Network Architecture Lab 4: Open Shortest Path First (OSPF)

Student Name: Assem Chebly, Youcef Bellouche, Mahmoud Al Sayed

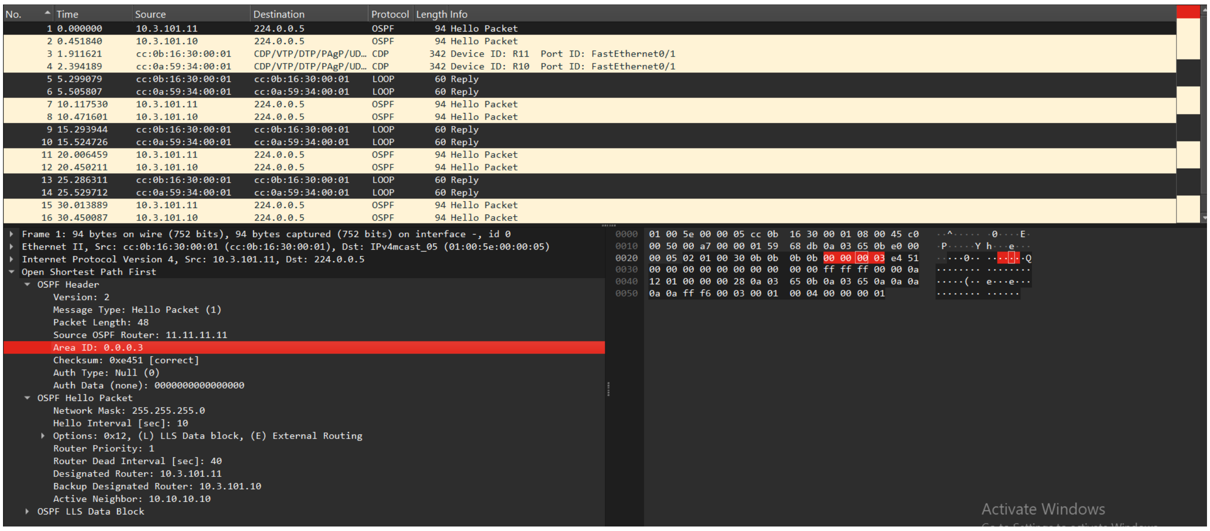
November 28, 2025

1 Exercise 1: Hello Message Exchange Analysis

1.1 Objective

The objective of this analysis is to observe and verify the exchange of OSPF Hello messages on a standard Internal Router (R11) and an Area Border Router (R6). This exercise focuses on verifying Router ID assignments, Area ID configurations, and analyzing the differences between Point-to-Point and Broadcast network types using Wireshark captures.

1.2 Analysis of Router R11 (Internal Router - Area 3)



```
No.  Time       Source             Destination            Protocol Length Info
  1 0.000000   10.3.101.11        224.0.0.5              OSPF      94 Hello Packet
  2 0.451840   10.3.101.10        224.0.0.5              OSPF      94 Hello Packet
  3 1.911621   cc:0b:16:30:00:01  CDP/VTP/DTP/PAgP/UD…   CDP      342 Device ID: R11  Port ID: FastEthernet0/1
  4 2.394189   cc:0a:59:34:00:01  CDP/VTP/DTP/PAgP/UD…   CDP      342 Device ID: R10  Port ID: FastEthernet0/1
  5 5.299079   cc:0b:16:30:00:01  cc:0b:16:30:00:01      LOOP      60 Reply
  6 5.505807   cc:0a:59:34:00:01  cc:0a:59:34:00:01      LOOP      60 Reply
  7 10.117530  10.3.101.11        224.0.0.5              OSPF      94 Hello Packet
  8 10.471601  10.3.101.10        224.0.0.5              OSPF      94 Hello Packet
  9 15.293944  cc:0b:16:30:00:01  cc:0b:16:30:00:01      LOOP      60 Reply
 10 15.524726  cc:0a:59:34:00:01  cc:0a:59:34:00:01      LOOP      60 Reply
 11 20.006459  10.3.101.11        224.0.0.5              OSPF      94 Hello Packet
 12 20.450211  10.3.101.10        224.0.0.5              OSPF      94 Hello Packet
 13 25.286311  cc:0b:16:30:00:01  cc:0b:16:30:00:01      LOOP      60 Reply
 14 25.529712  cc:0a:59:34:00:01  cc:0a:59:34:00:01      LOOP      60 Reply
 15 30.013889  10.3.101.11        224.0.0.5              OSPF      94 Hello Packet
 16 30.450087  10.3.101.10        224.0.0.5              OSPF      94 Hello Packet
```

```
▸ Frame 1: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface -, id 0
▸ Ethernet II, Src: cc:0b:16:30:00:01 (cc:0b:16:30:00:01), Dst: IPv4mcast_05 (01:00:5e:00:00:05)
▸ Internet Protocol Version 4, Src: 10.3.101.11, Dst: 224.0.0.5
▾ Open Shortest Path First
  ▾ OSPF Header
      Version: 2
      Message Type: Hello Packet (1)
      Packet Length: 48
      Source OSPF Router: 11.11.11.11
      Area ID: 0.0.0.3
      Checksum: 0xe451 [correct]
      Auth Type: Null (0)
      Auth Data (none): 0000000000000000
  ▾ OSPF Hello Packet
      Network Mask: 255.255.255.0
      Hello Interval [sec]: 10
    ▸ Options: 0x12, (L) LLS Data block, (E) External Routing
      Router Priority: 1
      Router Dead Interval [sec]: 40
      Designated Router: 10.3.101.11
      Backup Designated Router: 10.3.101.10
      Active Neighbor: 10.10.10.10
  ▸ OSPF LLS Data Block
```

