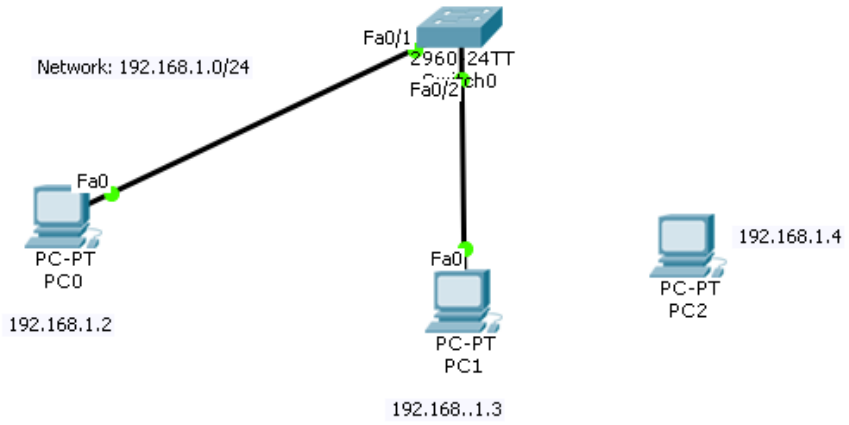
Packet Tracer - Configuring Port Security

Topology:



By using port security, you can limit the number of MAC addresses that can be assigned dynamically to a port, set static MAC addresses, and—here's my favorite part—set penalties for users who abuse your policy!

Table 26-2 Actions When Port Security Violation Occurs

Option on the switchport port-security violation Command	Protect	Restrict	Shutdown
Discards offending traffic	Yes	Yes	Yes
Sends log and SNMP messages	No	Yes	Yes
Disables the interface, discarding all traffic	No	No	Yes

Learning Objectives

- Configure IP address for PC.
- Configure dynamic port security.
- Test dynamic port security.

Part-1: Configure basic port security on port Fa0/1.

- **Step 1: Enable VLAN 1.**

  Packet Tracer opens with the VLAN 1 interface in the down state, which is not how an actual switch operates. You must enable VLAN 1 with the **no shutdown** command before the interface becomes active in Packet Tracer.

```
S1(config)# interface vlan 1

S1(config-if)# no shutdown
```

- **Step 2: Configure basic port security on port Fa0/1.**
  Set the maximum number of learned MAC addresses to **2**, allow the MAC address to be learned dynamically, and set the violation to **shutdown**.

  Note: A switch port must be configured as an access port to enable port security.

```
Switch> enable

Switch# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Switch(config)# interface fa0/1

Switch(config-if)# switchport mode access

Switch(config-if)# switchport port-security

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

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

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

- **Step 3: Verify port security.**

```
Switch#
Switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)         (Count)
---------------------------------------------------------------------
        Fa0/1        2           0                0          Shutdown
---------------------------------------------------------------------
Switch#
Switch#
Switch#show port-security interface fa0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0

Switch#
Switch#
```

Part-2: Configure Dynamic Port Security FastEthernet 0/2

- **Step 1: Enter interface configuration mode for FastEthernet 0/2 and enable port security.**

  Before any other port security commands can be configured on the interface, port security must be enabled.

```
Switch(config)# interface fa0/2

Switch(config-if)# switchport mode access

Switch(config-if)# switchport port-security
```

  Notice that you do not have to exit back to global configuration mode before entering interface configuration mode for fa0/2.

- **Step 2: Configure the maximum number of MAC addresses.**

  To configure the port to learn only one MAC address, set the **maximum** to **1**:

```
Switch(config-if)# switchport port-security maximum 1
```

- **Step 3: Configure the port to add the MAC address to the running configuration.**

  The MAC address learned on the port can be added to ("stuck" to) the running configuration for that port.

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

- **Step 4: Configure the port to automatically shut down if port security is violated.**

  If you do not configure the following command, Switch0 only logs the violation in the port security statistics but does not shut down the port.

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

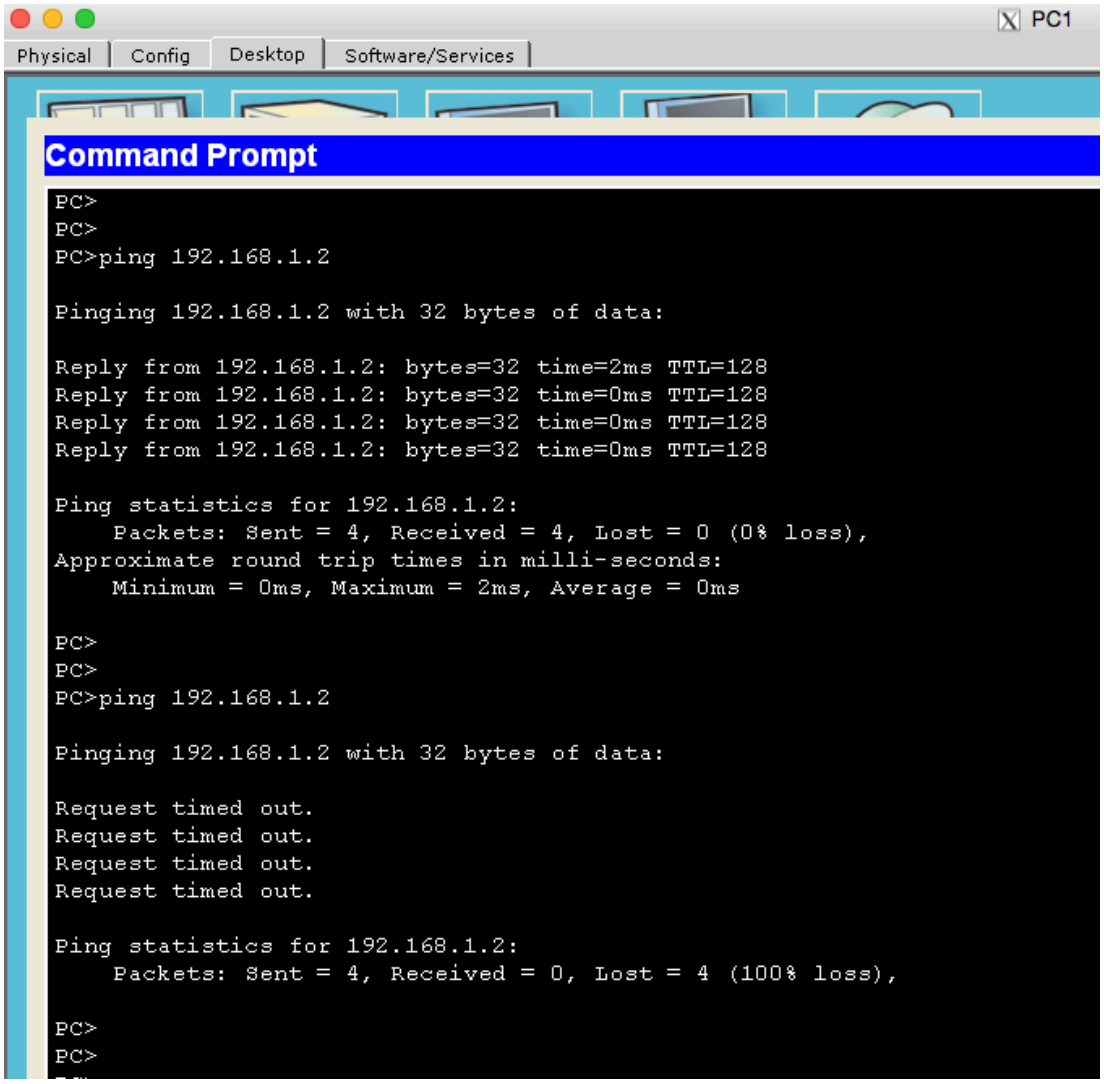
- **Step 5: Confirm that S1 has learned the MAC address.**

```
Switch#show port
Switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
---------------------------------------------------------------------
        Fa0/1        2           0                0          Shutdown
        Fa0/2        1           0                0          Shutdown
---------------------------------------------------------------------
Switch#
Switch#show run
Switch#show running-config
Building configuration...

Current configuration : 1261 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
!
interface FastEthernet0/2
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
```

- **Step 6: Test Dynamic Port Security**

  - To test port security, ping from PC1 to PC2.
  - Delete the Ethernet connection between PC1 and S1 and simply reconnect PC2 to Fa0/2 on Switch0. Wait for the amber link light to turn green and then ping from PC2 to PC2. The port should then automatically shut down.



- **Step 7: Restore the connection between PC1 and S1 and reset port security.**

  - Remove the connection between PC2 and Switch0. Reconnect PC1 to the Fa0/2 port on Switch0.

  - Notice that the port is still down even though you reconnected the PC1 that is allowed on the port. A port that is in the down state because of a security violation must be manually reactivated. Shut down the port and then activate it with **no shutdown**.

University of Technology – Iraq
Computer Engineering Department

Experiment 2
Port Security PART 2

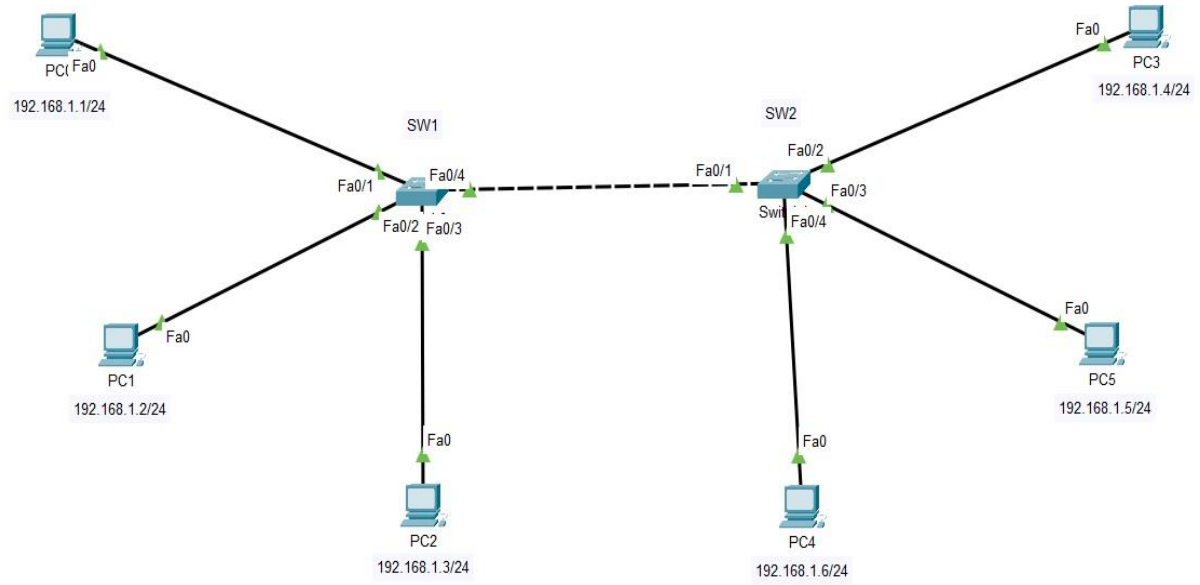
Dr. Ameer Mosa Al-Sadi **M.Sc. Ali E. Al Bayati**

2022- 2021

Network Laborator

Port Security – Configuring Port Security part 2

Topology:



Learning Objectives

- Configure IP address for PC.
- Configure dynamic port security.
- Test dynamic port security.

Overview

When configuring the security for a network, it is important to take advantage of the security features of all deployed devices. One of the security features available with Cisco switches (among other vendors) is switchport security. While the name of this feature is a bit vague, it makes it possible to limit the number and type of devices that are allowed on the individual switchports. This article takes a look at the concepts behind the switchport security feature.

Switchport Violations

Before getting into the mechanics of how switchport security operates; it is important to review what happens should a violation occur. On Cisco equipment there are three different main violation types: shutdown, protect, and restrict. These are described in more detail below:

- **Shutdown** – When a violation occurs in this mode, the switchport will be taken out of service and placed in the err-disabled state. The switchport will remain in this state until manually removed; this is the default switchport security violation mode.

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

- **Protect –** When a violation occurs in this mode, the switchport will permit traffic from known MAC addresses to continue sending traffic while dropping traffic from unknown MAC addresses. When using this mode, no notification message is sent when this violation occurs.

