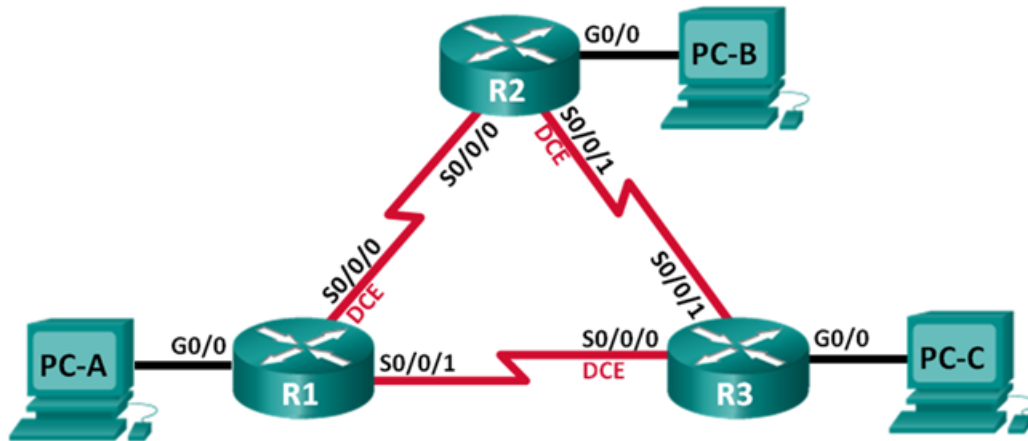


## Lab 1.1 – Single Area OSPF Configuration

### Topology



### Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.12.1	255.255.255.252	N/A
	S0/0/1	192.168.13.1	255.255.255.252	N/A
R2	G0/0	192.168.2.1	255.255.255.0	N/A
	Lo0	209.165.200.226	255.255.255.252	N/A
	S0/0/0	192.168.12.2	255.255.255.252	N/A
	S0/0/1 (DCE)	192.168.23.1	255.255.255.252	N/A
R3	G0/0	192.168.3.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.13.2	255.255.255.252	N/A
	S0/0/1	192.168.23.2	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

### Objectives

**Part 1: Build the Network and Configure Basic Device Settings**

**Part 2: Configure and Verify OSPF Routing**

**Part 3: Change Router ID Assignments**

**Part 4: Configure OSPF Passive Interfaces**

**Part 5: Propagate a Default Route**

### Background / Scenario

Open Shortest Path First (OSPF) is a link-state routing protocol for IP networks. OSPFv2 is defined for IPv4 networks, and OSPFv3 is defined for IPv6 networks. OSPF detects changes in the topology, such as link failures, and converges on a new loop-free routing structure very quickly. It computes each route using Dijkstra's algorithm, a shortest path first algorithm.

In this lab, you will configure the network topology with OSPFv2 routing, change the router ID assignments, configure passive interfaces, use OSPF to propagate a default route into the routing domain, and use a number of CLI commands to display and verify OSPF routing information.

#### Part 1: **Build the Network and Configure Basic Device Settings**

In Part 1, you set up the network topology and configure basic settings on the PC hosts and routers.

**Step 1: Cable the network as shown in the topology.**

**Step 2: Configure basic settings for each router.**

- a. Configure device name as shown in the topology.
- b. Configure the IP address listed in the Addressing Table for all interfaces.
- c. Copy the running configuration to the startup configuration.

**Step 3: Configure PC hosts.**

**Step 4: Test connectivity.**

The routers should be able to ping one another, and each PC should be able to ping its default gateway. The PCs are unable to ping other PCs until OSPF routing is configured. Verify and troubleshoot if necessary.

#### Part 2: **Configure and Verify OSPF Routing**

In Part 2, you will configure OSPFv2 routing on all routers in the network and then verify that routing tables are updated correctly.

**Step 1: Configure OSPF on R1.**

- a. Start the OSPF routing process on R1. Use process ID 1.

```
R1(config)# router ospf 1
```

**Note:** The OSPF process id is kept locally and has no meaning to other routers on the network.

- b. Configure networks for OSPF routing using network commands and wildcard masks.

How many statements are required to configure OSPF to route all the networks attached to router R1?	2
The LAN attached to router R1 has a /24 mask. What is the equivalent of this mask in dotted decimal representation?	255.255.255.0
Subtract the dotted decimal subnet mask from 255.255.255.255. What is the result?	0.0.0.255
What is the dotted decimal equivalent of the /30 subnet mask?	255.255.255.252
Subtract the dotted decimal representation of the /30 mask from 255.255.255.255. What is the result?	0.0.0.3

- c. Using the syntax below, configure the **network** statements for the networks on R1. Use an area ID of 0.

```
Router(config-router)# network network-address wildcard-mask area area-id
```

What are the network commands that need to be configured on R1?

```
network 192.168.1.0 0.0.0.255 area 0
network 192.168.12.0 0.0.0.3 area 0
```

### Step 2: Configure OSPF on R2 and R3

Following the same procedure, configure OSPF on R2 and R3 using process ID 0. Do not include the network 209.165.200.224/30 in those to be advertised by R2. Place networks in area 0

What are the network commands that need to be configured on R2?

```
network 192.168.2.0 0.0.0.255 area 0
network 192.168.12.0 0.0.0.3 area 0
```

What are the network commands that need to be configured on R3?

Neighbor adjacency messages display on R1 when OSPF routing is configured on R2 and R3.

R1#

```
00:22:29: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.23.1 on Serial0/0/0 from LOADING to FULL, Loading Done
```

R1#

```
00:23:14: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.23.2 on Serial0/0/1 from LOADING to FULL, Loading Done
```

R1#

### Step 3: Verify OSPF neighbors and routing information.

- a. Issue the **show ip ospf neighbor** command to verify that each router lists the other routers in the network as neighbors.

```
R1# show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.23.2	0	FULL/ -	00:00:33	192.168.13.2	Serial0/0/1
192.168.23.1	0	FULL/ -	00:00:30	192.168.12.2	Serial0/0/0

- b. Issue the **show ip route** command to verify that all networks display in the routing table on all routers.

```
R1# 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, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.1.0/24 is directly connected, GigabitEthernet0/0
L    192.168.1.1/32 is directly connected, GigabitEthernet0/0
O    192.168.2.0/24 [110/65] via 192.168.12.2, 00:32:33, Serial0/0/0
O    192.168.3.0/24 [110/65] via 192.168.13.2, 00:31:48, Serial0/0/1
192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.12.0/30 is directly connected, Serial0/0/0
L    192.168.12.1/32 is directly connected, Serial0/0/0
192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.13.0/30 is directly connected, Serial0/0/1
L    192.168.13.1/32 is directly connected, Serial0/0/1
192.168.23.0/30 is subnetted, 1 subnets
O    192.168.23.0/30 [110/128] via 192.168.12.2, 00:31:38, Serial0/0/0
                        [110/128] via 192.168.13.2, 00:31:38, Serial0/0/1
```

What do the values '[110 / 65]' and '[110 / 128]' indicated in the OSPF routes mean?

The values indicated in the OSPF routes mean the router metric administrative distance.

### Step 4: Verify OSPF protocol settings.

The **show ip protocols** command is a quick way to verify vital OSPF configuration information. This information includes the OSPF process ID, the router ID, networks the router is advertising, the neighbors the router is receiving updates from, and the default administrative distance, which is 110 for OSPF.

```
R1# show ip protocols
```

```
*** IP Routing is NSF aware ***
```

```
Routing Protocol is "ospf 1"
```

```
Outgoing update filter list for all interfaces is not set
```

```
Incoming update filter list for all interfaces is not set
```

```
Router ID 192.168.13.1
```

```
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
  192.168.1.0 0.0.0.255 area 0
  192.168.12.0 0.0.0.3 area 0
  192.168.13.0 0.0.0.3 area 0
Routing Information Sources:
  Gateway         Distance      Last Update
  192.168.23.2    110          00:19:16
  192.168.23.1    110          00:20:03
```

### Step 5: Verify end-to-end connectivity.

Each PC should be able to ping the other PCs in the topology. Verify and troubleshoot if necessary.

## Part 3: Change Router ID Assignments

The OSPF router ID is used to uniquely identify the router in the OSPF routing domain. Cisco routers derive the router ID in one of three ways and with the following precedence:

- 1) IP address configured with the OSPF **router-id** command, if present
- 2) Highest IP address of any of the router's loopback addresses, if present
- 3) Highest active IP address on any of the router's physical interfaces

Because no router IDs or loopback interfaces have been configured on the three routers, the router ID for each router is determined by the highest IP address of any active interface.

In Part 3, you will change the OSPF router ID assignment using loopback addresses. You will also use the **router-id** command to change the router ID.

### Step 1: Change router IDs using loopback addresses.

- a. Assign an IP address to loopback 0 on R1.

```
R1(config)# interface lo0
R1(config-if)# ip address 1.1.1.1 255.255.255.255
R1(config-if)# end
```

- b. Assign IP addresses to Loopback 0 on R2 and R3. Use IP address 2.2.2.2/32 for R2 and 3.3.3.3/32 for R3.
- c. Save the running configuration to the startup configuration on all three routers.
- d. You must reload the routers in order to reset the router ID to the loopback address. Issue the **reload** command on all three routers. Press Enter to confirm the reload.
- e. After the router completes the reload process, issue the **show ip protocols** command to view the new router ID.

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

```
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
```

```
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
  192.168.1.0 0.0.0.255 area 0
  192.168.12.0 0.0.0.3 area 0
  192.168.13.0 0.0.0.3 area 0
Routing Information Sources:
  Gateway         Distance      Last Update
  3.3.3.3          110           00:01:00
  2.2.2.2          110           00:01:14
Distance: (default is 110)
```

- f. Issue the **show ip ospf neighbor** command to display the router ID changes for the neighboring routers.

```
R1# show ip ospf neighbor
```

What are the neighbor IDs listed in the output?

The neighbor ID listed in the output is 2.2.2.2

### Step 2: Change the router ID on R1 using the router-id command.

The preferred method for setting the router ID is with the **router-id** command.

- a. Issue the **router-id 11.11.11.11** command on R1 to reassign the router ID. Notice the informational message that appears when issuing the **router-id** command.

```
R1(config)# router ospf 1
R1(config-router)# router-id 11.11.11.11
Reload or use "clear ip ospf process" command, for this to take effect
R1(config)# end
```

- b. You will receive an informational message telling you that you must either reload the router or use the **clear ip ospf process** command for the change to take effect. Issue the **clear ip ospf process** command on all three routers. Type **yes** to reply to the reset verification message, and press ENTER.
- c. Set the router ID for R2 to **22.22.22.22** and the router ID for R3 to **33.33.33.33**. Then use **clear ip ospf process** command to reset ospf routing process.
- d. Issue the **show ip protocols** command to verify that the router ID changed on R1.

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

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 11.11.11.11
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    192.168.12.0 0.0.0.3 area 0
    192.168.13.0 0.0.0.3 area 0
  Passive Interface(s):
```

```
GigabitEthernet0/1
Routing Information Sources:
  Gateway         Distance      Last Update
  33.33.33.33      110           00:00:19
  22.22.22.22      110           00:00:31
  3.3.3.3          110           00:00:41
  2.2.2.2          110           00:00:41
Distance: (default is 110)
```

- e. Issue the **show ip ospf neighbor** command on R1 to verify that new router ID for R2 and R3 is listed.

```
R1# show ip ospf neighbor
```

What are the neighbor IDs listed in the output?

