
Mini Internet Project

In this project, you together with more than 100 of your fellow classmates will build and operate your very own mini-Internet. Your main goal? Enabling end-to-end connectivity across ≈ 80 Autonomous Systems (ASes) composed of hundreds of network devices. In doing so, you will experiment with the most common switching and routing technologies used today in the Internet. You will also face the same challenges actual network operators experience every day.

To reach Internet-wide connectivity, you will first need to enable internal connectivity, *within* your own AS, before interconnecting your AS with others ASes, managed by other groups of students. To establish connectivity *within* your AS, you will use the Open Shortest Path First (OSPF) protocol. To establish connectivity *across* different ASes, you will use the only inter-domain routing protocol available today: the Border Gateway Protocol (BGP). At the end of the project, any end-host should be able to communicate with each other, independently of the AS they are located in.

To help you, we have pre-built a base network topology on top of virtual layer-2 switches, running Open vSwitch [1] and virtual routers, running the FRRouting software routing suite [2]. You will configure the virtual switches and routers through a Command Line Interface (CLI). This interface is virtually identical to the one used by actual network operators.

The rest of this document is organized as follows: Section 1 provides general information about the project, including **submission instructions**. Section 2 gives an overview of the mini-Internet and the network you will be configuring.

1 General Information

This section tells you what to do if you have questions, how to backup and submit your work and how it will be graded. Furthermore, it explains our policies on academic integrity and misuse of the resources.

1.1 If you have questions

In case of questions, please ask the TAs during the exercise sessions or use the Moodle forum.

1.2 Regularly backup your work

We provide you with a script that automatically saves all configs of all your routers and switches (`save_configs.sh`) in one place (see also the tutorial pdf). We advise you to use this script regularly and to copy the generated folder to your local machine in order to prevent losing your work in the case of unexpected problems.

1.3 Submit your work

Send your **report and configuration** using TURNIN. Make sure that your deliverable includes a zip or tar.gz archive containing a PDF report as well as all your configuration files (the directory generated with the `save_configs.sh` script). Please make sure that your PDF report includes

your group number as well as the name of the members in your group. The maximum length for your PDF report is 10 A4 pages (including screenshots, traceroutes, looking glass etc.).

Important: Do not use the mailing list for your questions.

1.4 Our grading policy

This assignment will be graded and counts for 40% of your final grade. The project consists of 2 phases with 5 questions per phase.

1.5 Academic integrity

We adopt a strict zero tolerance policy when it comes to cheating. Cheating will immediately result in the group failing the assignment. In particular, you can only do your assignment with the other members of your group. Do not look at other groups' configuration and do not copy configurations from anywhere. It is OK to discuss things or find help online, but you must do the work by yourself.

Your configuration and report may be checked with automated tools so as to discover plagiarism. Again, **do not copy-and-paste** code, text, etc.

1.6 Misuse of the resources and infrastructure

It is prohibited to use and modify the network in other ways than expressly allowed in this task description. The forbidden misuse includes, but is not limited to, BGP hijacks, DDoS attacks, resource-/bandwidth-hungry programs, and the attempt to access the docker containers of other groups. We monitor, investigate, and apply the appropriate disciplinary actions for cases of misuse.

2 Network Topologies

Similarly to real networks, your network spans over layer-2 (using switches) and layer-3 (using routers). Your network also connects (at layer-3) to other networks, creating an *Internet*. We now describe each aspect of the network topology.

L2 topology Your layer-2 network is composed of three switches (Fig. 1) located at three different locations: ETHZ, EPFL, and CERN. The switch at ETHZ is connected to a layer-3 router (ZURI), the one at CERN is connected to GENE. Both routers can act as a gateway, meaning that a host in the local network must send a packet to it to reach any non-local destination. The router will then take care of sending that packet to the destination.