  ```
  Switch(config-if)# switchport port-security violation Protect
  ```

- **Restrict –** When a violation occurs in this mode, the switchport will permit traffic from known MAC addresses to continue sending traffic while dropping traffic from unknown MAC addresses. However, unlike the protect violation type, a message is also sent indicating that a violation has occurred.

  ```
  Switch(config-if)# switchport port-security violation Restrict
  ```

Switchport Security MAC Addresses

When using the switchport security feature, source MAC addresses are separated into three different categories, these include:

- **Static –** Static secure MAC addresses are statically configured on each switchport and stored in the address table. The configuration for a static secure MAC address is stored in the running configuration by default and can be made permanent by saving them to the startup configuration.

- **Dynamic –** Dynamic secure MAC addresses are learned from the device (or devices) connected to the switchport. These addresses are stored in the address table only and will be lost when the switchport state goes down or when the switch reboots.

- **Sticky –** Sticky secure MAC addresses are a hybrid. They are learned dynamically from the devices connected to the switchport, are put into the address table AND are entered into the running configuration as a static secure MAC address.

commands Configure:

SW1:

To show your Mac-address **PC → DESKTOP→ Command prompt → ipconfig /all**

```
Switch# conf t
Switch(config)# interface fa0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security violation shutdown
Switch(config-if)# switchport port-security mac-address sticky

Switch(config)# interface fa0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security violation shutdown
Switch(config-if)#end
Switch# clear mac-address table
Switch# conf t
Switch(config)# interface fa0/2
Switch(config-if)# switchport port-security mac-address ????

Switch(config)# interface fa0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security violation shutdown
Switch(config-if)#end
Switch# clear mac-address table
Switch# conf t
Switch(config)# interface fa0/3
Switch(config-if)# switchport port-security mac-address ????
```

Or we can shorten the command lines above with the commands below

```
Switch# conf t
Switch(config)# interface range fa0/1-3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address OR sticky
Switch(config-if)#  switchport port-security violation shutdown OR
Restrict OR Protect


Switch(config)# interface fa0/4            (TRUNK PORT)
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 3 (ANY NUMBER
YOU CAN USE)
Switch(config-if)# switchport port-security mac-address OR sticky
Switch(config-if)#  switchport port-security violation shutdown OR
Restrict OR Protect
```

SW2:

```
Switch# conf t
Switch(config)# interface fa0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security violation Restrict
Switch(config-if)# switchport port-security mac-address sticky

Switch(config)# interface fa0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security violation Restrict
Switch(config-if)#end
Switch# clear mac-address table
Switch# conf t
Switch(config)# interface fa0/3
Switch(config-if)# switchport port-security mac-address ?????

Switch(config)# interface fa0/4
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security violation Protect
Switch(config-if)#end
Switch# clear mac-address table
Switch# conf t
Switch(config)# interface fa0/4
Switch(config-if)# switchport port-security mac-address ?????

Switch(config)# interface fa0/1     (TRUNK PORT)
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 3 (ANY NUMBER
YOU CAN USE)
Switch(config-if)# switchport port-security mac-address OR sticky
Switch(config-if)#  switchport port-security violation shutdown OR
Restrict OR Protect
```

important commands:

To show the status of the port:

1- Switch# **Show port security interface fa0/?**

2- Switch# **Show port security**

3- Switch# **Show interface fa0/?**

to show the commands that were previously written:

Switch# **show running-config**

To check the status of the port, if it is static or dynamic:

Switch# **show mac-address-table**

University of Technology – Iraq
Computer Engineering Department

Experiment no.3

Constructing WAN

“(1) Single Router”

Dr. Ameer Mosa Al-Sadi M.Sc. Ali E. Al Bayati

2021-2022

Network Laboratory

3.1 Introduction to Wide Area Network (WAN)

A WAN is a data communications network that covers a relatively wide geographic area and often uses transmission facilities provided by public carriers, such as telephone companies. WAN technologies operate in the lower three layers of the OSI reference model: (the physical layer, the data link layer, and the network layer), So in simply a wide area network (WAN) is a collection of local area networks (LANs) or other networks that communicate with each other.so will explain some experiments of WAN.

3.2 WAN with single Router

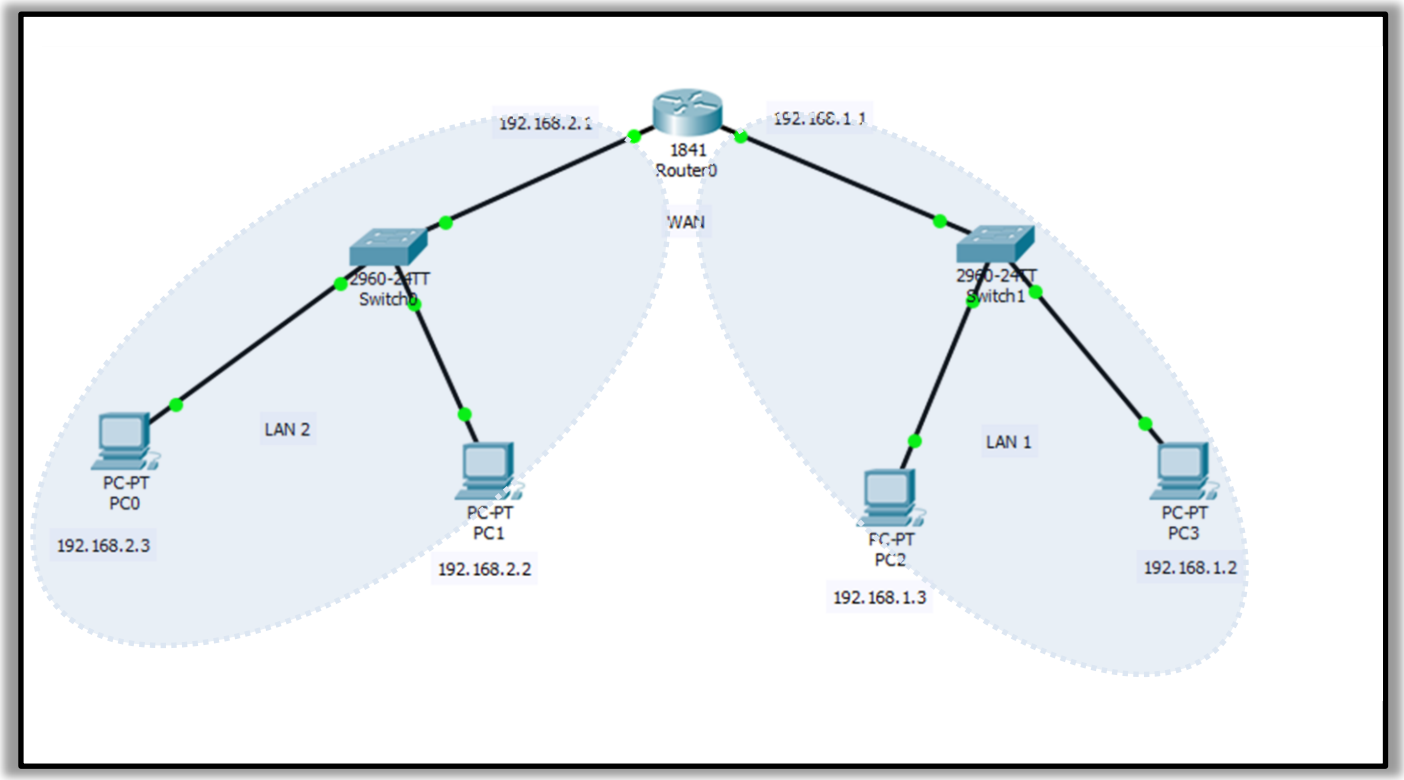


Figure (1) : WAN with Single Router.

In this Figure Connected two LANs using the Single Router.

Now will explain how to connect this topology in the follow steps:

Step 1: Connect the topology according to Figure 1.

Step2: Now we should enter to the Router's settings and configure it to work

configuration on router

Router> enable

Router# configuration terminal

Router(config)# interface fastEthernet 0/0

Router(config-if)#ip address 192.168.1.1 255.255.255.0

Router(config-if)#no shutdown

Router(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

Router(config-if)#exit

Router(config)#interface fastEthernet 0/1

Router(config-if)#ip address 192.168.2.1 255.255.255.0

Router(config-if)#no shutdown

Router(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

Router(config-if)#exit

Step 3: Now we should configure each PCs connected to the router.

(PC IP address same domain of gateway IP address)

The IP address assigned to the PCs connected to the router should be within the same range of the IP address of the router port, which it connects this LAN.

-Now configure the PCs by pressing double click to each pc and then the window will appear choose Desktop as shown in Figure (3.3)

LAN2: gateway IP= 192.168.***1***.1, So:

PC2: IP address 192.168.1.3 **subnet mask** 255.255.255.0 **gateway** 192.168.1.1

PC3: **IP address** 192.168.1.2 **subnet mask** 255.255.255.0 **gateway** 192.168.1.1

LAN2: gateway IP= 192.168.***2***.1, So:

PC0: IP address 192.168.2.3 **subnet mask** 255.255.255.0 **gateway** 192.168.2.1

PC1: **IP address** 192.168.2.2 **subnet mask** 255.255.255.0 **gateway** 192.168.2.1

Step3: Verify addressing

a. Issue the command to verify IPv4 assignments to the interfaces on R0.

```
R0# show ip interface brief
```

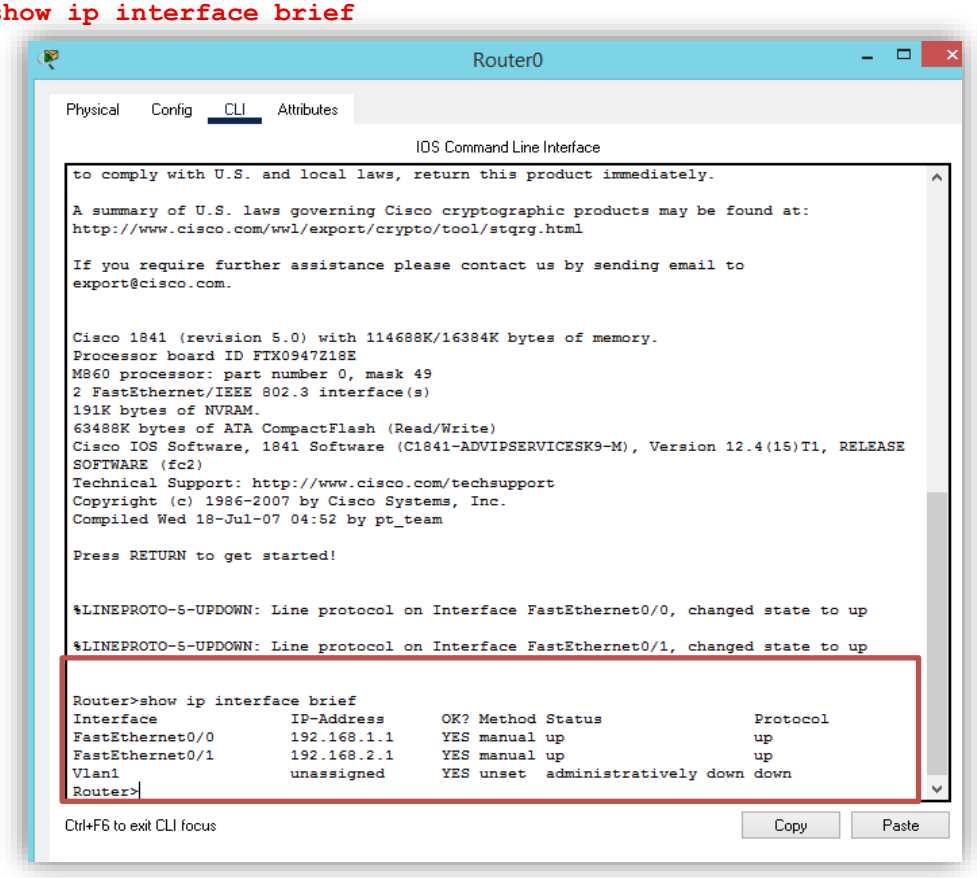


Figure (2): Implement command **show ip interface brief on "CLI" of "R0"**

Step4: Save your configuration

Save the running configuration to the startup configuration file on both routers.