The neighbor ID listed in the output is 22.22.22.22

### Part 2: Configure OSPF Passive Interfaces

The **passive-interface** command prevents routing updates from being sent through the specified router interface. This is commonly done to reduce traffic on the LANs as they do not need to receive dynamic routing protocol communication. In Part 4, you will use the **passive-interface** command to configure a single interface as passive.

#### Step 1: Configure a passive interface.

- a. Issue the **show ip ospf interface g0/0** command on R1. Notice the timer indicating when the next Hello packet is expected. Hello packets are sent every 10 seconds and are used between OSPF routers to verify that their neighbors are up.

```
R1# show ip ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 192.168.1.1/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 11.11.11.11, Network Type BROADCAST, Cost: 1
  Topology-MTID      Cost      Disabled      Shutdown      Topology Name
    0                1         no            no            Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 11.11.11.11, Interface address 192.168.1.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:02
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

- b. Issue the **passive-interface** command to change the G0/0 interface on R1 to passive.

```
R1(config)# router ospf 1
R1(config-router)# passive-interface g0/0
```

- c. Re-issue the **show ip ospf interface g0/0** command to verify that G0/0 is now passive.

```
R1# show ip ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 192.168.1.1/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 11.11.11.11, Network Type BROADCAST, Cost: 1
  Topology-MTID      Cost      Disabled      Shutdown      Topology Name
    0                1          no            no            Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 11.11.11.11, Interface address 192.168.1.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
  No Hellos (Passive interface)
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

- d. Issue the **show ip route** command on R2 and R3 to verify that a route to the 192.168.1.0/24 network is still available.

```
R2# 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
       + - replicated route, % - next hop override
```

```
Gateway of last resort is not set
```

```
    2.0.0.0/32 is subnetted, 1 subnets
C        2.2.2.2 is directly connected, Loopback0
O        192.168.1.0/24 [110/65] via 192.168.12.1, 00:58:32, Serial0/0/0
    192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, GigabitEthernet0/0
L        192.168.2.1/32 is directly connected, GigabitEthernet0/0
O        192.168.3.0/24 [110/65] via 192.168.23.2, 00:58:19, Serial0/0/1
    192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.12.0/30 is directly connected, Serial0/0/0
```



```
L      192.168.12.2/32 is directly connected, Serial0/0/0
      192.168.13.0/30 is subnetted, 1 subnets
O      192.168.13.0 [110/128] via 192.168.23.2, 00:58:19, Serial0/0/1
      [110/128] via 192.168.12.1, 00:58:32, Serial0/0/0
      192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.23.0/30 is directly connected, Serial0/0/1
L      192.168.23.1/32 is directly connected, Serial0/0/1
```

### Step 2: Set passive interface as the default on a router.

- a. Issue the **show ip ospf neighbor** command on R1 to verify that R2 is listed as an OSPF neighbor.

```
R1# show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
33.33.33.33	0	FULL/ -	00:00:31	192.168.13.2	Serial0/0/1
22.22.22.22	0	FULL/ -	00:00:32	192.168.12.2	Serial0/0/0

- b. Issue the **passive-interface default** command on R2 to set the default for all OSPF interfaces as passive.

```
R2(config)# router ospf 1
```

```
R2(config-router)# passive-interface default
```

```
R2(config-router)#
```

```
*Apr  3 00:03:00.979: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on Serial0/0/0 from
FULL to DOWN, Neighbor Down: Interface down or detached
```

```
*Apr  3 00:03:00.979: %OSPF-5-ADJCHG: Process 1, Nbr 33.33.33.33 on Serial0/0/1 from
FULL to DOWN, Neighbor Down: Interface down or detached
```

- c. Re-issue the **show ip ospf neighbor** command on R1. After the dead timer expires, R2 will no longer be listed as an OSPF neighbor.

```
R1# show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
33.33.33.33	0	FULL/ -	00:00:34	192.168.13.2	Serial0/0/1

- d. Issue the **show ip ospf interface S0/0/0** command on R2 to view the OSPF status of interface S0/0/0.

```
R2# show ip ospf interface s0/0/0
```

```
Serial0/0/0 is up, line protocol is up
```

```
Internet Address 192.168.12.2/30, Area 0, Attached via Network Statement
```

```
Process ID 1, Router ID 22.22.22.22, Network Type POINT_TO_POINT, Cost: 64
```

Topology-MTID	Cost	Disabled	Shutdown	Topology Name
0	64	no	no	Base

```
Transmit Delay is 1 sec, State POINT_TO_POINT
```

```
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
```

```
oob-resync timeout 40
```

```
No Hellos (Passive interface)
```

```
Supports Link-local Signaling (LLS)
```

```
Cisco NSF helper support enabled
```

```
IETF NSF helper support enabled
```

```
Index 2/2, flood queue length 0
```

```
Next 0x0(0)/0x0(0)
```

```
Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
```

- e. Using the **show ip route** command, check the routing tables of R1 and R3.

Do R1 and R3 still have a route to the 192.168.2.0/24 network? Explain why or why not.

R1 no longer has a route to the 192.168.2.0/24 network because interface S0/0/0 of R2 was set to a passive interface. Thus, not receiving routing updates.

- f. On R2, issue the **no passive-interface** command so the router will send and receive OSPF routing updates. After entering this command, you will see an informational message that a neighbor adjacency has been established with R1.

```
R2(config)# router ospf 1
```

```
R2(config-router)# no passive-interface s0/0/0
```

```
R2(config-router)#
```

```
*Apr  3 00:18:03.463: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on Serial0/0/0 from
LOADING to FULL, Loading Done
```

- g. Re-issue the **show ip route** and **show ip ospf neighbor** commands on R1 and R3, and look for a route to the 192.168.2.0/24 network.

What interface is R3 using to route to the 192.168.2.0/24 network?	
What is the accumulated cost metric for the 192.168.2.0/24 network on R3?	
Does R2 show up as an OSPF neighbor on R1?	Yes
Does R2 show up as an OSPF neighbor on R3?	

Based on these information, what path does a packet take from to reach the 192.168.2.0/24 network from R3?

--

- h. Change interface S0/0/1 on R2 to allow it to advertise OSPF routes the re-issue the **show ip route** and **show ip ospf neighbor** commands on R3.

What interface is R3 using to route to the 192.168.2.0/24 network?	
What is the accumulated cost metric for the 192.168.2.0/24 network on R3 this time?	
Does R2 show up as an OSPF neighbor on R3?	

### Part 3: Configure and Propagate a Static Default Route

In Part 5, you will create a static default route on R2, and then OSPF will propagate that route to the other two routers on the network.

### Step 1: Configure a static default route on R2 to the LO0 Interface.

Configure a static default route on R2 that uses its Loopback0 interface as the next hop.

### Step 2: Have OSPF propagate the default static route.

Issue the **default-information originate** command to include the static default route in the OSPF updates that are sent from R2.

```
R2(config)# router ospf 1
R2(config-router)# default-information originate
```

### Step 3: Verify OSPF static route propagation.

- a. Issue the **show ip route static** command on R2.

```
R2# 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, 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
       + - replicated route, % - next hop override
```

```
Gateway of last resort is 209.165.200.226 to network 0.0.0.0
```

```
S* 0.0.0.0/0 [1/0] via 209.165.200.226
```

- b. Issue the **show ip route** command on R1 to verify the propagation of the static route from R2.

```
R1# 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
       + - replicated route, % - next hop override
```

```
Gateway of last resort is 192.168.12.2 to network 0.0.0.0
```

```
O*E2 0.0.0.0/0 [110/1] via 192.168.12.2, 00:02:57, Serial0/0/0
    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.1.0/24 is directly connected, GigabitEthernet0/0
L      192.168.1.1/32 is directly connected, GigabitEthernet0/0
O      192.168.3.0/24 [110/15634] via 192.168.12.2, 00:03:35, Serial0/0/0
    192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.12.0/30 is directly connected, Serial0/0/0
L      192.168.12.1/32 is directly connected, Serial0/0/0
    192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
```

```
C      192.168.13.0/30 is directly connected, Serial0/0/1
L      192.168.13.1/32 is directly connected, Serial0/0/1
      192.168.23.0/30 is subnetted, 1 subnets
O      192.168.23.0 [110/15624] via 192.168.12.2, 00:05:18, Serial0/0/0
```

Is the default route present in R1?	Yes
-------------------------------------	-----

## Reflection

1. Why is it important to control the router ID assignment when using the OSPF protocol?

This is important because it provides routers unique identification most especially when identifying neighbor adjacencies. Additionally, if interface priorities among routers connected to multiaccess links are equal, router IDs will be the basis for election of DR and BDR.

2. Does a DR/BDR election happen in this lab topology? Why or why not?

No, because the link connecting R1 and R2 is not a multiaccess network type like Ethernet but a Serial . In addition to this, we only have two routers in our topology, meaning that we do not have a multi-access network. Because of this,

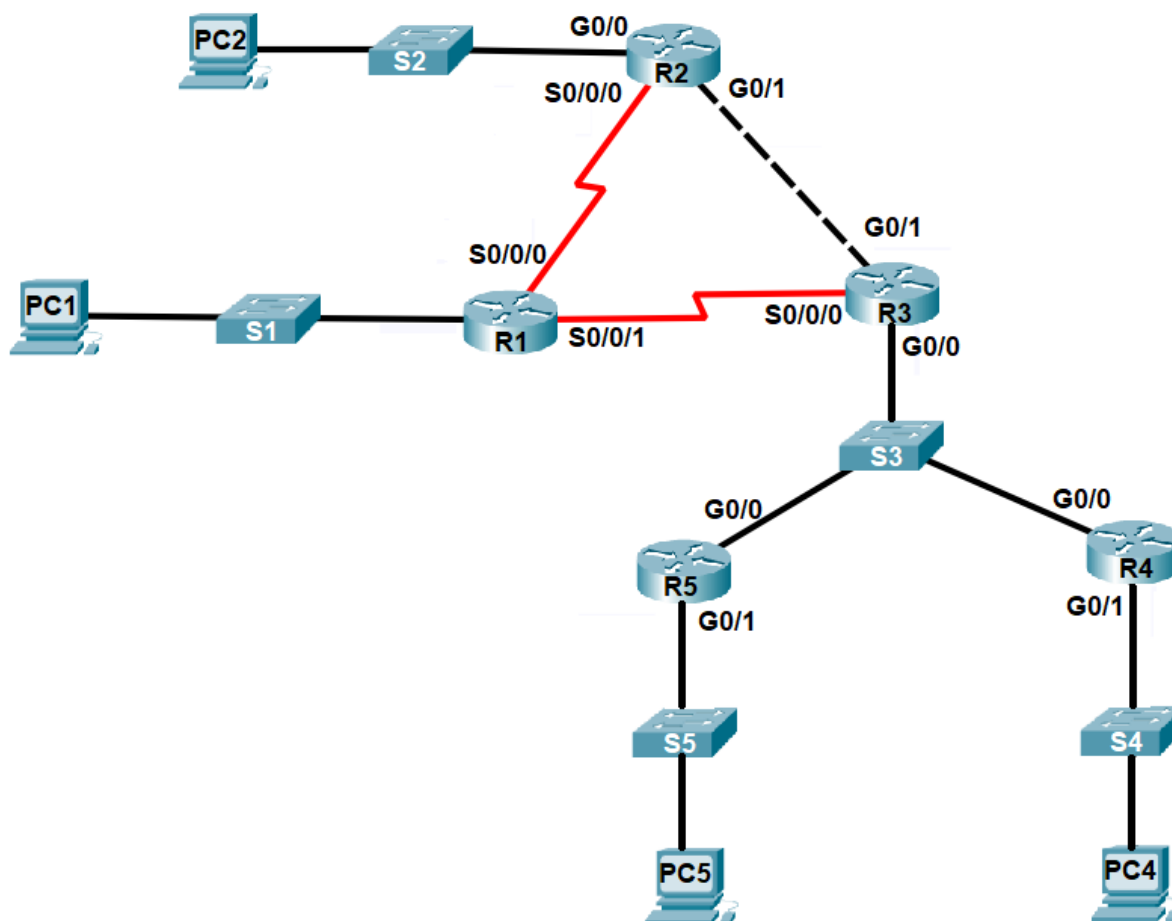
3. Compare the procedures of configuring RIP and OSPF on routers. Give at least 2 similarities and 2 differences that you can observe.

