Advanced Cisco Networking Academy: Designing a Multi-Area OSPF Network

Colin J. Faletto, CCNA

Networking Academy

Purpose

This lab is intended to be a refresher course to review the skills required to set up an OSPF network. Simultaneously, the lab adds a layer of complexity compared to the content taught in year 1 Cisco by making students learn how OSPF connects across multiple areas, and how to route IPv4/IPv6 traffic through a Layer 3 Switch.

Background

Open Shortest Path First is a routing protocol that uses link state advertisements to automatically build a network topology and provide end-to-end connectivity across networks. It was developed by the Internet Engineering Task Force, or IETF, a group that develops standards and operates under the Internet Society non-profit organization. This lab uses both OSPFv2 and OSPFv3, which operate similarly but use IPv4 and IPv6 addresses respectively. OSPFv2 is specified in RFC 2328 and OSPFv3 is specified in RFC 5320.

OSPF regularly updates its topology by detecting network changes such as dead routers. OSPF-enabled routers send hello messages to their neighbors at a given interval and assumes a neighboring router is dead after a longer interval.

OSPF-enabled routers can have two different types of relationships with each other: neighbor relationships and adjacencies. Neighbor relationships, which are automatically formed in P2P, broadcast, and point-to-multipoint networks, are formed using hello messages and simply inform routers of each other's existence on the network. Adjacencies are a more complex type of relationship that allows routers to exchange routing information with each other.

The OSPF protocol has several different network types, each of which affect how relationships between routers are formed and maintained: point-to-point (P2P), broadcast, non-broadcast multi-access (NBMA), point-to-multipoint, and point-to-multipoint non-broadcast. A broadcast network is used by default and is the most common type of network. Broadcast networks and NBMA networks are the only type of networks to hold designated router elections. In a broadcast network, each router forms an adjacency to the designated and backup designated routers automatically. In an NBMA network, adjacencies to the DR/BDR can be formed, but neighbors must be manually configured before these adjacencies are formed. P2P and broadcast networks have hello timers of 10 seconds and dead timers of 40 seconds, while the other network types have hello timers of 30 seconds and dead timers of 120 seconds.

OSPF allows its network to be compartmentalized through areas. For the protocol to work, a backbone area (area 0 by default) must be set up and connected to all other areas. OSPF-enabled routers can have interfaces in more than one area as long as the next-hop router's connected interface is in the same area.

OSPF has several different types of routers which each work in harmony to connect different areas: backbone routers, internal routers, area border routers, and autonomous system border routers. OSPF routers can fall under one or more of these router types. Backbone routers have all their interfaces reside entirely within the backbone area. Internal routers have all their interfaces reside within one area that isn't

the backbone. Area border routers have interfaces in more than one area and serve as an inter-area connection, maintaining separate routing information for each area. Autonomous system border routers maintain a connection to a network outside of the OSPF protocol. They can translate information from this outside network to OSPF routes.

Lab Summary

In this lab, we set up a multi-area OSPF network with three areas and six total network devices. In area 0, we set up two area border routers. In area 1, we set up two internal routers, with the edge router connected to a PC. In area 2, we set up one internal router and one Layer 3 switch acting as an OSPF-enabled internal router, which also acted as the opposite network edge and was connected to another PC. We gave each network device a basic configuration with a hostname, passwords, and an MOTD, and assigned them each a unique OSPF router ID. We then configured IPv4 and IPv6 addresses on each connected interface, opting to configure OSPF through the interfaces rather than using network statements.

Lab Commands

```
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
```

Sets the Switch Database Management (SDM) template to a template that supports IPv4 and IPv6. This command will only work after a reload, is persistent regardless of the startup configuration, and must be entered on a L3 switch before IPv6 services will function.

```
Switch(config)# ip routing

Switch(config)# ipv6 unicast-routing
```

Enables IP services on a switch for IPv4 and IPv6. These commands must be entered on a L3 switch before IP addresses can be configured.

```
Switch(config)# router ospf 1

Switch(config-router)# router-id <id>
```

Configures OSPF for IPV4 with a process ID of 1, and configures a router ID.

```
Switch(config)# ipv6 router ospf 1

Switch(config-rtr)# router-id <id>
```

Configures OSPF for IPV6 with a process ID of 1, and configures a router ID.

