**CAPTURING STUBBY OSPF PACKETS**

BINGNAN XU

ccnp (cisco certified network professional)

oct. 2018

NEWPORT HIGH SCHOOL, WA

## LSA (link state advertisment) types

Link State Advertisement (LSA) is the message that routers send to each other so that they can establish dedicated routes to each other. Imagine each router is a student in a classroom: each router is speaking (broadcasting) their IPs and routing tables to every other router in its OSPF area.

## OSPF stubby options summary

However, LSA data can have substantial size in a large OSPF network, thus taking a lot of router resources and slowing down the network. Stubby OSPF reduces routers’ memory consumption and CPU workload by using default routes inside an area (so instead of letting everyone look for everyone else in a giant room, ABRs direct routers to find other routers). In this way, only 1 router in the area (ABR) needs to maintain the OSPF routing table. In another word, ABRs in stubby area advertise a default route into their area, so other routers in the area are freed from OSPF calculation.

| Normal | Any LSA types are allowed |
| --- | --- |
| Stubby | No Type 4, 5 LSA allowed |
| Totally Stubby | No Type 3, 4, or 5 LSA allowed, though default summary routes are allowed |
| NSSA (No So Stubby Area) | No Type 4, 5 LSA allowed, but Type 7 LSAs are allowed (Type 5 converted by NSSA ASBR) |
| Totally NSSA | No Type 3, 4, or 5 LSA Allowed: default summary routes and Type 7 LSAs. |

## types of packets expected in different ospf modes

If I were to distinguish different OSPF mode in an established network, I would capture the traffic packets in the network. In normal OSPF network, I will see every LSA types except type 7. In a stubby network, I will likely to find Type 1, 2, 3 LSAs, because LSAs for external networks are blocked (Type 4 and 5 are filtered). In a totally stubby area, I can only fine Type 1 and 2, because Type 3 (interarea LSA) is blocked. In a nssa network, 1, 2, 3, and 7 LSA packets would be captured, because nssa turn LSA type 5 into type 7. In a Totally NSSA, interarea Summary LSA is filtered and I will find LSA Type 1, 2, 7.

[Grab your reader’s attention with a great quote from the document or use this space to emphasize a key point. To place this text box anywhere on the page, just drag it.]

| Normal OSPF | LSA type 1, 2, 3, 4, 5 |
| --- | --- |
| Stubby | LSA type 1, 2, 3 |
| Totally Stubby | LSA type 1, 2 |
| NSSA (no so stubby area) | LSA type 1, 2, 3, 7 |
| Totally NSSA | LSA type 1, 2, 7 |