```
R0> en      enter
R0# copy running-config startup-config
```

```
Router>en
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
```

Figure (3): Implement command **copy running-config startup-config on "CLI" of "R0"**

Step5: Now after we completed the saving, then we must make sure whether the connection was done correctly or not by:

A) using the ***ping tool (ping From PC0 to PC3)***:

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Figure (4): Ping to Check Connection.

If the ping work correctly, So, the connection was successful.

B) using PDU message ***From PC0 to PC3***:

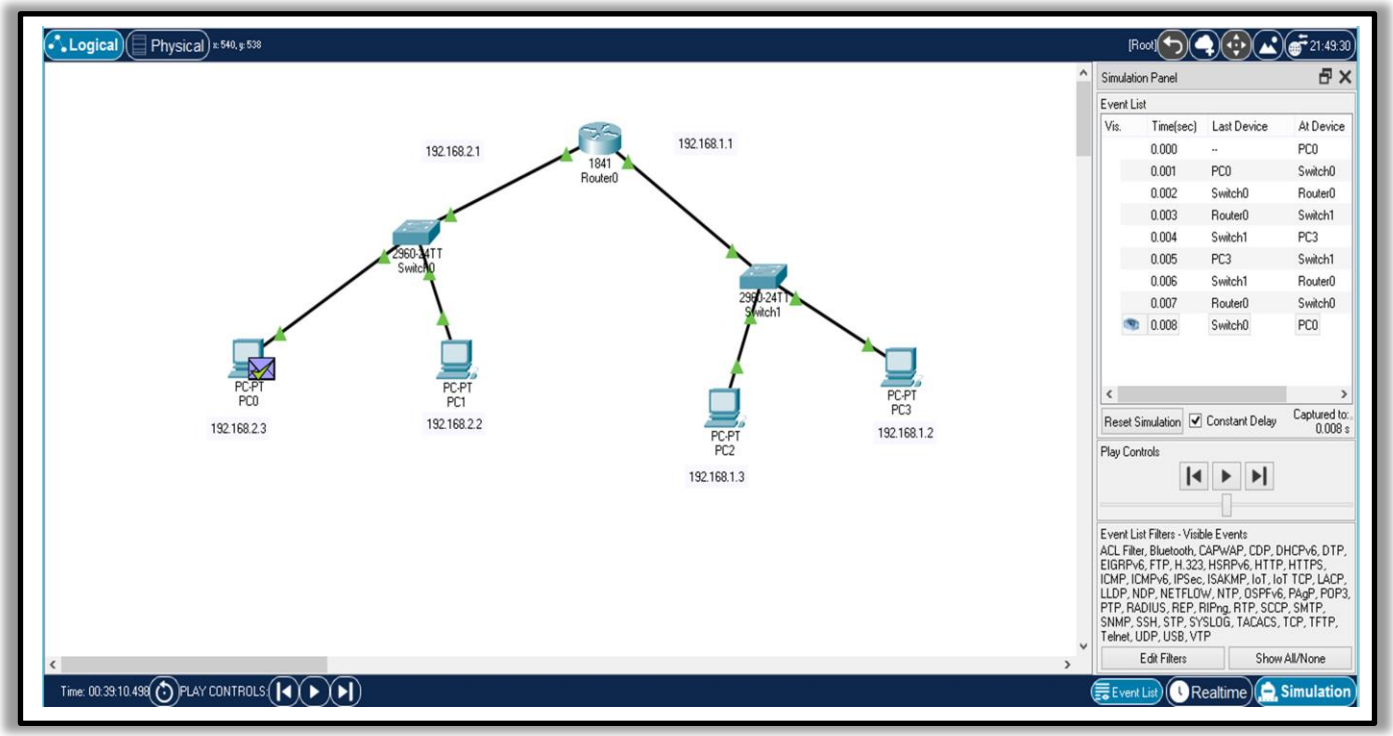


Figure (5): Simple PDU between PCs.

The connection was successful.

<u>Remark:</u> Why the routing is success without any type of routing configuration?

That happen because of Default Gateway

- If your local network has only one router, it will be the ***default gateway router*** and all hosts and switches on your network must be configured with this information.
- But, if your local network has multiple routers, you ***must select one of them to be the default gateway router***. This topic will be explained in the next experiments.

Acknowledgment:

This sheet and its attached configuration of experiments is produced by the help of the graduation project for the students

(Sara Chasib Jber) and (Ayaat Rikan Hameed)

In 2021

Under the supervision of Dr. Ameer Mosa Al-Sadi.

University of Technology – Iraq
Computer Engineering Department

Experiment no.4

Constructing WAN

"(1) Static and Default Routing"

Dr. Ameer Mosa Al-Sadi M.Sc. Ali E. Al Bayati

2021-2022

Network Laboratory

4.1 Routing algorithms

Routing is the process of creating the routes that data packets must follow to reach a destination. when the packet arrivals to router, the router have a forwarding table which contain the information about path to send data from source to destination.

Types of Routing:

There are two type of Routing:

- **Static and Default Routing:** is also known as non-adaptive routing which does not change the routing table if the network administrator doesn't change or modify it. Static routing does not use complex routing algorithms and provides more security than dynamic routing.
- **Dynamic Routing:** is also known as adaptive routing which change the routing table when the topology or traffic load changes. it uses complex routing algorithms and it does not provide high security like static routing.

4.2 Types Static and Default Routes

This section will only state the four types of Static and Default Routes, which will have explained in experiment below:

1. Recursive Static Route: A recursive static route relies on the next hop router in order for packets to be sent to its destination. A recursive static route requires two routing table lookups. (Example R1)
2. Directly Attached Static Route: A directly attached static route relies on its exit interface in order for packets to be sent to its destination, while a recursive static route uses the IP address of the next hop router. (Example R2)
3. Default Route: A default route, also known as the gateway of last resort, is the network route used by a router when no other known route exists for a destination network. A static route is used to route traffic to a specific network. (Example R3)
4. Fully Specified Route: A fully specified route is a static route that is configured with an exit interface and the next hop address.

4.3 Types Static and Default Routes

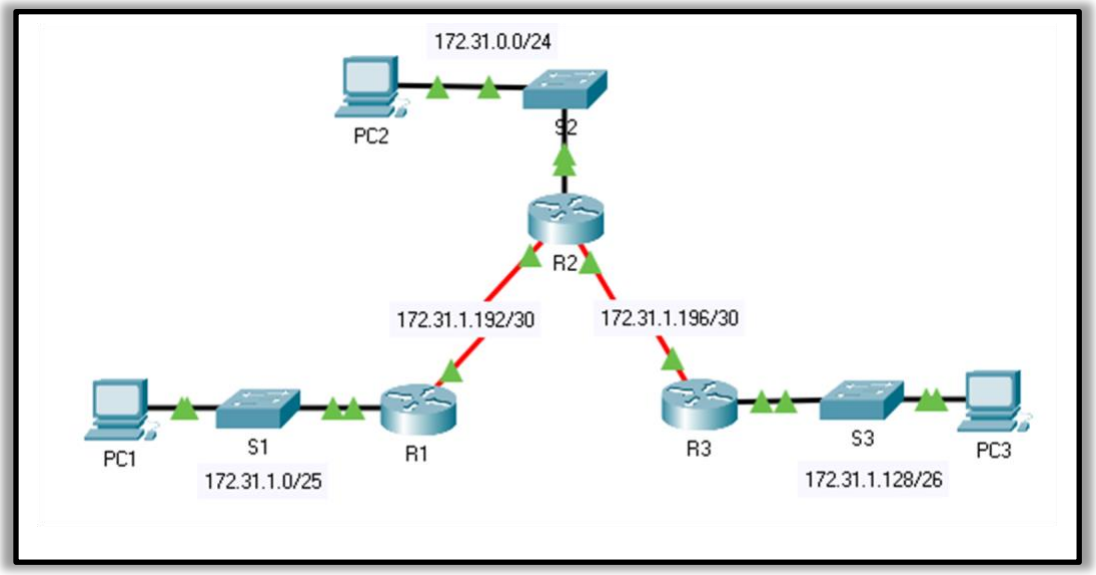


Figure (1): Used Topology.

In this Figure Connected Two Routers as table below

Addressing Table

Device	Interface	IPv4 Address	Subnet Mask	Default Gateway
R1	G0/0	172.31.1.1	255.255.255.128	N/A
	S0/0/0	172.31.1.194	255.255.255.252	N/A
R2	G0/0	172.31.0.1	255.255.255.0	N/A
	S0/0/0	172.31.1.193	255.255.255.252	N/A
	S0/0/1	172.31.1.197	255.255.255.252	N/A
R3	G0/0	172.31.1.129	255.255.255.192	N/A
	S0/0/1	172.31.1.198	255.255.255.252	N/A
PC1	NIC	172.31.1.126	255.255.255.128	172.31.1.1
PC2	NIC	172.31.0.254	255.255.255.0	172.31.0.1
PC3	NIC	172.31.1.190	255.255.255.192	172.31.1.129

Objectives

Setup topology: Cable the network as shown in the topology.
Part 1: Examine the Network and Evaluate the Need for Static Routing
Part 2: Configure Static and Default Routes
Part 3: Verify Connectivity

Background

In this activity, you will configure static and default routes. A static route is a route that is entered manually by the network administrator to create a reliable and safe route. There are four different static routes that are used in this activity: a recursive static route, a directly attached static route, a fully specified static route, and a default route.

Setup topology: Cable the network as shown in the topology.

you will set up the network topology and configure basic settings on the PC hosts and switches.

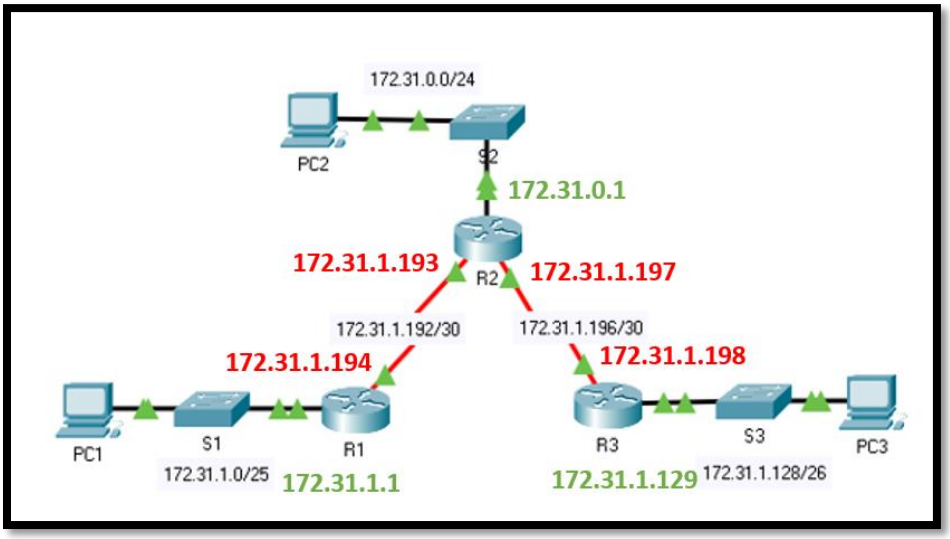


Figure (2): Show interfaces IPs.

Part 1: Examine the Network and Evaluate the Need for Static Routing

a. Looking at the topology diagram, how many networks are there in total? **5**

b. How many networks are directly connected to R1, R2, and R3? **R1 has 2, R2 has 3, and R3 has 2.**

c. How many static routes are required by each router to reach networks that are not directly connected? **R1 needs 3 static routes, R2 needs 2 static routes, and R3 needs 3 static routes.**

d. Test connectivity to the R2 and R3 LANs by pinging PC2 and PC3 from PC1.
Why were you unsuccessful? Because there are no routes to these networks on R1.

Part 2: Configure and verify IPv4 addressing on R1 and R2

Step 1: Configure recursive static routes on R1.

a. What is recursive static route? A recursive static route relies on the next hop router in order for packets to be sent to its destination. A recursive static route requires two routing table lookups.

b. Why does a recursive static route require two routing table lookups? It must first look in the routing table for the destination network and then look up the exit interface/direction of the network for the next hop router.

c. Configure a recursive static route to every network not directly connected to R1, including the WAN link between R2 and R3.

 # IP route <Destination Address> < Destination Mask > <via interface of next-hop>

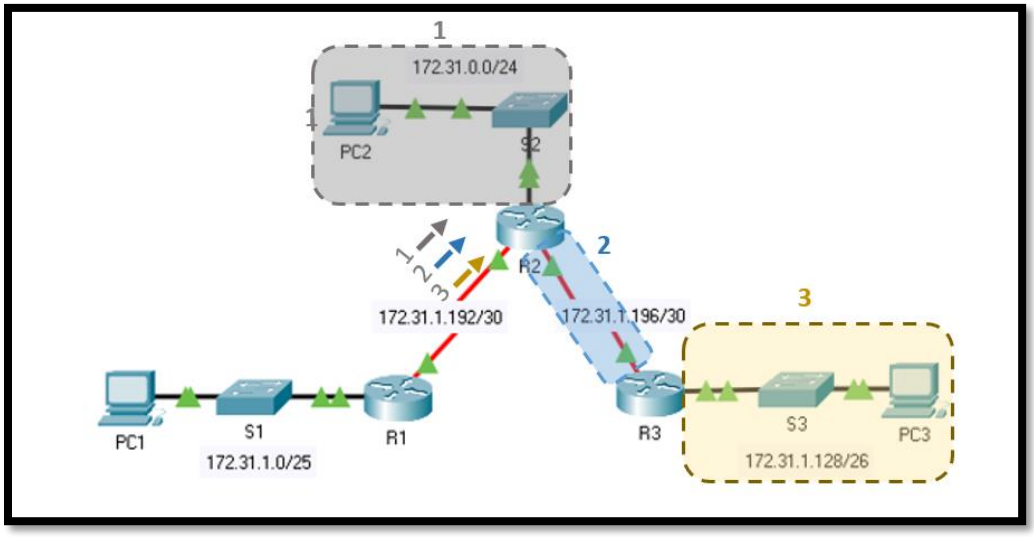


Figure (3): recursive static routes on R1.

- R1(config)# ip route 172.31.0.0 255.255.255.0 172.31.1.193
- R1(config)# ip route 172.31.1.196 255.255.255.252 172.31.1.193
- R1(config)# ip route 172.31.1.128 255.255.255.192 172.31.1.193

d. Test connectivity to the R2 LAN and ping the IP addresses of PC2 and PC3.

- Why were you unsuccessful? R1 has a route to the R2 and R3 LANs, but R2 and R3 do not have a routes to R1.

Step 2: Configure directly attached static routes on R2.

a. How does a directly attached static route differ from a recursive static route? A directly attached static route relies on its exit interface in order for packets to be sent to its destination, while a recursive static route uses the IP address of the next hop router.

b. Configure a directly attached static route from R2 to every network not directly connected.

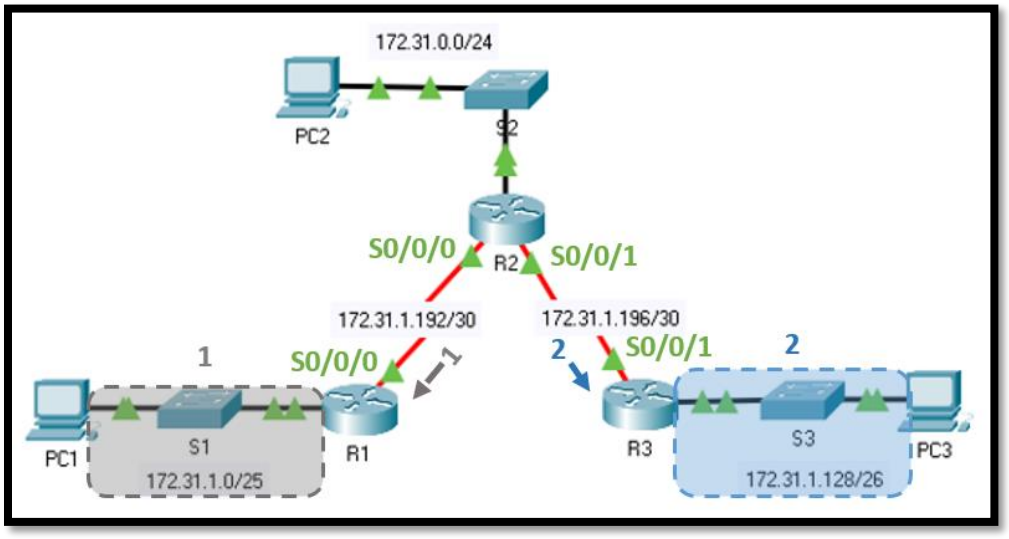


Figure (4): directly attached static routes on R2.

