

Module 6 – OSPF Areas

Objective: To implement OSPF areas and neighbour authentication in the lab network.

Prerequisite: Module 1 and OSPF presentation

Topology:

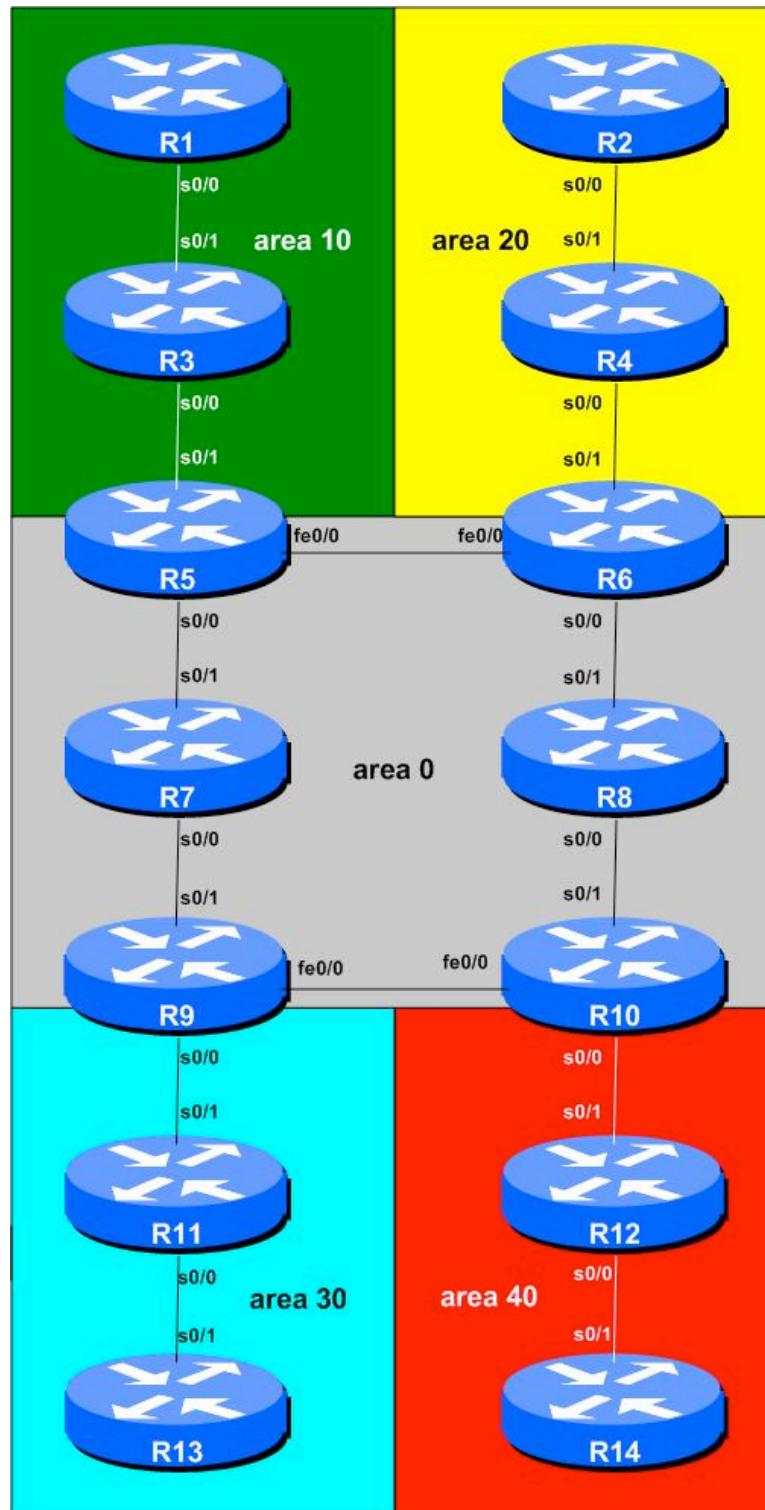


Figure 1 – OSPF Areas

Lab Notes

This module provides an introduction to areas in OSPF as used in ISP networks. The module forms the basis for the Route Reflector Module which follows. It is strongly recommended that the OSPF presentation is reviewed prior to starting this module. Prerequisites for this Module are Module 1, and the OSPF presentation. As before, ask the workshop instructors or refer to the CD Documentation if there is any doubt.

Before starting, decide which routers in the network will represent the core network, and which will represent other portions of the backbone. The example given in Figure 1 allows the student to configure the best combination for the study of OSPF areas.

Functional assignments of routers in Figure 1:

- Routers 5 to 10 represent the “core network” and the core interfaces are all in OSPF area 0. In a typical ISP backbone, these routers would carry all the internal link routes known in the ISPs network. Routers 5, 6, 9 and 10 are **Area Border Routers**, whereas Routers 7 and 8 are **Internal Routers**.
- Routers 1 and 3 are completely in OSPF area 10. This area is a **stub area**. Router 5 is the boundary between area 0 and area 10, so requires configuration for both areas.
- Routers 2 and 4 are completely in OSPF area 20. This area is also a **stub area**. Router 6 is the boundary between area 0 and area 20, so requires configuration for both areas.
- Routers 11 and 13 are completely in OSPF area 30. This area is also a **stub area**. Router 9 is the boundary between area 0 and area 30, so requires configuration for both areas.
- Routers 12 and 14 are completely in OSPF area 40. This area is also a **stub area**. Router 10 is the boundary between area 0 and area 40, so requires configuration for both areas.

Lab Exercise

1. **Reset the configuration of each router** so that it is as it was at the end of Step 11 of Module 1. Basically IP addresses need to be assigned to interfaces, inactive interfaces as per the diagram should be disabled (either shutdown the interface, or remove its configuration), and the new ethernet connection between Router 7 and Router 8 should be activated.