## routers and layer 3 switches configuration

**MainRouter(config)#**do show run

network 10.10.2.0 0.0.0.255 area 0

network 10.10.6.0 0.0.0.255 area 2

**R3(config)# hostname R3**

interface GigabitEthernet0/0

ip address 10.10.3.2 255.255.255.0

interface GigabitEthernet0/1

ip address 10.10.7.1 255.255.255.0

router ospf 1

network 10.10.3.0 0.0.0.255 area 0

network 10.10.7.0 0.0.0.255 area 3

**SwitchR4(config)# hostname SwitchR4**

interface Loopback1

ip address 10.10.33.1 255.255.255.0

interface FastEthernet1/0/1

no switchport

ip address 10.10.4.2 255.255.255.0

interface FastEthernet1/0/2

no switchport

ip address 10.10.9.1 255.255.255.0

interface FastEthernet1/0/3

no switchport

ip address 10.10.8.1 255.255.255.0

interface GigabitEthernet0/1/0

ip address 192.168.6.1 255.255.255.0

router eigrp 1

network 10.10.9.0 0.0.0.255

network 10.10.9.0 0.0.0.255 area 4

network 10.10.33.0 0.0.0.255 area 4

redistribute ospf 1 metric 1544 200 255 1 1500

router ospf 1

area 4 nssa

redistribute eigrp 1 metric 100 subnets

network 10.10.4.0 0.0.0.255 area 0

network 10.10.9.0 0.0.0.255 area 4

network 10.10.33.0 0.0.0.255 area 4

monitor session 1 source interface Fa1/0/2

monitor session 1 destination interface Fa1/0/24

Ip routing

**hostname MainRouter**

interface FastEthernet1/0/1

no switchport

ip address 10.10.1.1 255.255.255.0

interface FastEthernet1/0/2

no switchport

ip address 10.10.2.1 255.255.255.0

interface FastEthernet1/0/3

no switchport

ip address 10.10.3.1 255.255.255.0

interface FastEthernet1/0/4

no switchport

ip address 10.10.4.1 255.255.255.0

router ospf 1

network 10.10.1.0 0.0.0.255 area 0

network 10.10.2.0 0.0.0.255 area 0

network 10.10.3.0 0.0.0.255 area 0

network 10.10.4.0 0.0.0.255 area 0

**R1(config)#** **hostname R1**

interface GigabitEthernet0/0

ip address 10.10.1.2 255.255.255.0

interface GigabitEthernet0/1

ip address 10.10.5.1 255.255.255.0

router ospf 1

area 1 stubby

network 10.10.1.0 0.0.0.255 area 0

network 10.10.5.0 0.0.0.255 area 1

**R2(config)#hostname R2**

interface GigabitEthernet0/0

ip address 10.10.2.2 255.255.255.0

interface GigabitEthernet0/1

ip address 10.10.6.1 255.255.255.0

router ospf 1

area 2 stubby no-summary

hostname R5

interface Loopback1

ip address 10.10.51.1 255.255.255.0

interface GigabitEthernet0/0

ip address 10.10.9.2 255.255.255.0

interface GigabitEthernet0/1

ip address 10.10.10.1 255.255.255.0

router eigrp 1

network 10.10.9.0 0.0.0.255

network 10.10.10.1 0.0.0.255

network 10.10.51.1 0.0.0.255

**R5(config)# hostname R5**

interface Loopback1

ip address 10.10.51.1 255.255.255.0

interface GigabitEthernet0/0

ip address 10.10.9.2 255.255.255.0

interface GigabitEthernet0/1

ip address 10.10.10.1 255.255.255.0

router eigrp 1

network 10.10.9.0 0.0.0.255

network 10.10.10.1 0.0.0.255

network 10.10.51.1 0.0.0.255

Configurations for monitoring router **(example area 1).**

I need one layer 3 switch for each area to attend the traffic that stub area routers send to their neighbors (I need 4 more switches theoretically). However, there is not enough layer 3 switch available for the lab. So, I used one switch and change its ip address, OSPF area number, and stub configuration to get the packets that different stub routers send to their areas.