RIP and OSPF are both open standard routing protocols and support both IPv4 and IPv6. RIP is a distance vector routing protocol while OSPF is a link state routing protocol. This means that RIP uses the distance or hop counts to determine the transmission path while OSPF analyzes different sources like speed, cost, and path congestion while identifying the shortest path. RIP protocol also allows only up to 15 hops, while OSPF has no restriction with its hop count.

## Lab 1.2 – Fine Tuning OSPF

This activity comes with an accompanying Packet Tracer file with a partially configured network. Make sure to download the Packet Tracer file from the Animospace assignment page.

### Topology



## Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	172.16.1.1	255.255.255.0	N/A
	S0/0/0	172.16.3.1	255.255.255.252	N/A
	S0/0/1	192.168.10.5	255.255.255.252	N/A
R2	G0/0	172.16.2.1	255.255.255.0	N/A
	S0/0/0	172.16.3.2	255.255.255.252	N/A
	G0/1	192.168.10.1	255.255.255.252	N/A
R3	G0/0	192.168.10.9	255.255.255.248	N/A
	S0/0/0	192.168.10.6	255.255.255.252	N/A
	G0/1	192.168.10.2	255.255.255.252	N/A
R4	G0/0	192.168.10.10	255.255.255.248	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
R4	G0/0	192.168.10.11	255.255.255.248	N/A
	G0/1	192.168.2.1	255.255.255.0	N/A
PC1	NIC	172.16.1.2	255.255.255.0	172.16.1.1
PC2	NIC	172.16.2.2	255.255.255.0	172.16.2.1
PC4	NIC	192.168.1.2	255.255.255.0	192.168.1.1
PC5	NIC	192.168.2.2	255.255.255.0	192.168.2.1

## Objectives

**Part 1: Configure and Verify OSPF Routing**

**Part 2: Change OSPF Metrics**

**Part 3: Configure OSPFv2 Interface Priority to Determine the DR and BDR**

**Part 4: Manually Set Link Type to Bypass DR and BDR Election**

## Background / Scenario

Open Shortest Path First (OSPF) can be fine tuned to optimize performance according to network design. Among these are configurations that control metric calculation, and DR/BDR election.

In this lab, you will configure OSPF routing and use additional commands to adjust path cost, router interface priorities for DR and BDR election, and adjust OSPF link types..

### 1. Configure and Verify OSPF Routing

In Part 1, you will configure OSPFv2 routing on all routers in the network and then verify that routing tables are updated correctly.

### 1. Configure OSPF on routers.

Configure OSPF on all routers using process ID 10 to ensure full connectivity among all hosts in the network. Configure passive interfaces on user LANs.

### 2. Verify OSPF operations.

- a. Using the appropriate commands, verify the OSPF router ID, number of OSPF neighbors, and remote routes learned through OSPF of each router.

Which command is needed to view the OSPF router ID?	show ip protocols
Which command is needed to view the number of OSPF neighbors?	show ip ospf neighbor
Which command is needed to view to routes to remote networks learned through OSPF?	show ip route ospf

Fill in the table below based on the information gathered:

Router	OSPF Router ID	Number of OSPF Neighbors	Number of OSPF Routes
R1	192.168.10.5	2	5
R2	192.168.10.1	2	5
R3	192.168.10.9	4	5
R4	192.168.10.10	2	6
R5	192.168.10.11	2	6

- b. Verify connectivity between hosts by performing ping tests.

Can PC1 ping PC5?	Yes
Can PC2 ping PC4?	Yes
Can PC1 ping PC2?	Yes
Can PC4 ping PC5?	Yes

If any of these do not work, troubleshoot your OSPF configurations.

## 2. Change OSPF Metrics

In Part 2, you will change OSPF metrics using the **auto-cost reference-bandwidth** command, the **bandwidth** command, and the **ip ospf cost** command.

### 1. Change the reference bandwidth on the routers.

The default reference-bandwidth for OSPF is 100Mb/s (Fast Ethernet speed). However, most modern infrastructure devices have links that are faster than 100Mb/s. Because the OSPF cost metric must be an integer, all links with transmission speeds of 100Mb/s or higher have a cost of 1. This results in Fast Ethernet, Gigabit Ethernet, and 10G Ethernet interfaces all having the same cost. Therefore, the reference-bandwidth must be changed to a higher value to accommodate networks with links faster than 100Mb/s.

- a. Issue the **show interface** command on R1 to view the default bandwidth setting for the G0/0 interface.

```
R1# show interface g0/0
GigabitEthernet0/0 is up, line protocol is up
```

```
Hardware is CN Gigabit Ethernet, address is c471.fe45.7520 (bia c471.fe45.7520)
MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full Duplex, 100Mbps, media type is RJ45
output flow-control is unsupported, input flow-control is unsupported
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output 00:17:31, output hang never
Last clearing of "show interface" counters never
...
```

- b. Issue the **show ip route ospf** command on R1 to determine the route to the 192.168.10.8/29 network.

```
R1# show ip route ospf
```

```
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
       + - replicated route, % - next hop override
```

```
Gateway of last resort is not set
```

```
172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
O       172.16.2.0 [110/65] via 172.16.3.2, 00:01:53, Serial0/0/0
O       192.168.1.0 [110/66] via 192.168.10.6, 00:01:18, Serial0/0/1
O       192.168.2.0 [110/66] via 192.168.10.6, 00:01:08, Serial0/0/1
192.168.10.0/24 is variably subnetted, 4 subnets, 3 masks
O       192.168.10.0 [110/65] via 192.168.10.6, 00:00:24, Serial0/0/1
        [110/65] via 172.16.3.2, 00:00:24, Serial0/0/0
O       192.168.10.8 [110/65] via 192.168.10.6, 00:01:18, Serial0/0/0
```

**Note:** The accumulated cost to the 192.168.10.8/29 network from R1 is 65.

- c. Issue the **show ip ospf interface** command on R3 to determine the routing cost for G0/0.

```
R3# show ip ospf interface g0/0
```

```
GigabitEthernet0/0 is up, line protocol is up
Internet address is 192.168.10.9/29, Area 0
Process ID 10, Router ID 192.168.10.9, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DROTHER, Priority 1
Designated Router (ID) 192.168.10.11, Interface address 192.168.10.11
Backup Designated Router (ID) 192.168.10.10, Interface address 192.168.10.10
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:09
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
```



```
Neighbor Count is 2, Adjacent neighbor count is 2
Adjacent with neighbor 192.168.10.11 (Designated Router)
Adjacent with neighbor 192.168.10.10 (Backup Designated Router)
Suppress hello for 0 neighbor(s)
```

- d. Issue the **show ip ospf interface s0/0/1** command on R1 to view the routing cost for S0/0/1.

```
R1# show ip ospf interface s0/0/1
Serial0/0/1 is up, line protocol is up
Internet address is 192.168.10.5/30, Area 0
Process ID 10, Router ID 192.168.10.5, Network Type POINT-TO-POINT, Cost: 64
Transmit Delay is 1 sec, State POINT-TO-POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:02
Index 3/3, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 192.168.10.9
Suppress hello for 0 neighbor(s)
```

The sum of the costs of these two interfaces is the accumulated cost for the route to the 192.168.10.8/29 network on R3 ( $1 + 64 = 65$ ), as can be seen in the output from the **show ip route** command.

- e. Issue the **auto-cost reference-bandwidth 10000** command on R1 to change the default reference bandwidth setting. With this setting, 10Gb/s interfaces will have a cost of 1, 1 Gb/s interfaces will have a cost of 10, and 100Mb/s interfaces will have a cost of 100.

```
R1(config)# router ospf 10
R1(config-router)# auto-cost reference-bandwidth 10000
% OSPF: Reference bandwidth is changed.
Please ensure reference bandwidth is consistent across all routers.
```

- f. Issue the **auto-cost reference-bandwidth 10000** command on routers R2 to R5.
- g. Issue the **show ip ospf interface** command on R1 S0/0/1 and R3 G0/0 to determine the recalculated link costs.

What is the new link cost of R3 G0/0?	10
What is the new link cost of R1 S0/0/1?	6476

- h. Re-issue the **show ip route ospf** command to view the new accumulated cost for the 192.168.10.8/29 route.

What is the new accumulated cost of the route?	6486
------------------------------------------------	------

- i. To reset the reference-bandwidth back to its default value, issue the **auto-cost reference-bandwidth 100** command on all routers.

```
R1(config)# router ospf 10
R1(config-router)# auto-cost reference-bandwidth 100
% OSPF: Reference bandwidth is changed.
Please ensure reference bandwidth is consistent across all routers.
```

### 2. Change the bandwidth for an interface.

On most serial links, the bandwidth metric will default to 1544 Kbits. If this is not the actual speed of the serial link, the bandwidth setting will need to be changed to match the actual speed to allow the route cost to be calculated correctly in OSPF. Use the **bandwidth** command to adjust the bandwidth setting on an interface.

**Note:** A common misconception is to assume that the **bandwidth** command will change the physical bandwidth, or speed, of the link. The command modifies the bandwidth metric used by OSPF to calculate routing costs, and does not modify the actual bandwidth (speed) of the link.

- a. Issue the **show interface s0/0/0** command on R1 to view the current bandwidth setting on S0/0/0. Even though the clock rate, link speed on this interface is set to 128Kb/s, the bandwidth is still showing 1544Kb/s.

```
R1# show interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 192.168.12.1/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
<Output omitted>
```

- b. Issue the **show ip route ospf** command on R1 to view the accumulated cost for the route to network 192.168.23.0/24 using S0/0/0. Note that there are two equal-cost (128) routes to the 192.168.10.0/30 network, one via S0/0/0 and one via S0/0/1.

```
R1# show ip route ospf
...
  172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
O       172.16.2.0 [110/65] via 172.16.3.2, 00:01:53, Serial0/0/0
O       192.168.1.0 [110/66] via 192.168.10.6, 00:01:18, Serial0/0/1
O       192.168.2.0 [110/66] via 192.168.10.6, 00:01:08, Serial0/0/1
  192.168.10.0/24 is variably subnetted, 4 subnets, 3 masks
O       192.168.10.0 [110/65] via 192.168.10.6, 00:00:24, Serial0/0/1
O       [110/65] via 172.16.3.2, 00:00:24, Serial0/0/0
O       192.168.10.8 [110/65] via 192.168.10.6, 00:01:18, Serial0/0/0
```

- c. Issue the **bandwidth 128** command to set the bandwidth on S0/0/0 to 128Kb/s.

```
R1(config)# interface s0/0/0
R1(config-if)# bandwidth 128
```

- d. Issue the **show ip ospf interface s0/0/0** command. The cost for S0/0/0 has changed from 64 to 781 which is an accurate cost representation of the link speed.
- e. Re-issue the **show ip route ospf** command and check the route to the 192.168.10.0/30 network.

