Table of Contents

Summary

A defined route is critical for devices to communicate in a network regardless of distance or any other means. Therefore, every device in the network should have an IP address that is unique, as this aids the host in maintaining its identity over the network, given that a route is one of the essential criteria for the devices to connect. Based on several factors, routes and their protocols are further divided into different categories, and each protocol has a unique set of benefits and drawbacks.

In the IPv4 lab exercise below, Juniper routers and host computers were assigned specified IP addresses. Then, network measurements and other metrics were tested by capturing packets using *tcpdump* and routing mechanisms using the RIP (Routing Information Protocol) and OSPF (Open Shortest Path First). The routing protocols were observed operating in practice when preferred routes were disabled.

Introduction and Background

Internet Protocol is a critical technology element that enables us to connect devices over the internet. Two versions of Internet Protocols, IPv4 and IPv6, are classified based on complexity and efficiency. The abbreviation for IPv4 is Internet Protocol version 4. IP addresses allow the network to identify the device and enable further connectivity and communication. In addition, whenever a device is connected to the internet, a unique IP address is assigned to the device. Due to this, each device has an individual and a separate identity over the internet. [1]

Similarly, several other crucial elements, such as routing, are also necessary for the devices to communicate effectively over the internet. The routing takes place on layer 3 and helps the networks to become more efficient to enhance device communication and connectivity.

Specific routing protocols are required to exchange routing and network information between routers and devices. For instance, the Interior gateway protocol enables the routers and the gateways to dynamically exchange routing tables and network information. The two prominent examples are RIP (Routing Information Protocol) and OSPF (Open Shortest Path First). [2]

Objective of Performing the Lab

The main objective of the IPv4 lab is to construct a test network utilizing Juniper routers (vMX) with Ubuntu 14.04.1 LTS running as the base operating system. IP addresses and loopback addresses have to be assigned to the router interfaces, which are restricted inside a specified address space.

The topology also included host computers connected to the Local area Networks of Helsinki and Oulu that would obtain their IP address through DHCP. Therefore, DHCP servers also had to be configured over Helsinki and Oulu.

Finally, after the entire environment is set up, the end goal is to verify the routing and network connectivity using a set of routing protocols (i.e.) using RIP (Routing Information Protocol) and OSPF (Open Shortest Path First). Later, to comprehend the results and compare them, network packets were captured using tcpdump.

This was required to thoroughly examine the network drops and connectivity and compare the latency and ping values across the networks using traditional methods and by using open-source software like Wireshark.

Description of Experimental Setup

Six Juniper routers (vMX) running over Ubuntu 14.04.1 LTS base operating system are the foundation of the complete configuration and environment. The Juniper routers are named after the six famous cities of Finland, (i.e.) Helsinki, Oulu, Vaasa, Tampere, Turku, and Lappeenranta.

Furthermore, there are two Local area networks connected to the routers, one in Oulu and the other one in Helsinki. Over the LAN in Helsinki, there are 13 host machines connected, and 4 host machines are connected to the LAN in Oulu. These host machines acquire the IP addresses from DHCP. The gateway is preconfigured over the network which is connected to Turku's interface. The network schematic can be seen in Figure 1.

The local area networks require sufficient address spaces for the number of host machines they contain. Thus, they were allocated address spaces the size of four bits for Helsinki and three bits for Oulu, 10.38.161.17/28 and 10.38.161.9/29, which provide addresses for 13 computers in Helsinki and a potential five computers in Oulu.

The rest of the interfaces were allocated one by one from 2-bit address spaces. The loopback interfaces were given single addresses from the remaining addresses from near the end of the allowed range.

Table 1: Address allocations

Interface	Helsinki	Turku	Tampere	Lappeenranta	Oulu	Vaasa
ge-0/0/1	10.38.161.5/30	10.38.161.6/30	10.38.161.33/30	10.38.161.50/30	10.38.161.46/30	10.38.161.42/30
ge-0/0/2	10.38.161.37/30	10.38.161.34/30	10.38.161.41/30	10.38.161.54/30	10.38.161.57/30	10.38.161.45/30
ge-0/0/3	10.38.161.49/30	-	10.38.161.53/30	10.38.161.58/30	-	-
ge-1/0/0	-	-	10.38.161.38/30	-	-	-
lo0	10.38.161.60/32	10.38.161.61/32	10.38.161.62/32	10.38.161.65/32	10.38.161.63/32	10.38.161.64/32
LAN	10.38.161.17/28	-	-	-	10.38.161.9/29	-
LAN PC	10.38.161.18	-	-	-	10.38.161.10	-
Gateway	-	10.38.161.1/30	-	-	-	-