**layer3switchOSPFarea1(config)# hostname layer3switchOSPFarea1**

ip routing

interface FastEthernet1/0/1

no switchport

ip address 10.10.8.2 255.255.255.0

no shutdown

router ospf 1

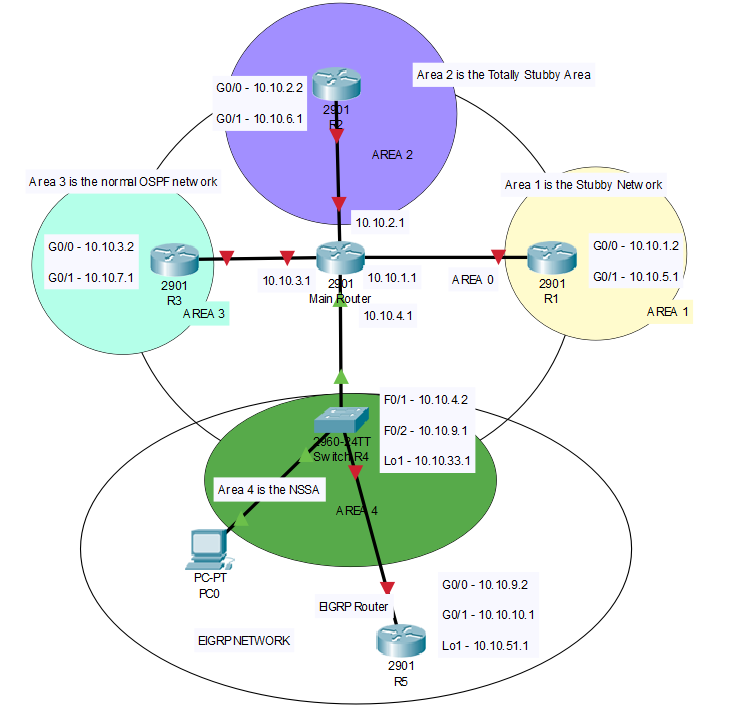
area 1 stub

network 10.10.8.0 0.0.0.255 area 1

monitor session 1 source interface Fa1/0/1

monitor session 1 destination interface Fa1/0/24

Then, my PC receives WireShark packets from Switchport Fa1/0/24



* Main Router is in backbone area 0.
* R1, R2, R3, SwitchR4 are all connected to area 0, but each is also independently in area 1, 2, 3, 4.
* R5 is the EIGRP router that LSAs from provides external network. R5 is not a part of OSPF areas, but it is connected to OSPF network.
* I used SwitchR4 for ASBR instead of an actual router, because I want to capture the nssa LSA type 7 traffic that it sends to area 4. In order to do this, I need three ports, one to Main Router, one to my PC and another one to R5. However, there are only two ports on the routers I have. Thus, I must use a layer 3 switch as a router.

## router IPv4 routes

**MainRouter(config)#**do show ip routes

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, 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