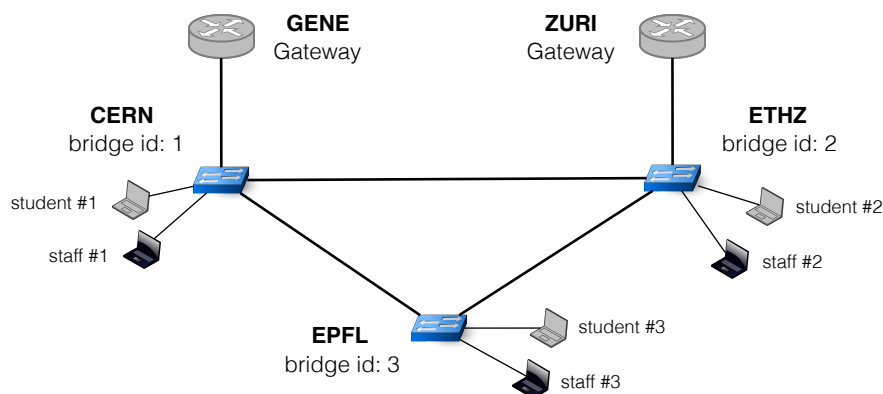


Figure 1: Each group will have to manage its own local network. This layer-2 network is composed of three Open vSwitches located at different locations. The switch at ETHZ connects to a layer-3 router (ZURI) which acts as the gateway and CERN is connected to GENE.

Two types of users exist in your layer-2 network: students and staff. Each switch is connected to one student and one staff member. Each switch also has a bridge ID which is indicated in Figure 1. For example, the switch at ETHZ has bridge ID 2.

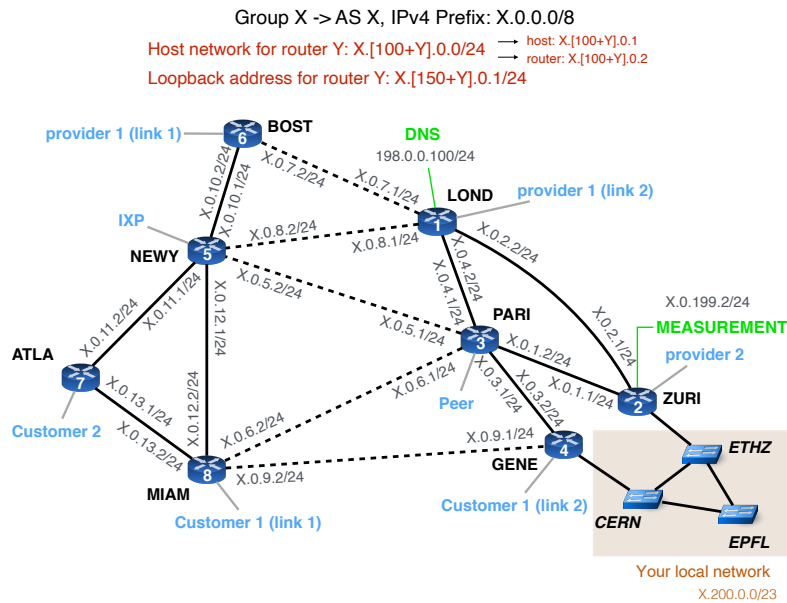


Figure 2: Each group will have to manage an entire AS. Your AS is composed of 8 routers. A /8 prefix has been assigned to each group. You can use it to configure your local networks. One host is also connected to each router, but ZURI and GENE. The subnets you must use are indicated on each interface. ZURI and GENE are connected to your local network.

L3 topology For this project, imagine that your layer-2 network is part of an AS spanning across the atlantic that you also manage. Your AS number is your group number: *e.g.*, AS 28 for group 28. Your AS has routers located on two continents: four routers in Europe (Geneva, London, Paris, and Zürich) and four in the US (Atlanta, Boston, New York, and Miami) see Figure 2.

Every AS has been allocated one /8 prefix that it can allocate internally. If you are group X, then the prefix X.0.0.0/8 is yours, meaning that group 48 has the prefix 48.0.0.0/8. You will use this IP space to allocate IP addresses to your hosts and routers.

Finally, one host is connected to each router with the exception of ZURI and GENE as these two routers are connected to your local network.

Internet topology Every router has an external connection to one of your neighboring ASes. Some are connected to a provider, some to a customer and others to a peer. NEWY is connected to an Internet eXchange Point (IXP). You will have to establish eBGP sessions on these external links. Figure 3 shows the mini-Internet topology you will end up building.

