A white rectangular sign with black text

Description automatically generated

**Purpose**

The objective of this lab is to set up a multi-area OSPF network using the knowledge from our previous lab and analyze the different kinds of OSPF traffic using Wireshark. We investigated the different types of LSAs and stub areas and figured out which traffic from the LSAs were accepted into which kind of area. We also learned how to set up switches to allow us to monitor traffic traveling through switch ports.

**Background Information**

OSPF (Open Shortest Path First) is a link-state routing protocol that helps routers determine the best path to take for information to get across efficiently. To do this, OSPF exchanges routing information between routers with Link State Advertisements (LSAs). Using what we learned from the previous OSPF lab, we set up a multi-area OSPF topology and set each area as a special type of OSPF area in addition to the backbone area: Stub Areas, Totally Stubby Areas, Not So Stubby Areas, and Totally Not So Stubby Areas. Each area has a different kind of stubbiness associated with it.

There are six types of LSAs in OSPF: Router LSAs (Type 1), Network LSAs (Type 2), Summary LSAs (Type 3), ASBR Summary LSAs (Type 4), External LSAs (Type 5), and NSSA LSAs (Type 7). Depending on which type of LSA is being delivered, routers receive different kinds of information from them. LSA flooding can occur, overloading the amount of information being passed on a network. The objective of LSA flooding is to advertise all LSAs to all routers so that all routers learn their required LSA. These are what the different kinds of LSAs mean:

**LSA Type 1** – Router LSAs send information to a router’s directly connected interfaces with other routers in order to share its own information to other routers.

**LSA Type 2** – Network LSAs are generated by the Designated Router (DR) on a network and sent to other routers for them to learn about each other.

**LSA Type 3** – Summary LSAs are used by Area Border Routers (ABR), routers in two or more areas, to transfer information about all the areas that it is connected to, which allows areas to discover one another.

**LSA Type 4** – ASBR Summary LSA allows the other routers to find the Autonomous System Border Router (ASBR). First the ASBR receives information using a routing protocol other than OSPF, and then the ABR receives a Type 1 LSA from the ASBR and sends a Type 4 LSA to all other areas to acknowledge where the ASBR is.

**LSA Type 5** – External LSA is sent when information from an outside source not using OSPF is being sent by the ASBR to all the other areas.

**LSA Type 7** – Not So Stubby Area (NSSA) LSAs are just like External LSAs but are intended to operate in NSSA areas.

Furthermore, each area accepts certain types of LSAs and prevents others to prevent LSA flooding and allows the traffic to flow smoothly. Each area accepts these LSAs:

**Stub Area** – Type 1, Type 2, Type 3  
**Totally Stub Area** – Type 1, Type 2  
**Not So Stubby Area (NSSA)** – Type 1, Type 2, Type 3, Type 7  
**Totally NSSA** – Type 1, Type 2, Type 7  
**Backbone Area (Standard Area)** – ALL LSA Types

**Lab Summary**

To complete this lab, we followed these procedures:

1. Designed a topology with a backbone area 0 to host S1 and the g0/0/0 interfaces of routers 1-4. Configured different levels of stubby areas with router loopback interfaces in each area, and strategically placed switches between all connected routers in order to monitor traffic.
2. Used the new topology to set up a physical router network with 6 routers and 3 switches.
3. Configured IPv4 and IPv6 address on router Gigabit Ethernet interfaces.
4. Configured router IDs in OSPF mode for all routers.
5. Configured OSPF on all interfaces on their assigned areas based on the topology.
6. Entered **no shut** command to enable interfaces and waited for OSPF adjacencies to form.
7. Established levels of stubbiness for specific areas.
8. Tested connectivity with pings.
9. Went to Wireshark to analyze traffic and see which LSA types were distributed by routers in the different stub areas.

**Commands**

**area** [area number] **stub**Configures a certain OSPF area as a stub.

**area** [area number] **nssa**Configures a certain OSPF area as a not so stubby area.

**area** [area number] **stub no-summary**Specifies an area as a totally stubby area that only allows type 1, type 2, and specific type 3 (default route) LSAs from the ABR and blocks all other LSA types.