10.0.0.0/8 is variably subnetted, 11 subnets, 2 masks

C 10.10.1.0/24 is directly connected, FastEthernet1/0/1

L 10.10.1.1/32 is directly connected, FastEthernet1/0/1

C 10.10.2.0/24 is directly connected, FastEthernet1/0/2

L 10.10.2.1/32 is directly connected, FastEthernet1/0/2

C 10.10.3.0/24 is directly connected, FastEthernet1/0/3

L 10.10.3.1/32 is directly connected, FastEthernet1/0/3

C 10.10.4.0/24 is directly connected, FastEthernet1/0/4

L 10.10.4.1/32 is directly connected, FastEthernet1/0/4

O IA 10.10.9.0/24 [110/2] via 10.10.4.2, 00:19:13, FastEthernet1/0/4

O IA 10.10.33.1/32 [110/2] via 10.10.4.2, 00:22:40, FastEthernet1/0/4

O E2 10.10.51.0/24 [110/100] via 10.10.4.2, 00:18:27, FastEthernet1/0/4

**R1(config)#**do show ip routes

10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks

C 10.10.1.0/24 is directly connected, GigabitEthernet0/0

L 10.10.1.2/32 is directly connected, GigabitEthernet0/0

O 10.10.2.0/24 [110/2] via 10.10.1.1, 00:08:20, GigabitEthernet0/0

O 10.10.3.0/24 [110/2] via 10.10.1.1, 00:08:20, GigabitEthernet0/0

O 10.10.4.0/24 [110/2] via 10.10.1.1, 00:08:20, GigabitEthernet0/0

O IA 10.10.9.0/24 [110/3] via 10.10.1.1, 00:08:20, GigabitEthernet0/0

O IA 10.10.33.1/32 [110/3] via 10.10.1.1, 00:08:20, GigabitEthernet0/0

O E2 10.10.51.0/24 [110/100] via 10.10.1.1, 00:08:20, GigabitEthernet0/0

**R2(config)#**do show ip routes

10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks

O 10.10.1.0/24 [110/2] via 10.10.2.1, 00:07:53, GigabitEthernet0/0

C 10.10.2.0/24 is directly connected, GigabitEthernet0/0

L 10.10.2.2/32 is directly connected, GigabitEthernet0/0

O 10.10.3.0/24 [110/2] via 10.10.2.1, 00:07:58, GigabitEthernet0/0

O 10.10.4.0/24 [110/2] via 10.10.2.1, 00:07:58, GigabitEthernet0/0

O IA 10.10.9.0/24 [110/3] via 10.10.2.1, 00:07:58, GigabitEthernet0/0

O IA 10.10.33.1/32 [110/3] via 10.10.2.1, 00:07:58, GigabitEthernet0/0

O E2 10.10.51.0/24 [110/100] via 10.10.2.1, 00:07:58, GigabitEthernet0/0

**R3(config)#**do show ip routes

10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks

O 10.10.1.0/24 [110/2] via 10.10.3.1, 00:06:56, GigabitEthernet0/0

O 10.10.2.0/24 [110/2] via 10.10.3.1, 00:07:50, GigabitEthernet0/0

C 10.10.3.0/24 is directly connected, GigabitEthernet0/0

L 10.10.3.2/32 is directly connected, GigabitEthernet0/0

O 10.10.4.0/24 [110/2] via 10.10.3.1, 00:08:47, GigabitEthernet0/0

O IA 10.10.9.0/24 [110/3] via 10.10.3.1, 00:08:47, GigabitEthernet0/0

O IA 10.10.33.1/32 [110/3] via 10.10.3.1, 00:08:47, GigabitEthernet0/0

O E2 10.10.51.0/24 [110/100] via 10.10.3.1, 00:08:47, GigabitEthernet0/0

**SwitchR4(config)#**do show ip routes

10.0.0.0/8 is variably subnetted, 10 subnets, 2 masks

O 10.10.1.0/24 [110/2] via 10.10.4.1, 00:10:01, FastEthernet1/0/1

O 10.10.2.0/24 [110/2] via 10.10.4.1, 00:10:55, FastEthernet1/0/1

O 10.10.3.0/24 [110/2] via 10.10.4.1, 00:12:35, FastEthernet1/0/1

C 10.10.4.0/24 is directly connected, FastEthernet1/0/1

L 10.10.4.2/32 is directly connected, FastEthernet1/0/1

C 10.10.9.0/24 is directly connected, FastEthernet1/0/2

L 10.10.9.1/32 is directly connected, FastEthernet1/0/2

C 10.10.33.0/24 is directly connected, Loopback1

L 10.10.33.1/32 is directly connected, Loopback1

D 10.10.51.0/24 [90/156160] via 10.10.9.2, 00:17:27, FastEthernet1/0/2

**R4(config)#**do show ip routes

10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks

D EX 10.10.1.0/24

[170/1711616] via 10.10.9.1, 00:02:20, GigabitEthernet0/0

D EX 10.10.2.0/24

[170/1711616] via 10.10.9.1, 00:03:15, GigabitEthernet0/0

D EX 10.10.3.0/24

[170/1711616] via 10.10.9.1, 00:04:55, GigabitEthernet0/0

D EX 10.10.4.0/24

[170/1711616] via 10.10.9.1, 00:09:47, GigabitEthernet0/0

C 10.10.9.0/24 is directly connected, GigabitEthernet0/0

L 10.10.9.2/32 is directly connected, GigabitEthernet0/0

D EX 10.10.33.0/24

[170/1711616] via 10.10.9.1, 00:09:47, GigabitEthernet0/0

C 10.10.51.0/24 is directly connected, Loopback1

L 10.10.51.1/32 is directly connected, Loopback1

## Opsf Packet captured with wireshark

### Normal ospf area

### 

Legend: yellows are the hello packets, and blacks are anything other than the hellos packets. Type 1-2 LSA for intra-area, type 3 for inter-OSPF areas, and type 4-5 for external networks (in this case, our EIGRP network).

In a normal OSPF area, I found that LSA-type 1 through 5 packets flow freely in OSPF networks, creating lots of traffic. In this specific diagram, type 1-2 LSA are not showed, but I did capture them in other packets.