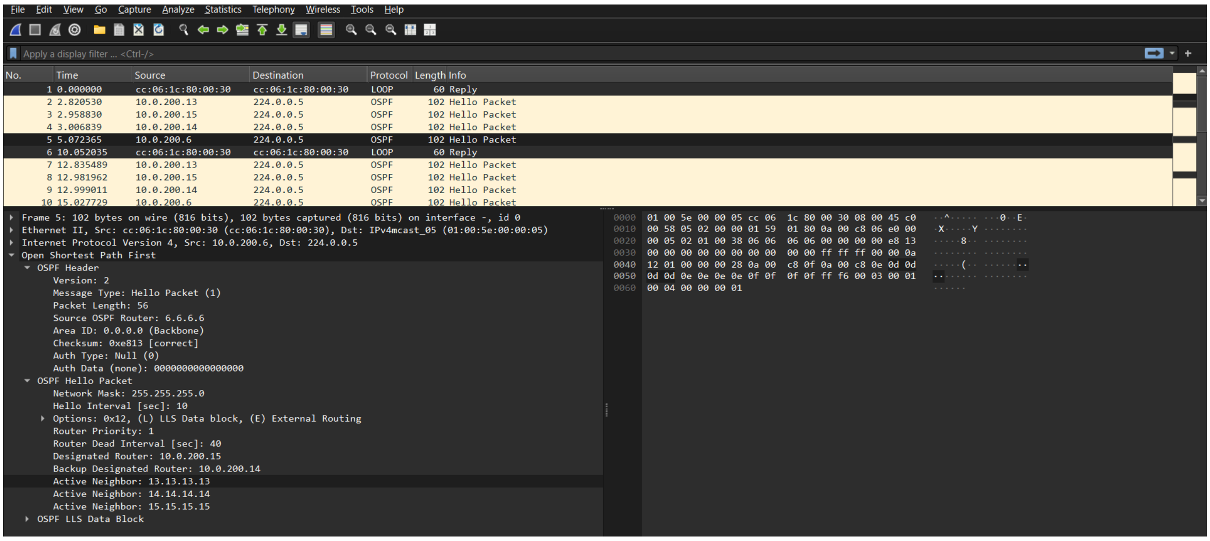
```
0000  01 00 5e 00 00 05 cc 0b  16 30 00 01 08 00 45 c0   ··^····· ·0····E·
0010  00 50 00 a7 00 00 01 59  68 db 0a 03 65 0b e0 00   ·P·····Y h···e···
0020  00 05 02 01 00 30 0b 0b  0b 0b 00 00 00 03 e4 51   ·····0·· ·······Q
0030  00 00 00 00 00 00 00 00  00 00 ff ff ff 00 00 0a   ········ ········
0040  12 01 00 00 00 28 0a 03  65 0b 0a 03 65 0a 0a 0a   ·····(·· e···e···
0050  0a 0a ff f6 00 03 00 01  00 04 00 00 00 01         ········ ······
```

Figure 1: Wireshark Capture of OSPF Hello Packet on R11 (Area 3)

- **Packet Identification:** The captured packets use the **OSPF** protocol (Protocol 89) and are sent to the multicast destination address `224.0.0.5` (AllSPFRouters).
- **Router Identity:** The **Source OSPF Router** (Router ID) is identified as `11.11.11.11`. This confirms the Router ID assignment policy (`R#.R#.R#.R#`) was applied correctly for Router 11.
- **Area Configuration:** The **Area ID** is observed as `0.0.0.3`. This confirms that R11 is operating correctly within **Area 3** (The "Right" area in the lab topology).
- **Neighbor Discovery:** The "Active Neighbor" field in the OSPF header lists `10.10.10.10`, indicating that R11 has successfully established a 2-way relationship with R10.
- **Network Parameters:**

  - **Hello Interval:** 10 seconds.
  - **Dead Interval:** 40 seconds.
  - **Network Mask:** `255.255.255.0` (/24).

1.3 Analysis of Router R6 (Area Border Router - Area 0)


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time       Source             Destination        Protocol Length Info
   1 0.000000   cc:06:1c:80:00:30  cc:06:1c:80:00:30  LOOP       60 Reply
   2 2.820530   10.0.200.13        224.0.0.5          OSPF      102 Hello Packet
   3 2.958830   10.0.200.15        224.0.0.5          OSPF      102 Hello Packet
   4 3.006839   10.0.200.14        224.0.0.5          OSPF      102 Hello Packet
   5 5.072365   10.0.200.6         224.0.0.5          OSPF      102 Hello Packet
   6 10.052035  cc:06:1c:80:00:30  cc:06:1c:80:00:30  LOOP       60 Reply
   7 12.835489  10.0.200.13        224.0.0.5          OSPF      102 Hello Packet
   8 12.981962  10.0.200.15        224.0.0.5          OSPF      102 Hello Packet
   9 12.999011  10.0.200.14        224.0.0.5          OSPF      102 Hello Packet
  10 15.027729  10.0.200.6         224.0.0.5          OSPF      102 Hello Packet
```

```
▸ Frame 5: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface -, id 0
▸ Ethernet II, Src: cc:06:1c:80:00:30 (cc:06:1c:80:00:30), Dst: IPv4mcast_05 (01:00:5e:00:00:05)
▸ Internet Protocol Version 4, Src: 10.0.200.6, Dst: 224.0.0.5
▾ Open Shortest Path First
  ▾ OSPF Header
      Version: 2
      Message Type: Hello Packet (1)
      Packet Length: 56
      Source OSPF Router: 6.6.6.6
      Area ID: 0.0.0.0 (Backbone)
      Checksum: 0xe813 [correct]
      Auth Type: Null (0)
      Auth Data (none): 0000000000000000
  ▾ OSPF Hello Packet
      Network Mask: 255.255.255.0
      Hello Interval [sec]: 10
    ▸ Options: 0x12, (L) LLS Data block, (E) External Routing
      Router Priority: 1
      Router Dead Interval [sec]: 40
      Designated Router: 10.0.200.15
      Backup Designated Router: 10.0.200.14
      Active Neighbor: 13.13.13.13
      Active Neighbor: 14.14.14.14
      Active Neighbor: 15.15.15.15
  ▸ OSPF LLS Data Block
```