- R2(config)# ip route 172.31.1.0 255.255.255.128 Serial0/0/0
- R2(config)# ip route 172.31.1.128 255.255.255.192 Serial0/0/1

c. Which command only displays directly connected networks? show ip route connected

d. Which command only displays the static routes listed in the routing table? show ip route static

e. When viewing the entire routing table, how can you distinguish between a directly attached static route and a directly connected network? The static route has an S and a directly connected network has a C.

Step 3: Configure a default route on R3.

a. How does a default route differ from a regular static route? A default route, also known as the gateway of last resort, is the network route used by a router when no other known route exists for a destination network. A static route is used to route traffic to a specific network.

b. Configure a default route on R3 so that every network not directly connected is reachable.

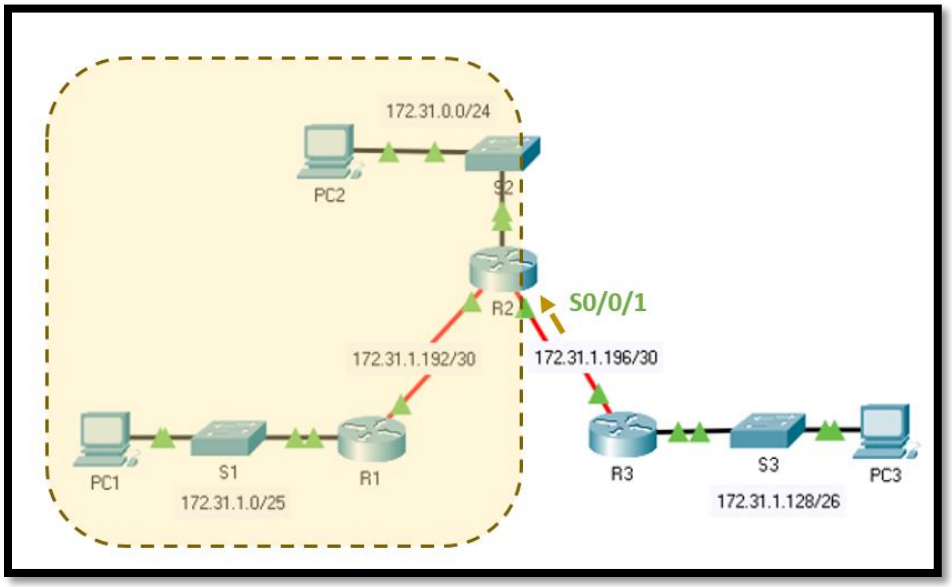


Figure (5): default route on R3.

- R3(config)# ip route 0.0.0.0 0.0.0.0 Serial0/0/1

c. How is a static route displayed in the routing table? S* 0.0.0.0/0

Step 4: Document the commands for fully specified routes.

Note: Packet Tracer does not currently support configuring fully specified static routes. Therefore, in this step, document the configuration for fully specified routes.

a. Explain a fully specified route. A fully specified route is a static route that is configured with an exit interface and the next hop address.

b. Which command provides a fully specified static route from R3 to the R2 LAN?

- R3(config)# ip route 172.31.0.0 255.255.255.0 s0/0/1 172.31.1.197

c. Write a fully specified route from R3 to the network between R2 and R1. Do not configure the route; just calculate it.

- R3(config)# ip route 172.31.1.192 255.255.255.252 s0/0/1 172.31.1.197

d. Write a fully specified static route from R3 to the R1 LAN. Do not configure the route; just calculate it.

- R3(config)# ip route 172.31.1.0 255.255.255.128 s0/0/1 172.31.1.197

Step 5: Verify static route configurations.

Use the appropriate **show** commands to verify correct configurations.

Which **show** commands can you use to verify that the static routes are configured correctly? show ip route, show ip route static, and the show ip route [network] commands

Part 3: Verify Connectivity

Every device should now be able to ping every other device. If not, review your static and default route configurations.

Acknowledgment:

This sheet and its attached configuration of experiments is produced by the help of the graduation project for the students

(Sara Chasib Jber) and (Ayaat Rikan Hameed)

In 2021

Under the supervision of Dr. Ameer Mosa Al-Sadi.

University of Technology – Iraq
Computer Engineering Department

Experiment no.5

Constructing WAN

“Dynamic Routing”

Distance Vector Protocol

Ex. Routing Information Protocol (RIP):

Dr. Ameer Mosa Al-Sadi M.Sc. Ali E. Al Bayati

2021-2022

Network Laboratory

5.1 Dynamic routing

Routing protocols are used to facilitate the exchange of routing information between routers without an administrator's help. A routing protocol is a set of processes, algorithms, and messages that are used to exchange routing information and populate the routing table with the routing protocol's choice of best paths. The purpose of dynamic routing protocols includes:

- Discovery of 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

Unlike static routing, the route needs to be reconfigured by the administrator in the event of any change.

Limitations of static routing:

- In large networks, configuring and adding a static route to the routing table is very difficult.
- Configuring static routes requires background knowledge of the network topology by the network administrator.
- Static route is error-prone.

5.2 Types of Dynamic Routing Protocols:

Dynamic routing protocols can be categorized into two groups:

Note: Any network under the administrative control of a single organization is known as **Autonomous System (AS)**.

1. **Interior Gateway Protocols (IGP)** - Used for routing within an Autonomous System (AS).
   A) Distance vector: RIP and IGRP.
   B) link-state: EIGRP, OSPF, and IS-IS.

2. **Exterior Gateway Protocols (EGP)** - Used for routing between Autonomous Systems, Such as, BGP.

.

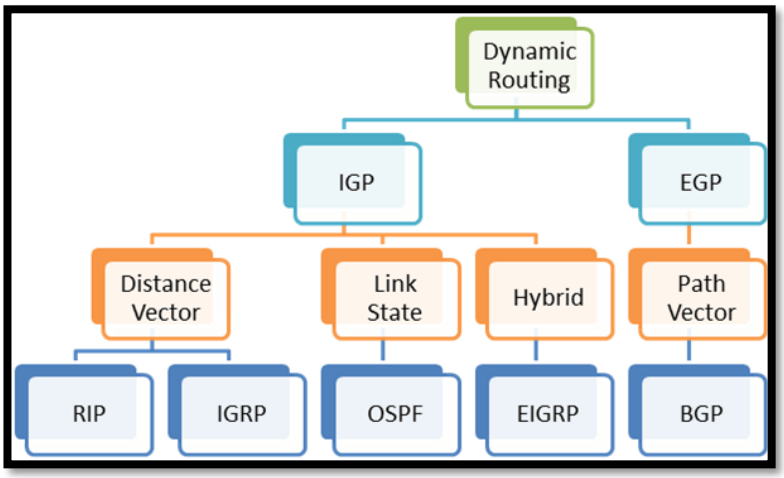


Figure (1): Tree of dynamic routing protocols.

No.	Distance vector	link-state
1	**Each router tells its neighbour what it knows about whole network.**	**each router tells the whole network what it knows about its neighbours**
2	**Based on count of hops**	**Based on accumulative Cost (BW, link length)**
3	**Send periodic update of entire table**	**Updates are sent only after a topology is changed.**
4	**Moderate convergence time**	**Low convergence time**
5	**Use Bellman-Ford Equation algorithm to calculate path**	**use Dijkstra algorithm to calculate path**

5.3 Metrics of Some Dynamic Routing Protocols:

1. **RIP** – Hop count
2. **OSPF** – the default Cost based on cumulative bandwidth, or can use any accumulative value such as link length.
3. **EIGRP** - Bandwidth, delay, load, and reliability

5.4 Example of Distance vector:

Routing Information Protocol (RIP):

an open routing protocol defined by the IETF. RIP is rarely used in today's production networks. It is a dynamic routing protocol that uses hop count as a routing metric to find the best path between the source and the destination network.

Characteristics:

- The metric is the number of hops to reach the destination.
- RIP has a maximum hop count of 15 and thus has a maximum network diameter in which it can function.
- A hop count of 16 indicates an unreachable network
- RIP is comparatively slow to converge
- RIP routers periodically exchange routing information every 30 seconds by default.
-

Forwarding table:

A forwarding table in RIP is a three-column table in which the first column is the address of the destination network, the second column is the cost (the number of hops) to reach the destination network, and the third column is the address of the next router to which the packet should be forwarded shown in Figure (2)

Figure (2): Forwarding Table in RIP.

This example of Distance vector:

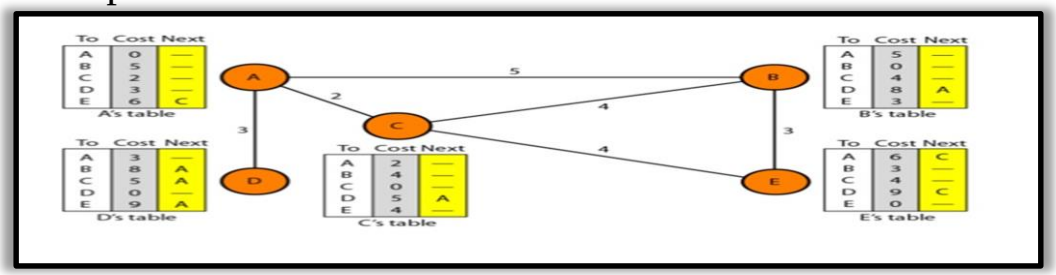


Figure (3) Example of Distance Vector.

5.5 Implementing RIP:

In this configuration we will use the routing protocol one of these routing protocol is Routing Information Protocol (RIP).

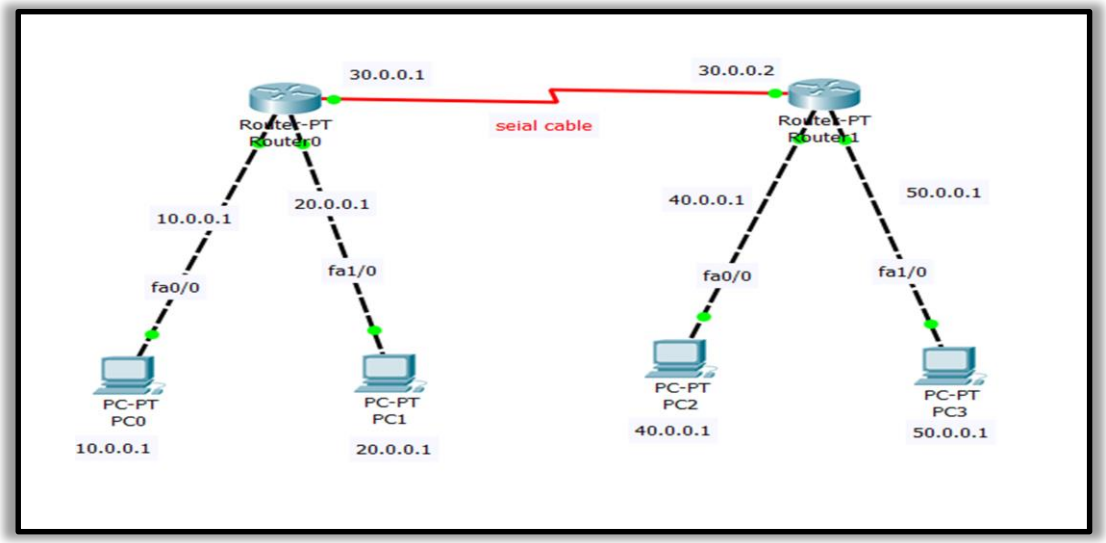


Figure (4): WAN with RIP.

To connect this topology, following this steps:

Step 1: take the devices into the working space and connect them with connectors.

Step 2: Configuration on-a-Stick – Router.

Router 0 :

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa0/0            //  to set IP to port Fast Ethernet 0/0.
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#no shut           //  to turn the port on .
```

```
Router(config-if)#int fa1/0          //  to set IP to port Fast Ethernet 1/0.
Router(config-if)#ip address 20.0.0.1 255.0.0.0
Router(config-if)#no shut            // to turn the port on.

Router(config-if)#int serial2/0      // to set IP to port serial 2/0.
Router(config-if)#ip address 30.0.0.1 255.0.0.0
Router(config-if)#no shut
```

