# Lab 6 - final report team 10

מגישים:

זיו זידמן 208660365

גיא לייבה 208279620

**Chapter 2**

2.11

We start by configuring the router with OSPF protocol 1. Next, we assign it a unique Router ID that it will use to identify itself to its neighbors. Finally, we define the network that OSPF will route, using a WILDCARD mask. The wildcard is the "reverse" of the subnet mask, meaning that "0" represents the bits of the network that must match, and "1" represents the bits of hosts/subnetworks where no match is required. Additionally, we assign the network to an area (AREA).

2.12

It uses "encapsulation" of type OSPF

2.13

It starts with an Hello packet which job is to meet new neighbours and to keep alive.

If it is a new neighbour he will send him the DataBase Description with an explanation on the topology he knows.

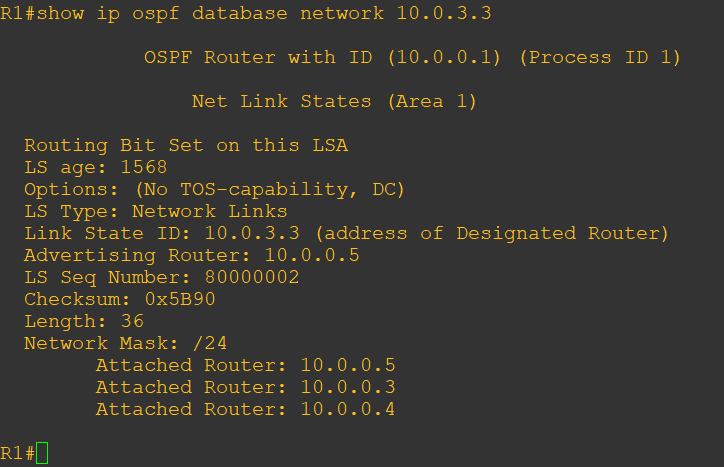
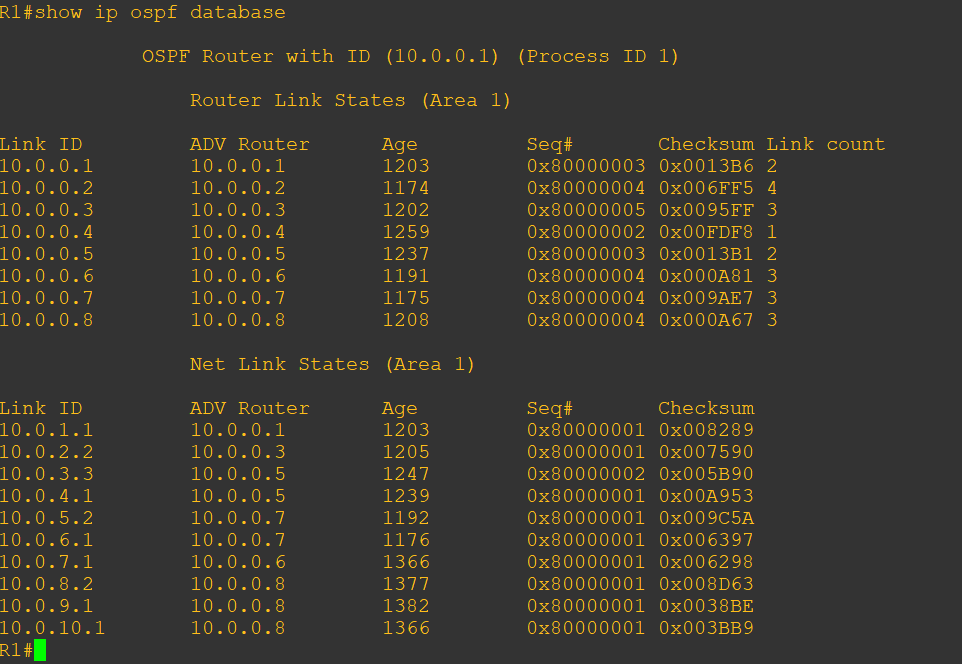
If the neighbour needs to update part of its topology it will send a request.