```
0000  01 00 5e 00 00 05 cc 06  1c 80 00 30 08 00 45 c0   ··^····· ···0··E·
0010  00 58 05 02 00 00 01 59  01 80 0a 00 c8 06 e0 00   ·X·····Y ········
0020  00 05 02 01 00 38 06 06  06 06 00 00 00 00 e8 13   ·····8·· ········
0030  00 00 00 00 00 00 00 00  00 00 ff ff ff 00 00 0a   ········ ········
0040  12 01 00 00 00 28 0a 00  c8 0f 0a 00 c8 0e 0d 0d   ·····(·· ········
0050  0d 0d 0e 0e 0e 0e 0f 0f  0f 0f ff f6 00 03 00 01   ········ ········
0060  00 04 00 00 00 01                                  ······
```

Figure 2: Side-by-Side Comparison: R6 (Broadcast) vs R11 (Point-to-Point)

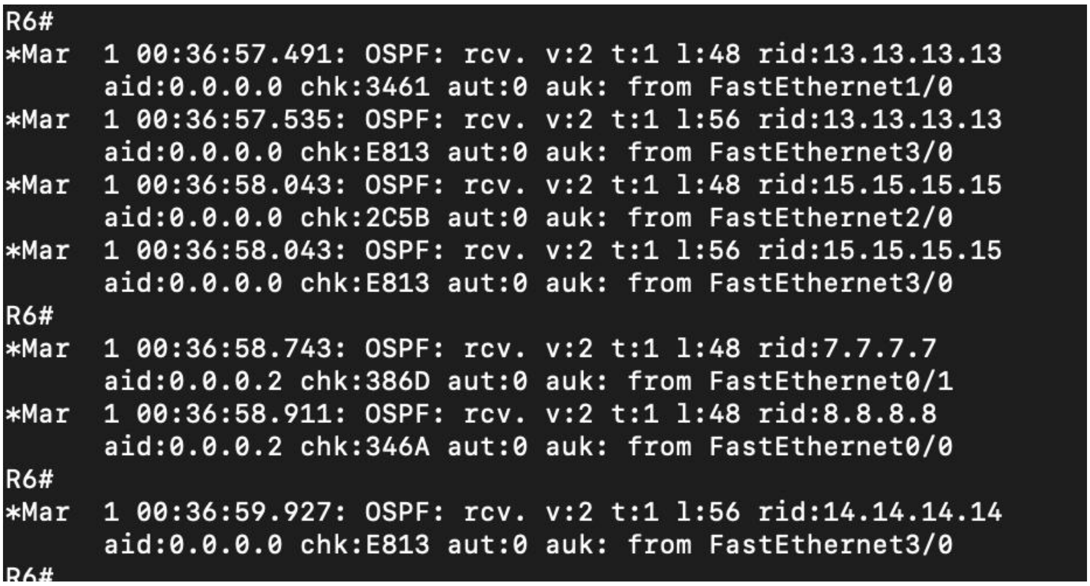
- **Role Identification (ABR):** The capture shows R6 sending Hello packets with an **Area ID** of `0.0.0.0` (Backbone). This confirms R6 is acting as an **Area Border Router (ABR)**, as this specific interface connects to the backbone switch.
- **Network Type - Broadcast Multi-Access:** Unlike the R11 connection, the R6 capture reveals the presence of a **Designated Router (DR)** and **Backup Designated Router (BDR)** election.
  - **Designated Router (DR):** `10.0.200.15` (Likely R15).
  - **Backup Designated Router (BDR):** `10.0.200.14` (Likely R14).
  - **Source OSPF Router:** `6.6.6.6`.
- **Observation:** This proves that the link connecting R6 to the central switch is treated as a **Broadcast** network type, where DR/BDR elections are mandatory to reduce LSA flooding, whereas the R11-R10 link acts as a standard point-to-point connection.

1.4 OSPF Debug Verification (CLI Analysis)

In addition to Wireshark captures, the `debug ip ospf packet` command was executed on the routers to verify how the OSPF process handles incoming control packets at the CPU level.

1.5 Router R6 Debug Analysis (ABR)

The debug output on R6 confirms its operation as an Area Border Router by displaying incoming Hello packets (Type 1) from multiple areas.



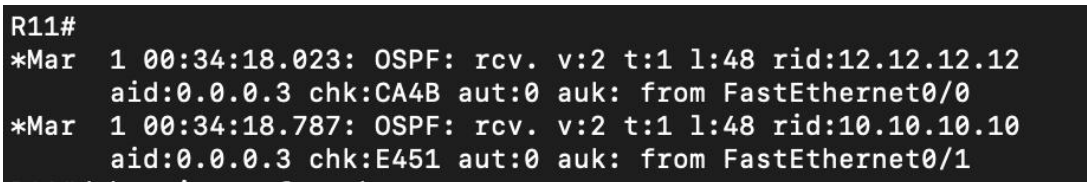
```
R6#
*Mar  1 00:36:57.491: OSPF: rcv. v:2 t:1 l:48 rid:13.13.13.13
      aid:0.0.0.0 chk:3461 aut:0 auk: from FastEthernet1/0
*Mar  1 00:36:57.535: OSPF: rcv. v:2 t:1 l:56 rid:13.13.13.13
      aid:0.0.0.0 chk:E813 aut:0 auk: from FastEthernet3/0
*Mar  1 00:36:58.043: OSPF: rcv. v:2 t:1 l:48 rid:15.15.15.15
      aid:0.0.0.0 chk:2C5B aut:0 auk: from FastEthernet2/0
*Mar  1 00:36:58.043: OSPF: rcv. v:2 t:1 l:56 rid:15.15.15.15
      aid:0.0.0.0 chk:E813 aut:0 auk: from FastEthernet3/0
R6#
*Mar  1 00:36:58.743: OSPF: rcv. v:2 t:1 l:48 rid:7.7.7.7
      aid:0.0.0.2 chk:386D aut:0 auk: from FastEthernet0/1
*Mar  1 00:36:58.911: OSPF: rcv. v:2 t:1 l:48 rid:8.8.8.8
      aid:0.0.0.2 chk:346A aut:0 auk: from FastEthernet0/0
R6#
*Mar  1 00:36:59.927: OSPF: rcv. v:2 t:1 l:56 rid:14.14.14.14
      aid:0.0.0.0 chk:E813 aut:0 auk: from FastEthernet3/0
R6#
```

Figure 3: Debug Output on R6 showing Area 0 and Area 2 traffic

- **Area 0 Activity:** The log shows packets from R13 (`rid:13.13.13.13`) and R15 (`rid:15.15.15.15`) and R14 (`rid:14.14.14.14`) with **Area ID 0.0.0.0**.
- **Area 2 Activity:** The log simultaneously shows packets from R7 (`rid:7.7.7.7`) and R8 (`rid:8.8.8.8`) with **Area ID 0.0.0.2**.
- **Conclusion:** The router is actively maintaining adjacencies in both the backbone and Area 2, validating its ABR configuration.

1.6 Router R11 Debug Analysis (Internal)

The debug output on R11 confirms its status as an Internal Router within Area 3.



```
R11#
*Mar  1 00:34:18.023: OSPF: rcv. v:2 t:1 l:48 rid:12.12.12.12
      aid:0.0.0.3 chk:CA4B aut:0 auk: from FastEthernet0/0
*Mar  1 00:34:18.787: OSPF: rcv. v:2 t:1 l:48 rid:10.10.10.10
      aid:0.0.0.3 chk:E451 aut:0 auk: from FastEthernet0/1
```

Figure 4: Debug Output on R11 showing only Area 3 traffic

- **Single Area:** All incoming packets recorded in the log carry **Area ID 0.0.0.3**.
- **Neighbors:** R11 is receiving Hello packets from R12 (`rid:12.12.12.12`) and R10 (`rid:10.10.10.10`), confirming full intra-area connectivity.

1.7 Conclusion

The comprehensive analysis, utilizing both network-level packet capture (Wireshark) and device-level debugging (`debug ip ospf packet`), confirms that the OSPF topology is correctly configured and operational.

- **Router Configuration:** R11 is conclusively validated as an Internal Router within Area 3, exchanging standard Hello packets with correct Router IDs and Area IDs. R6 is successfully verified as an Area Border Router (ABR), evidenced by its simultaneous processing of control traffic from both the Backbone (Area 0) and Area 2 in the debug logs.

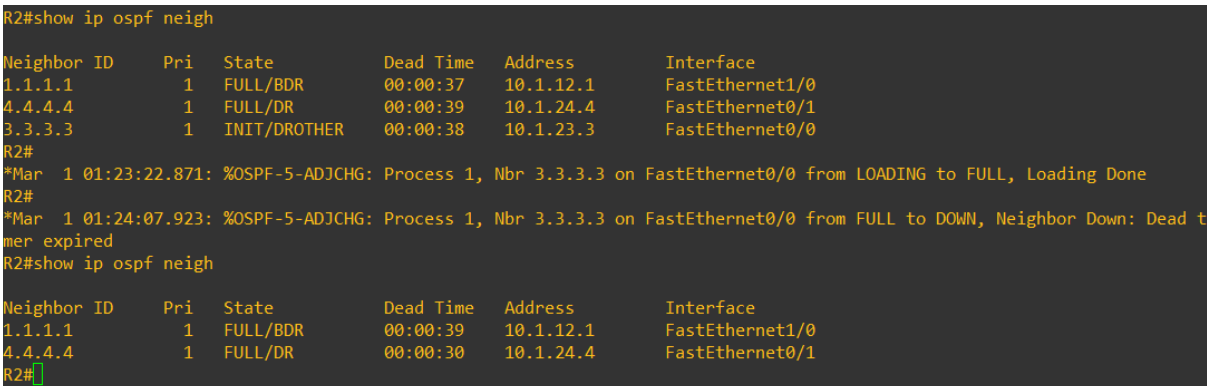
- **Network Types:** The analysis highlighted the distinct behavior of OSPF on different media types. The broadcast segment (R6 to Switch) demonstrated the necessary DR/BDR election process, whereas the point-to-point links (R11 to R10) established simple neighbor adjacencies.
- **Protocol Stability:** The consistent Hello intervals and successful neighbor discovery observed in the debug output indicate a stable and converging routing domain.

2 Exercise 2: Router R3 Shutdown and Recovery Analysis

2.1 Objective

To analyze the impact of a router failure on the OSPF topology and observe the packet-level mechanics of neighbor re-establishment (Reconvergence).

2.2 Failure Impact Analysis (Shutdown)