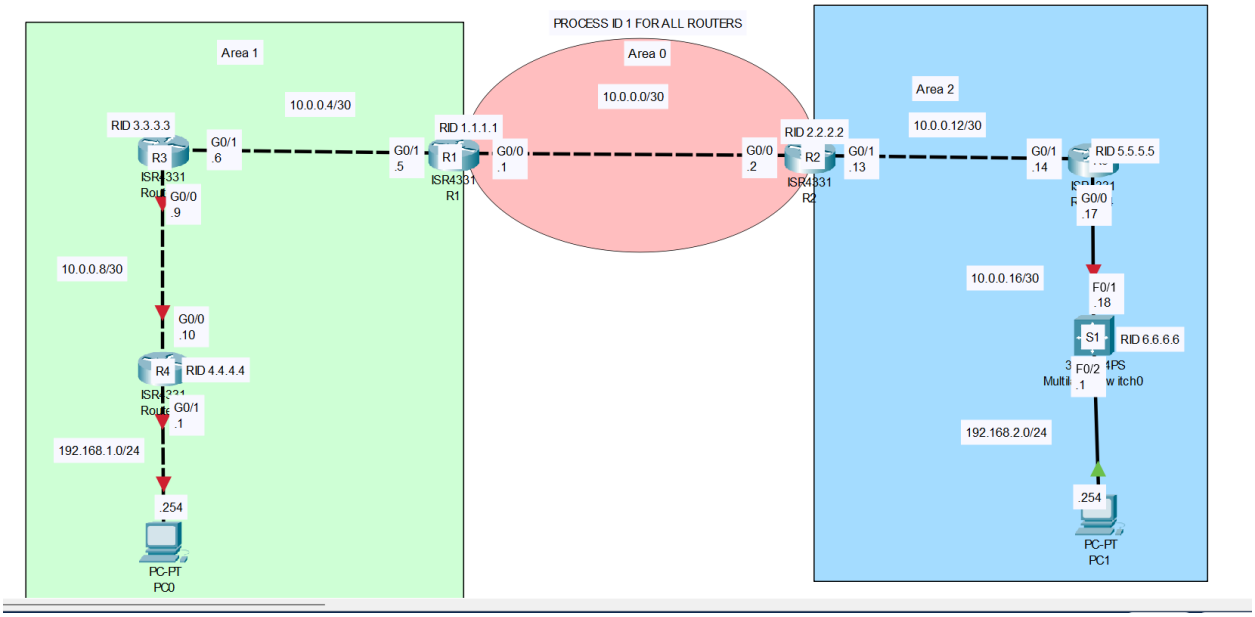
```
Switch(config-if)# ip ospf 1 area <area>

Switch(config-if)# ipv6 ospf 1 area <area>
```

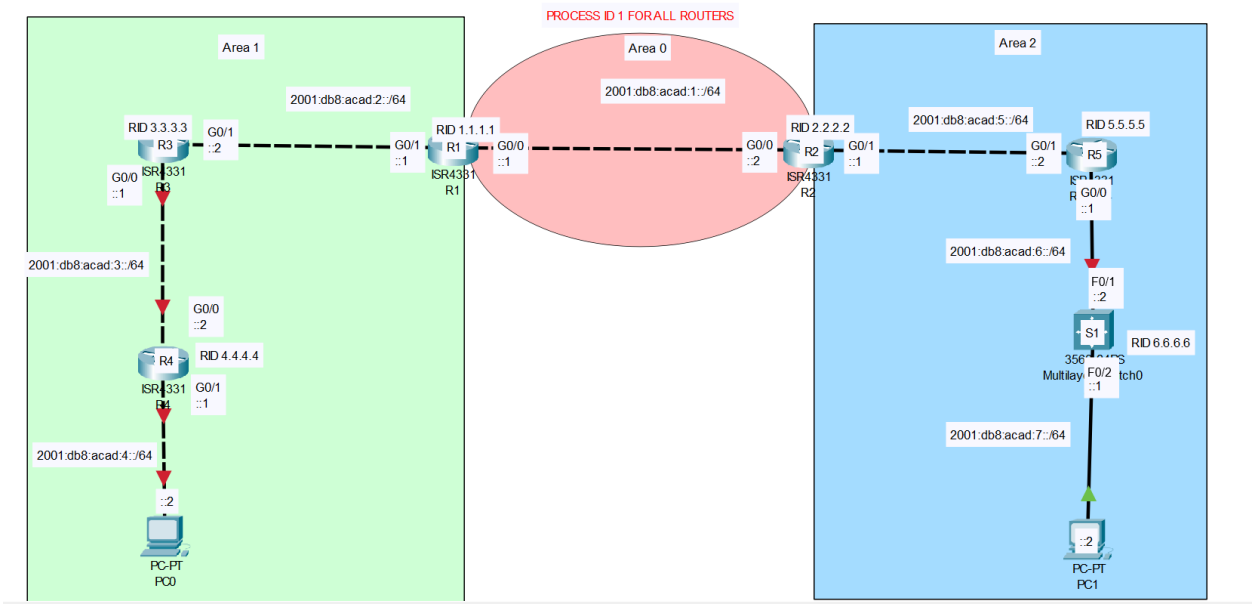
Configures OSPF on an interface for both IPv4 and IPv6 with a process ID of 1 and a specified area ID.