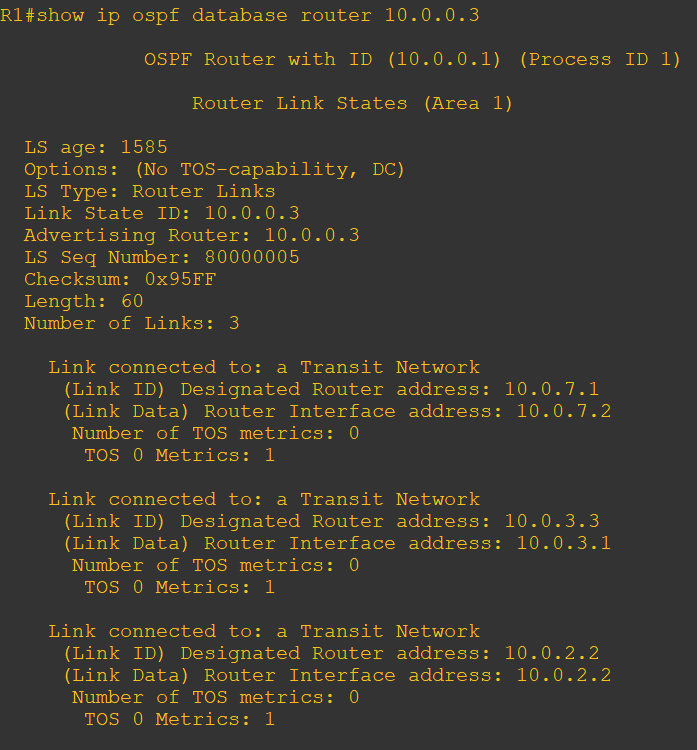
The Router will answer the details with an UPDATE message, then the neighbor will answer that everything is correct with a proper ACK message.

2.14

We will write which routers are connected to the correct network

:





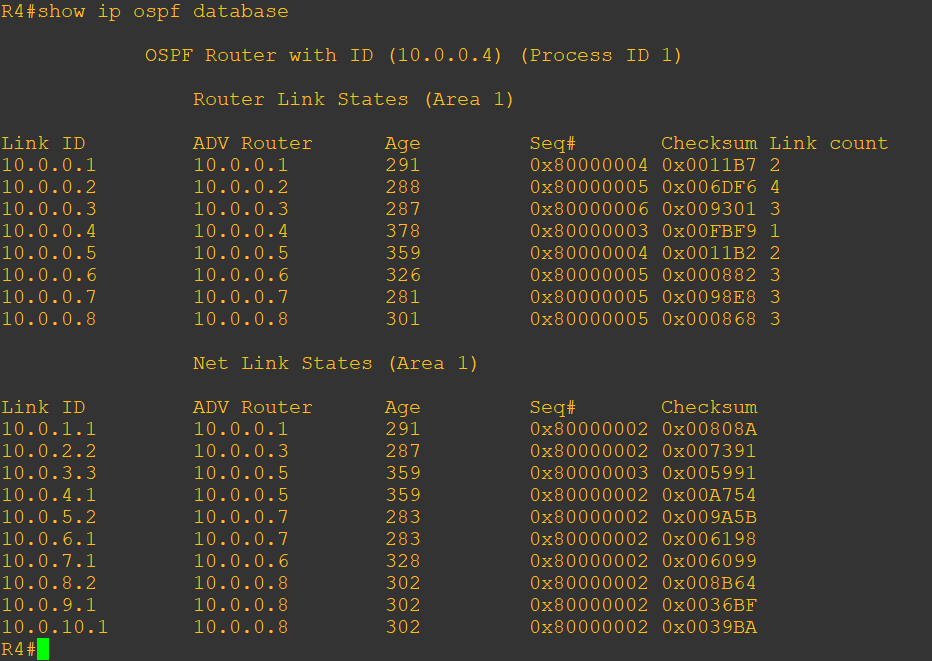
We will check which networks each router knows, in this example it is 10.0.0.3, we will notice that the router is holding a connection also to 10.0.1.1.

We found a route from our router to the designated network, there is a possibility to check routes through other routers that we saw that are connected to other networks.

2.15

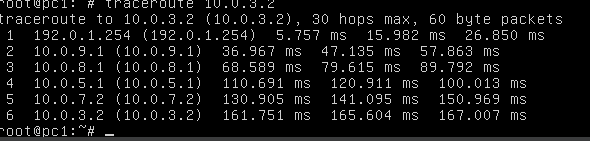
The OSPF database is identical across all routers in the same area because OSPF synchronizes the database to ensure all routers have the same view of the network. Each router independently calculates its routing table so the database is the same.

