Config Files

```
root@CN-R1:/home/student# cat /etc/frr/frr.conf
frr version 7.1
frr defaults traditional
hostname CN-R1
log syslog informational
service integrated-vtysh-config
!
interface eth1
 ip address 10.10.10.1/29
!
router ospf
 network 10.10.10.0/29 area 0
!
line vty
!
root@CN-R1:/home/student#
```

Figure 1: R1 Config

```
root@CN-R2:/home/student# cat /etc/frr/frr.conf
frr version 7.1
frr defaults traditional
hostname CN-R2
log syslog informational
service integrated-vtysh-config
!
ip route 0.0.0.0/0 10.10.10.1
!
interface eth0
 ip address 10.10.10.2/29
!
interface eth1
 ip address 10.10.11.1/30
!
interface eth2
 ip address 10.10.11.5/30
!
router ospf
 network 10.10.10.0/29 area 0
 network 10.10.11.0/30 area 1
 network 10.10.11.4/30 area 1
!
line vty
!
root@CN-R2:/home/student#
```

Figure 2: R2 Config

```
root@CN-R3:/home/student# cat /etc/frr/frr.conf
frr version 7.1
frr defaults traditional
hostname CN-R3
log syslog informational
service integrated-vtysh-config
!
ip route 0.0.0.0/0 10.10.10.1
!
interface eth0
 ip address 10.10.11.2/30
!
interface eth1
 ip address 10.10.11.9/30
!
router ospf
 network 10.10.11.0/30 area 1
 network 10.10.11.8/30 area 1
!
line vty
!
root@CN-R3:/home/student#
```

Figure 3: R3 Config

```
root@CN-R4:/home/student# cat /etc/frr/frr.config
cat: /etc/frr/frr.config: No such file or directory
root@CN-R4:/home/student# cat /etc/frr/frr.conf
frr version 7.1
frr defaults traditional
hostname CN-R4
log syslog informational
service integrated-vtysh-config
!
ip route 0.0.0.0/0 10.10.10.1
!
interface eth0
 ip address 10.10.11.10/30
!
interface eth1
 ip address 10.10.11.6/30
!
interface eth2
 ip address 10.10.11.17/28
!
router ospf
 passive-interface eth2
 network 10.10.11.4/30 area 1
 network 10.10.11.8/30 area 1
!
line vty
!
root@CN-R4:/home/student#
```

Figure 4: R4 Config

Ping Files

```
root@CN-R3:/home/student# ping 10.10.10.1
PING 10.10.10.1 (10.10.10.1) 56(84) bytes of data.
64 bytes from 10.10.10.1: icmp_seq=1 ttl=63 time=0.765 ms
64 bytes from 10.10.10.1: icmp_seq=2 ttl=63 time=0.821 ms
64 bytes from 10.10.10.1: icmp_seq=3 ttl=63 time=0.833 ms
64 bytes from 10.10.10.1: icmp_seq=4 ttl=63 time=1.03 ms
64 bytes from 10.10.10.1: icmp_seq=5 ttl=63 time=0.958 ms
64 bytes from 10.10.10.1: icmp_seq=6 ttl=63 time=1.11 ms
64 bytes from 10.10.10.1: icmp_seq=7 ttl=63 time=0.796 ms
64 bytes from 10.10.10.1: icmp_seq=8 ttl=63 time=0.758 ms
64 bytes from 10.10.10.1: icmp_seq=9 ttl=63 time=0.869 ms
64 bytes from 10.10.10.1: icmp_seq=10 ttl=63 time=0.812 ms
64 bytes from 10.10.10.1: icmp_seq=11 ttl=63 time=0.832 ms
64 bytes from 10.10.10.1: icmp_seq=12 ttl=63 time=0.800 ms
^C
--- 10.10.10.1 ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 218ms
rtt min/avg/max/mdev = 0.758/0.865/1.111/0.109 ms
root@CN-R3:/home/student#
```

