

## TTM4240 - Semester Assignment 2: IPv6 Addressing, Routing, Tunneling And MPLS

---

### Learning objectives:

- Learn how to make an IPv6 plan for a network.
- Understand basic router (FRR and VyOS) and host configuration.
- Understand routing with OSPF and BGP.
- Use packet capture to see how a protocol like OSPF works.
- Write Access Control Lists to control traffic.
- Set up an IPv6-over-IPv4 tunnel.
- Configure MPLS in the network.
- Explain the reasoning behind your choices, and describe some strengths and weaknesses of routing protocols.

Due date: 12.10.2026

---

For this lab assignment, you will need to use a local GNS3-client to interact with a GNS3-server, running on a VM accessed through OpenVPN. Instruction on how to connect to the server are provided in a wiki which can be found here: <https://pages.git.ntnu.no/ie-iik/ttm4240-web/latest/wiki/Setup/>. We will update the wiki based on your feedback and questions on a regular basis. You will be working in the GNS3 virtual environment. FRR, VyOS and switch images are provided.

---

### Guidelines:

- You are advised to start as early as possible with the assignment tasks and use the tuition hours to ask about unclear or ambiguous parts in this assignment. We advise you to read the whole task first before starting to work on it.
  - Ensure the work done gets preserved. You can work with a router's configuration in two ways:
    - ensure selected router is stopped, open its configuration file via context menu ("Edit config"), edit and save it
    - or start selected router and introduce changes via its console. Do not forget to make your changes permanent: execute **write** command in the terminal, or your changes are going to be lost after the router's restart
  - List of the useful FRR and VyOS commands that you might want to use can be found in NTNU Wiki: <https://pages.git.ntnu.no/ie-iik/ttm4240-web/latest/wiki/>. Other relevant FRR commands can be found in: <https://docs.frrouting.org/en/latest/basic.html>. Other relevant VyOS commands can be found in: <https://docs.vyos.io/en/rolling/cli.html>.
  - You should deliver an export of your completed project as part of the report. Be patient when exporting the project file from GNS3 and uploading it to Canvas. Don't interrupt it while it's uploading to Canvas. It takes some time, but tends to work out in the end.
  - Note that all VMs are restarted at 04:00 each night. Make sure to save your files before that time.
  - When using packet-capture to inspect traffic, remember to stop the capture when you've gathered enough information.
-

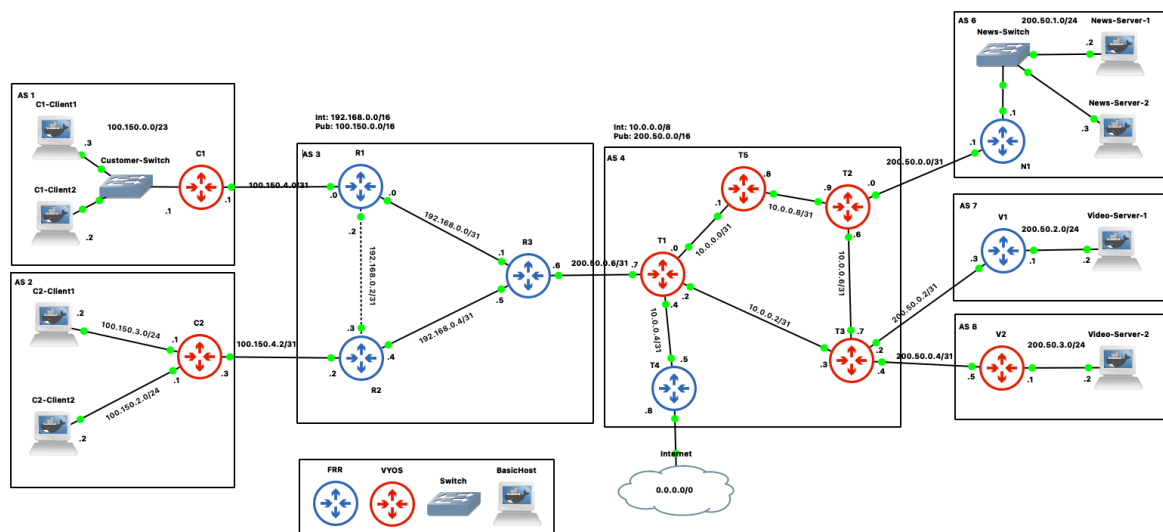


Figure 1: Topology for Assignment 2.