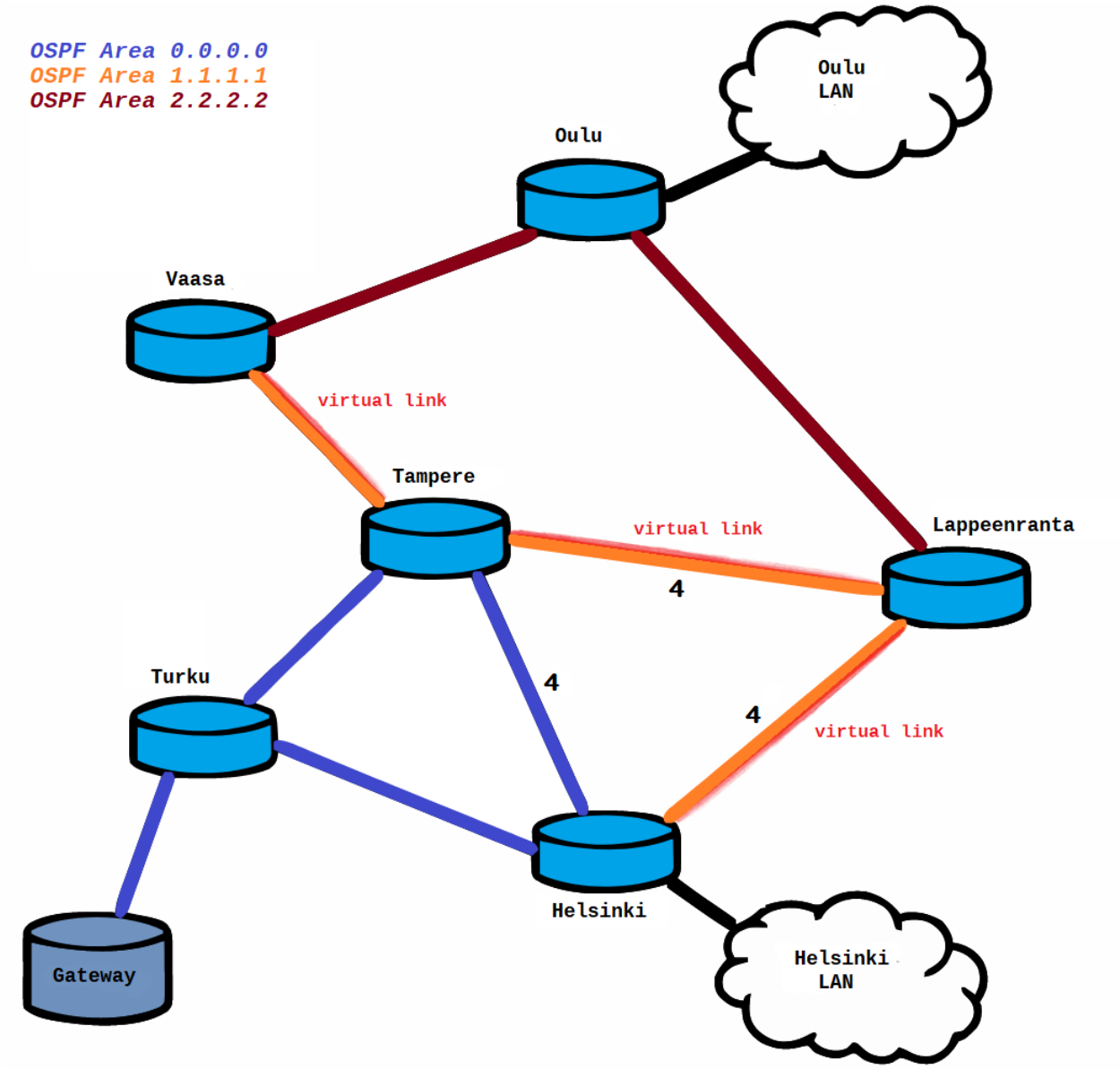

Figure 1: The network with OSPF areas, virtual links and specific link costs marked.

Procedure

1. The IP address allocations were planned before distributing the addresses. The addresses were set to the interfaces with the router's command line interface. The links were tested with ICMP echo requests. A DHCP server was configured to Helsinki and Oulu, while the default gateway was set to Turku. Setting a name server is useful so that the DHCP server can advertise it to the host machines. The connection from Helsinki to Turku was tested with an echo request to the loopback address of Turku, which was unsuccessful because no routing protocol had been applied yet. The loopback interface, not being in the same address space as the link, could not be reached without a routing protocol.