Figure 5: Ping from R3 to R1

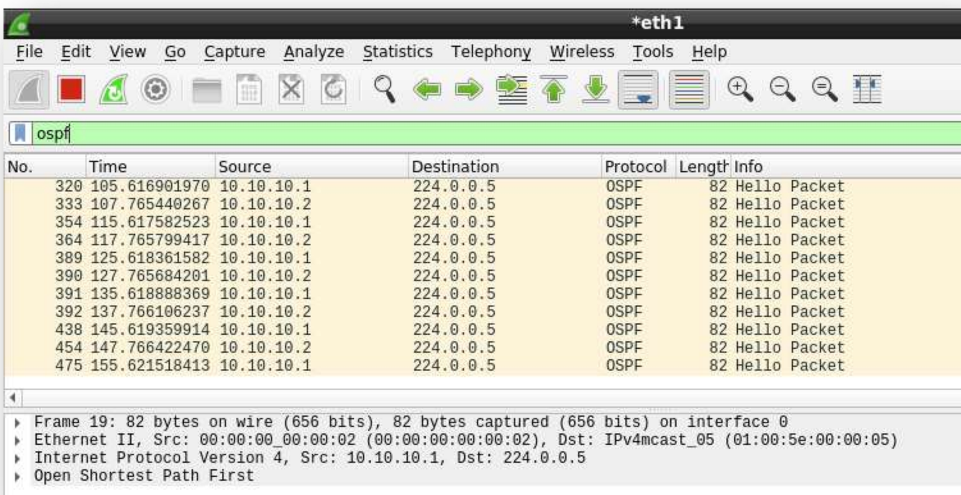

Figure 6: OSPF, Wireshark Traffic in R1

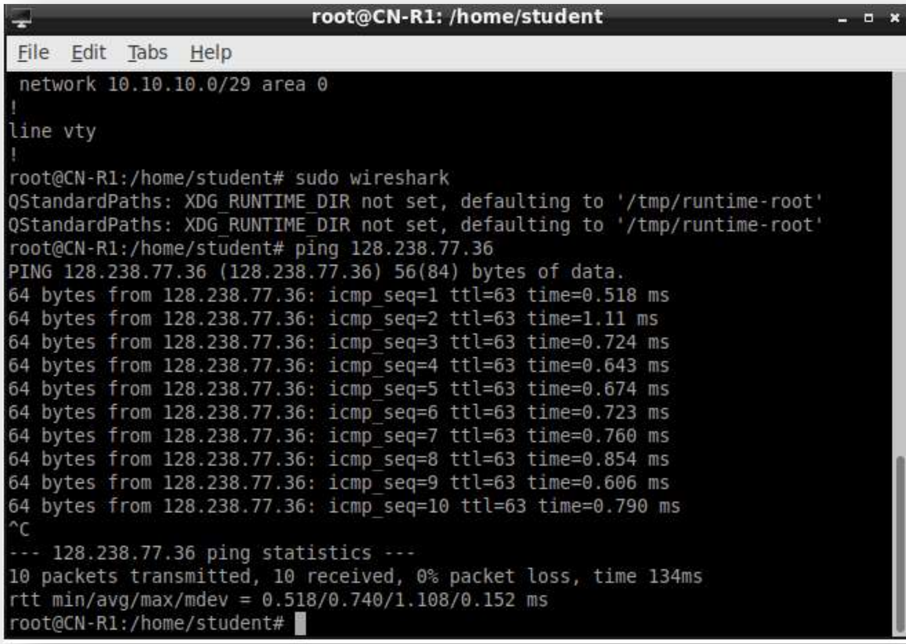

Figure 7: R1 ping to SFTP Server

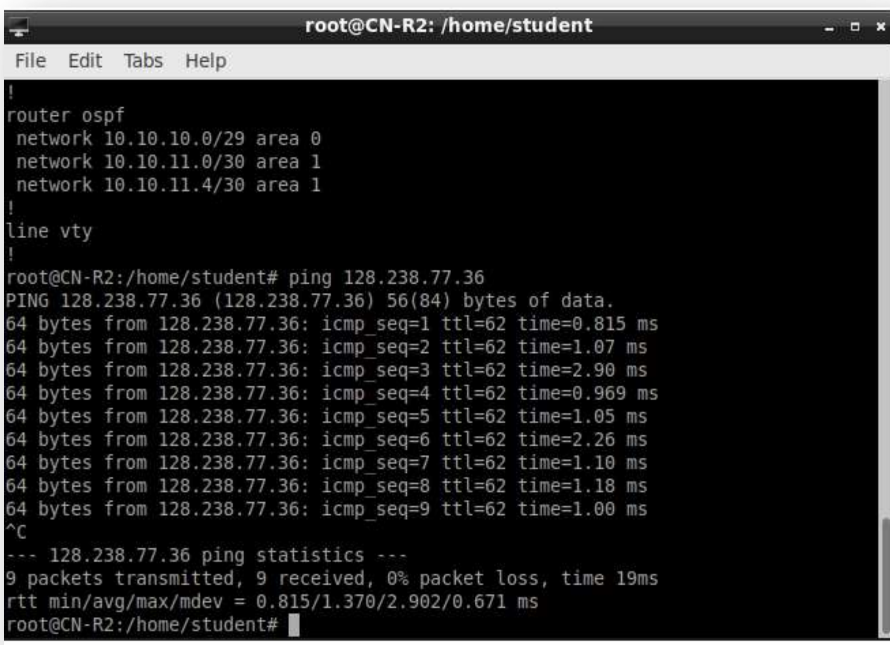

Figure 8: R2 ping to SFTP Server

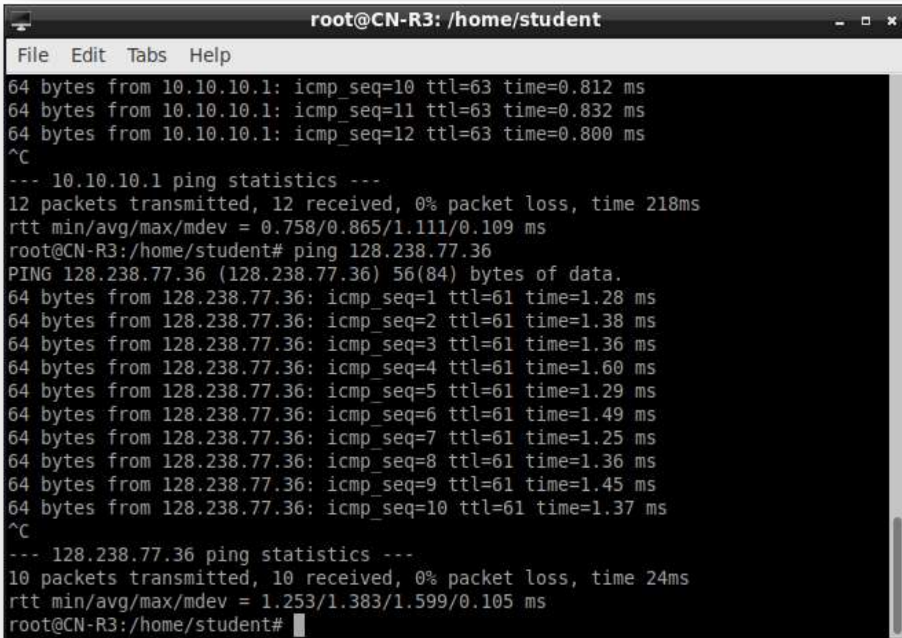

Figure 9: R3 ping to SFTP Server

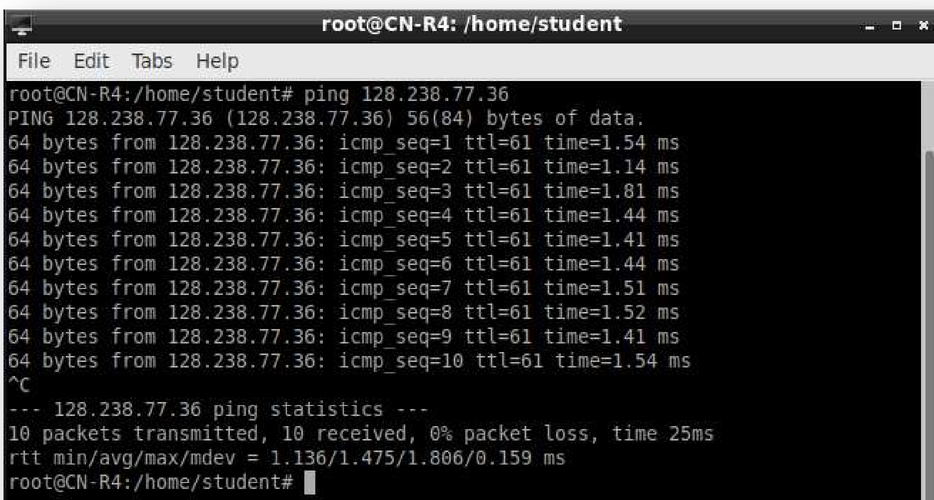

Figure 10: R4 ping to SFTP Server

Part 5: Configure OSPF in Area 1

a) **Power on all routers and run Wireshark on R1. Apply a filter for OSPF and look at the Hello Packets. How frequently are these packets sent, and why must they be sent periodically?**

Answer:

OSPF Hello packets are essential for neighbour discovery and maintenance. These packets are sent regularly on all OSPF-enabled interfaces. Most Ethernet ports have a 10-second delay by default, although network demands can change that.

OSPF Hello packets' primary goals:

1. Neighbour Discovery: When an OSPF router comes online, it sends Hello packets to neighbouring OSPF routers. Routers that receive this packet will add the sender to their neighbour database and exchange routing information.

2. Neighbour Reachability: OSPF routers must constantly check neighbour availability. Hello packets are a network keep-alive method that verifies neighbours' connectivity.