## Task 1 Advertisement and Packet Capture

### Task 1.1 Advertisement

Ensure Loopbacks and both the ISP's internal link-addresses are not advertised outside of their respective AS. Show updated routing tables (C1 and N1) to verify that the private addresses are hidden.

### Task 1.2 Packet Capture

Capture packet exchange on any chosen link within OSPF domain to illustrate how the protocol works. Can you identify the OSPF states? Why? Remember to close your packet capture when done.

Note: You can reset the OSPF states with `clear ospf...` commands.

### Task 1.3 Access Control List

The Tier1-ISP has experienced attempts of attacks from the regional-ISP against their internal network. They're not sure how the actors are reaching their internal network as they were sure that the routes to their internal network weren't distributed. As an extra precaution, they want to implement Access Control Lists to ensure that actors coming from the internet cannot send packets toward their internal subnets or loopback addresses. You only have to block traffic that would originate from the regional-ISP or their customers.

For the report, try to traceroute from one of the customer networks toward one of Tier1-ISP's internal addresses and then show that your ACL blocks the traffic when implemented. Include a print of the access control list(s) you've made and where you've implemented it/them. Why was the traceroute seemingly routed correctly before being blocked?

## IPv6

The Tier1-ISP acquires a new business-customer, Customer B, connecting to T4. The new business customer is very forward thinking and therefore only uses IPv6. Customer B really wants to gain access to the Video Service 2 and is willing to lend IP-addresses from their IPv6 subnet to accommodate that they gain access to the service.

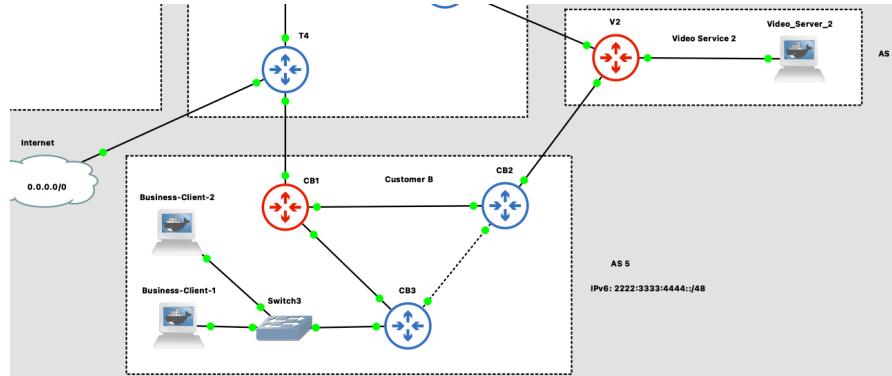


Figure 2: Updated Topology with Customer B.

## Task 2 Update Topology

Customer B owns a single overall range of IPv6 addresses 2222:3333:4444::0/48, where they allocate some of their subnets to:

- Subnet 2222:3333:4444:5000::0/52 for their client networks (CB3 to hosts)
- Subnet 2222:3333:4444:6000::0/52 for their internal network (Between CB1, CB2 and CB3)
- Subnet 2222:3333:4444:a000::0/52 for external networks
- Subnet 2222:3333:4444:f000::0/52 for loopback addresses and tunnels

They provide the subnet 2222:3333:4444:abcd/64 for Video Service 2's public address uses.

Add Customer B to the topology according to figure 2 and update IP addressing plan from IPv4 Routing, giving the IPv6 addresses to Customer B (AS 5) and Video Service 2 (AS 8). Video Service 2's units must function in dual-stack IPv4 and IPv6. Customer B also receives an IPv4 address from Tier1-ISP to connect to T4. Allocate 1 client-network for Customer B allowing for multiple clients to be connected in the network.

Apply your IP-plan in GNS3 and verify that there is IPv6 connectivity between the routers.

For the report, include a screenshot of your topology in GNS3 visualizing your IP-plan and screenshots of pings between V2 and CB2.