What changes can you observe?

Some of the changes that I can observe is the presence of entries in the routing table of R1 that passes through port S0/0/1 unlike before where some passed through port S0/0/0.

Why did this happen?

This change happened because R1 prefers port S0/0/1 after the bandwidth of port S0/0/0 was increased.

- f. Change the bandwidth for interface S0/0/1 to the same setting as S0/0/0 on R1.
- g. Re-issue the **show ip route ospf** command to view the accumulated cost of both routes to the 192.168.10.0/30 network. Note that there are again two equal-cost (782) routes to the network, one via S0/0/0 and one via S0/0/1.

```
R1# show ip route ospf
...
Gateway of last resort is not set

172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
O       172.16.2.0 [110/782] via 172.16.3.2, 00:00:09, Serial0/0/0
O       192.168.1.0 [110/783] via 192.168.10.6, 00:00:09, Serial0/0/1
O       192.168.2.0 [110/783] via 192.168.10.6, 00:00:09, Serial0/0/1
        192.168.10.0/24 is variably subnetted, 4 subnets, 3 masks
O       192.168.10.0 [110/782] via 192.168.10.6, 00:00:09, Serial0/0/1
        [110/782] via 172.16.3.2, 00:00:09, Serial0/0/0
O       192.168.10.8 [110/782] via 192.168.10.6, 00:00:09, Serial0/0/1
```

- h. Issue the **show ip route ospf** command on R3. The accumulated cost of the 172.16.1.0/24 is still showing as 65.

```
R3# show ip route ospf
...
        172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O       172.16.1.0 [110/65] via 192.168.10.5, 00:18:45, Serial0/0/0
O       172.16.2.0 [110/2] via 192.168.10.1, 00:17:55, GigabitEthernet0/1
O       172.16.3.0 [110/65] via 192.168.10.1, 00:17:55, GigabitEthernet0/1
O       192.168.1.0 [110/2] via 192.168.10.10, 00:17:55, GigabitEthernet0/0
O       192.168.2.0 [110/2] via 192.168.10.11, 00:17:55, GigabitEthernet0/0
```

For consistency of cost calculation, the **bandwidth** command needs to be applied on each side of a serial link.

- i. Issue the **bandwidth 128** command on ALL remaining serial interfaces in the topology.

### 3. Change the route cost.

OSPF uses the bandwidth setting to calculate the cost for a link by default. However, you can override this calculation by manually setting the cost of a link using the **ip ospf cost** command. Like the **bandwidth** command, the **ip ospf cost** command only affects the side of the link where it was applied.

- a. Issue the **show ip route ospf** on R1.

```
R1# show ip route ospf
...
172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
O       172.16.2.0 [110/782] via 172.16.3.2, 00:16:45, Serial0/0/0
O       192.168.1.0 [110/783] via 192.168.10.6, 00:16:45, Serial0/0/1
O       192.168.2.0 [110/783] via 192.168.10.6, 00:16:45, Serial0/0/1
        192.168.10.0/24 is variably subnetted, 4 subnets, 3 masks
O       192.168.10.0 [110/782] via 192.168.10.6, 00:16:45, Serial0/0/1
        [110/782] via 172.16.3.2, 00:16:45, Serial0/0/0
O       192.168.10.8 [110/782] via 192.168.10.6, 00:16:45, Serial0/0/1
```

- b. Apply the **ip ospf cost 800** command to the S0/0/1 interface on R1. A cost of 1565 is higher than the accumulated cost of the route through R2 which is 783.

```
R1(config)# interface s0/0/1
R1(config-if)# ip ospf cost 800
```

- c. Re-issue the **show ip route ospf** command on R1 to display the effect this change has made on the routing table. All OSPF routes for R1 are now being routed through R2.

```
R1# show ip route ospf
...
    172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
O       172.16.2.0 [110/782] via 172.16.3.2, 00:18:51, Serial0/0/0
O       192.168.1.0 [110/784] via 172.16.3.2, 00:00:03, Serial0/0/0
O       192.168.2.0 [110/784] via 172.16.3.2, 00:00:03, Serial0/0/0
    192.168.10.0/24 is variably subnetted, 4 subnets, 3 masks
O       192.168.10.0 [110/782] via 172.16.3.2, 00:00:03, Serial0/0/0
O       192.168.10.8 [110/783] via 172.16.3.2, 00:00:03, Serial0/0/0
```

**Note:** Manipulating link costs using the **ip ospf cost** command is the easiest and preferred method for changing OSPF route costs. In addition to changing the cost based on bandwidth, a network administrator may have other reasons for changing the cost of a route, such as preference for a particular service provider or the actual monetary cost of a link or route.

Explain why the route of R1 to the 192.168.10.0/29 network on is now going through R2.

The route of R1 to the 192.168.10.0/29 network is now going through R2 because the OSPF cost of S0/0/1 is higher than OSPF route cost of S0/0/0.

### 3. Configure OSPFv2 Interface Priority to Determine the DR and BDR

In Part 3, you will manipulate the DR and BDR election among R3, R4 and R5. The DR and BDR election process takes place as soon as the first router has its interface enabled on the multiaccess network. This can happen as the routers are powered-on or when the OSPF network command for that interface is configured. If a new router enters the network after the DR and BDR have already been elected, it does not become the DR or BDR, even if it has a higher OSPF interface priority or router ID than the current DR or BDR. Configure the OSPF process on the router with the highest router ID first to ensure that this router becomes the DR.

#### 1. Change router IDs using manual assignment.

Assign router IDs to R3, R4 and R5 as follows: R3 – 192.168.31.33; R4 – 192.168.31.44; R5 – 192.168.31.55. Remember to reset the OSPF process for the new router IDs to take effect. A sample is shown below:

```
R3(config)#router ospf 10
R3(config-router)#router-id 192.168.31.33
R3(config-router)#Reload or use "clear ip ospf process" command, for this to
take effect
R3(config-router)#end
R3#clear ip ospf process
Reset ALL OSPF processes? [no]: y
```

#### 2. Observe the results of an election.

- Force a DR election by reloading S3.
- Wait for the link lights of S3 to turn green then use the command **show ip ospf interface G0/0** on R3, R4 and R5. The output shows the current role of the router in the 192.168.10.8/29 multiaccess network.

```
R3#do show ip ospf interface g0/0
```

```
GigabitEthernet0/0 is up, line protocol is up
Internet address is 192.168.10.9/29, Area 0
Process ID 10, Router ID 192.168.31.33, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DROTHER, Priority 1
Designated Router (ID) 192.168.31.55, Interface address 192.168.10.11
Backup Designated Router (ID) 192.168.31.44, Interface address 192.168.10.10
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:03
...
```

What is the role of R3?	DROTHER
What is the role of R4?	BDR
What is the role of R5?	DR

Why did the election result in these roles for R3, R4 and R5?

The election resulted in these roles for routers R3, R4, and R5 because the router IDs were manually assigned wherein the one with the highest was elected DR, the second to the highest was elected BDR, and the remaining was elected DROTHER.

### 3. Examine changing roles

- a. Monitor the DR and BDR election process with a **debug** command. On R3 and R4, enter the following command.

```
R3# debug ip ospf adj
```

```
R4# debug ip ospf adj
```

Disable the link between R5 and S3 to cause roles to change then wait about 30 seconds for the dead timers to expire on R3 and R4. You can click **Fast Forward Time** to speed up the process.

According to the debug output, which router was elected DR and which router was elected BDR?

R4 was elected DR while Router 3 was elected BDR.

- b. Restore the connection of R5 to S3 and wait for the new DR/BDR elections to occur. You can click **Fast Forward Time** to speed up the process.

Did DR and BDR roles change? Why or why not?

No DR and BDR roles changed because elections were already done between R3 and R4.

- c. Disconnect the Gigabit Ethernet 0/0 interface on R4 to cause roles to change and wait 30 seconds for the holddown timers to expire on R3 and R5. You can click **Fast Forward Time** to speed up the process.

According to the debug output on R3 which router was elected DR and which router was elected BDR?

According to the debug output on R3, R3 was elected BDR while Router 5 or R5 was elected DR.

- d. Restore the connection of the Gigabit Ethernet 0/0 interface on R4.
- e. Turn off debugging on R3 and R4 by entering the command **undebug all**.

### 4. Modify OSPF Priority and Force Elections

- a. Configure R3 G0/0 with OSPF priority 255. A value of 255 is the highest possible interface priority.

```
R3(config)# interface g0/0
R3(config-if)# ip ospf priority 255
R3(config-if)# end
```

- b. Configure R4 G0/0 with OSPF priority 100.

```
R4(config)# interface g0/0
R4(config-if)# ip ospf priority 100
R4(config-if)# end
```

- c. Configure R5 G0/0 with OSPF priority 0. A priority of 0 causes the router to be ineligible to participate in an OSPF election and does not become a DR or BDR.

```
R5(config)# interface g0/0
R5(config-if)# ip ospf priority 0
R5(config-if)# end
```

- d. Force an election by reloading S3. Wait long enough for OSPF to converge and for the DR/BDR election to occur. This should take a few minutes. You can click **Fast Forward Time** to speed up the process.
- e. Use the **show ip ospf interface** command on the appropriate R3, R4 and R5 interfaces to recheck the interface priorities and resulting router roles.

Which router is now DR and which router is now BDR?

Router 4 is now BDR while Router 3 is now DR.

## 2. Manually Set Link Type to Bypass DR and BDR Election

The role of the DR and BDR are needed only in a multiaccess network where multiple OSPF routers are connected to the same link to reduce the number of adjacencies and LSA flooding. For Cisco routers, the election of the DR and BDR are automatically assumed based on the type of interface used to connect to the link. Since Ethernet is considered a multiaccess network type, a DR/BDR election automatically takes place when OSPF is enabled on an Ethernet interface. This election however, is unnecessary if an Ethernet interface is directly connected to another router since it is essentially a point-to-point connection. In Part 4, you will observe the differences in neighbor adjacencies established over point-to-point and multiaccess networks; and manually set an Ethernet connection to point-to-point link type

### 1. Observe the neighbor adjacency of a P2P and multiaccess link.

- a. Issue the **show ip ospf neighbor** command on R2. Notice that although R2 is connected via direct physical links to both R1 and R3, the adjacency status for these 2 routers are different in the output

```
R2# show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.31.33	1	FULL/DR	00:00:37	192.168.10.2	GigabitEthernet0/1
192.168.10.5	0	FULL/-	00:00:37	172.16.3.1	Serial0/0/0

- b. Issue the **show ip ospf interface** command for G0/1 and S0/0/0 on R2 to view the interface link.

```
R2# show ip ospf interface s0/0/0
```

```
Serial0/0/0 is up, line protocol is up
Internet address is 172.16.3.2/30, Area 0
```

```
Process ID 10, Router ID 192.168.10.1, Network Type POINT-TO-POINT, Cost: 781
Transmit Delay is 1 sec, State POINT-TO-POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:04
Index 3/3, flood queue length 0
...
```

R2# **show ip ospf interface g0/1**

```
GigabitEthernet0/1 is up, line protocol is up
Internet address is 192.168.10.1/30, Area 0
Process ID 10, Router ID 192.168.10.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State BDR, Priority 1
Designated Router (ID) 192.168.31.33, Interface address 192.168.10.2
Backup Designated Router (ID) 192.168.10.1, Interface address 192.168.10.1
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:02
Index 2/2, flood queue length 0
...
```

Notice that OSPF considered these links as different types. The G0/1 connection was automatically classified as a 'BROADCAST' type (multiaccess) because of the Ethernet interface; hence a DR/BDR took place even if the physical link is actually a point-to-point connection between 2 routers.

### 2. Manually set the OSPF link type.

- a. Change the OSPF link type of the connection between R2 and R3 to point-to-point. This must be done on both R2 and R3 G0/1.