2. The routers were configured to use the routing protocol RIP, and Turku was set to advertise the default route. The network was tested by sending an echo request from the Helsinki LAN to the Oulu LAN. Then, the corresponding route was checked with the Traceroute tool. The configuration files from Turku and Lappeenranta can be seen in Appendix A and B.

3. Packet capture was started in Helsinki for the interfaces facing Tampere and Lappeenranta before starting continuous echo requests from the local area network to the loopback interface in Oulu. The interface facing Oulu was disabled in Lappeenranta to study the rerouting process, and the duration was measured. After the new route was established and the connection restored, the packet capture files were saved. While the echo requests were ongoing, a new packet capture was started, and the disabled link was re-enabled. The time for the network to revert to the previous route was recorded, after which the packet capture and echo requests were ended

4. RIP routing was disabled to configure each router with the OSPF routing protocol. The links between Helsinki and Tampere, Tampere and Lappeenranta, and Helsinki and Lappeenranta were set at a link cost of four instead of the default value of one. In addition, virtual links were set up between Tampere and Vaasa, Tampere and Lappeenranta, and Helsinki and Lappeenranta. This was done to connect Area 2.2.2.2 to the backbone area. The configuration files from Turku and Lappeenranta in this phase can be seen in Appendix C and D.

5. The Traceroute tool was used to check the path from the Helsinki LAN to the Oulu LAN. Packet capture was started between Helsinki and Turku and between Helsinki and Lappeenranta, along with continuous echo requests from the Helsinki LAN to the loopback interface of Oulu. First, the Tampere-facing interface was disabled in Vaasa, and the time measured before the echo requests reached Oulu again. The interface was then enabled to record the time before the previous route was used again. After that, both interfaces in Vaasa were disabled to measure how long it takes for the alternative route to be used again. The interfaces in Vaasa were then enabled again.

6. The Oulu-facing interface in Lappeenranta was configured with the password "comnet." First, the route from the Oulu LAN to the Helsinki-facing interface of Lappeenranta was traced, and the OSPF neighbor information was studied. Then the interfaces in Oulu leading to Vaasa and Lappeenranta were configured with the same password along with the Oulu-facing interface in Vaasa.

7. In previous phases the network was set up to use either RIP or OSPF routing protocol. For the usage of both simultaneously Tampere and Lappeenranta were configured to use both protocols. The configuration file from Lappeenranta can be found in Appendix E. Vaasa and Oulu were configured to use only RIP while Helsinki and Turku were set up to use only OSPF. Link costs of OSPF remained unchanged. The network was tested with echo requests from the Helsinki LAN to the Oulu LAN. Continuous echo requests were sent from the Helsinki LAN to the loopback interface of Oulu and packet traffic was captured from Oulu's interfaces leading to Vaasa and Lappeenranta. The Oulu-facing interface in Lappeenranta was disabled to measure how long finding an alternative route takes. The interface was then re-enabled and time for the previous route to be restored measured.

Data

The data includes rerouting times measured during the experiment and gathered later from the captured packet data. Rediscovery times of routes after interfaces have been re-enabled are not present in the packet data as the interface’s enabling time is unknown.

Table 2: Routing time data

Event	Protocol	Duration from packet data	Measured duration
Rerouting after the Oulu facing interface is disabled in Lappeenranta.	RIP	4m 57s	4m 54s
Rediscovering the shortest route after the interface is enabled again.	RIP	N/A	33s

Rerouting after the Tampere facing interface in Vaasa is disabled.	OSPF	41s	44s
Rediscovering the preferred route after the Vaasa interface is enabled again.	OSPF	N/A	14s
Rerouting after both interfaces is disabled in Vaasa.	OSPF	41s	43s
Rerouting after the Oulu facing interface in Lappeenranta is disabled.	OSPF and RIP	5m 33s	5m 40s
Rediscovering the preferred route after the interface is enabled again.	OSPF and RIP	N/A	2s

Analysis of Data

The packet capture data shows that RIP sends Request and Response messages for requesting and distributing routing information. OSPF sends Hello Packets, LS Updates, and LS Acknowledgements which it uses to communicate with neighboring nodes and to convey information about link states.

The nodes send Hello Packets periodically to keep track of their neighbors.[3] After a link is broken, RIP sends multiple Response messages between nodes to establish the new routing information. When a link is broken in OSPF, multiple Hello Packets are broadcasted before LS Updates, and LS Acknowledgements are sent.