Network Diagram

Topology with IPv4 addresses



Topology with IPv6 addresses



Configurations

R1:

```
version 16.9
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
hostname R1
boot-start-marker
boot-end-marker
vrf definition Mgmt-intf
```

```
 address-family ipv4
 exit-address-family
 address-family ipv6
 exit-address-family
enable secret 5 $1$zVRm$yUTiLs9dyCcsZTfRXJ6BK/
no aaa new-model
no ip domain lookup
login on-success log
subscriber templating
vtp domain cisco
vtp mode transparent
ipv6 unicast-routing
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FLM240608PJ
no license smart enable
diagnostic bootup level minimal
spanning-tree extend system-id
redundancy
 mode none
interface GigabitEthernet0/0/0
 ip address 10.0.0.1 255.255.255.252
 ip ospf 1 area 0
 negotiation auto
 ipv6 address 2001:DB8:ACAD:1::1/64
 ipv6 ospf 1 area 0
interface GigabitEthernet0/0/1
 ip address 10.0.0.5 255.255.255.252
 ip ospf 1 area 1
 negotiation auto
 ipv6 address 2001:DB8:ACAD:2::1/64
 ipv6 ospf 1 area 1
interface GigabitEthernet0/1/0
 no ip address
 shutdown
 negotiation auto
interface GigabitEthernet0/1/1
 no ip address
 shutdown
 negotiation auto
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
router ospf 1
 router-id 1.1.1.1
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
ip tftp source-interface GigabitEthernet0
ipv6 router ospf 1
```

```
 router-id 1.1.1.1
control-plane
banner motd ^CUnauthorized access is illegal. Ad Victoriam.^C
line con 0
 password vaulttec
 login
 transport input none
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 password vaulttec
 login
line vty 5 15
 password vaulttec
 login
end
```

R2:

```
version 16.9
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
platform punt-keepalive disable-kernel-core
hostname R2
boot-start-marker
boot-end-marker
vrf definition Mgmt-intf
 address-family ipv4
 exit-address-family
 address-family ipv6
 exit-address-family
enable secret 5 $1$g0AR$29jrWfeKkSNfHOYqPvIYH0
no aaa new-model
no ip domain lookup
login on-success log
subscriber templating
vtp domain cisco
vtp mode transparent
ipv6 unicast-routing
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FLM2406090M
no license smart enable
diagnostic bootup level minimal
spanning-tree extend system-id
redundancy
 mode none
interface GigabitEthernet0/0/0
 ip address 10.0.0.2 255.255.255.252
 ip ospf 1 area 0
 negotiation auto
```

```
 ipv6 address 2001:DB8:ACAD:1::2/64
 ipv6 ospf 1 area 0
interface GigabitEthernet0/0/1
 ip address 10.0.0.13 255.255.255.252
 ip ospf 1 area 2
 negotiation auto
 ipv6 address 2001:DB8:ACAD:5::1/64
 ipv6 ospf 1 area 2
interface GigabitEthernet0/1/0
 no ip address
 shutdown
 negotiation auto
interface GigabitEthernet0/1/1
 no ip address
 shutdown
 negotiation auto
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
router ospf 1
 router-id 2.2.2.2
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
ip tftp source-interface GigabitEthernet0
ipv6 router ospf 1
 router-id 2.2.2.2
control-plane
banner motd ^CUnauthorized access is illegal. Ad Victoriam.^C
line con 0
 password vaulttec
 login
 transport input none
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 password vaulttec
 login
line vty 5 15
 password vaulttec
 login
end
```