Router 1 : Repeat the same steps in the Router 0, but with the difference is IP

```
Router>en
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#ip address 40.0.0.1 255.0.0.0
Router(config-if)#no shut

Router(config-if)#int fa1/0
Router(config-if)#ip address 50.0.0.1 255.0.0.0
Router(config-if)#no shut

Router(config-if)#int serial2/0
Router(config-if)#ip address 30.0.0.2 255.0.0.0
Router(config-if)#no shut
```

Step 3: Set IP address to PCs:

- Click on PC .
- Go to desktop.
- IP configuration.

PC0: IP address: 10.0.0.2 Subnet mask 255.0.0.0 Default Gateway 10.0.0.1

PC1: IP address: 20.0.0.2 Subnet mask 255.0.0.0 Default Gateway 20.0.0.1

PC2: IP address: 40.0.0.2 Subnet mask 255.0.0.0 Default Gateway 40.0.0.1

PC3: IP address: 50.0.0.2 Subnet mask 255.0.0.0 Default Gateway 50.0.0.1

Step 4: **configuration RIP2 on stick router**

Router 0:

```
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 10.0.0.0
Router(config-router)#network 20.0.0.0
Router(config-router)#network 30.0.0.0
Router(config-router)#exit
```

Router 1:

```
Router(config)#router rip
Router(config-router)#version 2
 Router(config-router)#network 40.0.0.0
 Router(config-router)#network 50.0.0.0
 Router(config-router)#network 30.0.0.0
 Router(config-router)#exit
```

Step 5: we can verify the connection by send simply PDU between PCs

Acknowledgment:

This sheet and its attached configuration of experiments is produced by the help of the graduation project for the students

(Sara Chasib Jber) and (Ayaat Rikan Hameed)

In 2021

Under the supervision of Dr. Ameer Mosa Al-Sadi.

University of Technology – Iraq
Computer Engineering Department

Experiment no.6

Constructing WAN

"Dynamic Routing"

Link State Routing Protocols

Ex. Open Shortest Path First (OSPF):

Dr. Ameer Mosa Al-Sadi **M.Sc. Ali E. Al Bayati**

2021-2022

Network Laboratory

6.1 Link State Routing Protocols

Link state routing protocols ***have a complete picture of the network topology***. Hence they know more about the whole network than any distance vector protocol.

Three separate tables are created on each link state routing enabled router. One table is used to hold details about directly connected neighbors, one is used to hold the topology of the entire internetwork and the last one is used to hold the actual routing table.

Link state protocols send information about directly connected links to all the routers in the network. Examples of Link state routing protocols include **OSPF - Open Shortest Path First** and **IS-IS - Intermediate System to Intermediate System.**

There are also routing protocols that are considered to be hybrid in the sense that they use aspects of both distance vector and link state protocols. **EIGRP - Enhanced Interior Gateway Routing Protocol** is one of those hybrid routing protocols.

It is possible to Summarize the above information in points as below:

- In this algorithm each router tells the whole network what it knows about its neighbors.
- Maintains an entire map of the network topology within each participating router.
- No periodic updates, unlike distance vector protocols.
- Updates are sent only after a topology change.
- Examples of Link-state routing protocols:
  Open Shortest Path First (OSPF) an open routing protocol defined by the IETF.
- Intermediate system to Intermediate system (IS-IS) designed by the ISO.

6.2 Link state database (LSDB): Collection of information defined the map of whole network. to create least cost tree we need to find LSDB, The LSDB can be represented as a two-dimensional array (matrix) in which the value of each cell defines the cost of the corresponding link.

The node creates LSDB by sending hello message to immediate neighbors to collect two pieces of information for each neighboring node: the identity of the node and the cost of the link. The combination of these two pieces of information is called the LS packet (LSP).

LSP is sent from each interface, when the LSP node receives from one of its interfaces, it compares the LSP to the one it might already have. If the newly arrived LSP is older than the one found, it ignores LSP. If it is the newest or first one received, the node ignores the old LSP (if there is one) and maintains the received node. It then sends a copy of it from every interface except for the one from which the package arrived

6.3 Example of link State:

Open Shortest Path First (OSPF):

- Open Shortest Path First (OSPF) is a unicast routing protocol developed by the Internet Engineering Task Force (IETF) Working Group.
- OSPF is widely used in today's production networks.
- It is an open protocol and supports multiple vendors.
- OSPFv2 supports classless routing.
- OSPFv3 supports IPv6 addressing.
- Updates are only sent when topological changes occur.

OSPF Area:

Its logical collection of OSPF networks, router and links that have the **same area identification**. A router within an area must maintain a topological database for the area to which it belongs. When the sub-domains of OSPF network are divided this is called areas **The router does not have information about network topology outside of its area**, which reduces the size of its database.