When using RIP, the route from the Helsinki LAN to the Oulu LAN went from Helsinki to Lappeenranta to Oulu as that was the route with the least intermediate nodes, or hops. In OSPF the route went from Helsinki to Turku, Tampere, Vaasa and Oulu avoiding the links with high costs. It was the route with the lowest link costs.

When the interface in Lappeenranta was disabled, RIP found the second shortest route from Helsinki to Oulu via Tampere and Vaasa.

Configuring the Oulu-facing interface in Lappeenranta with an authentication password made Oulu unable to reach that interface. However, when the rest of the interfaces in area 2.2.2.2 were configured with the same password, communication was successful again.

Routing loops are possible when a link or node goes down. One node may be unaware of a broken route while another is aware and routes the data back the other way. There are techniques in RIP that ensure that the loop does not persist infinitely.[4]

A misconfigured OSPF network may develop routing loops. If there is no backbone area some areas may learn conflicting routing information from different sources and loops may form, or if connection to the backbone is lost and an area is unable to learn new routing information.

Conclusions

Routing protocols are necessary for the devices to communicate with one another in the topology and network. In order to test and examine the routing phenomena and their corresponding protocols, the entire lab was set up. Two major routing protocols (i.e.) RIP (Routing Information Protocol) and OSPF (Open Shortest Path First), were taken into consideration. The communication was established only after the first protocol (RIP) was enabled between the routers and the host machines.

The routing protocols were seen to function by their specified working principles. For example, RIP works on the principle of hop count matrix, and the communication is established only with the following potential hop in the topology. Comparatively, the OSPF protocol is much faster than the RIP protocol. The OSPF protocol, in contrast, operates according to the link state routing principle and has the ability to identify the optimal routes between the source and the destination. Therefore, OSPF is frequently utilized in complex network architecture and has several benefits.

Therefore, during the analysis, out of the two protocols, RIP appears to be significantly slower at discovering an alternative route after a link is broken, while OSPF was several minutes faster at the task. When using both protocols in the network, alternative route discovery was slow but returning to the previous route was very fast.

References

[1] Jadhav, S. Routing protocols, Scaler Topics. 2022.

[2] Sarao, Dr & Sindhu, P. & Navakishor, V. Analysis of Routing Protocols based on Network parameters in WANET. International Journal of Computer Sciences and Engineering. 2018.

[3] J. Moy. RFC 2328 OSPF Version 2. 1998.

[4] https://study-ccnp.com/rip-loop-prevention/. Cited 1.11.2022.

Appendices

Appendix A, configuration file from the Turku router when the network used RIP:

```
interfaces {
      ge-0/0/23 {
      unit 0 {
            description ->Helsinki;
            family inet {
                  address 10.38.161.6/30;
            }
      }
      }
      ge-0/0/24 {
      unit 0 {
            description ->Tampere;
            family inet {
                  address 10.38.161.34/30;
            }
      }
      }
      ge-0/0/25 {
      unit 0 {
            description ->GW;
            family inet {
                  address 10.38.161.1/30;
            }
      }
      }
      lo0 {
      unit 1 {
            family inet {
                  address 10.38.161.61/32;
            }
      }
      }
}
protocols {
      rip {
      group Turku {
            export P2;
            neighbor ge-0/0/23.0;
            neighbor ge-0/0/24.0;
            neighbor ge-0/0/25.0;
      }
      }
}
policy-options {
      policy-statement P2 {
      from protocol [ direct rip ];
      then accept;
      }
}
```

Appendix B, configuration file from the Lappeenranta router when the network used RIP:

```
interfaces {
      ge-0/0/14 {
      unit 0 {
            description ->Oulu;
            family inet {
                  address 10.38.161.58/30;
            }
```

```
        }
        }
        ge-0/0/15 {
        unit 0 {
              description ->Tampere;
              family inet {
                    address 10.38.161.54/30;
              }
        }
        }
        ge-0/0/16 {
        unit 0 {
              description ->Helsinki;
              family inet {
                    address 10.38.161.50/30;
              }
        }
        }
        lo0 {
        unit 5 {
              family inet {
                    address 10.38.161.65/32;
              }
        }
        }
}
protocols {
        rip {
        group lappeenranta {
              export P3;
              neighbor ge-0/0/14.0;
              neighbor ge-0/0/15.0;
              neighbor ge-0/0/16.0;
        }
        }
}
policy-options {
        policy-statement P3 {
        from protocol [ direct rip ];
        then accept;
        }
}
```