### OSPF stubby area Wireshark Capture

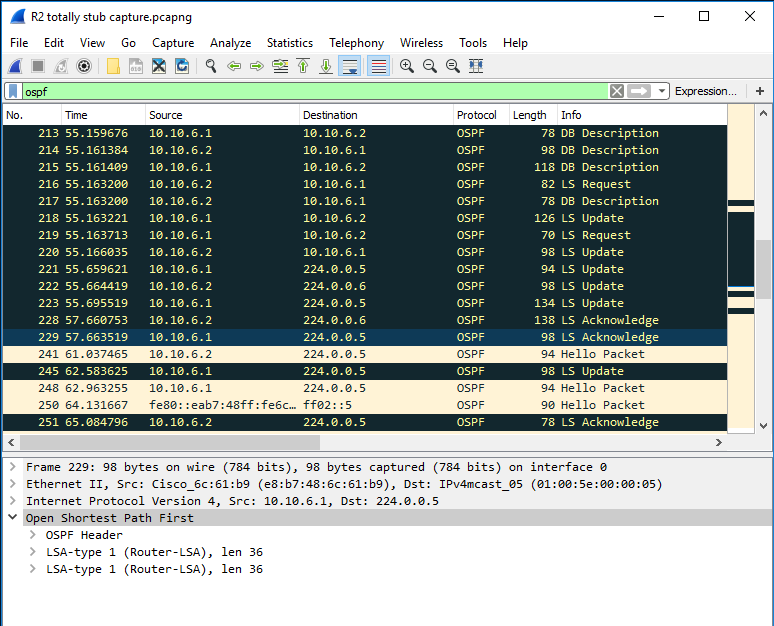
### 

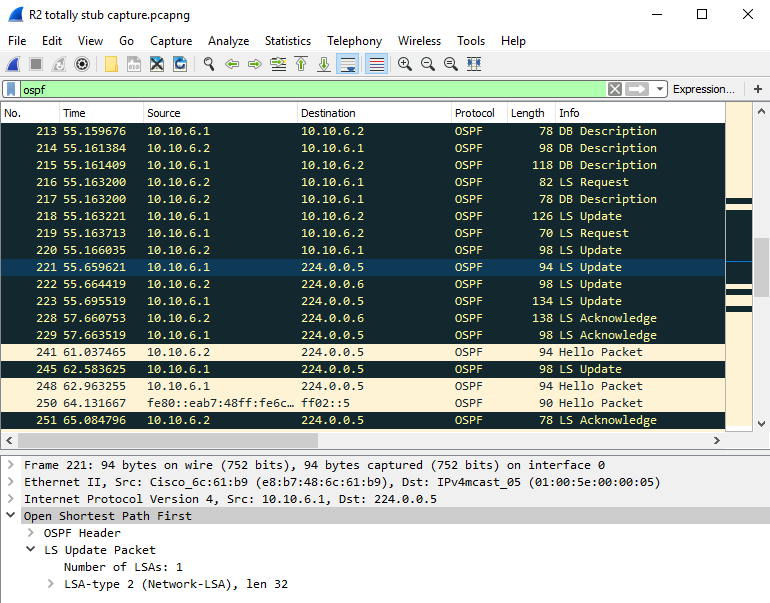
As you can see for the OSPF picket type summary, only LSA-type 1, 2 and 3 are circulating in this network. Since LSA-type 4 and 5—which are associated the propagation of external routes—are filtered, only OSPF area packets (including OSPFs in other areas) are presented in a Stubby OSPF area.