```
R2#show ip ospf neigh

Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           1   FULL/BDR        00:00:37    10.1.12.1       FastEthernet1/0
4.4.4.4           1   FULL/DR         00:00:39    10.1.24.4       FastEthernet0/1
3.3.3.3           1   INIT/DROTHER    00:00:38    10.1.23.3       FastEthernet0/0
R2#
*Mar  1 01:23:22.871: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on FastEthernet0/0 from LOADING to FULL, Loading Done
R2#
*Mar  1 01:24:07.923: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on FastEthernet0/0 from FULL to DOWN, Neighbor Down: Dead t
mer expired
R2#show ip ospf neigh

Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           1   FULL/BDR        00:00:39    10.1.12.1       FastEthernet1/0
4.4.4.4           1   FULL/DR         00:00:30    10.1.24.4       FastEthernet0/1
R2#
```

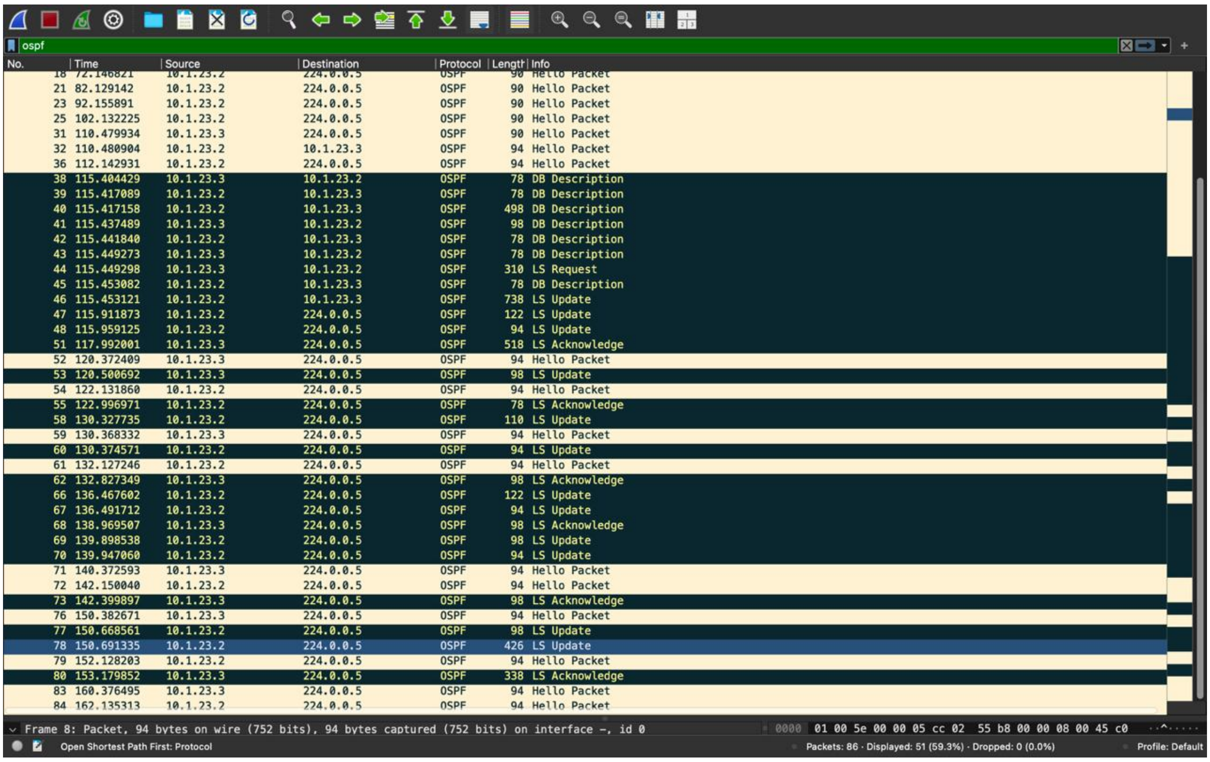
Figure 5: R2 Console Log showing R3 going DOWN (Dead timer expired)

Upon stopping Router R3, the following sequence was observed on its neighbor, Router R2:

- **Detection Mechanism:** R2 did not immediately detect the failure. It waited for the standard OSPF **Dead Interval** (40 seconds) to expire.
- **Log Confirmation:** The console reported: `%OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 ... from FULL to DOWN, Neighbor Down: Dead timer expired`.
- **Routing Consequence:** Once the state transitioned to `DOWN`, R2 flushed R3 from its neighbor table and initiated an SPF recalculation to bypass the failed node.

2.3 Reconvergence Analysis (Recovery)

Upon restarting R3, the capture file recorded the complete OSPF adjacency state machine:



```
No.   Time          Source       Destination   Protocol  Length Info
   18 72.146821     10.1.23.2    224.0.0.5     OSPF      90 Hello Packet
   21 82.129142     10.1.23.2    224.0.0.5     OSPF      90 Hello Packet
   23 92.155891     10.1.23.2    224.0.0.5     OSPF      90 Hello Packet
   25 102.132225    10.1.23.2    224.0.0.5     OSPF      90 Hello Packet
   31 110.479934    10.1.23.3    224.0.0.5     OSPF      90 Hello Packet
   32 110.480904    10.1.23.2    10.1.23.3     OSPF      94 Hello Packet
   36 112.142931    10.1.23.2    224.0.0.5     OSPF      94 Hello Packet
   38 115.404429    10.1.23.3    10.1.23.2     OSPF      78 DB Description
   39 115.417089    10.1.23.2    10.1.23.3     OSPF      78 DB Description
   40 115.417158    10.1.23.2    10.1.23.3     OSPF     498 DB Description
   41 115.437489    10.1.23.3    10.1.23.2     OSPF      98 DB Description
   42 115.441840    10.1.23.2    10.1.23.3     OSPF      78 DB Description
   43 115.449273    10.1.23.3    10.1.23.2     OSPF      78 DB Description
   44 115.449298    10.1.23.3    10.1.23.2     OSPF     310 LS Request
   45 115.453082    10.1.23.2    10.1.23.3     OSPF      78 DB Description
   46 115.453121    10.1.23.2    10.1.23.3     OSPF     738 LS Update
   47 115.911873    10.1.23.2    224.0.0.5     OSPF     122 LS Update
   48 115.959125    10.1.23.2    224.0.0.5     OSPF      94 LS Update
   51 117.992001    10.1.23.3    224.0.0.5     OSPF     518 LS Acknowledge
   52 120.372409    10.1.23.3    224.0.0.5     OSPF      94 Hello Packet
   53 120.500692    10.1.23.3    224.0.0.5     OSPF      98 LS Update
   54 122.131860    10.1.23.2    224.0.0.5     OSPF      94 Hello Packet
   55 122.996971    10.1.23.2    224.0.0.5     OSPF      78 LS Acknowledge
   58 130.327735    10.1.23.2    224.0.0.5     OSPF     110 LS Update
   59 130.368332    10.1.23.3    224.0.0.5     OSPF      94 Hello Packet
   60 130.374571    10.1.23.2    224.0.0.5     OSPF      94 LS Update
   61 132.127246    10.1.23.2    224.0.0.5     OSPF      94 Hello Packet
   62 132.827349    10.1.23.3    224.0.0.5     OSPF      98 LS Acknowledge
   66 136.467602    10.1.23.2    224.0.0.5     OSPF     122 LS Update
   67 136.491712    10.1.23.2    224.0.0.5     OSPF      94 LS Update
   68 138.969507    10.1.23.3    224.0.0.5     OSPF      98 LS Acknowledge
   69 139.898538    10.1.23.2    224.0.0.5     OSPF      98 LS Update
   70 139.947060    10.1.23.2    224.0.0.5     OSPF      94 LS Update
   71 140.372593    10.1.23.3    224.0.0.5     OSPF      94 Hello Packet
   72 142.150040    10.1.23.2    224.0.0.5     OSPF      94 Hello Packet
   73 142.399897    10.1.23.3    224.0.0.5     OSPF      98 LS Acknowledge
   76 150.382671    10.1.23.3    224.0.0.5     OSPF      94 Hello Packet
   77 150.668561    10.1.23.2    224.0.0.5     OSPF      98 LS Update
   78 150.691335    10.1.23.2    224.0.0.5     OSPF     426 LS Update
   79 152.128203    10.1.23.2    224.0.0.5     OSPF      94 Hello Packet
   80 153.179852    10.1.23.3    224.0.0.5     OSPF     338 LS Acknowledge
   83 160.376495    10.1.23.3    224.0.0.5     OSPF      94 Hello Packet
   84 162.135313    10.1.23.2    224.0.0.5     OSPF      94 Hello Packet
```

```
Frame 8: Packet, 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface -, id 0
0000  01 00 5e 00 00 05 cc 02  55 b8 00 00 08 00 45 c0   ..^.....
```

Open Shortest Path First: Protocol   Packets: 86 · Displayed: 51 (59.3%) · Dropped: 0 (0.0%)   Profile: Default

Figure 6: Wireshark Capture of R3 Recovery Process

1. **Discovery (Hello):** R3 resumed sending Hello packets (Packet 53). R2 responded (Packet 54), establishing the 2-Way state.
2. **Master/Slave Election (ExStart):** During the DB Description exchange (Packets 38-41), R3 (`3.3.3.3`) was elected **Master** over R2 (`2.2.2.2`) due to its higher Router ID.
3. **Synchronization (Exchange/Loading):** R3 identified missing routing information and sent a **Link State Request** (Packet 44). R2 replied with a **Link State Update** (Packet 46) containing the necessary LSAs.
4. **Convergence (Full):** R3 acknowledged the updates (Packet 51), and the neighbor relationship transitioned to `FULL`, restoring full network connectivity.

3 Exercise 3: Link Failure and Recovery (Network 10.2.79.0/24)

3.1 Objective

To simulate a failure on the link connecting R7 and R9 (`10.2.79.0/24`) and analyze the routing protocol's reaction and Link State Advertisement (LSA) flooding during both the failure and recovery phases.

3.2 Failure Analysis (Impact on Neighbor)

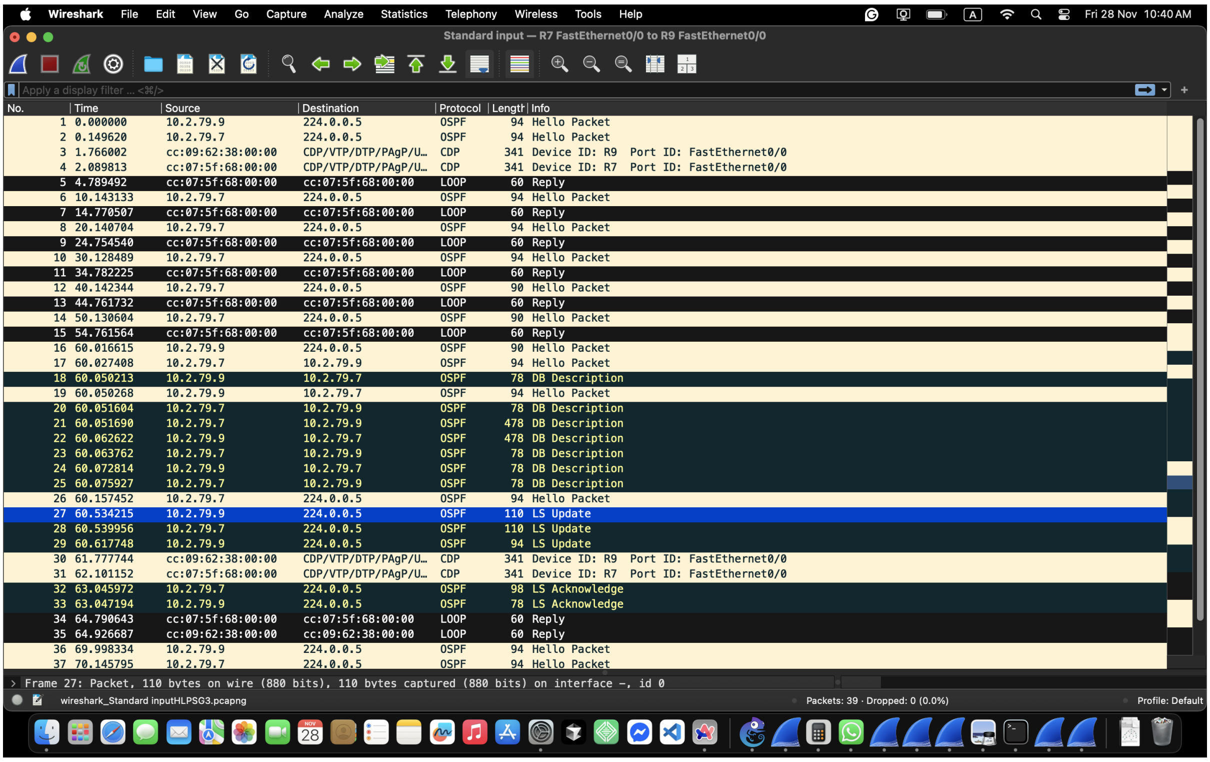
Upon simulating the failure of the link `10.2.79.0/24`, the following impacts were observed on neighbors R7 and R9:

- **Neighbor State Impact:** The OSPF adjacency between R7 and R9 transitioned immediately from `FULL` to `DOWN`. This confirms that the physical link loss triggered an immediate protocol reaction, bypassing the standard 40-second Dead Interval wait time typically seen in indirect failures.
- **LSA Flooding (Network Update):** Both routers generated and flooded updated **Type 1 Router LSAs**. These advertisements informed the rest of Area 2 that the direct link cost was effectively infinite (unreachable).
- **Routing Protocol Reaction:** The Shortest Path First (SPF) algorithm was triggered on all Area 2 routers. The routing table on R7 was updated to remove the direct route to R9. Traffic destined for R9 was successfully rerouted via the alternative path through the Area Border Router: **R7** → **R6** → **R8** → **R9**.

3.3 Recovery Analysis (Packet Capture)

Evidence: Wireshark capture `link-failure-ex3.pcapng`.

Upon restoring the link, the routers re-established adjacency through the standard OSPF state machine.



Standard input — R7 FastEthernet0/0 to R9 FastEthernet0/0