*GNS3 Configuration:* The FRR router images in GNS3 do not forward IPv6 or run OSPFv3 by default. To activate these functionalities, see wiki <https://pages.git.ntnu.no/ie-iik/ttm4240-web/latest/>.

## Task 3 IPv6 routing

Customer B **really** needs access to Video Service 2 which is why they have built up a network to give redundant routes towards Video Service 2. Configure routing, ensuring that routes to the internal network, the video service and the clients are available on routers that are configured with IPv6:

- Configure OSPF within the IPv6 domain of Customer B, ensuring that the GE-links are preferred over the FE-link. For the report, include a traceroute from one of the Customer B clients to CB2.
- Configure BGP to ensure that a route to Video Service 2 is known within Customer B's domain. Verify by pinging from one of Customer B's clients to Video Server 2.

## Task 4 Apply Tunneling

Configure an IPv6-over-IPv4 tunnel, to connect CB1 to V2. The tunnel should accommodate access to Video Server 2. Tier1-ISP's connection to Video Service 2 is better than Customer B's direct connection and this route should therefore be prioritized by Customer B and Video Service 2.

- Create and configure tunnel.
- Configure BGP over the tunnel.
- Configure BGP preference for the tunnel.

**Hint:** The IPv6 address of a tunnel should be chosen from an IP subnet you haven't been using in the rest of the project. What do the AS-paths look like to Video Service 2 from CB1 and CB2?

Verify that the preferred link works by showing a traceroute from a Customer B client to Video Service 2.

## Task 5 MPLS

The Tier1-ISP has added a new router, **T5**, on the internal link between T1 and T2. T5 has no customers and no external peers; its only job is to move traffic across the core. Every time the ISP gains a customer, however, T5 learns that customer's prefixes along with every other router in AS 4. T5 is handed to you fully configured.

### Task 5.1 Measure the Baseline

T5 is a member of the iBGP mesh of AS 4. Verify that traffic from a C1 client reaches the news service (200.50.1.0/24) and that the path crosses T5.

Record how many external prefixes T5 carries and how many iBGP sessions it maintains before you continue. These cannot be recovered once BGP has been removed.

- (a) Write down what you expect to happen to the traffic once T5 no longer runs BGP, and why.

### Task 5.2 Remove BGP from T5

Remove BGP from T5, and remove the T5 neighbour from T1, T2, T3 and T4. Delete the configuration. Do not shut down T5 and do not disable its OSPF. If T5 leaves the OSPF topology the traffic reroutes via T3 and keeps working.

Show where the traffic stops: from the client, and on T5 itself.

- (a) T5 still has an OSPF route to T2's loopback. Why does that not save the packet? Be precise about which address the forwarding decision is made on.
- (b) Why does OSPF not route around T5, given that a path through T3 exists?
- (c) The traceroute stops after T1 and shows no address for the router that dropped the packet, even though that router is up and its OSPF adjacencies are established. Explain why you see no reply at all.

### Task 5.3 Apply MPLS

Configure MPLS forwarding and LDP on the links **T1–T5** and **T5–T2** so that the traffic flows again, without giving T5 any BGP routes. T3 and T4 are not part of the MPLS path.

Two commands are required per interface: one enables MPLS forwarding in the data plane, the other starts LDP signalling. Configuring only the second brings the session up while the packets are still dropped.

**Do not remove OSPF:** LDP binds labels to FECs it learns from the IGP.

The egress router must advertise an **explicit null** label rather than an implicit one, or T5 will remove the label and you will not observe a swap. *Hint:* this is an LDP export policy, not an interface or discovery setting.

Show that T1, T5 and T2 each perform a **different** label operation, and which one each performs. Capture the frame on the links T1–T5, T5–T2 and T2–N1, and show how the label changes along the way.

Finally, measure the same two numbers as in Task 1.5.1 again.

- (a) Which router decided that the label should be removed?

- (b) Both T5 and T2 perform label operations. Why is only T5 unable to route to the destination on its own?
- (c) Here the egress router removes the label; most production networks let the penultimate router do it. What does that save, and what would it have cost here?
- (d) What does T5's forwarding state grow with as the ISP gains customers before MPLS, and after?
- (e) What does the ISP gain by introducing MPLS in its network?