R3:

```
version 16.9
service timestamps debug datetime msec
service timestamps log datetime msec
```

```
platform qfp utilization monitor load 80
platform punt-keepalive disable-kernel-core
hostname R3
boot-start-marker
boot-end-marker
vrf definition Mgmt-intf
 address-family ipv4
 exit-address-family
 address-family ipv6
 exit-address-family
enable secret 5 $1$uDoi$R4oGA00LM9k1HP9TpALsf1
no aaa new-model
no ip domain lookup
login on-success log
subscriber templating
vtp domain cisco
vtp mode transparent
ipv6 unicast-routing
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FLM240608H7
no license smart enable
diagnostic bootup level minimal
spanning-tree extend system-id
redundancy
 mode none
interface GigabitEthernet0/0/0
 ip address 10.0.0.9 255.255.255.252
 ip ospf 1 area 1
 negotiation auto
 ipv6 address 2001:DB8:ACAD:3::1/64
 ipv6 ospf 1 area 1
interface GigabitEthernet0/0/1
 ip address 10.0.0.6 255.255.255.252
 ip ospf 1 area 1
 negotiation auto
 ipv6 address 2001:DB8:ACAD:2::2/64
 ipv6 ospf 1 area 1
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
router ospf 1
 router-id 3.3.3.3
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
ip tftp source-interface GigabitEthernet0
ipv6 router ospf 1
 router-id 3.3.3.3
control-plane
```

```
banner motd ^CUnauthorized access is illegal. Ad Victoriam.^C
line con 0
 password vaulttec
 login
 transport input none
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 password vaulttec
 login
line vty 5 15
 password vaulttec
 login
end
```

R4:

```
version 16.9
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
hostname R4
boot-start-marker
boot-end-marker
vrf definition Mgmt-intf
 address-family ipv4
 exit-address-family
 address-family ipv6
 exit-address-family
enable secret 5 $1$NtJB$id4HUR5aCjy442xlUBPfa.
no aaa new-model
no ip domain lookup
login on-success log
subscriber templating
vtp domain cisco
vtp mode transparent
ipv6 unicast-routing
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO21482HZX
license boot level appxk9
no license smart enable
diagnostic bootup level minimal
spanning-tree extend system-id
redundancy
 mode none
interface GigabitEthernet0/0/0
 ip address 10.0.0.10 255.255.255.252
 ip ospf 1 area 1
 negotiation auto
 ipv6 address 2001:DB8:ACAD:3::2/64
```

```
 ipv6 ospf 1 area 1
interface GigabitEthernet0/0/1
 ip address 192.168.1.1 255.255.255.0
 ip ospf 1 area 1
 negotiation auto
 ipv6 address 2001:DB8:ACAD:4::1/64
 ipv6 ospf 1 area 1
interface Serial0/1/0
 no ip address
 shutdown
interface Serial0/1/1
 no ip address
 shutdown
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
router ospf 1
 router-id 4.4.4.4
ip forward-protocol nd
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0
ipv6 router ospf 1
 router-id 4.4.4.4
control-plane
banner motd ^CUnauthorized access is illegal. Ad Victoriam.^C
line con 0
 password vaulttec
 login
 transport input none
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 password vaulttec
 login
line vty 5 15
 password vaulttec
 login
end
```

R5:

```
version 16.9
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
platform punt-keepalive disable-kernel-core
hostname R5
boot-start-marker
```

```
boot-end-marker
vrf definition Mgmt-intf
 address-family ipv4
 exit-address-family
 address-family ipv6
 exit-address-family
enable secret 5 $1$2z/o$QtcBoq6ViZTuFJykFq5v/1
no aaa new-model
no ip domain lookup
login on-success log
subscriber templating
vtp domain cisco
vtp mode transparent
ipv6 unicast-routing
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO21482DWJ
license boot level appxk9
no license smart enable
diagnostic bootup level minimal
spanning-tree extend system-id
redundancy
 mode none
interface GigabitEthernet0/0/0
 ip address 10.0.0.17 255.255.255.252
 ip ospf 1 area 2
 negotiation auto
 ipv6 address 2001:DB8:ACAD:6::1/64
 ipv6 ospf 1 area 2
interface GigabitEthernet0/0/1
 ip address 10.0.0.14 255.255.255.252
 ip ospf 1 area 2
 negotiation auto
 ipv6 address 2001:DB8:ACAD:5::2/64
 ipv6 ospf 1 area 2
interface Serial0/1/0
 no ip address
 shutdown
interface Serial0/1/1
 no ip address
 shutdown
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
router ospf 1
 router-id 5.5.5.5
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
ip tftp source-interface GigabitEthernet0
```

```
ipv6 router ospf 1
 router-id 5.5.5.5
control-plane
banner motd ^CUnauthorized access is illegal. Ad Victoriam.^C
line con 0
 password vaulttec
 login
 transport input none
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 password vaulttec
 login
line vty 5 15
 password vaulttec
 login
end
```