### OSPF totally stubby Wireshark Capture

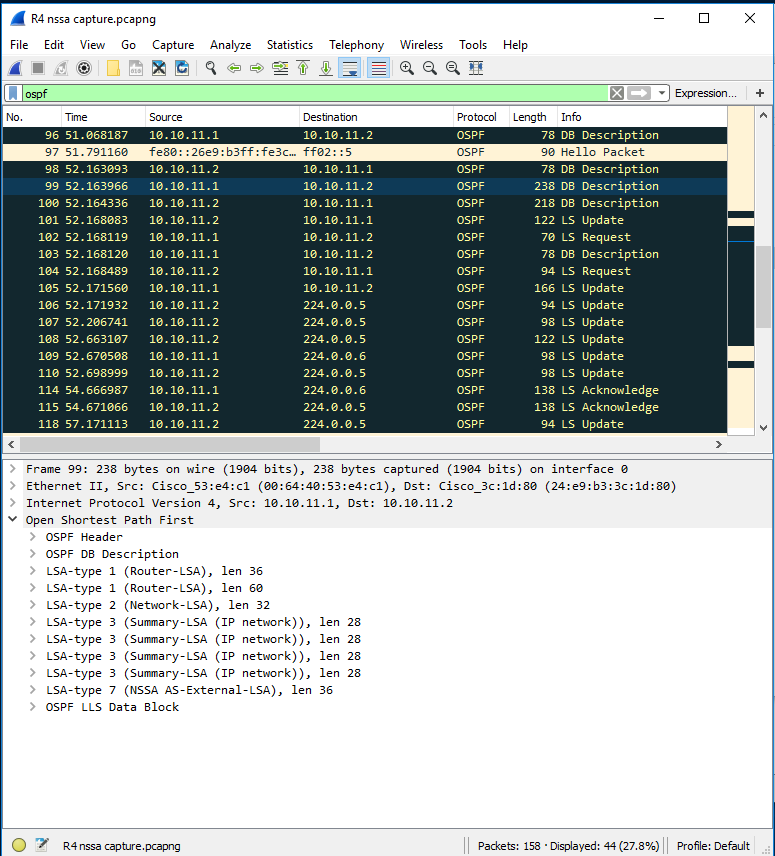
### 

### Like in Stubby area, no type 4 and 5 LSA are allowed. Type 3 LSAs are only allowed if they are default summary routes. In this packet, only one LSA-type 3 is seemed, so it is probably the default summary routes that summarized the OSPF networks other areas. In other packets, we mostly see LSA-type 1 or type 2 alone. Like what’s shown below:





### NSSA (no so stubby area)



In an nssa area, directly connected external routes are transferred, but not processed. It’s like telling a person to pass your note without looking at the content. So, in this way, external routes passed to area 0 the backbone in form of type 7 LSA, occupying much less routers resources in nssa area.

## problems encountered

1. **OSPF and EIGRP network can’t connect to each other.**

*Solution: OSPF network and EIGRP network need to properly be distributed into each other on ASBR. In practice, I go to OSPF in SwitchR4 and redistribute EIGRP, then go to EIGRP on SwitchR4 and redistribute OSPF. Note that EIGRP has five constants to calculate distances, so the redistribution statements are very different.*

I used these command:

**SwitchR4(config)#**

router eigrp 1

redistribute ospf 1 metric 1544 200 255 1 1500

router ospf 1

redistribute eigrp 1 metric 100 subnets

1. **WireShark on PC is not getting any OSPF messages besides hello packets.**

*Solution: at first, I thought I could get packets by plugging the PC into the router ports, but apparently, I need a switch to do monitor sessions, replicate the traffic to other routers, and forward it to my PC. So, I configured* **layer3switchOSPFarea#** *to accomplish this task.*

Commands for monitor sessions:

**layer3switchOSPFarea1 (config)#**

monitor session 1 source interface Fa1/0/1

monitor session 1 destination interface Fa1/0/24

1. **There were not enough ports on Router 4 for WireShark capture.**

*R4, the ASBR between EIGRP network and OSPF network, needs to have three ports for this lab: one connected to OSPF area, one connected to EIGRP area, and another one for WireShark Capture. However, our routers only have two viable ports.*

***Solution****: we turned a layer 3 switch into R4, making SwitchR4. In this way, routing works the same, and we have enough ports for the lab.*

1. **We found LSA type 3 in totally stubby OSPF.**

*Routers in totally stubby OSPF area should filter out type 3 LSAs, inter-OSPF area LSAs. After checking our configuration, we still captured a type 3 LSA in our packets.*

***Solution****: Though this is not a “solution”, but it looks like the type 3 LSA packet we captured is a default summary route.*

## conclusion

OSPF stub area are designed to minimize the router resources that are spent to maintain an OSPF routing table. Different stub flavors provide different levels of concision, without impacting the connectivity of the network.

Although I don’t need to configure OSPFv3 in this lab, it was not easy. The first obstacle that I need to overcome is the connection between different routing protocols. Each routing protocol use distinct algorithm to calculate route distance, so the redistribution commands are different for different routing protocols. After the connection is established, turning an OSPF area into stub area relatively straight forward. Just make sure all routers in the area are in the same stub mode. The command is:

**“R1(config-router)#** area 1(or whatever area) stub (or nssa) no-summary (depending on whether you want it to be ‘totally’) **”**

Capturing the packets is another challenging aspect of the lab. Switch can do monitor sessions and forward OSPF packets to PCs. And a layer 3 Switch can act both as a router and a switch.