2.16

R4 OSPF database: 

part 3:

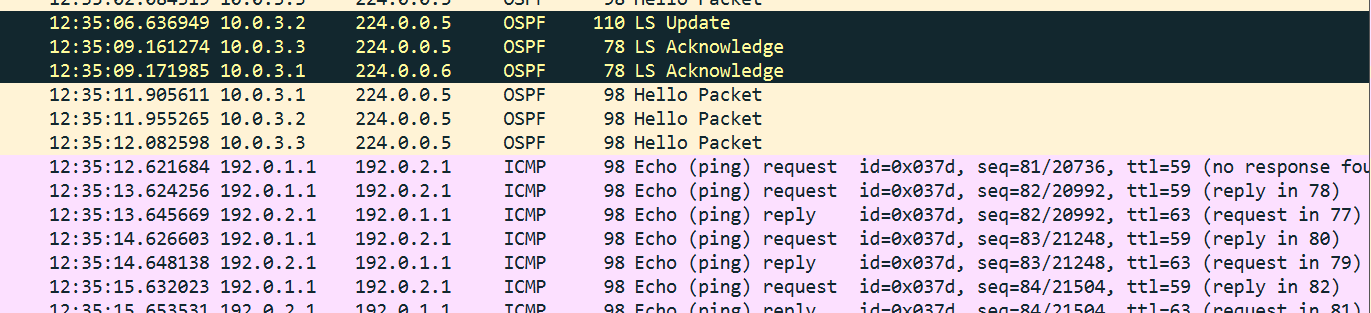
3.6:

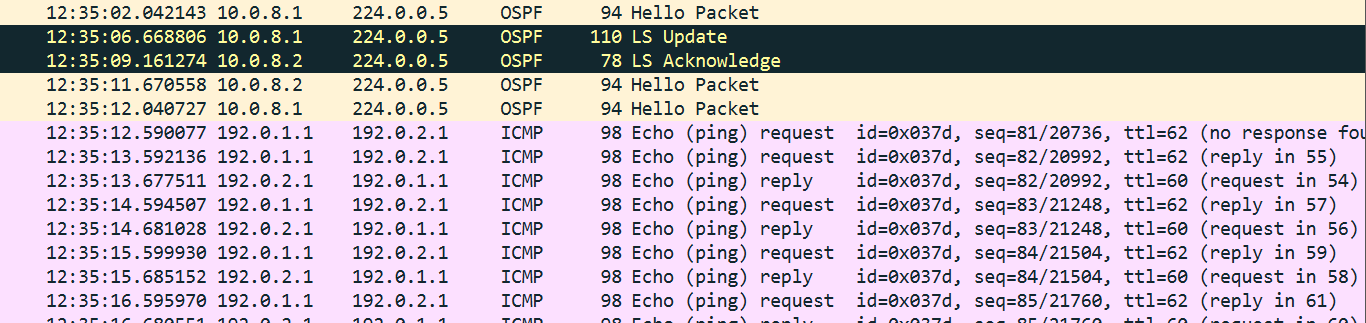


3.15

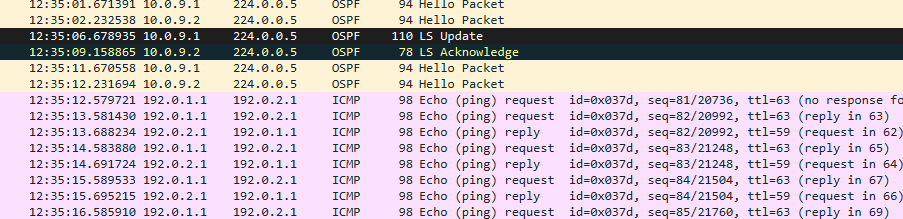
First R4 sends an update of the new link, in the form of LS update packet, which then spreads through R8 to R1. An acknowledge packet is sent to the transmitting router from every link it sent to (in the case of R4 there are two Routers connected, so we are seeing two ACKs).

R4:



R8:

R1:



Then, as we can see, PINGs are exchanged.

3.16

As can be seen in the “time” column of the captures, it takes 0.041986 seconds for the OSPF info to spread through the entire network and 0.010129 seconds to go through a single hop.

3.17

OSPF calculates the metric, cost of an interface as:

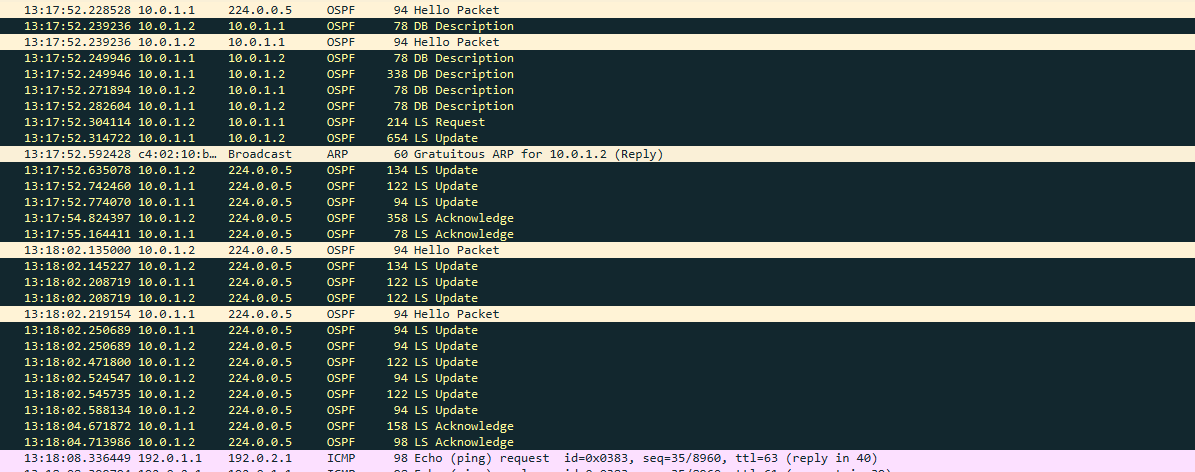
Cost = (Reference BandwidthInterface) / (Interface Bandwidth)​