The red ASes (1, 2, etc.) are all Tier1 ASes, meaning their neighboring ASes are either peers or customers. The grey ASes (13, 14, etc.) are stub ASes, meaning their neighboring ASes are either peers or providers but they have no customers. We (the TA team) will take care of the Tier1 ASes as well as the stub ASes.

The Tier2 ASes (blue ASes) have peers, customers and providers. For example, group 5 has two providers (3 and 4), two peers (6 and the IXP 81) and two customers (7 and 8).

There are seven IXPs within our mini-Internet. The primary purpose of an IXP is to allow networks to interconnect directly. One advantage of using an IXP is that an AS can directly peer with another AS through the IXP, instead of reaching it via a provider that it has to pay. Another advantage is that only one physical connection with an IXP is needed to potentially interconnect with all the other IXP participants. An IXP uses a BGP Route Server to advertise prefixes between its participants.

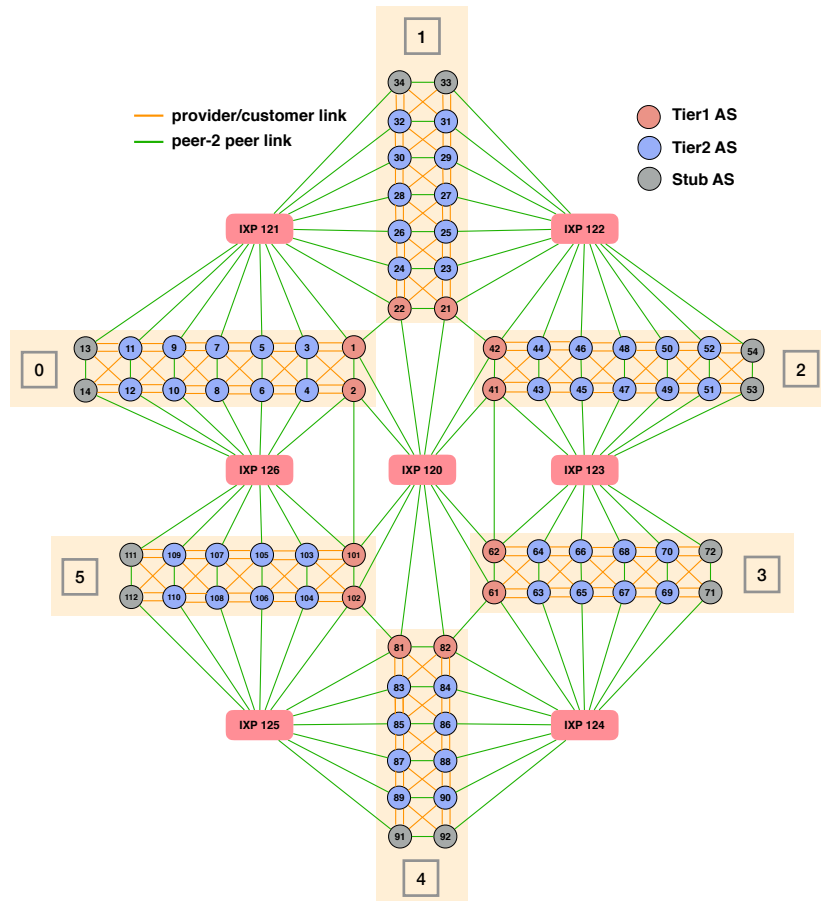


Figure 3: The AS-level topology of our mini-Internet. There are 12 Tier1 ASes, 12 stub ASes, and 54 Tier2 ASes. The topology is divided in 6 blocks (0, ..., 5), which are connected to each other via the Tier1 ASes or an IXP. The students operate the Tier2 ASes, while the Communication Networks TA team takes care of the Tier1 and the Stub ASes.

One IXP is connected to all the Tier1 ASes, allowing them to be connected in a full-mesh fashion. The other IXPs are always interconnecting two blocks. This enables these ASes to peer between them (as long as they respect the BGP customer/provider policies), instead of using (and paying!) their providers. The following example illustrates the benefit of being connected to an IXP: AS6 can send traffic to AS105 via the IXP126, instead of paying AS 4 to send the traffic via the path 4-2-101-103-105 if IXP126 is not used.