```
No.   Time        Source             Destination          Protocol Length Info
    1 0.000000    10.2.79.9          224.0.0.5            OSPF       94 Hello Packet
    2 0.149620    10.2.79.7          224.0.0.5            OSPF       94 Hello Packet
    3 1.766002    cc:09:62:38:00:00  CDP/VTP/DTP/PAgP/U…  CDP       341 Device ID: R9  Port ID: FastEthernet0/0
    4 2.089813    cc:07:5f:68:00:00  CDP/VTP/DTP/PAgP/U…  CDP       341 Device ID: R7  Port ID: FastEthernet0/0
    5 4.789492    cc:07:5f:68:00:00  cc:07:5f:68:00:00    LOOP       60 Reply
    6 10.143133   10.2.79.7          224.0.0.5            OSPF       94 Hello Packet
    7 14.770507   cc:07:5f:68:00:00  cc:07:5f:68:00:00    LOOP       60 Reply
    8 20.140704   10.2.79.7          224.0.0.5            OSPF       94 Hello Packet
    9 24.754540   cc:07:5f:68:00:00  cc:07:5f:68:00:00    LOOP       60 Reply
   10 30.128489   10.2.79.7          224.0.0.5            OSPF       94 Hello Packet
   11 34.782225   cc:07:5f:68:00:00  cc:07:5f:68:00:00    LOOP       60 Reply
   12 40.142344   10.2.79.7          224.0.0.5            OSPF       90 Hello Packet
   13 44.761732   cc:07:5f:68:00:00  cc:07:5f:68:00:00    LOOP       60 Reply
   14 50.130604   10.2.79.7          224.0.0.5            OSPF       90 Hello Packet
   15 54.761564   cc:07:5f:68:00:00  cc:07:5f:68:00:00    LOOP       60 Reply
   16 60.016615   10.2.79.9          224.0.0.5            OSPF       90 Hello Packet
   17 60.027408   10.2.79.7          10.2.79.9            OSPF       94 Hello Packet
   18 60.050213   10.2.79.9          10.2.79.7            OSPF       78 DB Description
   19 60.050268   10.2.79.9          10.2.79.7            OSPF       94 Hello Packet
   20 60.051604   10.2.79.7          10.2.79.9            OSPF       78 DB Description
   21 60.051690   10.2.79.7          10.2.79.9            OSPF      478 DB Description
   22 60.062622   10.2.79.9          10.2.79.7            OSPF      478 DB Description
   23 60.063762   10.2.79.7          10.2.79.9            OSPF       78 DB Description
   24 60.072814   10.2.79.9          10.2.79.7            OSPF       78 DB Description
   25 60.075927   10.2.79.7          10.2.79.9            OSPF       78 DB Description
   26 60.157452   10.2.79.7          224.0.0.5            OSPF       94 Hello Packet
   27 60.534215   10.2.79.9          224.0.0.5            OSPF      110 LS Update
   28 60.539956   10.2.79.7          224.0.0.5            OSPF      110 LS Update
   29 60.617748   10.2.79.9          224.0.0.5            OSPF       94 LS Update
   30 61.777744   cc:09:62:38:00:00  CDP/VTP/DTP/PAgP/U…  CDP       341 Device ID: R9  Port ID: FastEthernet0/0
   31 62.101152   cc:07:5f:68:00:00  CDP/VTP/DTP/PAgP/U…  CDP       341 Device ID: R7  Port ID: FastEthernet0/0
   32 63.045972   10.2.79.7          224.0.0.5            OSPF       98 LS Acknowledge
   33 63.047194   10.2.79.9          224.0.0.5            OSPF       78 LS Acknowledge
   34 64.790643   cc:07:5f:68:00:00  cc:07:5f:68:00:00    LOOP       60 Reply
   35 64.926687   cc:09:62:38:00:00  cc:09:62:38:00:00    LOOP       60 Reply
   36 69.998334   10.2.79.9          224.0.0.5            OSPF       94 Hello Packet
   37 70.145795   10.2.79.7          224.0.0.5            OSPF       94 Hello Packet