6.4 Implementing WAN with OSPF

In this topology we will use another type of routing protocol it is the Open Shortest Path First protocol (OSPF) and Figure (6.1) explain the topology that's will configuration it:

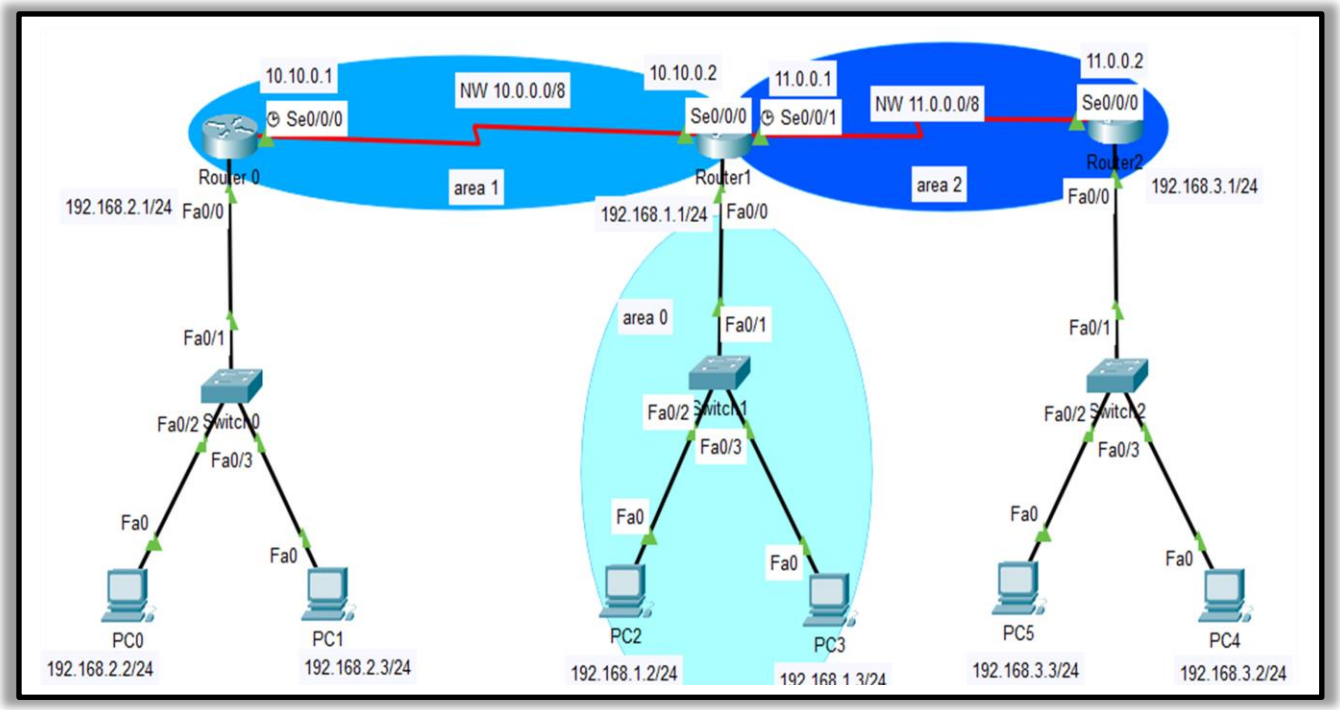


Figure (6.1): WAN with OSPF.

To connect and configuration this topology follows this steps:

Step 1: take the devices into the working space and connect them with connectors

Step 2: Configuration interfaces of Routers:

Router0:

```
Router>en
Router#config
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
      %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
Router(config-if)#exit


Router(config)#interface serial 0/0/0
Router(config-if)#ip address 10.10.0.1 255.0.0.0
Router(config-if)#no shutdown
   %LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
Router(config-if)#exit
Router(config)#
```

Router1:

Repeat same commands of Router 0 but with difference IP address

```
Router>en
Router#config
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
    %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
```

```
Router(config-if)#exit
Router(config)#interface serial 0/0/0
Router(config-if)#ip address 10.10.0.2 255.0.0.0
Router(config-if)#no shutdown
    %LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
Router(config-if)#exit


Router(config)#interface serial 0/0/1
Router(config-if)#ip address 11.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Routter(config)#
```

Router2:

```
Router>en
Router#configuration terminal
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 192.168.3.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
  %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
Router(config-if)#exit

Router(config)#interface serial 0/0/0
Router(config-if)#ip address 11.0.0.2 255.0.0.0
Router(config-if)#no shutdown
  %LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
Router(config-if)#exit
```

Step 3: set IP address to PCs

- Click on PC
- Go to desktop
- IP configuration

PC0: IP address: 192.168.2.2 Subnet mask 255.255.255.0 Default Gateway 192.168.2.1

PC1: IP address: 192.168.2.3 Subnet mask 255.255.255.0 Default Gateway 192.168.2.1

PC2: IP address: 192.168.1.2 Subnet mask 255.255.255.0 Default Gateway 192.168.1.1

PC3: IP address: 192.168.1.3 Subnet mask 255.255.255.0 Default Gateway 192.168.1.1

PC4: IP address: 192.168.3.2 Subnet mask 255.255.255.0 Default Gateway 192.168.3.1

PC5: IP address: 192.168.3.3 Subnet mask 255.255.255.0 Default Gateway 192.168.3.1

Step 4: configuration OSPF on router

Some notes that must be taken into consideration before starting the configuration process:

1) we will define on which interfaces OSPF will run and what networks will be advertised using network **IP ADDRESS WILDCARD MASK AREA** command in the OSPF configuration mode.

Remark: What is WILDCARD MASK AREA?

It is the same subnet mask but in reverse one shortcut method is to subtract the subnet mask from 255.255.255.255

For example: The IP address for a Specific Network is 192.168.3.0
With the subnet mask 255.255.255.0 what is the wildcard mask area?
Sole//

1) Starting value

```
255.255.255.255
–255.255.255. 0
```

Subtract the subnet mask

Resulting wildcard mask is **0. 0. 0.255**

2) We should put OSPF process ID like (OSPF 1, OSPF 2 and so on) different for each router

3) The **area** parameter has to be the same on all neighbouring routers in order for the routers to become neighbours.

Router0:

```
Router(config)#router ospf 1
Router(config-router)#network 10.0.0.0  0.255.255.255 area 1
Router(config-router)#network 192.168.2.0  0.0.0.255 area 1
Router(config-router)#exit
Router(config)#
```

Router1:

```
Router(config)#router ospf 2
Router(config-router)#network 10.0.0.0    0.255.255.255 area 1
Router(config-router)#network 11.0.0.0    0.255.255.255 area 2
Router(config-router)#
00:35:44: %OSPF-5-ADJCHG: Process 2, Nbr 192.168.3.1 on Serial0/0/1 from
LOADING to FULL, Loading Done
Router(config-router)#network 192.168.1.0  0.0.0.255 area 0
Router(config-router)#exit
Router(config)#
```

Router2:

```
Router(config)#router ospf 3
Router(config-router)#network 11.0.0.0   0.255.255.255 area 2
Router(config-router)#network 192.168.3.0   0.0.0.255 area 2
Router(config-router)#exit
Router(config)#
```

Step 5: we can verify the connection by send simply PDU between PCs.

Acknowledgment:

This sheet and its attached configuration of experiments is produced by the help of the graduation project for the students

(Sara Chasib Jber) and (Ayaat Rikan Hameed)

In 2021

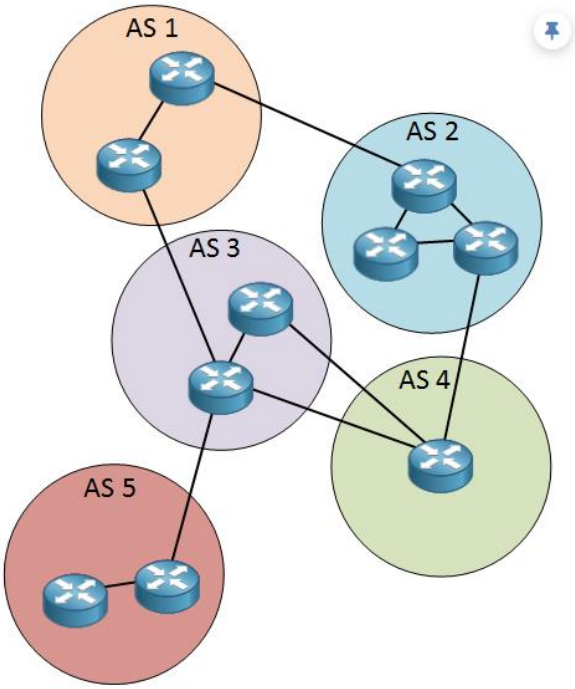
Under the supervision of Dr. Ameer Mosa Al-Sadi.

CCNPv7 ROUTE

Lab, Configuring BGP with Default Routing

Introduction: The Border Gateway Protocol (BGP), defined in RFC 1771, allows you to create loop free interdomain routing between autonomous systems. An autonomous system is a set of routers under a single technical administration. Routers in an AS can use multiple interior gateway protocols to exchange routing information inside the AS and an exterior gateway protocol to route packets outside the AS.

How does BGP work? BGP uses TCP as its transport protocol (port 179). Two BGP speaking routers form a TCP connection between one another (peer routers) and exchange messages to open and confirm the connection parameters. BGP routers will exchange network reachability information, this information is mainly an indication of the full paths (BGP AS numbers) that a route should take in order to reach the destination network. This information will help in constructing a graph of ASs that are loop free and where routing policies can be applied in order to enforce some restrictions on the routing behavior.



An AS is a collection of networks under a single administrative domain. The Internet is nothing more but a bunch of autonomous systems that are connected to each other. Within an autonomous system we use an IGP like OSPF or EIGRP.

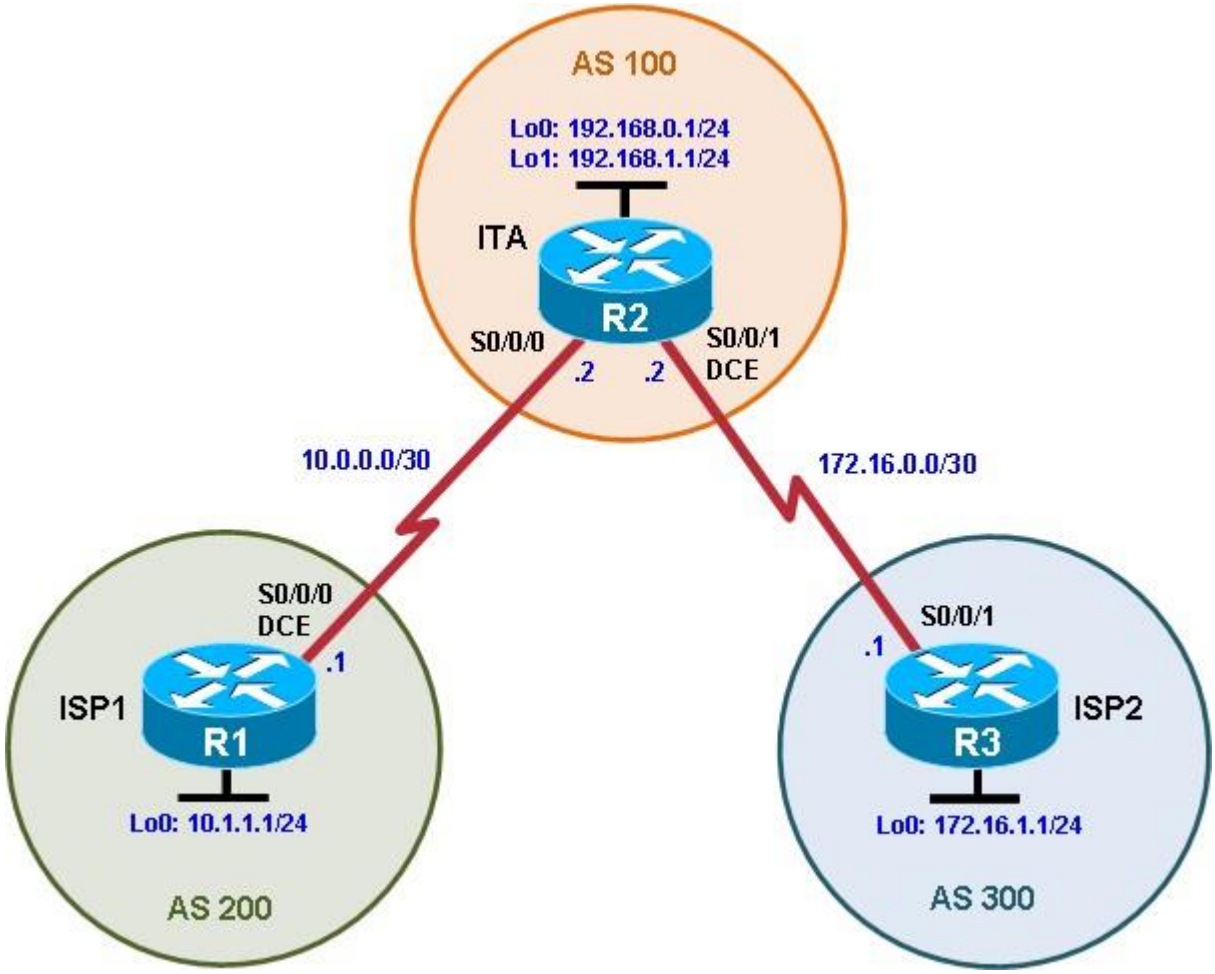
For routing between the different autonomous systems, we use an **EGP (external gateway protocol).**

Autonomous system numbers are 16-bit which means we have 65535 numbers to choose from. Just like private and **public IP addresses**, we have a range of public and private AS numbers.