The interface bandwidth is usually 100 Mbs, meaning that interfaces with lower bandwidths have a higher cost. The command “show interfaces FastEthernet interface-number” helps to calculate the cost because it provides, among other things, the bandwidth of said interface.

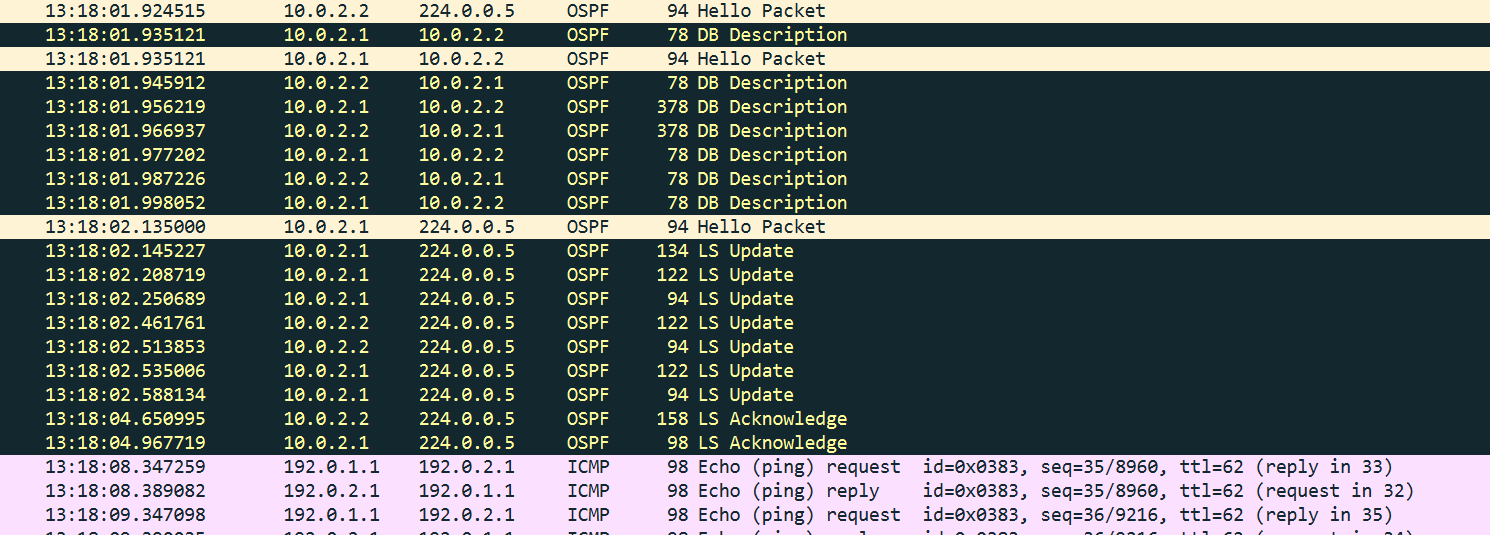
Part 4

4.10

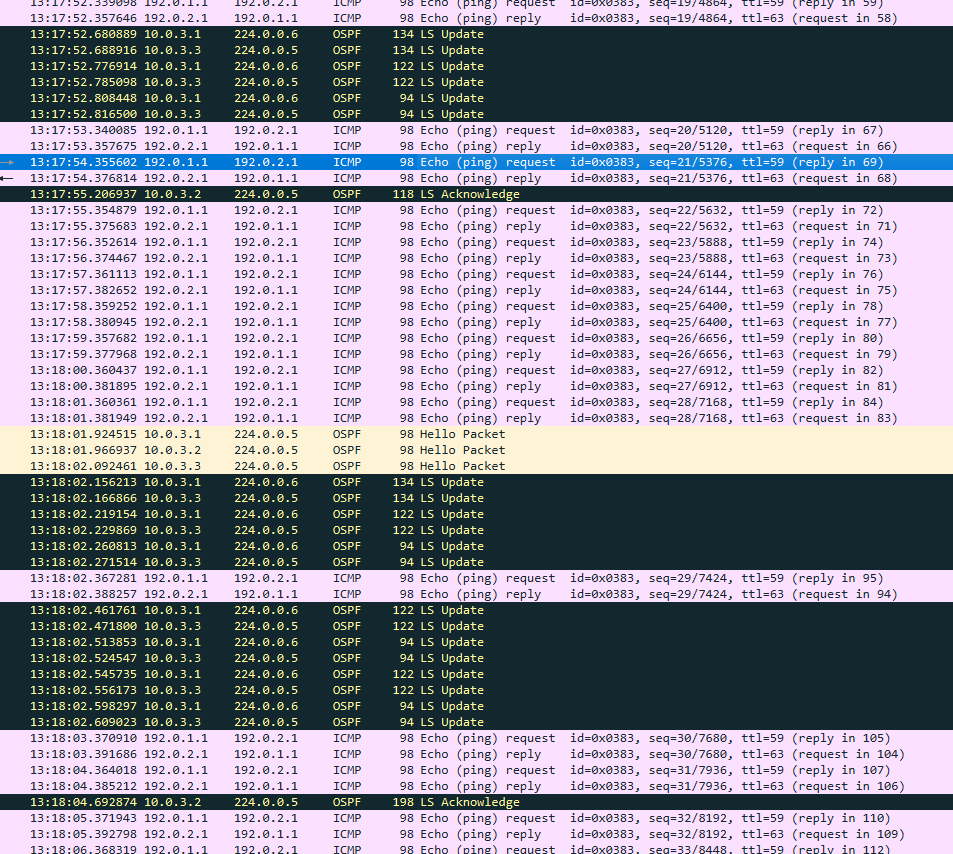
R1-R2:



R2-R3:



R4:

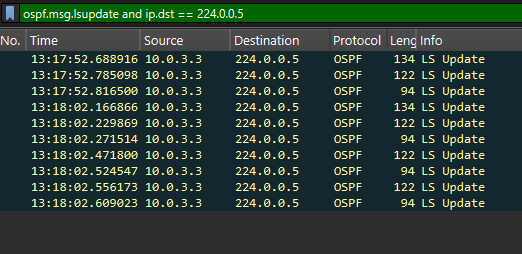


