

TTM4250 - Semester Assignment 2: MPLS VPNs

Learning Objectives

- Understand how MPLS L3 VPN works and configure one in practice
- Learn about MP-BGP (Multi-Protocol Border Gateway Protocol) by applying address family features in BGP to enable VPN
- Learn about VLANs and their association to sub-interfaces in routers
- Learn about VRFs (Virtual Routing and Forwarding) and realize multiple routing tables in a router

Guidelines

Start by downloading the template MPLS-lab GNS3 project and import it into your GNS3 instance in your lab VM. Note that lab deliverables must include an export of your finalized MPLS GNS3 project. When creating an export, keep it compact by not including base image or snapshots.

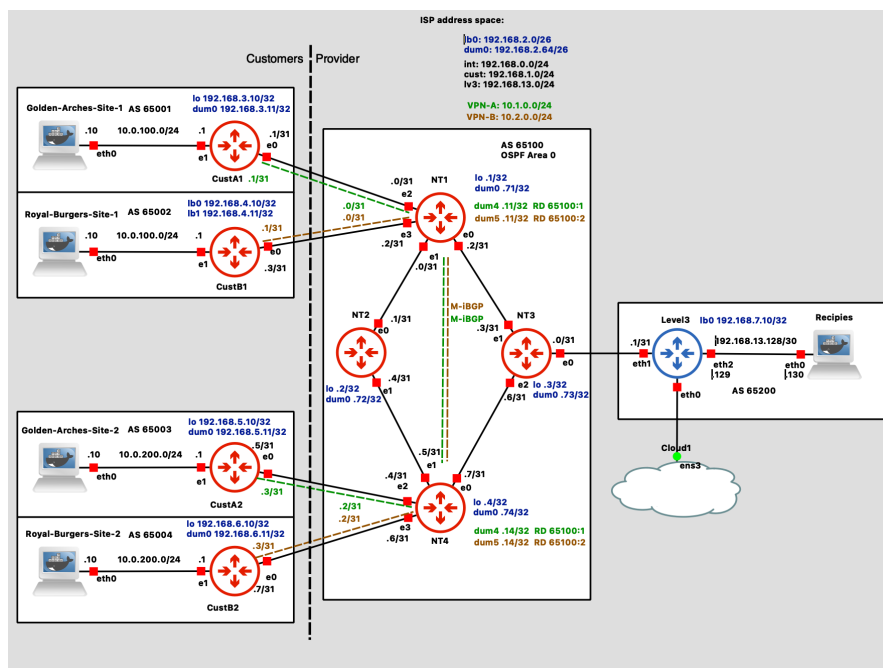


Figure 1: Target MPLS network

Introduction

Golden Arches and Royal Burgers each have two restaurants that are both being served by the ISP NextTel (NT). Business is running smoothly, with all restaurants having access to their precious recipes, stored on a cloud server. Both businesses have found that they need to start communicating between

their restaurants/sites. As their LANs are behind each their NAT, they do not have reachability to the other sites' hosts. A VPN is required to supply the businesses with their required access needs.

Anna is working as a network engineer at NextTel, but is unsure how to set up a provider-based VPN for her customers. In this lab, you will help Anna establish an MPLS-based L3VPN, leading to most of the configuration taking place on the provider network.

Task 2.1 Configuration and implementation of VRFs

First, you are required to lay the ground work for implementing the VPN. This is achieved by, first of all, creating and connecting VLANs in respective routers to isolate a VPN connection from the existing NAT-interface. You will also need to create VRFs to isolate the VPN from the global network.

- a) First we need to investigate the connectivity that is already implemented in the template provided. You are required to investigate and subsequently document the connectivity currently implemented in the template provided. How are the restaurants accessing the recipes? [Hint: You can do that by checking the router configurations and looking at wireshark-traces while pinging/tracerouting to the recipes server].
- b) The first step towards running a VPN is to add logical interfaces for the VPN to run over. In the provided configuration, the existing CE interfaces are used for NAT. To keep the VPN traffic separate from the NATed path, create a separate 802.1Q subinterface for the VPN. Identify which routers need to be configured and connected together and document your choice in the report. Assign the CE/PE/P roles to the different routers (ignore Level3) so that you have a clear picture of how to configure the VPN.