Appendix C, configuration file from the Turku router when the network used OSPF:

```
interfaces {
        ge-0/0/23 {
        unit 0 {
              description ->Helsinki;
              family inet {
                    address 10.38.161.6/30;
              }
        }
        }
        ge-0/0/24 {
        unit 0 {
              description ->Tampere;
              family inet {
                    address 10.38.161.34/30;
              }
        }
        }
```

```
      ge-0/0/25 {
      unit 0 {
            description ->GW;
            family inet {
                  address 10.38.161.1/30;
            }
      }
      }
      lo0 {
      unit 1 {
            family inet {
                  address 10.38.161.61/32;
            }
      }
      }
}
protocols {
      ospf {
      export pol1;
      area 0.0.0.0 {
            interface ge-0/0/23.0;
            interface ge-0/0/24.0;
      }
      }
      inactive: rip {
      group Turku {
            export P2;
            neighbor ge-0/0/23.0;
            neighbor ge-0/0/24.0;
            neighbor ge-0/0/25.0;
      }
      }
}
policy-options {
      policy-statement P2 {
      from protocol [ direct rip ];
      then accept;
      }
      policy-statement pol1 {
      from protocol [ direct ospf ];
      then accept;
      }
}
```

Appendix D, configuration file from the Lappeenranta router when the network used OSPF:

```
interfaces {
      ge-0/0/14 {
      unit 0 {
            description ->Oulu;
            family inet {
                  address 10.38.161.58/30;
            }
      }
      }
      ge-0/0/15 {
      unit 0 {
            description ->Tampere;
            family inet {
                  address 10.38.161.54/30;
            }
      }
```

```
        }
        ge-0/0/16 {
        unit 0 {
              description ->Helsinki;
              family inet {
                    address 10.38.161.50/30;
              }
        }
        }
        lo0 {
        unit 5 {
              family inet {
                    address 10.38.161.65/32;
              }
        }
        }
}
protocols {
        ospf {
        export pol4;
        area 2.2.2.2 {
              interface ge-0/0/14.0;
        }
        area 1.1.1.1 {
              interface ge-0/0/15.0 {
                    metric 4;
              }
              interface ge-0/0/16.0 {
                    metric 4;
              }
        }
        area 0.0.0.0 {
              virtual-link neighbor-id 10.38.161.60 transit-area 1.1.1.1;
              virtual-link neighbor-id 10.38.161.62 transit-area 1.1.1.1;
        }
        }
        inactive: rip {
        group lappeenranta {
              export P3;
              neighbor ge-0/0/14.0;
              neighbor ge-0/0/15.0;
              neighbor ge-0/0/16.0;
        }
        }
}
policy-options {
        policy-statement P3 {
        from protocol [ direct rip ];
        then accept;
        }
        policy-statement pol4 {
        from protocol [ direct ospf ];
        then accept;
        }
}
```

Appendix E, configuration file from the Lappeenranta router when both OSPF and RIP were used:

```
interfaces {
      ge-0/0/14 {
      unit 0 {
            description ->Oulu;
            family inet {
                  address 10.38.161.58/30;
            }
      }
      }
      ge-0/0/15 {
      unit 0 {
            description ->Tampere;
            family inet {
                  address 10.38.161.54/30;
            }
      }
      }
      ge-0/0/16 {
      unit 0 {
            description ->Helsinki;
            family inet {
                  address 10.38.161.50/30;
            }
      }
      }
      lo0 {
      unit 5 {
            family inet {
                  address 10.38.161.65/32;
            }
      }
      }
}
protocols {
      ospf {
      export pol4;
      area 2.2.2.2 {
            interface ge-0/0/14.0 {
                  authentication {
                  md5 1 key "$9$Qc6sn6AleWNdsreLN-Voa"; ## SECRET-DATA
                  }
            }
      }
      area 1.1.1.1 {
            interface ge-0/0/15.0 {
                  metric 4;
            }
            interface ge-0/0/16.0 {
                  metric 4;
            }
      }
      area 0.0.0.0 {
            virtual-link neighbor-id 10.38.161.60 transit-area 1.1.1.1;
            virtual-link neighbor-id 10.38.161.62 transit-area 1.1.1.1;
      }
      }
      rip {
      group lappeenranta {
            export P3;
            neighbor ge-0/0/14.0;
            neighbor ge-0/0/15.0;
            neighbor ge-0/0/16.0;
```

```
        }
        }
}
policy-options {
        policy-statement P3 {
        from protocol [ direct rip ];
        then accept;
        }
        policy-statement pol4 {
        from protocol [ direct ospf ];
        then accept;
        }
}
```