Range **1 – 64511 are globally unique AS numbers** and **range 64512 – 65535 are private** autonomous system numbers.

Finally, when BGP is running between routers belonging to two different ASs we will call it **EBGP** (Exterior BGP) and for BGP running between routers in the same AS we will call it **IBGP** (Interior BGP)

Lab Topology



Objectives

- Configure BGP to exchange routing information with two ISPs.

Background

The International Travel Agency (ITA) relies extensively on the Internet for sales. For this reason, the ITA has decided to create a multihomed ISP connectivity solution and contracted with two ISPs for Internet connectivity with fault tolerance. Because the ITA is connecting to two different service providers, you must configure BGP, which runs between the ITA boundary router and the two ISP routers.

Note: This lab uses Cisco 1941 routers with Cisco IOS Release 15.4 with IP Base. The switches are Cisco WS-C2960-24TT-L with Fast Ethernet interfaces, therefore the router will use routing metrics associated with a 100 Mb/s

interface. Depending on the router or switch model and Cisco IOS Software version, the commands available and output produced might vary from what is shown in this lab.

Step 1: Configure interface addresses.

a. Using the addressing scheme in the diagram, create the loopback interfaces and apply IPv4 addresses to these and the serial interfaces on **ISP1 (R1)**, **ITA (R2)** **and** **ISP2 (R3)**. The ISP loopbacks simulate real networks that can be reached through the ISP. The two loopbacks for the ITA router simulate the connections between the ITA boundary router and their core routers. Set a clock rate on the DCE serial interfaces.

- **ISP1 (R1) ----------**

- **Loopback Interface Configuration (Lo0):** Enters the configuration mode for the loopback interface Lo0. Loopback interfaces are virtual interfaces used for testing, management, and routing purposes. Then, assigns the IP address 10.1.1.1 with a subnet mask of 255.255.255.0 to the loopback interface. This IP can be used for management or routing protocols.

```
ISP1(config)# interface Lo0
ISP1(config-if)# ip address 10.1.1.1 255.255.255.0
ISP1(config-if)# exit
```

- **Serial Interface Configuration (Serial0/0/0):** Enters the configuration mode for the serial interface Serial0/0/0. Serial interfaces are typically used for WAN connections. Then, Assigns the IP address 10.0.0.1 with a subnet mask of 255.255.255.252 to the serial interface. The /30 subnet (255.255.255.252) allows for only **two usable IP addresses**.

```
ISP1(config)# interface Serial0/0/0
ISP1(config-if)# description ISP1 -> ITA
ISP1(config-if)# ip address 10.0.0.1 255.255.255.252
ISP1(config-if)# no shutdown
ISP1(config-if)# end
ISP1#
```

- **ITA (R2) ----------**

```
ITA(config)# interface Lo0
ITA(config-if)# ip address 192.168.0.1 255.255.255.0
ITA(config)# exit

ITA(config-if)# interface Lo1
ITA(config-if)# ip address 192.168.1.1 255.255.255.0
ITA(config-if)# exit

ITA(config)# interface Serial0/0/0
ITA(config-if)# ip address 10.0.0.2 255.255.255.252
ITA(config-if)# no shutdown
ITA(config-if)# exit

ITA(config)# interface Serial0/0/1
ITA(config-if)# ip address 172.16.0.2 255.255.255.252
```

```
ITA(config-if)# no shutdown
ITA(config-if)# end
ITA#
```

- ISP2 (R3) ----------

```
ISP2(config)# interface Lo0
ISP2(config-if)# ip address 172.16.1.1 255.255.255.0
ISP2(config)# exit

ISP2(config-if)# interface Serial0/0/1
ISP2(config-if)# ip address 172.16.0.1 255.255.255.252
ISP2(config-if)# no shutdown
ISP2(config-if)# end
ISP2#
```

b. Use **ping** to test the connectivity between the directly connected routers. Note that router ISP1 cannot reach router ISP2.

Step 2: Configure BGP on the ISP routers.

On the ISP1 and ISP2 routers, configure BGP to peer with the ITA boundary router and advertise the ISP loopback networks.

```
ISP1(config)# router bgp 200
ISP1(config-router)# neighbor 10.0.0.2 remote-as 100
ISP1(config-router)# network 10.1.1.0 mask 255.255.255.0

ISP2(config)# router bgp 300
ISP2(config-router)# neighbor 172.16.0.2 remote-as 100
ISP2(config-router)# network 172.16.1.0 mask 255.255.255.0
```

Step 3: Configure BGP on the ITA boundary router.

a. Configure the ITA router to run BGP with both Internet providers.

```
ITA(config)# router bgp 100
ITA(config-router)# neighbor 10.0.0.1 remote-as 200
ITA(config-router)# neighbor 172.16.0.1 remote-as 300
ITA(config-router)# network 192.168.0.0
ITA(config-router)# network 192.168.1.0
```

You should see BGP neighbor peering messages on the console similar to the following.

```
*Sep 8 16:00:21.587: %BGP-5-ADJCHANGE: neighbor 10.0.0.1 Up
```

b. To verify the configuration, check the ITA routing table with the **show ip route** command.

```
ITA# show ip route
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, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override
```

```
Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
C     10.0.0.0/30 is directly connected, Serial0/0/0
L     10.0.0.2/32 is directly connected, Serial0/0/0 B
10.1.1.0/24 [20/0] via 10.0.0.1, 00:01:10
      172.16.0.0/16 is variably subnetted, 3 subnets, 3 masks
C     172.16.0.0/30 is directly connected, Serial0/0/1
L     172.16.0.2/32 is directly connected, Serial0/0/1 B
172.16.1.0/24 [20/0] via 172.16.0.1, 00:00:53
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C     192.168.0.0/24 is directly connected, Loopback0
L      192.168.0.1/32   is   directly   connected,   Loopback0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C     192.168.1.0/24 is directly connected, Loopback1 L
192.168.1.1/32 is directly connected, Loopback1 ITA#
```

ITA has BGP routes to the loopback networks at each ISP router.

c. Run the following Tcl script on all routers to verify connectivity If these pings are not successful, troubleshoot. Use **exit** to exit the Tcl script.

Note: The WAN subnets connecting ITA (R2) to the ISPs (R1 and R3) are not advertised in BGP, so the ISPs will not be able to ping each other's serial interface address.

```
ITA# tclsh

foreach address
{ 10.0.0.1
10.0.0.2
10.1.1.1
172.16.0.1
172.16.0.2
172.16.1.1
192.168.0.1
192.168.1.1
} {
ping $address }
```

Step 4: Verify BGP on the routers.

a. To verify the BGP operation on ITA, issue the **show ip bgp** command.

```
ITA# show ip bgp
BGP table version is 5, local router ID is 192.168.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *> 10.1.1.0/24       10.0.0.1                 0             0 200 i
 *> 172.16.1.0/24     172.16.0.1               0             0 300 i
 *> 192.168.0.0       0.0.0.0                  0         32768 i
 *> 192.168.1.0       0.0.0.0                  0         32768 i
ITA#
```

What is the local router ID?

Which table version is displayed?

An asterisk (*) next to a route indicates that it is valid. An angle bracket (>) indicates that the route has been selected as the best route.

b. To verify the operation of ISP1, issue the **show ip bgp** command.

```
ISP1# show ip bgp
BGP table version is 5, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *> 10.1.1.0/24       0.0.0.0                  0         32768 i
 *> 172.16.1.0/24     10.0.0.2                               0 100 300 i
 *> 192.168.0.0       10.0.0.2                 0             0 100 i
 *> 192.168.1.0       10.0.0.2                 0             0 100 i
ISP1#
```

Which table version is displayed and is it the same as the BGP table version for ITA?

From ISP1, what is the path to network 172.16.1.0/24?

c. On the ISP1 router, issue the **shutdown** command on Loopback0. Then on ITA, issue the **show ip bgp** command again.

```
ISP1(config)# interface loopback 0
ISP1(config-if)# shutdown
ISP1(config-if)#

ITA# show ip bgp
BGP table version is 6, local router ID is 192.168.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *> 172.16.1.0/24     172.16.0.1               0             0 300 i
 *> 192.168.0.0       0.0.0.0                  0         32768 i
 *> 192.168.1.0       0.0.0.0                  0         32768 i
ITA#
```

Which table version is displayed? Why?

What happened to the route for network 10.1.1.0/24?

_____

d. Bring ISP1 router Loopback0 back up by issuing the **no shutdown** command.

```
ISP1(config)# interface loopback 0
ISP1(config-if)# no shutdown
ISP1(config-if)#
```

e. On ITA, issue the **show ip bgp neighbors** command. The following is a partial sample output of the command showing neighbor 172.16.0.1.

```
ITA# show ip bgp neighbors
BGP neighbor is 10.0.0.1, remote AS 200, external link
  BGP version 4, remote router ID 10.1.1.1
  BGP state = Established, up for 00:20:47
  Last read 00:00:49, last write 00:00:41, hold time is 180, keepalive interval is
60 seconds
  Neighbor sessions:
    1 active, is not multisession capable (disabled)
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
    Enhanced Refresh Capability: advertised and received
    Multisession Capability:
    Stateful switchover support enabled: NO for session 1
  Message statistics:
    InQ depth is 0
    OutQ depth is 0

                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                5          1
    Keepalives:            15         17
    Route Refresh:          0          0
    Total:                 21         19
  Default minimum time between advertisement runs is 30 seconds

<output omitted>
```

Based on the output of this command, what is the BGP state between this router and ISP2?

_____

_____

How long has this connection been up?