**area** [area number] **stub no-summary**Specifies an area as a not so stubby area which blocks type 3, type 4, and type 5 LSAs but allows a specific kind of type 3 LSA and type 7 LSAs internal to that area.

**network** [network ip address] [wildcard mask] **area** [number]  
Specifies a network address for a specific OSPF area.

**monitor session** [session number] **source interface** [interface connected to router] **both  
monitor session** [session number] **destination interface** [interface connected to computer]Helps view all OSPF traffic travelling through switch ports in Wireshark.

**default-information originate  
redistribute connected subnets**Helps force Type 5 or Type 7 LSAs propagate through the network/area.

**Topology & IP Scheme**

A diagram of a network

Description automatically generated

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | g0/0/0 | Area | g0/0/1 | Area | lo0 | Area | Router ID |
| R1 | 10.0.0.1/24 | 0 | N/A | N/A | 192.168.1.1/32 | 1 | 1.1.1.1 |
| R2 | 10.0.1.1/24 | 0 | 10.200.1.1/24 | 2 | N/A | N/A | 2.2.2.2 |
| R3 | 10.1.0.1/24 | 0 | N/A | 3 | 192.168.3.1/32 | 3 | 3.3.3.3 |
| R4 | 10.1.1.1/24 | 0 | 10.100.1.1/24 | 4 | N/A | N/A | 4.4.4.4 |
| R5 | N/A | N/A | 10.100.2.1/24 | 4 | 192.168.5.1/32 | N/A | 5.5.5.5 |
| R6 | N/A | N/A | 10.200.2.1/24 | 2 | N/A | N/A | 6.6.6.6 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **F1/0/1** | **F1/0/3** | **F1/0/5** | **F1/0/7** |
| S1 (all area 0) | 10.0.0.2/24 | 10.0.1.2/24 | 10.1.0.2/24 | 10.1.1.2/24 |
| S2 (all area 2) | 10.100.1.2/24 | 10.100.2.2/24 | N/A | N/A |
| S3 (all area 4) | 10.200.1.2/24 | 10.200.2.2/24 | N/A | N/A |

**Configurations**

**R1**

Show run:

Current configuration : 1781 bytes

! Last configuration change at 16:53:23 UTC Mon Oct 9 2023

version 16.7

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

no aaa new-model

subscriber templating

vtp domain cisco

vtp mode transparent

multilink bundle-name authenticated

license udi pid ISR4321/K9 sn FDO220523GF

license boot level appxk9

no license smart enable

diagnostic bootup level minimal

spanning-tree extend system-id

redundancy

mode none

interface Loopback0

ip address 192.168.1.1 255.255.255.255

ip ospf 1 area 1

interface GigabitEthernet0/0/0

ip address 10.0.0.1 255.255.255.0

ip ospf 1 area 0

negotiation auto

interface GigabitEthernet0/0/1

no ip address

shutdown

negotiation auto

interface Serial0/1/0

no ip address

shutdown

interface Serial0/1/1

no ip address

shutdown

interface GigabitEthernet0/2/0

no ip address

shutdown

negotiation auto

interface GigabitEthernet0/2/1

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

control-plane

line con 0

transport input none

stopbits 1

line aux 0

stopbits 1

line vty 0 4

login

wsma agent exec

wsma agent config

wsma agent filesys

wsma agent notify

end

**R2**

Show run:

Current configuration : 3899 bytes

! Last configuration change at 16:36:55 UTC Mon Oct 9 2023

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

no aaa new-model

login on-success log

subscriber templating

vtp domain cisco

vtp mode transparent

multilink bundle-name authenticated

crypto pki trustpoint TP-self-signed-2189345785

enrollment selfsigned

subject-name cn=IOS-Self-Signed-Certificate-2189345785

revocation-check none

rsakeypair TP-self-signed-2189345785

crypto pki certificate chain TP-self-signed-2189345785

certificate self-signed 01

  30820330 30820218 A0030201 02020101 300D0609 2A864886 F70D0101 05050030

  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274

  69666963 6174652D 32313839 33343537 3835301E 170D3233 31303039 31353436

  31325A17 0D333030 31303130 30303030 305A3031 312F302D 06035504 03132649

  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 31383933

  34353738 35308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201

  0A028201 0100C543 4A0C1518 EC15F19F 91137505 9D352502 482BFE2A EBCBFD64

  91958608 74B85854 7C7DB509 04747E11 E0E618F5 46A042EF 9ED00AF7 5798F547

  981EAEF6 0D0D3EFA C9473227 1B7C4222 8E7D6316 C17E5438 A7C63366 B94C8CB1

  77D55AEA 5A632471 81AA4C67 D48F35C8 F4042771 18BC8220 3CD5F4F4 E41DC8EC

  9EFC39F6 F4BC111A 035E2169 D49B43D8 E518D9C4 1EAA4E5C D303AE3C 06C75124

  0A9F216D 94723F96 D25E5EBA 8705C8D7 A55919FA 0952196C F7CC2640 8571810B

  707326EB AE15250A 2A89F17C 4F297D11 EF452A0E 47E5C1E1 4C6B603F 0EBBAEE3

  20B36ED8 65207A1B E5543EC6 00680DF1 A42966E6 00395777 B3AA265D 3BA13ED3

  DE460DCD 32370203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF

  301F0603 551D2304 18301680 14B5C913 B283FA6A E3B7BB36 FEC35A00 88667297

  EF301D06 03551D0E 04160414 B5C913B2 83FA6AE3 B7BB36FE C35A0088 667297EF

  300D0609 2A864886 F70D0101 05050003 82010100 141413A8 36B3BB43 87F97D67

  AA2B4F94 6FE69715 9CC12557 FF37F924 E75FB46E 3048909A 2B635C32 7BC27EE7

  46765FB7 9C0FB5B8 BE27778C 63718BEC DE881461 EEEC1CBC A546EC73 F631FC64

  2B7C2C9D AF4C141A C434FFCB 55A53BB8 CC726669 41D6453F EEB13755 C3E7EDEF

  E7CCCEEC 020FED26 586D5FE1 399E7099 AAC28512 31E016C4 ED9E33AF 732C1B39

  73927AF8 3AB3DF64 898CCEA3 360D98C2 315516B9 323E462E 62DE02E8 2403C416

  ED86779E 65BCA8CB E38ADA7C 59A6C1DB AC97CD12 91D2A52B 476DC276 60ED8280

  848476C2 55478124 089FC24F 84843CD2 F42D694A 83D1428C 06163968 5B3C2592

  CD545669 AECA5ED2 272EA8E8 EBA74829 C733977C

        quit

license udi pid ISR4321/K9 sn FDO21482DXE

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 10.0.1.1 255.255.255.0

ip ospf 1 area 0

negotiation auto

interface GigabitEthernet0/0/1

ip address 10.200.1.1 255.255.255.0

ip ospf 1 area 2

negotiation auto

interface Serial0/1/0

no ip address

shutdown

interface Serial0/1/1

no ip address

shutdown

interface GigabitEthernet0/2/0

no ip address

shutdown

negotiation auto

interface GigabitEthernet0/2/1

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

area 2 stub no-summary

ip forward-protocol nd

ip http server

ip http authentication local

ip http secure-server

ip tftp source-interface GigabitEthernet0

control-plane

line con 0

transport input none

stopbits 1

line aux 0

stopbits 1

line vty 0 4

login

end

**R3**

Show run:

Current configuration : 3925 bytes

! Last configuration change at 16:30:37 UTC Mon Oct 9 2023

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

no aaa new-model

login on-success log

subscriber templating

vtp domain cisco

vtp mode transparent

multilink bundle-name authenticated

crypto pki trustpoint TP-self-signed-2557841031

enrollment selfsigned

subject-name cn=IOS-Self-Signed-Certificate-2557841031

revocation-check none

rsakeypair TP-self-signed-2557841031

crypto pki certificate chain TP-self-signed-2557841031

certificate self-signed 01

  30820330 30820218 A0030201 02020101 300D0609 2A864886 F70D0101 05050030

  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274

  69666963 6174652D 32353537 38343130 3331301E 170D3233 31303039 31353432

  30365A17 0D333030 31303130 30303030 305A3031 312F302D 06035504 03132649

  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 35353738

  34313033 31308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201

  0A028201 0100B316 DE715FE2 B0BB29E4 573B72DF 3836B0E0 90C8CCB7 B031D43E

  09C7F323 EFCEB4E2 6964144A 260D6FE7 BDAC9C6C E830C597 061859D2 F05B7522

  341F495D A6BDA66A 7B5F448B 691A6E5B 883F8864 36B2BB7B CCEF433B 5C7AE48F

  FBB1A967 F7A7EB26 212CCF79 918AF394 8235EA9B 8BE293B8 2A01ED5B EE73E0D9

  6C6F99C3 6F44454D 452F2E35 CA030E46 C4AC2EA7 CD17F2A8 0060109C BFAC2345

  24780C49 56050733 2D329D6F 0D22CF28 EC2209A5 75E4C338 D9124ACF 2245CF0D

  9270155F 3F918E70 11F92E16 3ADDA912 44B8CECF 8711EBC3 EFFB7CE5 863006C9

  25F9AA75 F8A46AC5 50E2901D 2998F4AE FFB903EF 86D07D9E 7464B843 7B2F9E1B

  C892EB0E B4AB0203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF

  301F0603 551D2304 18301680 1401997E 015E5FEA CE2CCCD3 29183490 7D99630E

  17301D06 03551D0E 04160414 01997E01 5E5FEACE 2CCCD329 1834907D 99630E17

  300D0609 2A864886 F70D0101 05050003 82010100 4ADA6137 70EF9616 125AE8A6

  0BB85D5D 0FB2EF99 86AA7C8E 533124F0 1E69AFE1 701D3A24 C5C163A8 82709B77

  23C4300E 19321D46 CB44B7D8 047E6D42 7204986E DD04B469 3337CCE7 E124D919

  11BEEEB9 11E63928 C5DDAED9 40778568 943E952F 5020C1EA 0CD68B4E 35061FC8

  6207CB6B 030D8DFA F04B1169 ED34AC80 A8A9E134 1CBF4225 E29BD0DF 6754040E

  3E6AC4BC B389B639 262F67FF C2958E60 1B94D7A4 DC414854 4E6BDD53 DBF05A46

  4EC8C0E7 DBF32920 DA2E419D CCBE9BFA 778A5210 2081B543 78049A26 D723E423

  32587493 9399EB5B F934DFE3 00B55E7D 4F7C9CC8 26583EEB AF5446C1 75A42664

  3EE12D99 FC4BDE3D E54E7D85 765F2CB2 7819CAA8

        quit

license udi pid ISR4321/K9 sn FDO21500G1N

license boot level appxk9

no license smart enable

diagnostic bootup level minimal

spanning-tree extend system-id

redundancy

mode none

interface Loopback0

ip address 192.168.3.1 255.255.255.255

ip ospf 1 area 3

interface GigabitEthernet0/0/0

ip address 10.1.0.1 255.255.255.0

ip ospf 1 area 0

negotiation auto

interface GigabitEthernet0/0/1

no ip address

shutdown

negotiation auto

interface Serial0/1/0

no ip address

shutdown

interface Serial0/1/1

no ip address

shutdown

interface GigabitEthernet0/2/0

no ip address

shutdown

negotiation auto

interface GigabitEthernet0/2/1

no ip address

shutdown

negotiation auto

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

control-plane

line con 0

transport input none

stopbits 1

line aux 0

stopbits 1

line vty 0 4

login

end

**R4**

Show run:

Current configuration : 3691 bytes

! Last configuration change at 16:18:57 UTC Mon Oct 16 2023

version 16.9

service config

service timestamps debug datetime msec

service timestamps log datetime msec

platform qfp utilization monitor load 80

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

no aaa new-model

login on-success log

subscriber templating

vtp domain cisco

vtp mode transparent

multilink bundle-name authenticated

crypto pki trustpoint TP-self-signed-1457377718

enrollment selfsigned

subject-name cn=IOS-Self-Signed-Certificate-1457377718

revocation-check none

rsakeypair TP-self-signed-1457377718

crypto pki certificate chain TP-self-signed-1457377718

certificate self-signed 01

  30820330 30820218 A0030201 02020101 300D0609 2A864886 F70D0101 05050030

  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274

  69666963 6174652D 31343537 33373737 3138301E 170D3233 31303136 31353530

  32385A17 0D333030 31303130 30303030 305A3031 312F302D 06035504 03132649

  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 34353733

  37373731 38308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201

  0A028201 0100C334 4510355B A438F03B FEC900D2 AFC63509 4CB8B733 408B88B1

  D9766415 775E567D CFB58241 E5A3C290 1652C4F6 2D7DD46A A6C85E9C 6B9CA79E

  0510EE12 A150CE11 2CC3F911 C1131EC6 46CBD7CD 542336F9 696BC030 CCCDB75C

  6C3A6BDF C7A48AFE EAF725D8 ED46DACB 4F17B15D 9A0CBA7D 3CAD2B9F 94087C42

  9790255D 0A83A328 D42CEF6E 45E1F565 9D080997 DCA343BD 19FB1F88 F26DEA58

  217B40B0 F5549B6E 56D49A81 DC400DC7 F5A552F5 1ECDA1F0 6E9755A1 2EAF9876

  155E4874 8EE87544 0E796C89 23705E3A 56DBCC75 1F2EDBF4 4588B024 DD86316A

  B6BC4F5A A446E575 67CDE0E2 037C7547 9925B273 E6E8FCE1 D80B4C66 19DD9F5B

  2E5C0CBE F4BF0203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF

  301F0603 551D2304 18301680 14F34F09 D10441F0 21F052A1 9663B0FB 2FFED96F

  A3301D06 03551D0E 04160414 F34F09D1 0441F021 F052A196 63B0FB2F FED96FA3

  300D0609 2A864886 F70D0101 05050003 82010100 255BE40A C2DE4F3C 8275616E

  0EDCD2A6 53025B83 8EB6B4EB F6208F25 14B1CEE8 70162B4F 0D256B2A 97FB570B

  AF34BEF0 EAB8B2C0 25606CF4 355D7B60 538C7E0A 58DD42EA 8D009472 303493B8

  C5B63B1F 12169369 CFF85AAD 8E2A82FA 89816D54 C9ECFEEC 705D6E41 7B1FEE6F

  C8D90241 55980338 6D68A633 8F78EF82 ECA9DAD1 06110593 91B79F76 525EEF90

  FC95487A 1FEEEFB3 45D2CD98 56F21E5A 4A79AD71 E3220C3D F51D3FBD B3CEB85A

  EA0146FF 3F9935C9 4378F500 4E76735E 1E9F2B4D 981358F2 F0706207 652AC42E

  DAB023D7 ACC78AE6 4A0C1782 37F484C9 E2F013CB 33208741 D3E12950 3189B001

  446E445F DE8A479B 80C1019A D212948F AB0A49D7

        quit

license udi pid ISR4321/K9 sn FDO21441WDF

no license smart enable

diagnostic bootup level minimal

spanning-tree extend system-id

redundancy

mode none

interface GigabitEthernet0/0/0

ip address 10.1.1.1 255.255.255.0

ip ospf 1 area 0

negotiation auto

interface GigabitEthernet0/0/1

ip address 10.100.1.1 255.255.255.0

ip ospf 1 area 4

negotiation auto

interface Serial0/1/0

no ip address

interface Serial0/1/1

no ip address

interface GigabitEthernet0

vrf forwarding Mgmt-intf

no ip address

negotiation auto

router ospf 1

router-id 4.4.4.4

area 4 nssa

ip forward-protocol nd

ip http server

ip http authentication local

ip http secure-server

ip http client source-interface GigabitEthernet0/0/1

control-plane

line con 0

exec-timeout 0 0

transport input none

stopbits 1

line aux 0

stopbits 1

line vty 0 4

login

end

**R5**

Show run:

Current configuration : 1451 bytes

! Last configuration change at 16:53:39 UTC Mon Oct 9 2023

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

no aaa new-model

login on-success log

subscriber templating

multilink bundle-name authenticated

license udi pid ISR4321/K9 sn FDO215009QY

no license smart enable

diagnostic bootup level minimal

spanning-tree extend system-id

redundancy

mode none

interface Loopback0

ip address 192.168.5.1 255.255.255.255

interface GigabitEthernet0/0/0

no ip address

negotiation auto

interface GigabitEthernet0/0/1

ip address 10.100.2.1 255.255.255.0

ip ospf 1 area 4

negotiation auto

interface Serial0/1/0

no ip address

interface Serial0/1/1

no ip address

interface GigabitEthernet0

vrf forwarding Mgmt-intf

no ip address

negotiation auto

router eigrp 1

network 192.168.5.0 0.0.0.0

router ospf 1

router-id 5.5.5.5

area 4 nssa

ip forward-protocol nd

no ip http server

ip http secure-server

ip tftp source-interface GigabitEthernet0

control-plane

line con 0

transport input none

stopbits 1

line aux 0

stopbits 1

line vty 0 4

login

end

**R6**

Show run:

Current configuration : 3633 bytes

! Last configuration change at 16:26:50 UTC Mon Oct 9 2023

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 R6

boot-start-marker

boot-end-marker

vrf definition Mgmt-intf

address-family ipv4

exit-address-family

address-family ipv6

exit-address-family

no aaa new-model

login on-success log

subscriber templating

vtp domain cisco

vtp mode transparent

multilink bundle-name authenticated

crypto pki trustpoint TP-self-signed-318861592

enrollment selfsigned

subject-name cn=IOS-Self-Signed-Certificate-318861592

revocation-check none

rsakeypair TP-self-signed-318861592

crypto pki certificate chain TP-self-signed-318861592

certificate self-signed 01

license udi pid ISR4321/K9 sn FDO214420HM

no license smart enable

diagnostic bootup level minimal

spanning-tree extend system-id

redundancy

mode none

interface GigabitEthernet0/0/0

no ip address

shutdown

negotiation auto

interface GigabitEthernet0/0/1

ip address 10.200.2.1 255.255.255.0

negotiation auto

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 6.6.6.6

area 2 stub no-summary

ip forward-protocol nd

ip http server

ip http authentication local

ip http secure-server

ip tftp source-interface GigabitEthernet0/0/0

control-plane

line con 0

transport input none

stopbits 1

line aux 0

stopbits 1

line vty 0 4

login

end

**S1**

Show run:

Current configuration : 1835 bytes

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 aaa new-model

system mtu routing 1500

vtp domain cisco

vtp mode transparent

authentication mac-move permit

ip subnet-zero

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 10.0.0.2 255.255.255.0

interface FastEthernet0/2

interface FastEthernet0/3

no switchport

ip address 10.0.1.2 255.255.255.0

interface FastEthernet0/4

interface FastEthernet0/5

no switchport

ip address 10.1.0.2 255.255.255.0

interface FastEthernet0/6

interface FastEthernet0/7

no switchport

ip address 10.1.1.2 255.255.255.0

interface Vlan1

no ip address

shutdown

router ospf 1

log-adjacency-changes

network 10.0.0.0 0.0.0.255 area 0

network 10.0.1.0 0.0.0.255 area 0

network 10.1.0.0 0.0.0.255 area 0

network 10.1.1.0 0.0.0.255 area 0

ip classless

ip http server

ip http secure-server

ip sla enable reaction-alerts

line con 0

line vty 5 15

end

**S2**

Show run:

Current configuration : 2580 bytes

! Last configuration change at 01:46:42 UTC Mon Mar 1 1993

version 12.2

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

hostname S2

boot-start-marker

boot-end-marker

no aaa new-model

system mtu routing 1500

ip routing

vtp domain BUSD

vtp mode transparent

spanning-tree mode pvst

spanning-tree extend system-id

\*Mar 1 01:53:27.321: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0/19, changed state to down

\*Mar 1 01:53:28.479: %LINK-3-UPDOWN: Interface FastEthernet1/0/19, changed state to down!

vlan internal allocation policy ascending

interface FastEthernet1/0/1

no switchport

ip address 10.100.1.2 255.255.255.0

interface FastEthernet1/0/3

no switchport

ip address 10.100.2.2 255.255.255.0

interface Vlan1

ip address dhcp

router ospf 1

area 4 nssa

network 10.1.1.0 0.0.0.255 area 0

network 10.100.1.0 0.0.0.255 area 4

network 10.100.2.0 0.0.0.255 area 4

ip http server

ip http secure-server

logging esm config

line con 0

line vty 5 15

monitor session 1 source interface Fa1/0/1 , Fa1/0/3

monitor session 1 destination interface Fa1/0/5

end

**S3**

Show run:

Current configuration : 2647 bytes

! Last configuration change at 01:15:46 UTC Mon Mar 1 1993

version 12.2

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

hostname S3

boot-start-marker

boot-end-marker

no aaa new-model

system mtu routing 1500

ip routing

vtp domain CCNP

vtp mode transparent

spanning-tree mode pvst

spanning-tree extend system-id

vlan internal allocation policy ascending

interface FastEthernet1/0/1

no switchport

ip address 10.200.1.2 255.255.255.0

interface FastEthernet1/0/3

no switchport

ip address 10.200.2.2 255.255.255.0

speed auto 1000

interface Vlan1

no ip address

router ospf 1

area 2 stub no-summary

network 10.0.1.0 0.0.0.255 area 0

network 10.200.1.0 0.0.0.255 area 2

network 10.200.2.0 0.0.0.255 area 2

ip http server

ip http secure-server

logging esm config

line con 0

line vty 0 4

login

line vty 5 15

login

monitor session 1 source interface Fa1/0/1

monitor session 1 destination interface Fa1/0/5

end

**Wireshark Captures of LSA Types**

LSA Type 1

A computer screen shot of a computer code

Description automatically generated

LSA Type 2

A screenshot of a computer program

Description automatically generated

LSA Type 3

A computer screen shot of a computer program

Description automatically generated

A computer screen shot of a computer program

Description automatically generated

LSA Type 4

**A screenshot of a computer program

Description automatically generated**

LSA Type 5

A screenshot of a computer

Description automatically generated

LSA Type 7

A screenshot of a computer

Description automatically generated

**Problems**

When we originally started planning for this lab, we created a topology with all the routers directly connected with no switch in between; we weren’t able to see OSPF traffic on our Wireshark feed at all. We realized that we needed to combine our topology with switches and use the **monitor session** command to be able to see traffic appear in Wireshark.

Once we connected all routers to a switch, none of the routers could ping one another despite being connected through the switch ports. Turns out, since we didn’t have an initial configuration done on the switch, the routers could not communicate. We then configured all switch ports as routing ports and configured OSPF on the switch so the routers could navigate through.

When description packets did not appear in Wireshark, we restarted OSPF with **clear ip ospf process** command.

We had a hard time figuring out how to see Type 5 and Type 7 LSAs from networks using other routing protocols since the routes did not clearly distribute into OSPF. We used the **redistribute routes** command to send external LSAs.  
  
**Conclusion**

Through this lab, we learned to successfully configure and troubleshoot a multi-area OSPF network and incorporate different levels of stubby areas. We also learned to configure in a way to monitor traffic of different LSA types through Wireshark.

**Lab Signoff**

**A group of white rectangular objects with blue text

Description automatically generated with medium confidence**