3. Topology Maintenance: Dynamic networks change constantly. OSPF uses Hello packets to identify network topology changes quickly like routers going down or coming online.

4. Parameter Accord: OSPF Hello packets carry important parameters like Hello and Dead intervals, area ID, authentication information, etc. These parameters must be agreed upon for two routers to be neighbours. Any mismatch can prohibit the neighbourhood.

5. DR/BDR Elections: OSPF reduces routing update overhead on broadcast and non-broadcast multi-access networks (NBMA) with DR and BDR elections. Hello packets contain DR/BDR election router priorities.

- OSPF Hello packet frequency balances network change detection and traffic reduction. A faster Hello interval detects changes faster but uses more bandwidth and computing resources. However, a slower Hello interval saves bandwidth and processing but slows network change detection.
- When a router receives no Hello packet from a neighbour within four times the Hello period (default 40 seconds on Ethernet), it deems the neighbour down. This causes the OSPF routing algorithm to recalculate routes, which may modify the routing table and reroute traffic.
- Thus, delivering Hello packets periodically helps OSPF maintain an accurate network topology and route traffic over the most effective channels. It lets OSPF provide a dependable, adaptive routing system that swiftly adapts to network changes to optimise data pathways and network performance.

b) **Continue running Wireshark and turn off R4. You should now see new OSPF packet types captured on R1. Explain why Hello, Link State Update and Link State Acknowledgements use the same Destination IP address.**

Answer:

OSPF (Open Shortest Path First), Hello, Link State Update (LSU), and Link State Acknowledgement (LSAck) all use a shared multicast IP address that is explicitly reserved for OSPF messages to transmit packets.

OSPF stands for "Open Shortest Path First." This multicast address is a well-known address that OSPF routers listen to for OSPF-specific communication. All OSPF routers listen to this address. The following is a list of the standard multicast addresses used by OSPF:

- All OSPF routers have the destination address 224.0.0.5 (multicast).

The following is an explanation of the technical nature behind why these OSPF packets utilise the same multicast IP address:

OSPF The distribution of "hello packets" has the dual goals of establishing new relationships with neighbours and maintaining existing ones. OSPF routers on the same network segment will transmit Hello packets to the multicast address labelled "All OSPF routers" to establish and maintain adjacency with other OSPF routers on the same network segment.