```
R2(config)# interface g0/1
R2(config-if)# ip ospf network point-to-point
R2(config-if)# end
```

```
R3(config)# interface g0/1
R3(config-if)# ip ospf network point-to-point
R3(config-if)# end
```

- b. Reissue the **show ip ospf neighbor** command on R2 and observe its adjacency status for with R1 and R3.

What difference can you observe from the previous output in Step 1a?

The state of Neighbor ID 192.168.31.33 changed from FULL/DR to just FULL/-.

## Reflection

1. Under what situations would it be important to adjust the reference bandwidth of OSPF? Explain why.

It would be important to adjust the reference bandwidth of OSPF when a network has multi-access links or have faster links like Gigabit Ethernet because OSPF cannot give them a better cost than 1. By adjusting it, the relationship between costs and bandwidth in a network would avoid strange routing patterns.

2. Explain how the results of a DR / BDR elections are obtained in a multiaccess network in relation to the router interface priorities and router IDs.

The results of a DR/BDR election is determined by the router ID and router interface priority. The device with the highest router identifier would be elected the designated router (DR) while the device with the second highest router ID would be elected the backup designated router (BDR). However, if a router interface priority is manually specified, then it will be evaluated before the router ID and the two devices with the highest priorities will be elected DR and BDR, respectively. Moreover, if the router priorities of two devices were to tie, the election would be determined by the router IDs of the devices.

3. What is the benefit of manually setting the OSPF link type of an direct Ethernet connection to point-to-point instead of using the default type used by the router?

An advantage of manually setting the OSPF link type of an direct Ethernet connection to point-to-point instead of using the default type used by the router is that it reduces the number of subnets, which would also reduce the size and effort of the SPF calculation. A DR/BDR election would also not take place since there will always be one device that would receive a packet unlike in a multi-access network with multiple network adjacencies.



## Lab – Explore DNS Traffic

### Objectives

Part 1: Capture DNS Traffic

Part 2: Explore DNS Query Traffic

Part 3: Explore DNS Response Traffic

### Background / Scenario

Wireshark is an open source packet capture and analysis tool. Wireshark gives a detailed breakdown of the network protocol stack. Wireshark allows you to filter traffic for network troubleshooting, investigate security issues, and analyze network protocols. Because Wireshark allows you to view the packet details, it can be used as a reconnaissance tool for an attacker.

In this lab, you will install Wireshark on a Windows system and use Wireshark to filter for DNS packets and view the details of both DNS query and response packets.

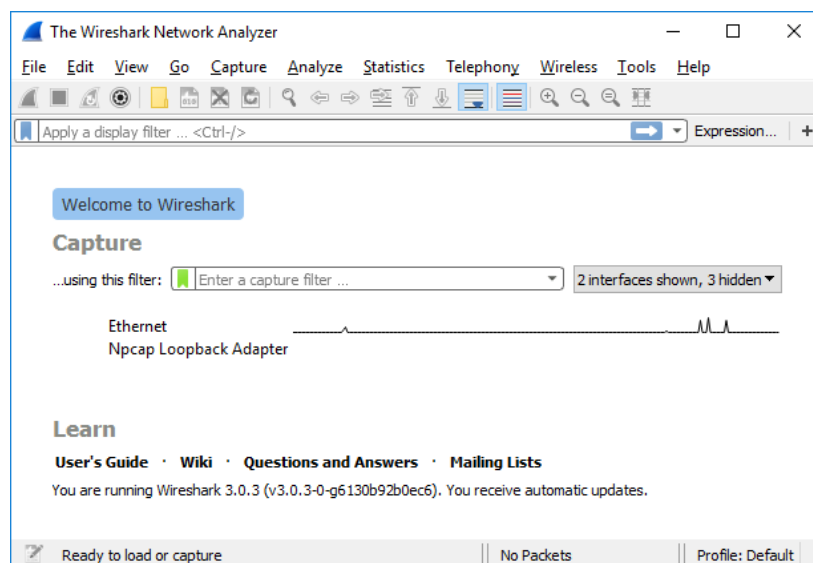
### Required Resources

- 1 Windows PC with internet access and Wireshark installed

### Instructions

#### Step 1: Capture DNS traffic.

- Open **Wireshark** and start a Wireshark capture by double clicking a network interface with traffic.



- At the Command Prompt, enter **ipconfig /flushdns** to clear the DNS cache.

```
C:\Users\Student> ipconfig /flushdns
```

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

- c. Enter **nslookup** at the prompt to enter the nslookup interactive mode.
- d. Enter the domain name of a website. The domain name [www.cisco.com](http://www.cisco.com) is used in this example. Enter **www.cisco.com** at the > prompt.