Once you have a plan of where to enable dot1q encapsulation, implement it in the router configurations. You are free to choose any valid VLAN you want. Include the commands used in your report. Also include wireshark-traces where you show the dot1q encapsulation in effect.

- c) In the next step you need to create VRFs (virtual routing and forwarding) named "VPN-A" and "VPN-B" in all the concerned routers, where VPN-A connects CustA1 to CustA2 and VPN-B connects CustB1 to CustB2. The VRFs will isolate functionality on the routers from the global view by utilizing separate **tables**. The VRFs might also need to be assigned to some interfaces, for instance your newly established sub-interfaces.

Task 2.2 Implementation of BGP and MPLS

Building upon the foundation laid in Task 2.1, you are required in this task to configure BGP on all the concerned routers. Subsequently, you will need to implement MPLS in the backbone network and test for its functioning.

- a) Now, new eBGP sessions need to be configured on the edges. Identify the routers that need to be configured and add IPv4 address family for the new eBGP-sessions. Make sure that the eBGP session is set up in the correct VRF on relevant routers. Also, ensure that the private user networks are distributed via BGP to the correct peers. Verify and document that PEs now learn routes to the target, but that they are not available in the global routing table [Hint: use "**show ip route vrf X**" to view VRF routing tables].
- b) To properly distinguish the routes of a VPN, route-distinguishers (RDs) and route targets (RT) must be applied. The RDs to be used is given in Figure 1. Select two distinct RT values for each of the two VPNs. Document all the steps you have taken in your report.

- c) The backbone network is now ready for implementing MPLS. Identify all the routers and their interfaces that need to be enabled for MPLS, and enable them. Test and document that MPLS is operational. [Hint: You may look for LDP in Wireshark traces. Also the LIB (LDP tables) and LFIB (Label forwarding table) should be appropriately populated.]

Task 2.3 Implementation of VPNs

After having BGP and MPLS running, you now need to enable VPN connectivity between target private networks.

- a) In this task, you need to enable VPN route transport between the edge routers. Identify which routers need to be configured for which VPN and apply the configurations. Ensure that you configure the correct VPNv4 address family and that the relevant neighboring relationships are specified.
- b) Now that the configurations are in place, you need to verify that the target private address pairs can communicate with each other. Show that the traffic between the private traffic is reaching the correct destination (Hint: You may use `ping`, `traceroute` and `sh ip route`, among other commands). Explain how MPLS labels are used to forward the `traceroute` probes, and relate them to the resulting `traceroute`/ICMP messages. Combine use of `traceroute`, `show mpls table` and WireShark captures to achieve this.

Task 2.4 Reflection

Why may MPLS have lower encapsulation overhead than, for instance, an IPv4 tunnel? [Hint: compare the additional bytes introduced by the tunnel header and by the MPLS label stack, and consider what happens to a 1500-byte IP packet when the outgoing interface MTU is 1500.]

Consumer VPN services often advertise that your ISP cannot inspect the contents of your traffic. Does this MPLS L3VPN provide the same property? Why or why not?

Submission details

Please submit an archive (.tar.gz or .zip) which contains all files you want to submit. Please have your group number in the file name and the directory name. Submission channel will be shared during the lectures. A report (one single PDF file, named MPLS-group(num).pdf) containing the following elements is mandatory:

- Your group number on the first page.
- For each question, the written answers with the **relevant** portions of output from all commands in text format. No screenshots of terminal windows are accepted.
- For each question, all **changed** parts in the configuration of routers and hosts (differences to the default config). For configurations that are essentially the same over multiple devices, you can provide one configuration and state which other devices the configuration has been applied to.
- **Never** include the full verbatim switch or router configuration in the pdf report.
- For all questions, state your assumptions, report what you did, describe what you observed, and explain your conclusions.

Also, include a export of your GNS3-project (Export Portable Project), without including the base-images of the project.

We can only grade what we find in your submission and what we understand. Please state your assumptions and observations as clearly as possible.

Due date: October, 16th 2026, 11:59 PM