Important: There should be no OSPF or BGP running in the lab network. Also ensure that there are no access-lists or route-maps remaining on the routers. Unused configuration should be deleted. OSPF and BGP configuration can be deleted by entering the commands:

```
no router bgp <ASN>
no router ospf <PID>
```

Checkpoint #1: *Call the lab assistant and show the router configuration and connectivity.*

2. **OSPF Configuration for routers in Area 0 only.** Configure OSPF for your router using PID 41. Remember all the tips and techniques which you have learned in previous modules. Recall the use of the *network* statement, and the *passive-interface default* command. You only want to configure OSPF with other routers in Area 0. Do **not** configure OSPF with routers in areas 10 to 40 yet.

Example for Router 5:

```

router ospf 41
 network 100.2.16.0 0.0.0.3 area 0      !link to Router6
 network 100.2.18.0 0.0.0.3 area 0      !link to Router7
 network 100.2.31.224 0.0.0.0 area 0    !loopback interface
 passive-interface default
 no passive-interface serial 0/0
 no passive-interface ethernet 0/0

```

- 3. OSPF configuration for routers with interfaces in Areas 10 to 40 only.** Configure OSPF for your router using PID 41. Remember the tips and techniques which you have learned in previous modules. Recall the use of the *network* statement, and the *passive-interface* statement. You only want to configure OSPF with other routers which have interfaces in your own area. Do **not** configure OSPF with routers in area 0 yet.

Example for Router 11:

```

router ospf 41
 area 30 stub                          !we are a stub area
 network 100.3.18.0 0.0.0.3 area 30    !link to Router9
 network 100.4.33.0 0.0.0.3 area 30    !link to Router13
 network 100.4.15.224 0.0.0.0 area 30  !loopback interface
 passive-interface default
 no passive-interface serial 0/0
 no passive-interface serial 0/1

```

Checkpoint #2: Call the lab instructors and show the function of your router. You should have neighbour relationships with all the routers in your area (called intra-area). You should also demonstrate the output from “show ip route” so that you can see which routes you are hearing from which routers.

- 4. Putting it all together!** We have now configured OSPF in the routers which are wholly in a particular area. We now need to join the areas together to rebuild our OSPF network. The next step should be carried out by the appropriate router teams to achieve this.
- 5. Connecting Area 0 to the Areas 10, 20, 30 and 40.** The teams running Routers 5, 6, 9 and 10, the Area Border Routers in the core of our lab network, now need to set up configuration so that the four other physically connected areas have an OSPF relationship with Area 0.

For example, the team operating Router 5 need to configure an OSPF network statement for the interface which connects to Router 3 in Area 10 so that the routers can try to establish a neighbour relationship. An example configuration might be:

```

router ospf 41
 network 100.2.17.0 0.0.0.3 area 10
 area 10 stub

```

This tells the router that the OSPF neighbour it finds will be in OSPF area 10, which is a stub area.

Routers 6, 9, and 10 should enter similar and appropriate configuration for their non-area 0 neighbours.

- 6. All router teams should check their routing table.** The routing table should look the same as it did in Module 1. All the prefixes in Area 0 will be available in Areas 10 through to 40.

Checkpoint #3: Call the lab instructors and show the function of your router. The inter-area OSPF “peerings” will now be up. If you have an area border router, demonstrate the neighbour relationships using “sh ip ospf neigh”. If you are not in an area border, you should now have a more complete routing table.

STOP AND WAIT HERE

- 7. Intra Area Authentication – Part 1.** OSPF supports router authentication within areas. This is quite important inside ISP networks to prevent the introduction of improperly configured or unintended equipment.

Each area will turn on authentication within that area. Routers which are **ABRs** will naturally have to enter configuration to cover all areas the router has interfaces in. This first step will enable each area to support authentication using the *area N authentication message-digest* command.

An example configuration for Router6 might be:

```
router ospf 41
  area 0 authentication message-digest
  area 20 authentication message-digest
!
```

Note that this does not affect the actual adjacencies on the routers – it only tells the router that the area mentioned will use authentication, if it is configured.

- 8. Intra Area Authentication – Part 2.** Now that support for authentication in each area has been configured, the second step is to actually set the authentication password to be used, and the interface it has to be used on. The password that should be used for all areas in this example is *cisco*. MD5 encryption should be used rather than the standard simple encryption – to do this, use the *message-digest-key* sub-interface command.

An example configuration for Router6 might be:

```
router ospf 41
  area 0 authentication message-digest
  area 20 authentication message-digest
!
interface ethernet 0/0
  ip ospf message-digest-key 1 md5 cisco
interface serial 0/0
  ip ospf message-digest-key 1 md5 cisco
interface serial 0/1
  ip ospf message-digest-key 1 md5 cisco
!
```

Notice now that the OSPF adjacencies do not come up unless the neighbouring router has also entered the same configuration and key. Notice also how the OSPF adjacencies were reset as the configuration was entered – security is being introduced, so the adjacencies are reset.

Note: the *message-digest-key* allows up to 255 keys to be set per interface. It is generally not recommended to set more than one per interface, as the router will try and communicate with its neighbours using all keys. If a key needs to be upgraded, common practice then is to set a second key, allowing a graceful changeover without compromising the functioning of the network. Once all the routers on the network are using the new key, the old one should be removed.

9. **Final check.** Use the various “*show ip ospf*” commands to see the OSPF status of the lab network now. Check the routing and the routing table.

Checkpoint #6: *Call the lab instructors and show the routing table and information asked for in the previous step.*

CONFIGURATION NOTES

Documentation is critical! You should record the configuration at each ***Checkpoint***, as well as the configuration at the end of the module.