```
C:\Users\Student> nslookup
```

```
Default Server: UnKnown
```

```
Address: 68.105.28.16
```

```
> www.cisco.com
```

```
Server: UnKnown
```

```
Address: 68.105.28.16
```

```
Non-authoritative answer:
```

```
Name: e2867.dsca.akamaiedge.net
```

```
Addresses: 2001:578:28:68d::b33
```

```
2001:578:28:685::b33
```

```
96.7.79.147
```

```
Aliases: www.cisco.com
```

```
www.cisco.com.akadns.net
```

```
wwwds.cisco.com.edgekey.net
```

```
wwwds.cisco.com.edgekey.net.globalredir.akadns.net
```

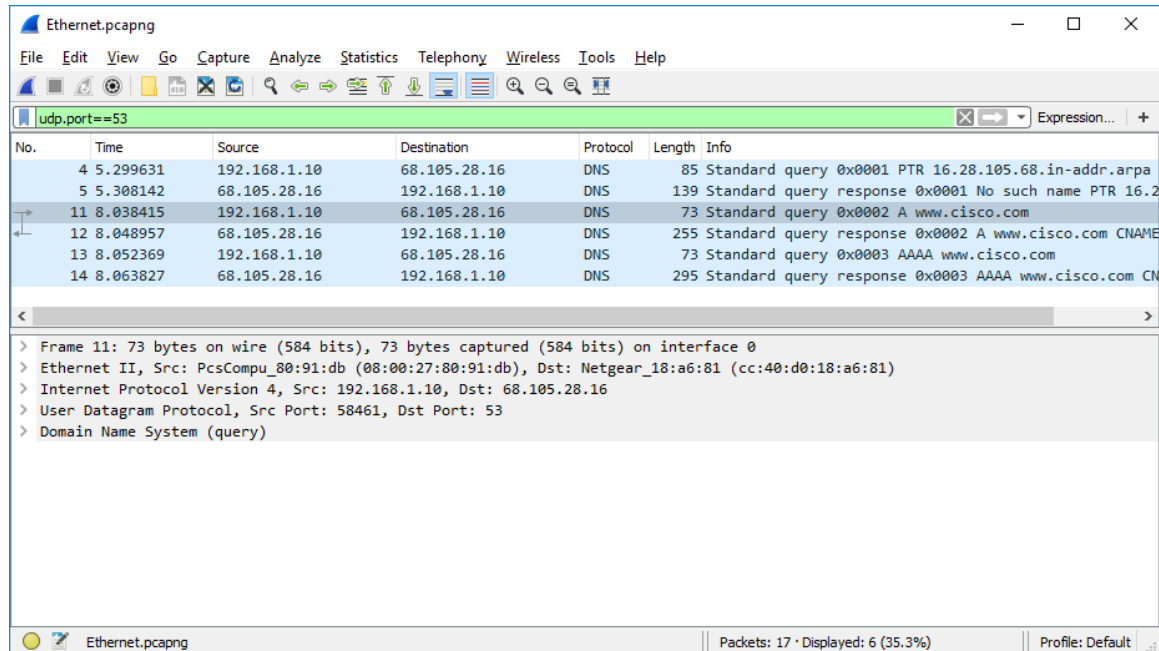
- e. Enter **exit** when finished to exit the nslookup interactive mode. Close the command prompt.
- f. Click **Stop capturing packets** to stop the Wireshark capture.

### Step 2: Explore DNS Query Traffic

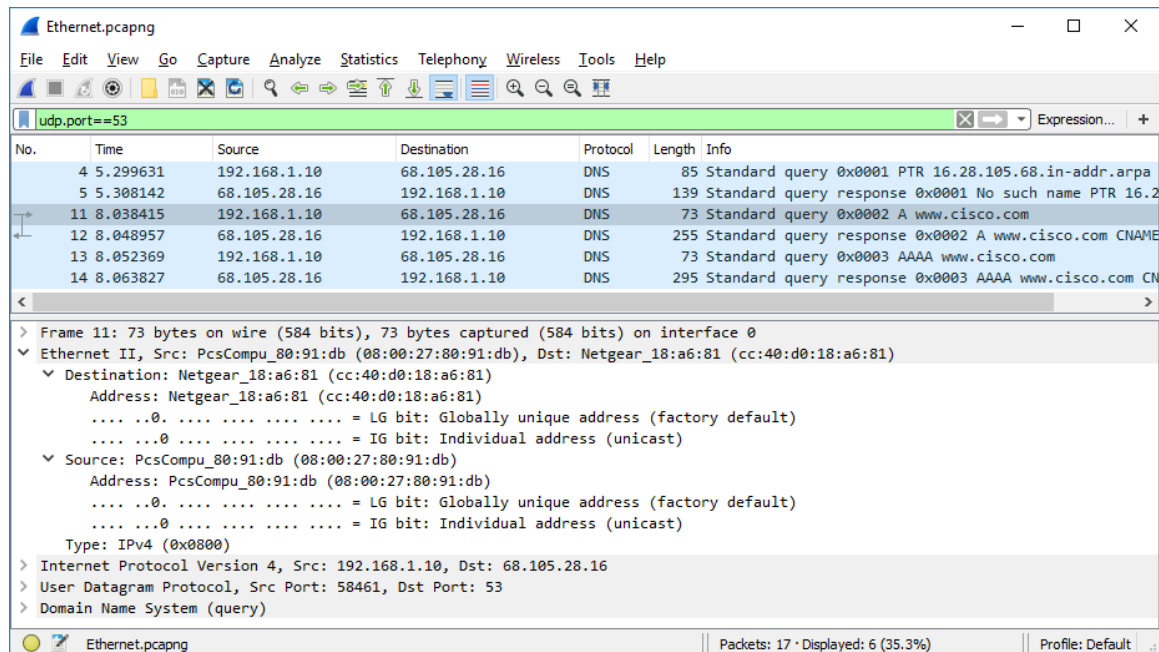
- a. Observe the traffic captured in the Wireshark Packet List pane. Enter **udp.port == 53** in the filter box and click the arrow (or press enter) to display only DNS packets.
- b. Select the DNS packet labeled **Standard query 0x0002 A www.cisco.com**.

## Lab – Explore DNS Traffic

In the Packet Details pane, notice this packet has Ethernet II, Internet Protocol Version 4, User Datagram Protocol and Domain Name System (query).



- c. Expand **Ethernet II** to view the details. Observe the source and destination fields.



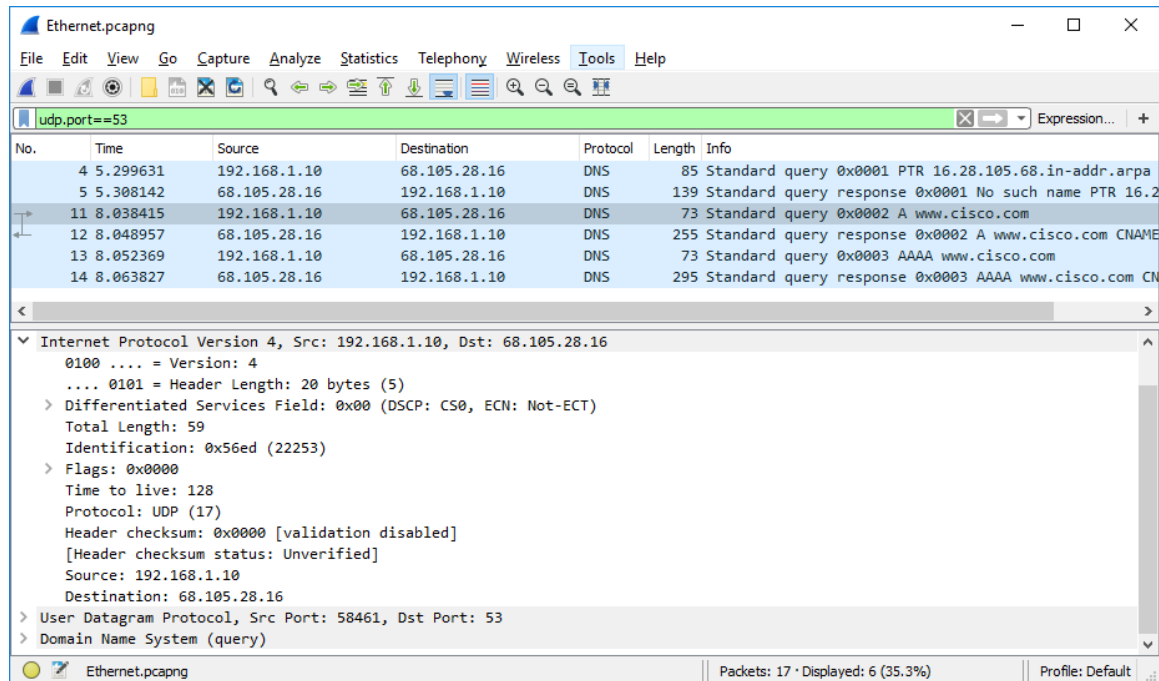
What are the source and destination MAC addresses?

The source MAC address is 28:ee:52:b9:eb:1e while the destination MAC address is 0c:7a:15:d6:9f:11

Which network interfaces are these MAC addresses associated with?

The source MAC address is associated with the NIC on the PC and the destination MAC address is associated with the default gateway or local DNS server.

- a. Expand **Internet Protocol Version 4**. Observe the source and destination IPv4 addresses.



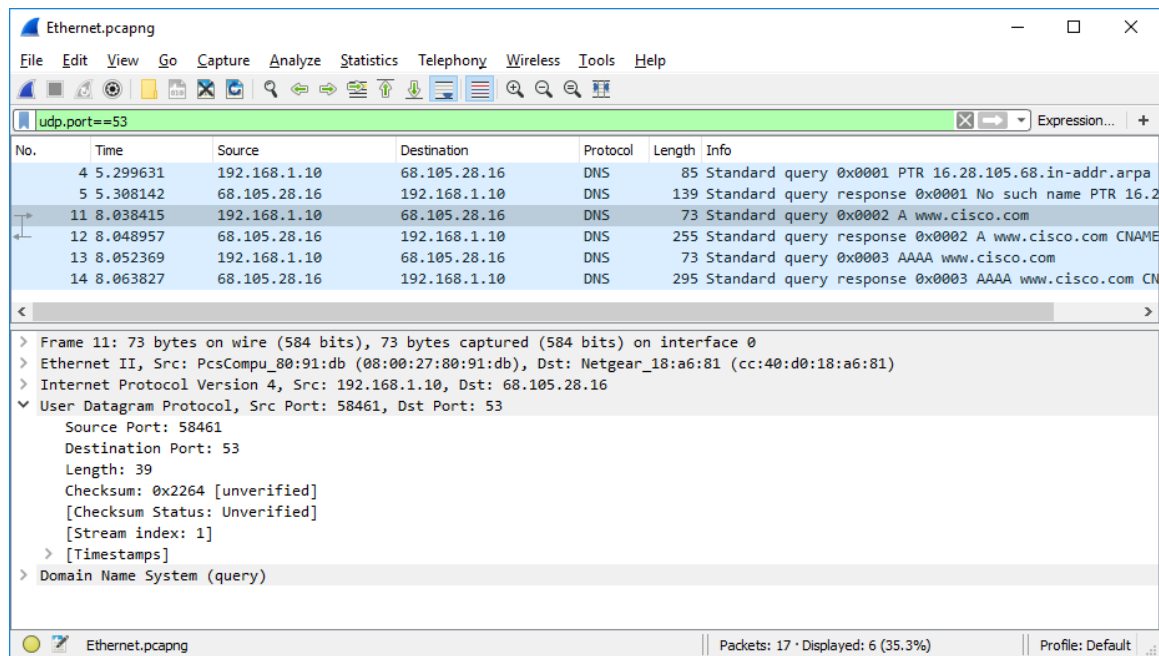
What are the source and destination IP addresses?

The source IP address is 192.168.100.1 while the destination IP address is 192.168.68.121

Which network interfaces are these IP addresses associated with?

The source IP address is associated with the NIC on the PC and the destination IP address is associated with the default gateway.

- b. Expand the **User Datagram Protocol**. Observe the source and destination ports.



What are the source and destination ports?

The source port is 53 while the destination port is 59736.

What is the default DNS port number?

The default DNS port number is 53.

- c. Open a Command Prompt and enter **arp -a** and **ipconfig /all** to record the MAC and IP addresses of the PC.

```
C:\Users\Student> arp -a
```

```
Interface: 192.168.1.10 --- 0x4
Internet Address      Physical Address      Type
192.168.1.1           cc-40-d0-18-a6-81     dynamic
192.168.1.122         b0-a7-37-46-70-bb     dynamic
192.168.1.255         ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.252           01-00-5e-00-00-fc     static
239.255.255.250       01-00-5e-7f-ff-fa     static
255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

```
C:\Users\Student> ipconfig /all
```

### Windows IP Configuration

```
Host Name . . . . . : DESKTOP
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
```

### Ethernet adapter Ethernet:

```
Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address. . . . . : 08-00-27-80-91-DB
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::d829:6d18:e229:a705%4(Preferred)
IPv4 Address. . . . . : 192.168.1.10(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Tuesday, August 20, 2019 5:39:51 PM
Lease Expires . . . . . : Wednesday, August 21, 2019 5:39:50 PM
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 50855975
DHCPv6 Client DUID. . . . . : 00-01-00-01-24-21-BA-64-08-00-27-80-91-DB
DNS Servers . . . . . : 68.105.28.16
                        68.105.29.16
NetBIOS over Tcpip. . . . . : Enabled
```

Compare the MAC and IP addresses in the Wireshark results to the results from the **ipconfig /all** results. What is your observation?

It can be observed that the Wireshark results are the same as the one in ipconfig/all but the MAC address of the gateway is not listed in ipconfig/all. It can also be seen that the packet is from the PC's network interface going towards the DNS server.

- d. Expand **Domain Name System (query)** in the Packet Details pane. Then expand the **Flags** and **Queries**.

## Lab – Explore DNS Traffic

Observe the results. The flag is set to do the query recursively to query for the IP address to [www.cisco.com](http://www.cisco.com).

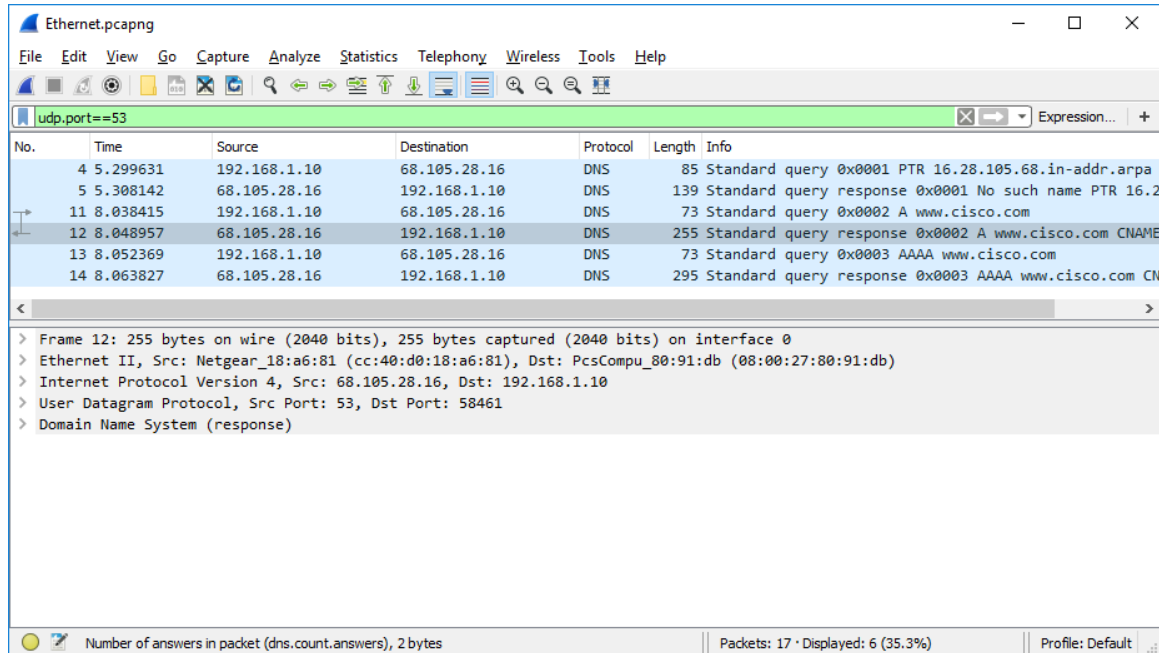
The image shows a Wireshark packet capture window titled "Ethernet.pcapng". The filter bar at the top is set to "udp.port==53". The packet list shows several DNS packets. Packet 11 is selected, showing a "Standard query" for "www.cisco.com". The packet details pane shows the following structure:

- Frame 11: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
- Ethernet II, Src: PcsCompu\_80:91:db (08:00:27:80:91:db), Dst: Netgear\_18:a6:81 (cc:40:d0:18:a6:81)
- Internet Protocol Version 4, Src: 192.168.1.10, Dst: 68.105.28.16
- User Datagram Protocol, Src Port: 58461, Dst Port: 53
- Domain Name System (query)
  - Transaction ID: 0x0002
  - Flags: 0x0100 Standard query
    - 0... .. = Response: Message is a query
    - .000 0... .. = Opcode: Standard query (0)
    - .... .. = Truncated: Message is not truncated
    - .... ..1 .... = Recursion desired: Do query recursively
    - .... .. .0.. .... = Z: reserved (0)
    - .... .. ...0 .... = Non-authenticated data: Unacceptable
  - Questions: 1
  - Answer RRs: 0
  - Authority RRs: 0
  - Additional RRs: 0
  - Queries
    - www.cisco.com: type A, class IN
      - Name: www.cisco.com
      - [Name Length: 13]
      - [Label Count: 3]
      - Type: A (Host Address) (1)
      - Class: IN (0x0001)

The status bar at the bottom indicates "Do query recursively? (dns.flags.recdesired), 2 bytes" and "Packets: 17 · Displayed: 6 (35.3%)".