S1:

```
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname S1
boot-start-marker
boot-end-marker
no logging console
enable secret 5 $1$oYEx$kFrhnH.RuapHzEeW1ddQ//
no aaa new-model
system mtu routing 1500
authentication mac-move permit
ip subnet-zero
ip routing
no ip domain-lookup
ipv6 unicast-routing
spanning-tree mode pvst
spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
vlan internal allocation policy ascending
interface FastEthernet0/1
 no switchport
 ip address 10.0.0.18 255.255.255.252
 ip ospf 1 area 2
 ipv6 address 2001:DB8:ACAD:6::2/64
 ipv6 ospf 1 area 2
interface FastEthernet0/2
 no switchport
 ip address 192.168.2.1 255.255.255.0
 ip ospf 1 area 2
```

```
 ipv6 address 2001:DB8:ACAD:7::1/64
 ipv6 ospf 1 area 2
interface FastEthernet0/3
interface FastEthernet0/4
interface FastEthernet0/5
interface FastEthernet0/6
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface FastEthernet0/25
interface FastEthernet0/26
interface FastEthernet0/27
interface FastEthernet0/28
interface FastEthernet0/29
interface FastEthernet0/30
interface FastEthernet0/31
interface FastEthernet0/32
interface FastEthernet0/33
interface FastEthernet0/34
interface FastEthernet0/35
interface FastEthernet0/36
interface FastEthernet0/37
interface FastEthernet0/38
interface FastEthernet0/39
interface FastEthernet0/40
interface FastEthernet0/41
interface FastEthernet0/42
interface FastEthernet0/43
interface FastEthernet0/44
interface FastEthernet0/45
interface FastEthernet0/46
interface FastEthernet0/47
interface FastEthernet0/48
interface GigabitEthernet0/1
interface GigabitEthernet0/2
interface GigabitEthernet0/3
interface GigabitEthernet0/4
```

```
interface Vlan1
 no ip address
router ospf 1
 router-id 6.6.6.6
 log-adjacency-changes
ip classless
ip http server
ip http secure-server
ip sla enable reaction-alerts
ipv6 router ospf 1
 router-id 6.6.6.6
 log-adjacency-changes
banner motd ^CUnauthorized access is illegal. Ad Victoriam.^C
line con 0
 password vaulttec
 login
line vty 0 4
 password vaulttec
 login
line vty 5 15
 password vaulttec
 login
end
```

Problems

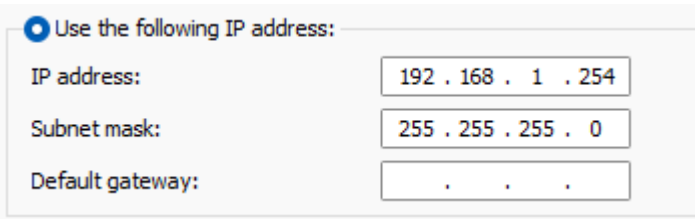
```
S1(config-if)#ipv6 address 2001:db8:acad:7::1 /64
                                               ^
% Invalid input detected at '^' marker.
```

The original configuration file we used for Switch 1 had a space in this line before the IPv6 mask. To fix this, we simply removed the space and reloaded the interface.

```
S1(config-if)#ip address 192.168.2.0 255.255.255.0
Bad mask /24 for address 192.168.2.0
```

```
R4(config-if)#ip add 192.168.1.0 255.255.255.0
Bad mask /24 for address 192.168.1.0
```

Originally, our configuration file for Switch 1 and Router 4 used the subnet addresses of their respective networks instead of the first usable host addresses. The fix was to change `192.168.<x>.0` to `192.168.<x>.1` in each configuration file.



After properly configuring our routers, our pings between PCs didn't work. This occurred because no IPv4 default gateway was set on PC1. To fix this, we set PC1's default

gateway to `192.168.1.1`. We also had no default IPv4/IPv6 gateway for PC2. To fix this, we set PC2's gateways to `192.168.2.1` and `2001:db8:acad:7::1` respectively.

Conclusion

This lab served as a great way to jog my memory and remember how to set up the OSPF routing protocol. The Layer 3 switch was the greatest obstacle in the lab, and I had to jump through a few hoops to make it route traffic properly. However, the setup process wasn't unbearably difficult, and I'm confident that I could set up a multi-area OSPF network with a Layer 3 switch in a real-world setting.