No, the PING application was not affected and no PING packets were lost. We can see that the TTL of the pings improved, before the update ping reached their destination with TTL=59. And after TTL of 61, meaning less hops on their way.

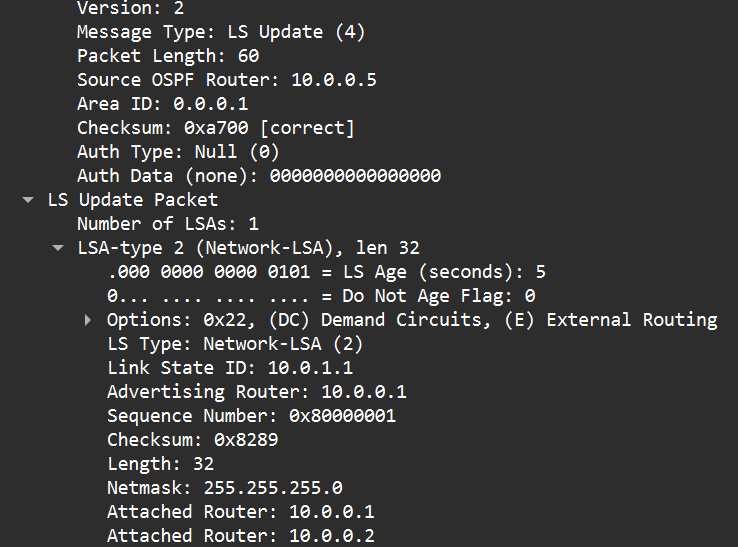
4.11

You can tell how long it took the network to converge by looking at the first update that R2 is sending, at 13:17:52.23, and when R4 sends and LS ACK packet to show that it received the update, at 13:18:04.69. Meaning that it took the network about 12.4 seconds to converge.