### Step 3: Explore DNS Response Traffic

- Select the corresponding response DNS packet labeled **Standard query response 0x0002 A www.cisco.com**.



What are the source and destination MAC and IP addresses and port numbers?

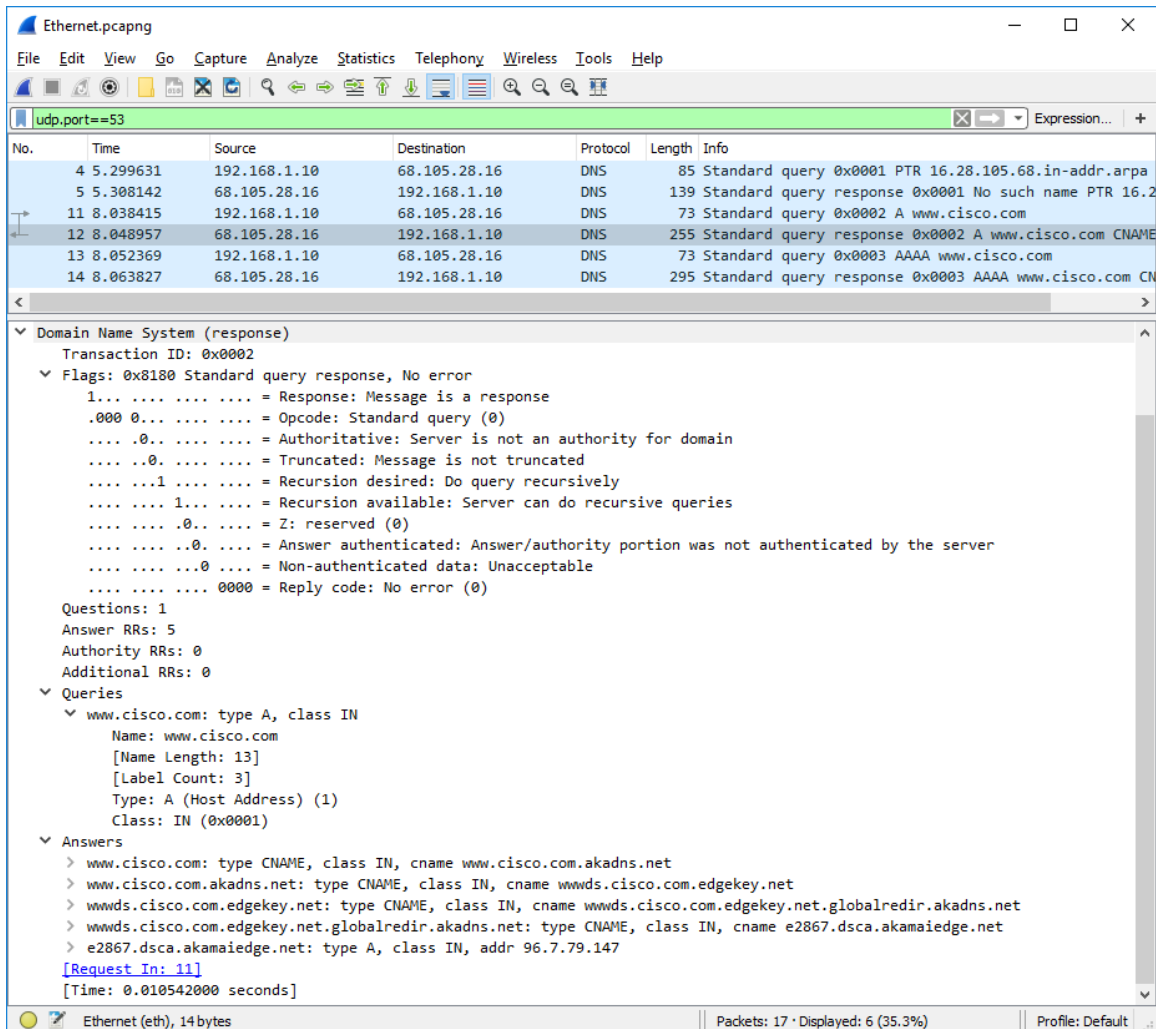
The source's MAC address is 0c:7a:15:d6:9f:11 while the IP address is 192.168.68.121 and the port number is 59736. On the other hand, the destination's MAC address is 28:ee:52:b9:eb:1e while the IP address is 192.168.100.1 and the port number is 53.

How do they compare to the addresses in the DNS query packets?

The roles of the two devices have switched wherein the host computer is now receiving packets from the gateway. This means that the source addresses and port numbers have become the destination addresses and port numbers, and vice versa.



- b. Expand **Domain Name System (response)**. Then expand the **Flags**, **Queries**, and **Answers**. Observe the results.



The screenshot shows a Wireshark packet capture of DNS traffic. The packet list at the top shows several DNS packets. The packet details pane is expanded to show the 'Domain Name System (response)' section for a specific packet. The flags section shows the response is a standard query response with no error. The queries section shows a query for 'www.cisco.com' of type A, class IN. The answers section shows several CNAME and A records, including 'www.cisco.com.akadns.net' and 'www.cisco.com.akadns.net.globalredir.akadns.net'.

```

Domain Name System (response)
  Transaction ID: 0x0002
  Flags: 0x8180 Standard query response, No error
    1... .. = Response: Message is a response
    .000 0... .. = Opcode: Standard query (0)
    .... 0... .. = Authoritative: Server is not an authority for domain
    .... 0... .. = Truncated: Message is not truncated
    .... 1... .. = Recursion desired: Do query recursively
    .... 1... .. = Recursion available: Server can do recursive queries
    .... 0... .. = Z: reserved (0)
    .... 0... .. = Answer authenticated: Answer/authority portion was not authenticated by the server
    .... 0... .. = Non-authenticated data: Unacceptable
    .... 0000 = Reply code: No error (0)
  Questions: 1
  Answer RRs: 5
  Authority RRs: 0
  Additional RRs: 0
  Queries
    www.cisco.com: type A, class IN
      Name: www.cisco.com
      [Name Length: 13]
      [Label Count: 3]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
  Answers
    www.cisco.com: type CNAME, class IN, cname www.cisco.com.akadns.net
    www.cisco.com.akadns.net: type CNAME, class IN, cname wwwds.cisco.com.edgekey.net
    wwwds.cisco.com.edgekey.net: type CNAME, class IN, cname wwwds.cisco.com.edgekey.net.globalredir.akadns.net
    wwwds.cisco.com.edgekey.net.globalredir.akadns.net: type CNAME, class IN, cname e2867.dsca.akamaiedge.net
    e2867.dsca.akamaiedge.net: type A, class IN, addr 96.7.79.147
  [Request In: 11]
  [Time: 0.010542000 seconds]
  
```

Can the DNS server do recursive queries?

Yes, the DNS server can do recursive queries.

- c. Observe the CNAME and A records in the answers details.

How do the results compare to nslookup results?

The results in the CNAME and A records class compared to the nslookup results are the same.

### Reflection Question

1. From the Wireshark results, what else can you learn about the network when you remove the filter?

From the Wireshark results, removing the filter shows other packets like DHCP and ARP. This means that one can gain information from these packets and gather information about the device and their function in the network.

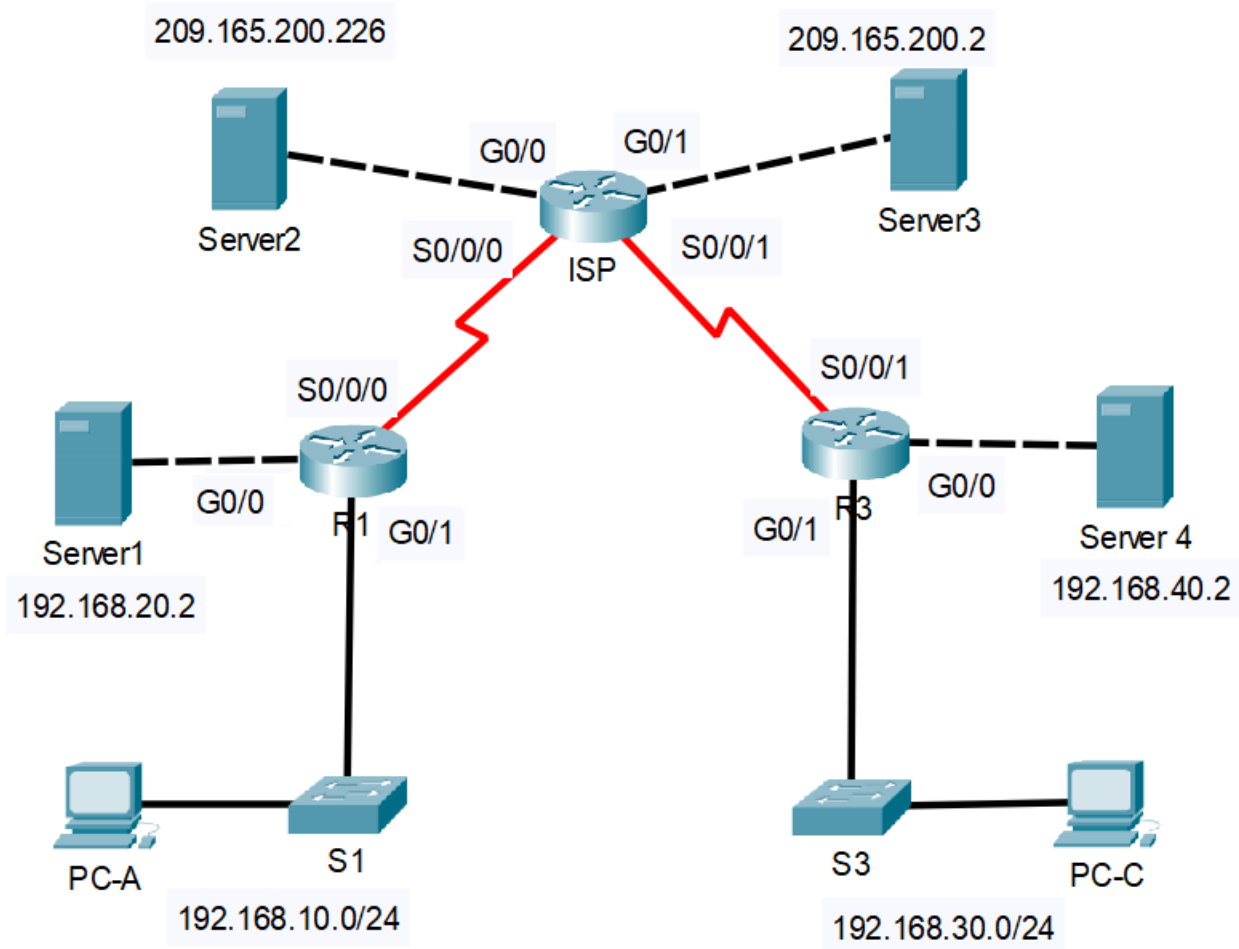
2. How can an attacker use Wireshark to compromise your network security?

Wireshark is a packet capture tool that would intercept, capture, and store network traffic. Thus, an attacker may be able to sniff the traffic flow between client and server that may contain sensitive information that would be used against users.

## Lab 3.1 Configuring and Verifying Extended ACLs

This activity comes with an accompanying Packet Tracer file with a partially configured network. Make sure to download the Packet Tracer file from the Animospace assignment page.