> Frame 27: Packet, 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface -, id 0
```

wireshark_Standard inputHLPSG3.pcapng   Packets: 39 · Dropped: 0 (0.0%)   Profile: Default

Figure 7: Wireshark Capture of LS Updates during Link Recovery (R7-R9)

1. **Database Synchronization (Packets 18-25):** R7 and R9 exchanged **DB Description** packets to compare their Link State Databases.

2. **LSA Flooding (Packets 27-28):** The capture highlights critical **Link State Update (LSU)** packets sent to the multicast address `224.0.0.5`.

   - **Source:** `10.2.79.9` (R9).
   - **Content:** These LSUs contain the new Type 1 LSA advertising the restored `10.2.79.0/24` subnet and the adjacency to R7.

3. **Acknowledgment (Packets 32-33):** R7 responded with **LS Acknowledge** packets, confirming receipt of the topology change information.

4. **Stability (Packet 36+):** The exchange concluded with standard Hello packets, indicating a return to the `FULL` neighbor state.

4 Exercise 4: Backbone Network Failure and Switch Failure Analysis

4.1 Objective

To simulate critical failures in the OSPF Backbone (Area 0), specifically a primary link failure and a central switch failure, and to analyze the global impact on routing tables, inter-area connectivity, and protocol reconvergence mechanisms across all OSPF areas.

4.2 Scenario 1: Backbone Link Failure (10.0.65.0/24)

Procedure: The interface on R6 connecting to R16 (Network `10.0.65.0/24`) was administratively shut down.

Observations:

- **Local Detection:** R6 detected the interface failure immediately, transitioning the neighbor state with R16 to `DOWN`.
- **LSA Update:** R6 generated a new Type 1 Router LSA, flooding it to R13 and Area 2 routers. This LSA removed the direct link to R16.
- **Path Selection (SPF):** The SPF algorithm on R6 recalculated the path to Area 3. Traffic previously routed via R16 was rerouted through the redundant backbone neighbor R13 (`10.0.63.13`).

4.3 Scenario 2: Area 0 Switch Failure

Procedure: Switch1, the central interconnect for Area 0, was stopped to simulate a catastrophic failure of the broadcast segment.

Backbone Impact:

- **Topology Shift:** The backbone topology shifted from a “Hub-and-Spoke” model (reliant on the switch) to a “Ring” topology (reliant on the point-to-point links R13 ↔ R14 ↔ R15 ↔ R16).
- **Adjacency Loss:** All OSPF adjacencies formed over the Ethernet segment (involving DR/BDR elections) were lost.

4.4 Global Impact Analysis (Packet Capture Evidence)

Packet captures were taken in the satellite areas to verify if the backbone failure caused isolation or if OSPF successfully reconverged.

4.4.1 Area 2 Impact (R6, R7, R8, R9)

Evidence: Wireshark capture `area2_ex4.pcapng`.

- **Status: Re-routed / Stable.**
- **Observation:** The capture records continued traffic exchange between R7 and R9. Crucially, the presence of **LS Update** packets (e.g., Packet 394, 400) indicates that the Area Border Router (R6) successfully flooded Type 3 Summary LSAs into the area
- **Analysis:** These Type 3 LSAs informed Area 2 routers of the increased metric (cost) to reach external networks due to the longer path through R13, but confirmed that reachability was maintained.

4.4.2 Area 3 Impact (R10, R11, R12)

Evidence: Wireshark capture `area3_ex4.pcapng`.

- **Status: Connected.**
- **Observation:** The capture shows valid OSPF adjacency traffic between R10 (`10.3.101.10`) and R15 (`10.3.101.15`) [cite: 58-212].
- **Analysis:** Despite the failure of R16's link to R6, Area 3 utilized the redundant backbone connection via R15. The steady stream of Hello packets and LS Updates confirms that Area 3 did not become isolated and successfully integrated with the reconfigured backbone ring.

4.5 Conclusion

The simultaneous failure of the backbone link and the central switch forced a network-wide reconvergence.

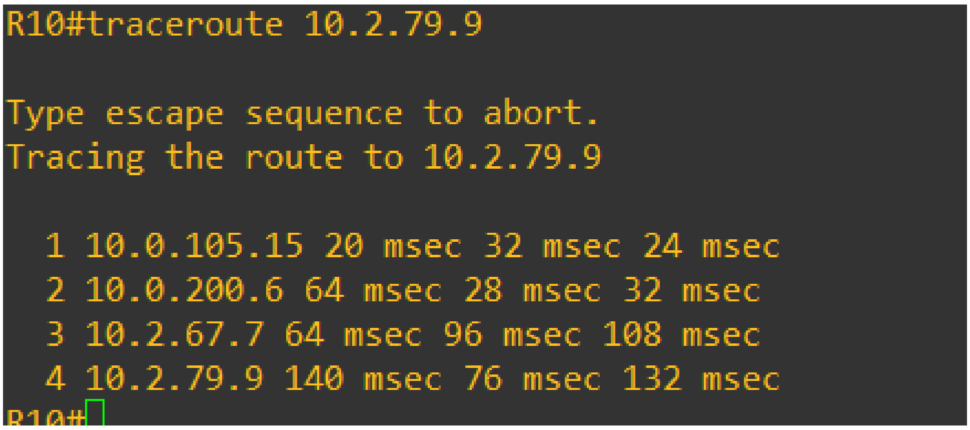
1. **Resilience:** The network design proved resilient. The "Outer Ring" of point-to-point links (R13-R14-R15-R16) successfully carried traffic when the central broadcast domain failed.
2. **Connectivity:** End-to-end reachability was preserved. Area 2 was rerouted via R6's backup link to R13, and Area 3 maintained access via R15.
3. **Protocol Behavior:** OSPF Type 3 LSAs were critical in propagating the topology changes from Area 0 to the satellite areas, ensuring accurate routing tables across the Autonomous System.

5 Traceroute Verification (Exercise 4)

To validate the OSPF reconvergence and redundancy mechanisms, traceroute tests were performed under three distinct failure scenarios.

5.1 Scenario 1: Link Failure (10.0.65.0/24)

Condition: The direct link between R6 and R16 is **DOWN**. The Switch is **UP**.

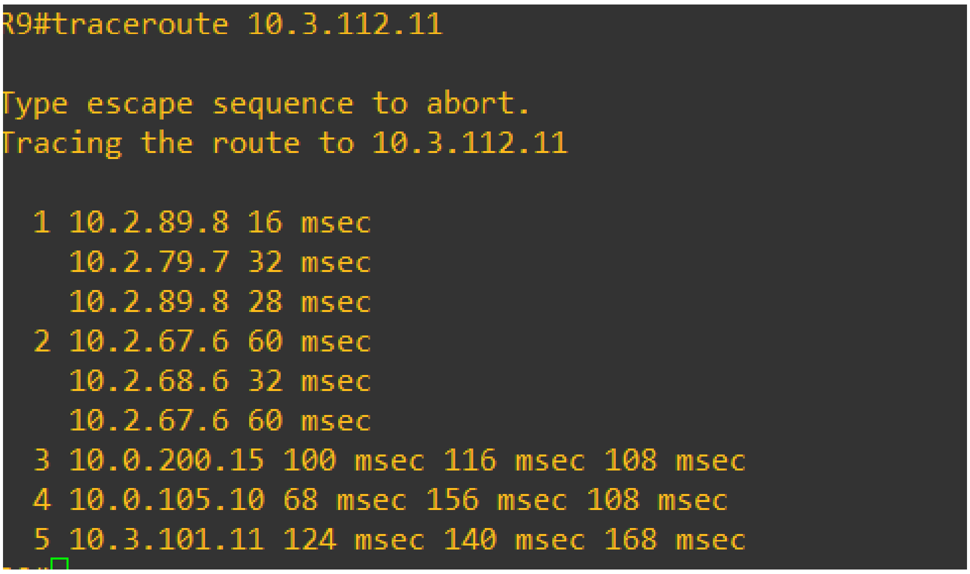


```
R10#traceroute 10.2.79.9

Type escape sequence to abort.
Tracing the route to 10.2.79.9

  1 10.0.105.15 20 msec 32 msec 24 msec
  2 10.0.200.6 64 msec 28 msec 32 msec
  3 10.2.67.7 64 msec 96 msec 108 msec
  4 10.2.79.9 140 msec 76 msec 132 msec
R10#
```

Figure 8: Trace from R10 to R9 (Link Failure)

Analysis: As seen in Figure 8, the traffic from R10 to R9 avoided the broken direct link. Instead, it utilized the backbone switch.

- **Hop 2:** `10.0.200.6` indicates that the packet reached R6 via the Ethernet segment (Switch1), successfully bypassing the severed point-to-point link.