4.12

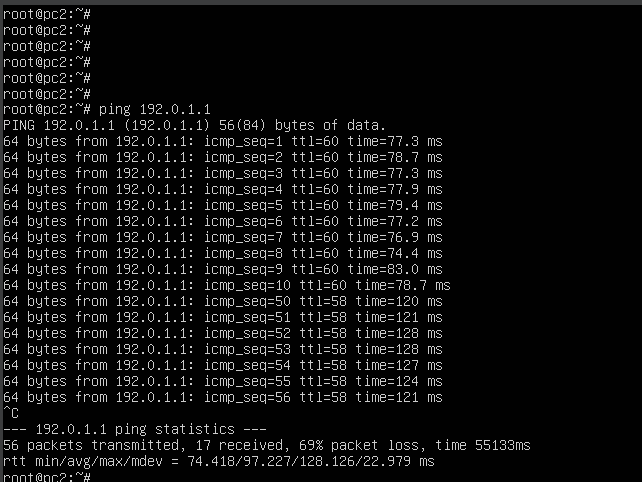


R5 is sending update messages to inform about changes in the network, for example:



An early message to inform the network that there is a network 10.0.1.0/24 between R1 and R2.

Part 5



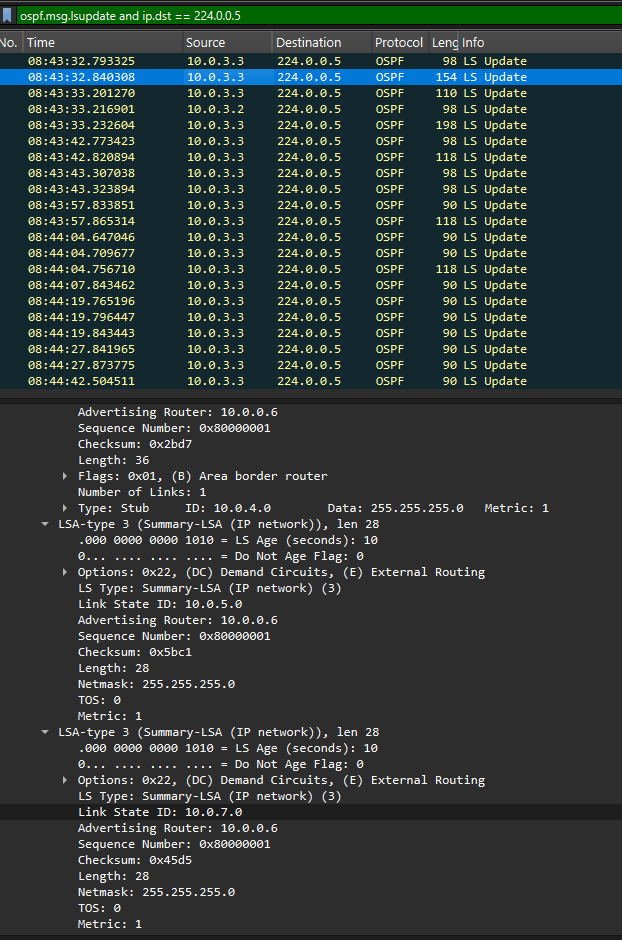
5.9

We turned R2 off about 8 seconds after the start of the PING sending, and saw the ACKs stop. Than, about 39 seconds later, ACKs started arriving again, taking more time to arrive (120 ms in compare to about 80 ms).

5.10

The waiting makes sense given the dead-interval protocol, which dictates that routers wait for usually 40 seconds between the last “hello” packet to declare a route as down. After the route is declared down, the network updates and finds the new shortest path, thats when we see the new ACK messages start arriving.