3 Questions

The assignment is split in two parts: (i) intra-domain, (ii) inter-domain and policy routing. In the first part you establish connectivity within your network (intra-domain). You will start by configuring the layer-2 network, followed by setting up your OSPF. The second part includes iBGP configuration as well as interconnecting all the networks (inter-domain). It involves bringing your eBGP sessions with your neighboring ASes up and advertising your prefixes. For the second you should also implement your BGP policies according to the business relationships that you have with your neighbors. As a last step, you will implement communication between the end hosts in your network using socket programming.

To help you, we will give you a crash course on how to configure FRRouting routers and Open vSwitches in a separate tutorial available in the project folder.

For each question, we precisely tell you what you must include in your report. In addition to your report, you must also send us your switch and router configurations. To make your life

easier, we provide you a script named `save_configs.sh` in the main docker container that puts all the configurations (routers and switches) in a single directory. It also generates a zip out of the directory. Then, you just need to download the zipped directory, add your report (pdf), and send it to us.

3.1 Phase I (45% of your project grade)

Question 1.1 (5% of your project grade)

Your first task is to enable end-to-end connectivity within your own local network. For this reason, you need to configure an IP address as well as a default gateway on each host (student and staff). For this question, you must use IP addresses belonging to your local subnet, which is `X.200.0.0/23` where `X` is your group number. You are free to use any IP address as long as it is in that subnet. To test connectivity, you can use `ping`.

In addition, every host needs to have a standard gateway to be able to reach external destinations. Configure it such that all hosts connected to CERN and EPFL use GENE as standard gateway and the hosts at ETHZ use ZURI.

To include in your report: In your report, include screenshots for the configuration in each host and router that you implemented. Explain what IP addresses you assigned to the different hosts. Finally, include 2 screenshots executing `ping` from student#1 to GENE router and from staff#2 to ZURI router.

Important: Please DO NOT remove any interface from routers, hosts or switches.

Question 1.2 (10% of your project grade)

As a network engineer, your goal for this question is to enable direct layer-2 connectivity between students, between staff members, but not in between them. Obviously, students and staff members should still be able to communicate between themselves, but via a layer-3 router. This will prevent typical layer-2 attacks such as MAC spoofing used to impersonate a type of user and get access to sensitive data.

For this reason, you have to configure VLANs: use VLAN 10 for the staff and VLAN 20 for the students. Please ignore VLAN 30. The interface of ZURI connected to ETHZ in VLAN 10 is named `ZURI-L2.10`, and the one in VLAN 20 is named `ZURI-L2.20` (you can see them with a `show interface brief` in the FRRouting CLI). The same holds for the interfaces in GENE: use `GENE-L2.10` for VLAN 10 and `GENE-L2.20` for VLAN 20. Do not use the interface `ZURI-L2` and `GENE-L2`.

Important: Similarly to previous question, all hosts connected to CERN and EPFL use GENE as standard gateway and the hosts at ETHZ use ZURI.

To include in your report: Explain what IP addresses you assigned to the different hosts and also explain possible changes that you made compared to the configuration presented in Question 1.1. Finally, show the output for one `traceroute` from EPFL-student to EPFL-staff, one from ETHZ-staff to EPFL-student and one from EPFL-student to ETHZ-staff. In a few sentences, explain what you observe.

4 Acknowledgments

The assignment is based on material from a similar course at ETH Zurich [3] and the corresponding platform [4].

References

- [1] B. Pfaff, J. Pettit, T. Koponen, E. Jackson, A. Zhou, J. Rajahalme, J. Gross, A. Wang, J. Stringer, P. Shelar, K. Amidon, and M. Casado, “The design and implementation of open vswitch,” in *12th USENIX Symposium on Networked Systems Design and Implementation (NSDI 15)*. Oakland, CA: USENIX Association, 2015, pp. 117–130. [Online]. Available: <https://www.usenix.org/conference/nsdi15/technical-sessions/presentation/pfaff>
- [2] FRRouting. [Online]. Available: <https://frrouting.org/>
- [3] ETH Zurich, Communication Networks. [Online]. Available: <https://comm-net.ethz.ch/>
- [4] T. Holterbach, T. Bühler, T. Rellstab, and L. Vanbever, “An open platform to teach how the internet practically works,” *arXiv preprint arXiv:1912.02031*, 2019.