```
R9#traceroute 10.3.112.11

Type escape sequence to abort.
Tracing the route to 10.3.112.11

  1 10.2.89.8 16 msec
    10.2.79.7 32 msec
    10.2.89.8 28 msec
  2 10.2.67.6 60 msec
    10.2.68.6 32 msec
    10.2.67.6 60 msec
  3 10.0.200.15 100 msec 116 msec 108 msec
  4 10.0.105.10 68 msec 156 msec 108 msec
  5 10.3.101.11 124 msec 140 msec 168 msec
```

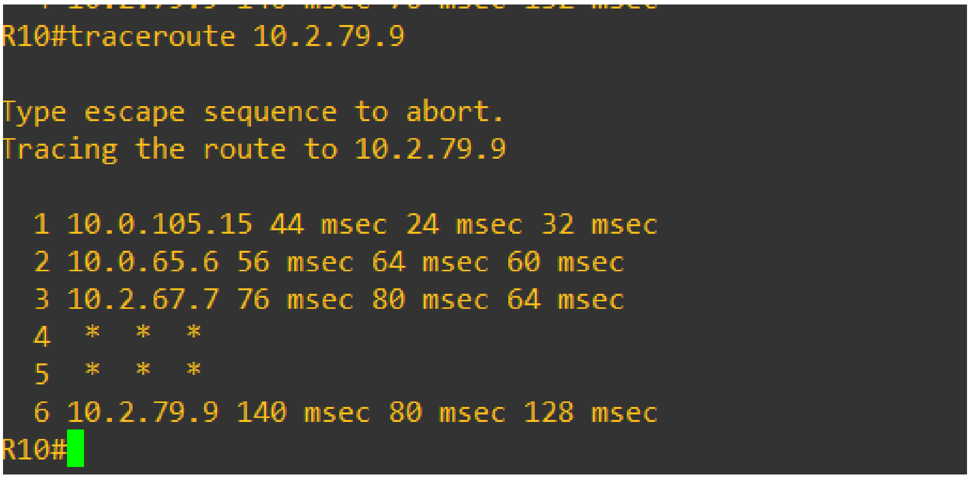
Figure 9: Trace from R9 to R11 (Link Failure)

Analysis: The return traffic from Area 2 (Figure 9) followed a symmetric logic.

- **Hop 3:** `10.0.200.15` confirms that R6 forwarded the traffic to R15 via the switch to reach the destination in Area 3.

5.2 Scenario 2: Switch Failure (Area 0)

Condition: The Switch is **DOWN**. The Link R6-R16 is **UP**.



```
R10#traceroute 10.2.79.9

Type escape sequence to abort.
Tracing the route to 10.2.79.9

  1 10.0.105.15 44 msec 24 msec 32 msec
  2 10.0.65.6 56 msec 64 msec 60 msec
  3 10.2.67.7 76 msec 80 msec 64 msec
  4  *  *  *
  5  *  *  *
  6 10.2.79.9 140 msec 80 msec 128 msec
R10#
```

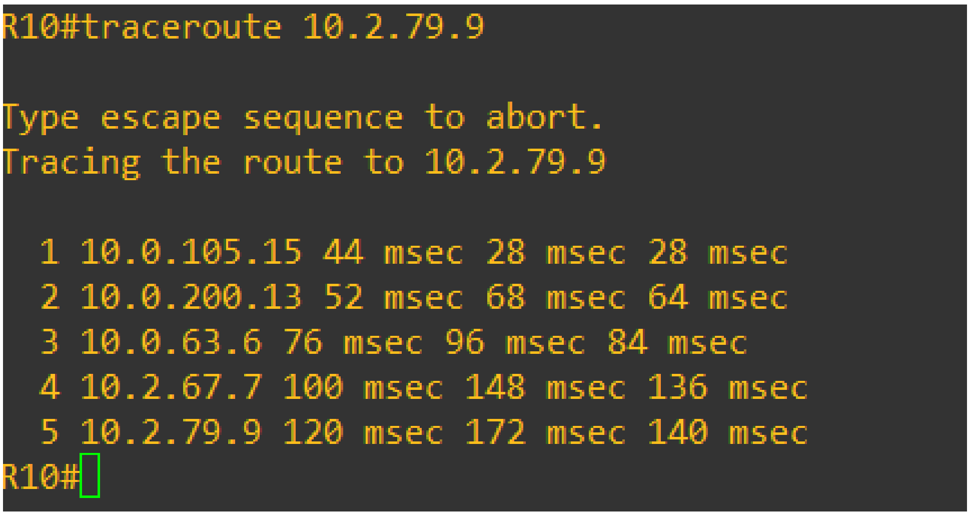
Figure 10: Trace from R10 to R9 (Switch Failure)

Analysis: With the broadcast domain unavailable, OSPF reverted to the point-to-point links.

- **Hop 2:** `10.0.65.6` confirms that traffic was forced to use the direct backbone link between R16 and R6. The `10.0.200.x` network was correctly avoided, proving the network survived the switch failure.

5.3 Scenario 3: Simultaneous Failure (Link + Switch)

Condition: The Link R6-R16 is **DOWN** and R6 is isolated from the Switch.



```
R10#traceroute 10.2.79.9

Type escape sequence to abort.
Tracing the route to 10.2.79.9

  1 10.0.105.15 44 msec 28 msec 28 msec
  2 10.0.200.13 52 msec 68 msec 64 msec
  3 10.0.63.6 76 msec 96 msec 84 msec
  4 10.2.67.7 100 msec 148 msec 136 msec
  5 10.2.79.9 120 msec 172 msec 140 msec
R10#
```

Figure 11: Trace from R10 to R9 (Dual Failure)

Analysis: This scenario represents the worst-case backbone failure.

- **Routing Logic:** Traffic could not use the direct link (R6-R16) or the direct switch path to R6.
- **Hop 2 & 3:** The trace shows traffic routing to R13 (`10.0.200.13`) and then entering R6 via the side link `10.0.63.6`.
- **Conclusion:** This confirms that the "Outer Ring" (via R13) successfully provided a backup path, maintaining connectivity to Area 2 despite the loss of its primary backbone connections.