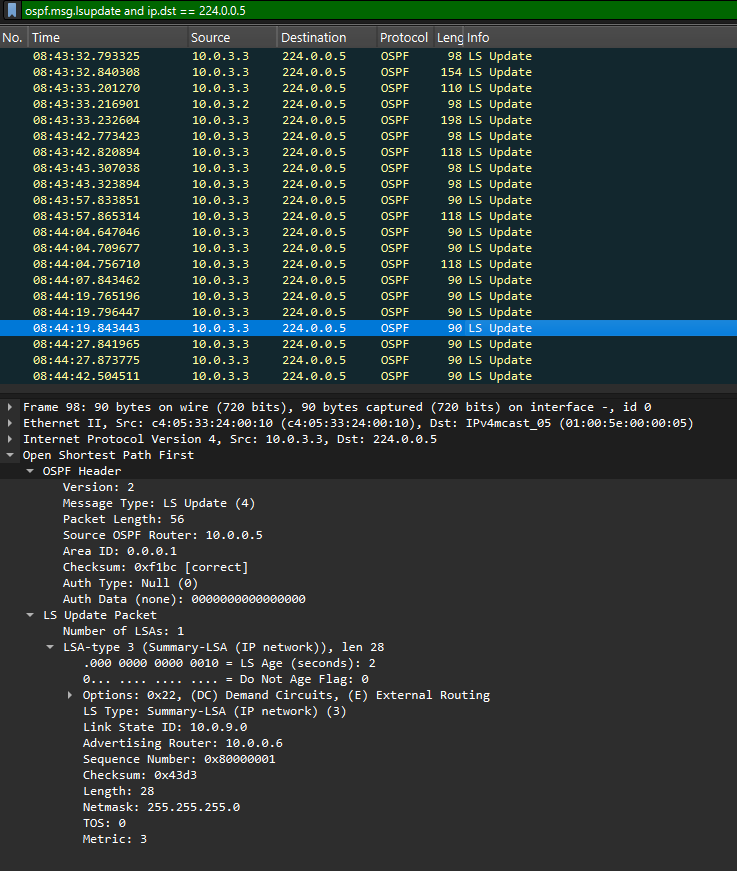
Part 6



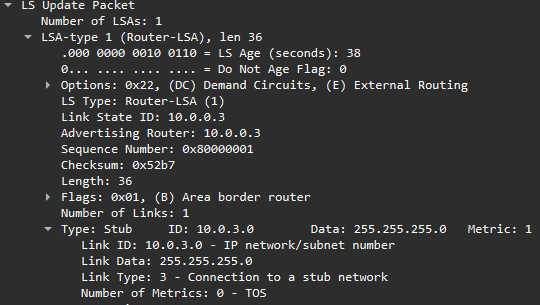
6.11

For the backbone area - R4 receives information about the router OSPF ip of R6 and R3 only, and the networks each is connected to - as can be seen in the picture above - R6 is 10.0.0.6 and connected to 10.0.5.0/24 and 10.0.7.0/24.

For area 2 R4 receives routing for the next router - but not information about the routers themselves, or the components in those networks. For example - to reach 10.0.9.0/24 go to R6:

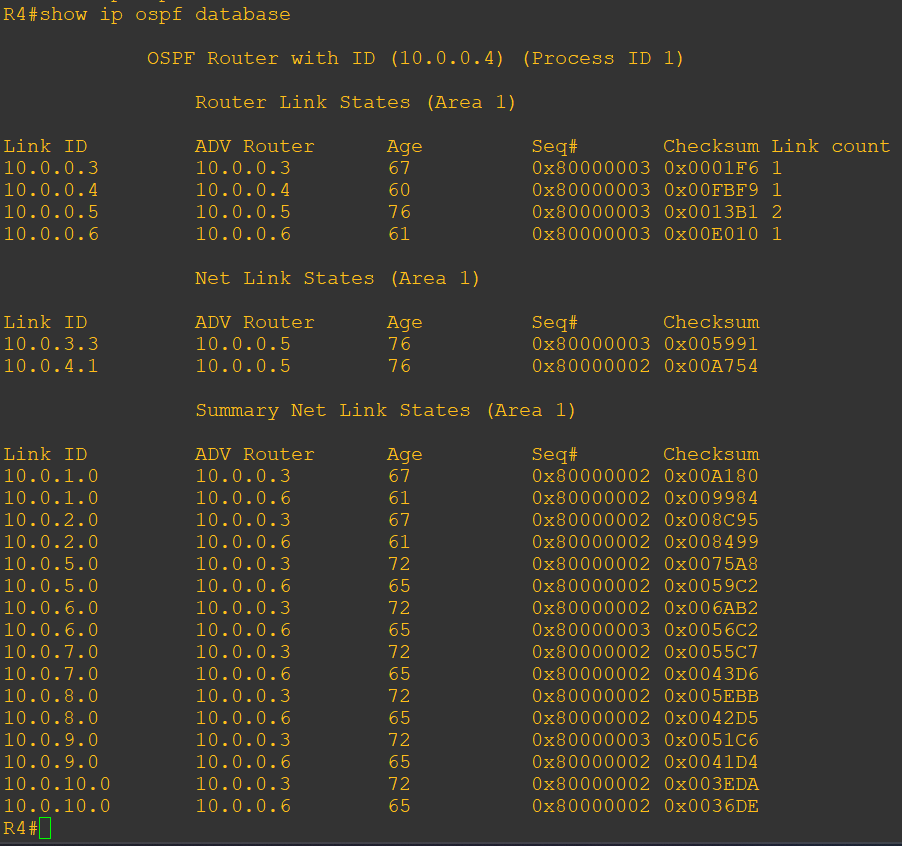


6.12



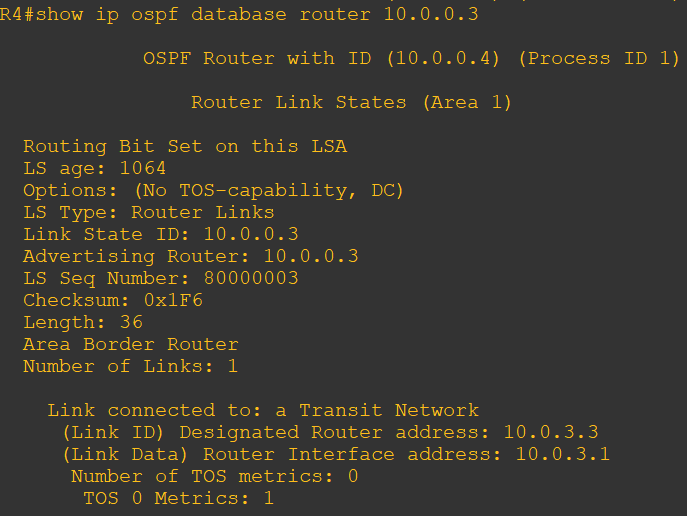
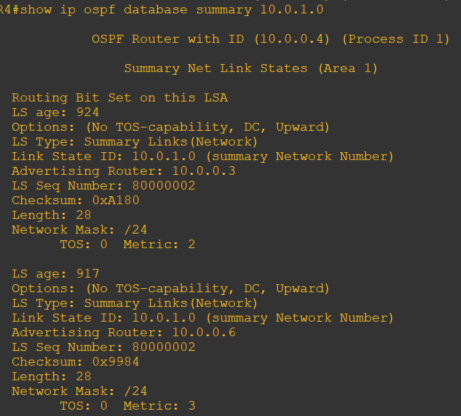
R3 advertises that it is the connection to 10.0.3.0/24 network.

6.13



This time R4, which is not a border router, does not hold the knowledge of the entire network.

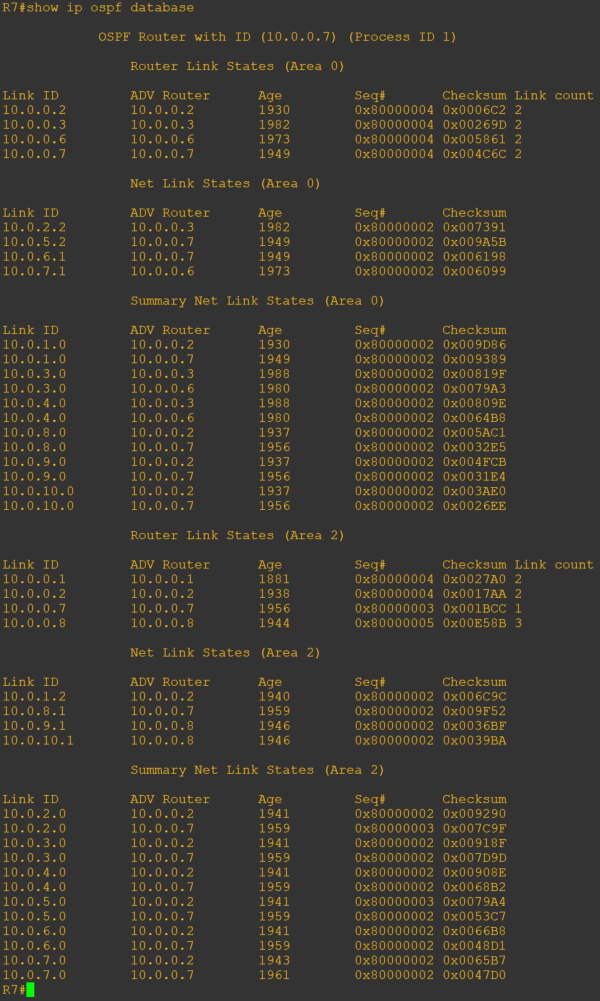
R4 knows the networks in area 1 and which router holds them(10.0.3.3 / 10.0.4.1 - R5), knows what routers are connected to area 1 in area 0 (R6,R3), and knows of the existence of all other networks in area 0 and area 2, and through which router in area 0 to reach these networks - but it isn't aware of the existence of other routers in area 0 or any in area 2.

6.14

From the given commands we can see that to reach network 10.0.1.0/24 we need to go through R3, 10.0.0.3. As we can tell from the show ip ospf database router 10.0.0.3 command, R3 is a link router, meaning it is connecting area 1 and area 0.

The given commands do not show us any information about other routers, such as R1 or R2 because this information does not exist in the R4 database

6.15



The first thing you can tell is that R7’s database is much larger. It holds information about all of area 0 and area 2 which includes all the networks and routers, and information about area 1 through area 0 links.

6.16

he advantage is the division into areas, which reduces the amount of data exchanged between routers. Each router only knows the routers within its area and the border routers. As a result, updates within a single area are faster (they pass through fewer routers and are smaller in size).

On the other hand, this is also a disadvantage—there’s no way to know the full topology, only the routers within the same area. If a border router fails and there’s no alternative connection to the backbone (or the desired area), communication will be disrupted, potentially causing significant issues.