OSPF Link State Update (LSU) Packets are responsible for transporting information that has been updated regarding the state of specific links. To guarantee that each router can keep an accurate and up-to-date link-state database, it is necessary for a router to make sure that, whenever it delivers an LSU, it also distributes this information to all of the other routers that are located within an OSPF area. It is necessary to send the LSU packets to the multicast address designated for "All OSPF routers" so that all routers can simultaneously receive and process the updates.

OSPF Link State Acknowledgement (LSAck) Packets are utilised to verify the successful acquisition of LSUs. The dependability of the OSPF link-state database synchronisation mechanism is directly correlated to the integrity of these packets. LSAcks are also transmitted to the multicast address labelled "All OSPF routers" to acknowledge the receipt of LSUs delivered to the neighbouring routers.

OSPF routers can quickly distribute and acknowledge link-state information to all routers within an OSPF area or network segment by utilising a single multicast address. This eliminates the need for OSPF routers to send individual unicast messages to each router. This multicast technique is a core feature of OSPF's operation, ensuring that the protocol is both scalable and efficient in maintaining a synchronised view of the network's topology across all routers in an area. This is accomplished by ensuring that all routers in an area receive the same information about the network's topology. OSPF can swiftly react to changes in the network because of this design, which also helps it preserve accurate routing information for optimal path selection.

c) Based on the above steps, explain why we do not see DB Descriptions and LS Requests on R1. Is there a situation where we get all OSPF packet types on R1?
Answer:

Within the Open Shortest Path First (OSPF) protocol, distinct packet types fulfil functions in the process of establishing and maintaining neighbour connections, as well as synchronising the Link-State Database (LSDB).
Under typical conditions, it is possible that Database Description (DBD) and Link-State Request (LSR) packets may not be observable.

The utilisation of Database Description (DBD) Packets is observed during the initial establishment of the OSPF adjacency between two routers. After the routers have successfully formed a complete adjacency and achieved full synchronisation, the exchange of these packets occurs periodically, just in the event of a network topology alteration that necessitates re-synchronization.

The OSPF router sends Link-State Request (LSR) Packets when it determines, based on the exchange of Database Description (DBD) packets, that its Link-State Database (LSDB) has obsolete or incomplete information. The Link-State Router (LSR) requests the precise Link-State Advertisements (LSAs) that require updating.

Suppose the absence of DBD or LSR packets on R1 is observed. In that case, it is indicative that R1 and its neighbouring routers have successfully established complete adjacency and their Link State Databases (LSDBs) are fully synchronised. There is no requirement to exchange any new or modified Local Security Authorities (LSAs).

Nevertheless, there are instances in which one may observe the presence of all Open Shortest Path First (OSPF) packet types, such as Database Description (DBD) and Link State Request (LSR), on Router 1 (R1).

In the event of a router restart or OSPF process restarts, it would be necessary for R1 or its neighbouring routers to initiate the re-establishment of neighbour adjacencies and the synchronisation of their Link State Database (LSDB). This procedure would entail the exchange of Database Description (DBD) and Link State Request (LSR) packets.

In the event of a network topology change, such as the introduction of a new router or the temporary disruption and subsequent restoration of a link, it becomes necessary for the routers to re-establish synchronisation of their databases. This process entails the transmission and reception of Database Description (DBD) and Link State Request (LSR) packets.

Configuration Modification**:** Modifications in the configuration of OSPF, such as alterations in OSPF area boundaries or adjustments in the interface cost, may result in a transient requirement for Database Description (DBD) and Link State Request (LSR) packets while the routers re-establish their perception of the network topology.

In such scenarios, one would witness a series of OSPF messages being exchanged, encompassing Hellos to discover neighbours, DBDs for exchanging database descriptions, LSAs for announcing updates regarding the state of links, LSRs for requesting LSAs that are missing or outdated, and LSUs for updating the LSDB. Subsequently, LSAcks are sent to acknowledge the LSUs.