### Topology



## Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.10.1	255.255.255.0	N/A
	G0/0	192.168.20.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
ISP	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
	G0/0	209.165.200.225	255.255.255.224	N/A
	G0/1	209.165.201.1	255.255.255.224	N/A
R3	G0/1	192.168.30.1	255.255.255.0	N/A
	G0/0	192.168.40.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
S1	VLAN 1	192.168.10.11	255.255.255.0	192.168.10.1
S3	VLAN 1	192.168.30.11	255.255.255.0	192.168.30.1
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-C	NIC	192.168.30.3	255.255.255.0	192.168.30.1
Server1	NIC	192.168.20.2	255.255.255.0	192.168.20.1
Server2	NIC	209.165.200.226	255.255.255.225	209.165.200.225
Server3	NIC	209.165.200.2	255.255.255.225	209.165.200.1
Server4	NIC	192.168.40.2	255.255.255.0	192.168.40.1

## Objectives

**Part 1: Configure Devices and Verify Connectivity**

**Part 2: Configure and Verify Extended Numbered and Named ACLs**

**Part 3: Modify and Verify Extended ACLs**

## Background / Scenario

Extended access control lists (ACLs) are extremely powerful. They offer a much greater degree of control than standard ACLs as to the types of traffic that can be filtered, as well as where the traffic originated and where it is going.

In this lab, you will set up filtering rules for two offices represented by R1 and R3. Management has established some access policies between the LANs located at R1 and R3, which you must implement. The ISP router between R1 and R3 does not have any ACLs placed on it.

Within your LAN, you have the following services enabled:

1. HTTP and HTTPS on Server1 and Server4
2. SSH service on R3 with username **admin** and password **class**

3. Telnet service on R1, R3, and S1 using the password **cisco**
4. Console access to R1, R3, ISP, S1 and S3 using the password **cisco**
5. Privileged EXEC mode access to R1, R3, ISP, S1 and S3 using the password **class**

### Part 1: **Configure Devices and Verify Connectivity**

In Part 1, you will configure additional settings on the routers. Refer to the Topology and Addressing Table for device names and address information.

#### Step 1: **Configure OSPF routing on R1, ISP, and R3.**

- a. Assign 1 as the OSPF process ID and advertise all networks on R1, ISP, and R3. The OSPF configuration for R1 is included for reference.

```
R1(config)# router ospf 1
R1(config-router)# network 192.168.10.0 0.0.0.255 area 0
R1(config-router)# network 192.168.20.0 0.0.0.255 area 0
R1(config-router)# network 10.1.1.0 0.0.0.3 area 0
```

- b. After configuring OSPF on R1, ISP, and R3, verify that all routers have complete routing tables listing all networks. Troubleshoot if this is not the case.

#### Step 2: **Verify connectivity between devices.**

**Note:** It is very important to verify connectivity **before** you configure and apply ACLs! Ensure that your network is properly functioning before you start to filter out traffic.

- a. From PC-A, ping PC-C, Server4, and the serial interfaces on R3.

Were your pings successful? **Yes**

- b. From R1, ping PC-C, Server4 and the serial interface on R3.

Were your pings successful? **Yes**

- c. From PC-C, ping PC-A, Server1 and the serial interface on R1.

Were your pings successful? **Yes**

- d. From R3, ping PC-A, Server1 and the serial interface on R1.

Were your pings successful? **Yes**

- e. From PC-A, ping Server2 and Server3

Were your pings successful? **Yes**

- f. From PC-C, ping Server2 and Server3

Were your pings successful? **Yes**

- g. Open a web browser on PC-A and go to <http://209.165.200.226>. You should be able to access the webpage hosted on Server2

- h. Open a web browser on PC-C and go to <http://192.168.20.2>. You should be able to access the webpage hosted on Server1.

### Part 2: **Configure and Verify Extended Numbered and Named ACLs**

Extended ACLs can filter traffic in many different ways. Extended ACLs can filter on source IP addresses, source ports, destination IP addresses, destination ports, as well as various protocols and services.

Security policies are as follows:

1. Allow web traffic originating from the 192.168.10.0/24 network to go to any network.
2. Allow an SSH connection to the R3 serial interface from PC-A.
3. Allow users on 192.168.10.0/24 network access to 192.168.20.0/24 network.
4. Allow web traffic originating from the 192.168.30.0/24 network to access Server1 and the 209.165.200.224/27 network on ISP. The 192.168.30.0/24 network should NOT be allowed to access any other network via the web.

In looking at the security policies listed above, you will need at least two ACLs to fulfill the security policies. A best practice is to place extended ACLs as close to the source as possible. We will follow this practice for these policies.

### Step 1: Configure a numbered extended ACL on R1 for security policy numbers 1 and 2.

You will use a numbered extended ACL on R1. What are the ranges for extended ACLs?

The ranges for extended ACLs are 100 to 199 and 2000 to 2699.

- a. Configure the ACL on R1. Use 100 for the ACL number.

```
R1(config)# access-list 100 remark Allow Web & SSH Access
R1(config)# access-list 100 permit tcp host 192.168.10.3 host 10.2.2.1 eq 22
R1(config)# access-list 100 permit tcp any any eq 80
```

What do the numbers 22 and 80 signify in the command output listed above?

The numbers are the destination ports. Port number 22 is for SSH while port 80 is for HTTP protocol.

To what interface should ACL 100 be applied?

ACL 100 should be applied to interface G0/1 of R1.

In what direction should ACL 100 be applied?

ACL 100 should be applied inward.

- b. Perform the necessary configurations to apply ACL 100 on the correct interface and direction
- c. Verify ACL 100.
- 1) Open up a web browser on PC-A, and access <http://209.165.200.226> (Server 2). It should be successful; troubleshoot, if not.
  - 2) Establish an SSH connection from PC-A to R3 using 10.2.2.1 for the IP address. Log in with **admin** and **class** for your credentials. It should be successful; troubleshoot, if not.
  - 3) From privileged EXEC mode prompt on R1, issue the **show access-lists** command.

```
R1# show access-lists
Extended IP access list 100
  10 permit tcp host 192.168.10.3 host 10.2.2.1 eq 22 (22 matches)
  20 permit tcp any any eq www (111 matches)
```

- 4) From the PC-A command prompt, issue a ping to 10.2.2.1. Describe what happens and explain your results.

The ping is unsuccessful and states Destination host unreachable. This could be because of the applied ACL that only allows web and SSH traffic and the implicit “deny any” of every ACL.

### Step 2: Configure a named extended ACL on R3 for security policy number 4.

- a. Configure the policy on R3. Name the ACL WEB-POLICY.

```
R3(config)# ip access-list extended WEB-POLICY
R3(config-ext-nacl)# permit tcp 192.168.30.0 0.0.0.255 host 192.168.20.2 eq 80
R3(config-ext-nacl)# permit tcp 192.168.30.0 0.0.0.255 209.165.200.224
0.0.0.31 eq 80
```

- b. The ACL WEB-POLICY will be applied to the S0/0/1 interface of R3.

Give the commands to do so with the correct ACL direction

```
R3(config)# int s0/0/1
R3(config-if)# ip access-group WEB-POLICY out
```

- c. Verify the ACL WEB-POLICY.

- 1) From R3 privileged EXEC mode command prompt, issue the **show ip interface s0/0/1** command.

What, if any, is the name of the ACL?

The name of the ACL is WEB-POLICY.

In what direction is the ACL applied?

The direction that the ACL is applied in is outbound.

- 2) Open up a web browser on PC-C and access <http://209.165.200.256> (Server2). It should be successful; troubleshoot, if not.
- 3) From PC-C, open a web session to <http://192.168.20.2> (Server1). It should be successful; troubleshoot, if not.
- 4) From PC-C, open a web session to <http://209.165.201.2> (Server3). It should fail; troubleshoot, if not.
- 5) From a PC-C command prompt, ping PC-A. What was your result and why?

The ping was unsuccessful and the result is “Destination host unreachable” because the applied ACL only allows web traffic to exit from network 192.168.30.0/24

### Part 3: Modify and Verify Extended ACLs

Because of the ACLs applied on R1 and R3, no pings or any other kind of traffic is allowed between the LAN networks on R1 and R3. Management has decided that all traffic between the 192.168.10.0/24 and 192.168.30.0/24 networks should be allowed. You must modify both ACLs on R1 and R3.

### Step 1: Modify ACL 100 on R1.

- a. From R1 privileged EXEC mode, issue the **show access-lists** command.

How many lines are there in this access list?

There are two lines in this access list.

- b. Enter global configuration mode and modify the ACL on R1.

```
R1(config)# ip access-list extended 100
R1(config-ext-nacl)# 30 permit ip 192.168.10.0 0.0.0.255 192.168.30.0
0.0.0.255
R1(config-ext-nacl)# end
```

- c. Issue the **show access-lists** command.

Where did the new line that you just added appear in ACL 100?

The new line appeared in the third line or end of ACL 100.

### Step 2: Modify ACL WEB-POLICY on R3.

- a. From R3 privileged EXEC mode, issue the **show access-lists** command.

How many lines are there in this access list?

There are two lines in this access list.

- b. Enter global configuration mode and modify the ACL on R3.

```
R3(config)# ip access-list extended WEB-POLICY
R3(config-ext-nacl)# 30 permit ip 192.168.30.0 0.0.0.255 192.168.10.0
0.0.0.255
R3(config-ext-nacl)# end
```

- c. Issue the **show access-lists** command to verify that the new line was added at the end of the ACL.

### Step 3: Verify modified ACLs.

- a. From PC-A, ping the IP address of PC-C. Were the pings successful?

Yes, the pings were successful.

- b. From PC-C, ping the IP address of PC-A. Were the pings successful?

Yes, the pings were successful.

Why did the ACLs work immediately for the pings after you changed them?

The ACLs worked immediately for the pings after we changed them because the ACLs were applied close to the traffic source and still applied in their interfaces with the "ip access-group" command.



### Reflection

1. Why is careful planning and testing of ACLs required?

Careful planning and testing of ACLs is required because if not ACLs are not implemented properly, they can prevent the network from being functional in the first place. This can be the scenario if traffic that is not meant to be blocked is blocked. It is also important to check if they are filtering traffic as intended, because if not, it is possible that traffic from specific sources that is meant to be blocked actually has access to the network. Ultimately, without careful planning and testing of ACLs, legitimate traffic may be unintentionally blocked from entering or leaving a network.

2. Why is it recommended to apply extended ACLS as close as possible to the source of the traffic to be filtered?

It is recommended to apply extended ACLs and ACLs in general as close as possible to the source of traffic to be filtered because it is undesirable for unwanted traffic to be able to enter the network in the first place. The sooner the unwanted traffic can be denied, the better, so that there will not be any unnecessary traffic within the topology.

3. Why are OSPF hello packets and routing updates not blocked by the implicit **deny any** access control entry (ACE) or ACL statement of the ACLs applied to R1 and R3?

The OSPF hello packets and routing updates are not blocked by the implicit deny any ACE because they originated from routers R1 and R3 and are not subject to outgoing ACL

4. What advantages do extended ACLs provide compared to standard ACLs?

Some of the advantages of extended ACL compared to standard ACLs is that it can distinguish and filter packets through source address, destination address, protocol and port number. Unlike standard ACL's it is only limited to permit or deny the source ip unable to confirm if the packet reached its destination. Additionally, since extended ACLs can also filter protocol and port number it is more specific, which allows it to filter virtually any kind of traffic generated.