_____

Step 5: Configure route filters.

a. Check the ISP2 routing table using the **show ip route** command. ISP2 should have a route that belongs to ISP1, network 10.1.1.0.

```
ISP2# show ip route
<output omitted>
```

```
      10.0.0.0/24 is subnetted, 1 subnets
B        10.1.1.0 [20/0] via 172.16.0.2, 00:09:26
      172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
C        172.16.0.0/30 is directly connected, Serial0/0/1
L        172.16.0.1/32 is directly connected, Serial0/0/1
C        172.16.1.0/24 is directly connected, Loopback0
L        172.16.1.1/32 is directly connected, Loopback0
B     192.168.0.0/24 [20/0] via 172.16.0.2, 00:28:05
B     192.168.1.0/24 [20/0] via 172.16.0.2, 00:28:05
ISP2#
```

If ITA advertises a route belonging to ISP1, ISP2 installs that route in its table. ISP2 might then attempt to route transit traffic through the ITA. This would make ITA a transit router. A traceroute to ISP1's Lo0 interface illustrates this issue.

```
ISP2# traceroute 10.1.1.1
Type escape sequence to abort.
Tracing the route to 10.1.1.1
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.0.2 8 msec 4 msec 8 msec
  2 * * *
  3 * * *
  4 * * * <control-shift-6 to break> ISP2#
```

The **traceroute 10.1.1.1** fails because ISP1 does not have a route to the source IPv4 address of the traceroute, 172.16.0.1. It is common in BGP networks not to advertise the links between providers in BGP. A traceroute using the source IPv4 address of ISP2' Lo0 interface is successful, showing that ITA is a transit router for this network.

```
ISP2# traceroute 10.1.1.1 source loopback0
Type escape sequence to abort.
Tracing the route to 10.1.1.1
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.0.2 8 msec 4 msec 8 msec
  2 10.0.0.1 12 msec * 12 msec
ISP2#
```

b. Configure the ITA router so that it advertises only ITA networks 192.168.0.0 and 192.168.1.0 to both providers. On the ITA router, configure the following access list.

```
ITA(config)# access-list 1 permit 192.168.0.0 0.0.1.255
```

c. Apply this access list as a route filter using the **distribute-list** keyword with the BGP **neighbor** statement.

```
ITA(config)# router bgp 100
ITA(config-router)# neighbor 10.0.0.1 distribute-list 1 out
ITA(config-router)# neighbor 172.16.0.1 distribute-list 1 out
```

d. Check the routing table for ISP2 again. The route to 10.1.1.0, ISP1, should still be in the table.

```
ISP2# show ip route
<output omitted>

      10.0.0.0/24 is subnetted, 1 subnets
B        10.1.1.0 [20/0] via 172.16.0.2, 00:25:14
      172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
C        172.16.0.0/30 is directly connected, Serial0/0/1
```

```
L        172.16.0.1/32 is directly connected, Serial0/0/1
C        172.16.1.0/24 is directly connected, Loopback0
L        172.16.1.1/32 is directly connected, Loopback0
B     192.168.0.0/24 [20/0] via 172.16.0.2, 00:43:53
B     192.168.1.0/24 [20/0] via 172.16.0.2, 00:43:53
ISP2#
```

e. Return to ITA and issue the **clear ip bgp *** command. Wait until the routers reach the established state, which might take several seconds, and then recheck the ISP2 routing table. The route to ISP1, network 10.1.1.0, should no longer be in the routing table for ISP2, and the route to ISP2, network 172.16.1.0, should not be in the routing table for ISP1.

```
ITA# clear ip bgp *
ITA#
*Sep 8 16:47:25.179: %BGP-5-ADJCHANGE: neighbor 10.0.0.1 Down User reset
*Sep 8 16:47:25.179: %BGP_SESSION-5-ADJCHANGE: neighbor 10.0.0.1 IPv4 Unicast
topology base removed from session User reset
*Sep 8 16:47:25.179: %BGP-5-ADJCHANGE: neighbor 172.16.0.1 Down User reset
*Sep 8 16:47:25.179: %BGP_SESSION-5-ADJCHANGE: neighbor 172.16.0.1 IPv4 Unicast
topology base removed from session User reset
*Sep 8 16:47:25.815: %BGP-5-ADJCHANGE: neighbor 10.0.0.1 Up
*Sep 8 16:47:25.819: %BGP-5-ADJCHANGE
ITA#: neighbor 172.16.0.1 Up
ITA#
```

Note: The **clear ip bgp *** command is disruptive because it completely resets all BGP adjacencies. This is acceptable in a lab environment but could be problematic in a production network. Instead, if only a change of inbound/outbound routing policies is to be performed, it is sufficient to issue the **clear ip bgp * in** or **clear ip bgp * out** commands**.** These commands perform only a new BGP database synchronization without the disruptive effects of a complete BGP adjacency reset. All current Cisco IOS versions support the route refresh capability that replaces the inbound soft reconfiguration feature that previously had to be configured on a per-neighbor basis.

```
ISP2# show ip route
<output omitted>


      172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
C        172.16.0.0/30 is directly connected, Serial0/0/1
L        172.16.0.1/32 is directly connected, Serial0/0/1
C        172.16.1.0/24 is directly connected, Loopback0 L
         172.16.1.1/32 is directly connected, Loopback0
B     192.168.0.0/24 [20/0] via 172.16.0.2, 00:00:06
B     192.168.1.0/24 [20/0] via 172.16.0.2, 00:00:06
ISP2#


ISP1# show ip route
<output omitted>

      10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks
C        10.0.0.0/30 is directly connected, Serial0/0/0
L        10.0.0.1/32 is directly connected, Serial0/0/0
C        10.1.1.0/24 is directly connected, Loopback0
L        10.1.1.1/32 is directly connected, Loopback0
B     192.168.0.0/24 [20/0] via 10.0.0.2, 00:00:42
B     192.168.1.0/24 [20/0] via 10.0.0.2, 00:00:42
```

```
ISP1#
```

Step 6: Configure primary and backup routes using floating static routes.

With bidirectional communication established with each ISP via BGP, configure the primary and backup routes. This can be done with floating static routes or BGP.

a. Issue the **show ip route** command on the ITA router.

```
ITA# show ip route
<output omitted>

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
C     10.0.0.0/30 is directly connected, Serial0/0/0
L      10.0.0.2/32 is directly connected, Serial0/0/0 B
10.1.1.0/24 [20/0] via 10.0.0.1, 00:03:51
      172.16.0.0/16 is variably subnetted, 3 subnets, 3 masks
C     172.16.0.0/30 is directly connected, Serial0/0/1
L      172.16.0.2/32 is directly connected, Serial0/0/1 B
172.16.1.0/24 [20/0] via 172.16.0.1, 00:03:51
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C     192.168.0.0/24 is directly connected, Loopback0
L       192.168.0.1/32   is   directly   connected,   Loopback0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.1.0/24 is directly connected, Loopback1 L
192.168.1.1/32 is directly connected, Loopback1 ITA#
```

Notice that there is no gateway of last resort defined. This is a problem because ITA is the border router for the corporate network.

b. Configure static routes to reflect the policy that ISP1 is the primary provider and that ISP2 acts as the backup by specifying a lower distance metric for the route to ISP1 (210) as compared to the backup route to ISP2 (distance metric 220).

```
ITA(config)# ip route 0.0.0.0 0.0.0.0 10.0.0.1 210
ITA(config)# ip route 0.0.0.0 0.0.0.0 172.16.0.1 220
```

c. Verify that a default route is defined using the **show ip route** command.

```
ITA# show ip route
<output omitted>
Gateway of last resort is 10.0.0.1 to network 0.0.0.0

S*    0.0.0.0/0 [210/0] via 10.0.0.1
      10.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
C        10.0.0.0/30 is directly connected, Serial0/0/0
L        10.0.0.2/32 is directly connected, Serial0/0/0
B        10.1.1.0/24 [20/0] via 10.0.0.1, 00:05:38
      172.16.0.0/16 is variably subnetted, 3 subnets, 3 masks
C        172.16.0.0/30 is directly connected, Serial0/0/1
L        172.16.0.2/32 is directly connected, Serial0/0/1
B        172.16.1.0/24 [20/0] via 172.16.0.1, 00:05:38
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.0.0/24 is directly connected, Loopback0
L        192.168.0.1/32 is directly connected, Loopback0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
```

```
C     192.168.1.0/24 is directly connected, Loopback1 L
192.168.1.1/32 is directly connected, Loopback1 ITA#
```

d. Test this default route by creating an unadvertised loopback on the router for ISP1.

```
ISP1# config t
ISP1(config)# interface loopback 100
ISP1(config-if)# ip address 192.168.100.1 255.255.255.0
```

e. Issue the **show ip route** command to ensure that the newly added 192.168.100.0 /24 network does not appear in the routing table.

```
ITA# show ip route
<output omitted>

Gateway of last resort is 10.0.0.1 to network 0.0.0.0

S*  0.0.0.0/0 [210/0] via 10.0.0.1
      10.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
C     10.0.0.0/30 is directly connected, Serial0/0/0
L     10.0.0.2/32 is directly connected, Serial0/0/0 B
10.1.1.0/24 [20/0] via 10.0.0.1, 00:07:08
      172.16.0.0/16 is variably subnetted, 3 subnets, 3 masks
C     172.16.0.0/30 is directly connected, Serial0/0/1
L     172.16.0.2/32 is directly connected, Serial0/0/1 B
172.16.1.0/24 [20/0] via 172.16.0.1, 00:07:08
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C     192.168.0.0/24 is directly connected, Loopback0
L       192.168.0.1/32   is   directly   connected,   Loopback0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C     192.168.1.0/24 is directly connected, Loopback1 L
192.168.1.1/32 is directly connected, Loopback1 ITA#
```

f. In extended ping mode, ping the ISP1 loopback 1 interface 192.168.100.1 with the source originating from the ITA loopback 1 interface 192.168.1.1.

```
ITA# ping
Protocol [ip]:
Target IP address: 192.168.100.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.100.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/14/16 ms
ITA#
```

Note: You can bypass extended ping prompted mode and ping while specifying a source address using one of these abbreviated commands:

```
ITA# ping 192.168.100.1 source 192.168.1.1
```

or

```
ITA# ping 192.168.100.1 source Lo1
```

Note: Testing the default route by creating an unadvertised network on ISP1 and pinging it works only because the default route also points toward ISP1. If the preferred default route pointed toward ISP2, the ping to that unadvertised network on ISP1 would not succeed. If the link to ISP1 failed, the default route to ISP2 would become active, but the pings would be successful only if ISP1 and ISP2 have another working interconnection and appropriate BGP peering between them, which is currently not the case.

Step 7: Using BGP to propagate a default route.

a. ISP router will be used to inject a default route via BGP. First, remove the current default routes on ITA.

```
ITA(config)# no ip route 0.0.0.0 0.0.0.0 10.0.0.1 210
ITA(config)# no ip route 0.0.0.0 0.0.0.0 172.16.0.1 220
```

b. Next, configure the ISP1 router to send a default route to its neighbor, the ITA router. This command does not require the presence of 0.0.0.0 in the local ISP1 router.

```
ISP1(config)# router bgp 200
ISP1(config-router)# neighbor 10.0.0.2 default-originate
ISP1(config-router)#
```

c. Verify that the default route was received by ITA using BGP.

```
ITA# show ip route
<output omitted>

Gateway of last resort is 10.0.0.1 to network 0.0.0.0

B*  0.0.0.0/0 [20/0] via 10.0.0.1, 00:01:43
      10.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
C     10.0.0.0/30 is directly connected, Serial0/0/0
L     10.0.0.2/32 is directly connected, Serial0/0/0 B
10.1.1.0/24 [20/0] via 10.0.0.1, 00:06:51
      172.16.0.0/16 is variably subnetted, 3 subnets, 3 masks
C     172.16.0.0/30 is directly connected, Serial0/0/1
L     172.16.0.2/32 is directly connected, Serial0/0/1 B
172.16.1.0/24 [20/0] via 172.16.0.1, 00:06:51
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C     192.168.0.0/24 is directly connected, Loopback0
L       192.168.0.1/32   is   directly   connected,   Loopback0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C     192.168.1.0/24 is directly connected, Loopback1 L
192.168.1.1/32 is directly connected, Loopback1 ITA#
```