IK2215: Project guideline

1 Objective

The project aims are to:

- give you hands-on experience in design and implement network and services as an Internet Service Provider (ISP);
- help you to gain insights into how an underlying network influences deployed services;
- provide a venue for you to describe and discuss network design and implementation; and
- learn to work professionally.

2 Deliverable

The final deliverable is a fully functioning ISP as well as a report containing details of your network design. During project development, you will also submit reports, including three revisions of network design report that describes your network design in detail and two peer review reports that review the network design reports of other students.

2.1 Network design report

A good project begins with proper planning. Therefore, you will start by designing your network before the actual implementation. You will develop the network and services of an ISP and document them as the network design report. Then, you will try to improve your design and the actual written report over two rounds of peer-review reports to produce a high-quality network design report as your final version. The network design report should not be longer than 6 pages.

2.2 Peer-review report

As a part of peer-review process, you will give constructive feedback to other students. You will review two other network design reports and produce two peer-review reports as part of your deliverables. During the process, we expect you to learn from other students and improve your network design. The peer-review report should not be longer than 4 pages.

2.3 ISP implementation

The final deliverable is a fully functioning implementation of your network design deployed using Kathará in the lab VM. The implementation must fulfill all constraints and requirements given in Section 4 and 5. Your ISP implementation must work and passed a verification test of the teaching staff to be considered as a pass. Only those whose ISP implementation passed the test are allowed to present in the demonstration session.

2.4 Demonstration

Only those whose ISP implementation passed the test are allowed to do the demonstration.

First, you are given **2 minutes** at the start of the demonstration to give a summary of what you did to fulfill the requirements in your network design. You must create a single page slide containing your network diagram and use it during the presentation. Then, the audience (teaching staff and students) will ask you questions related to your network design. Finally, we will run the ISP implementation that you submit and ask you questions related to the implementation, which we expect you to be able to answer. Thus, you will run the lab VM with your ISP implementation on your computer and demonstrate to the audience that you have an understanding of the underlying network that you design and can verify your answer in practice.

IMPORTANT: Ideally, your presentation should not be longer than 2 minutes, therefore we impose a strict maximum 3 minutes. If you cannot finish your presentation within 3 minutes, you will fail the presentation. We strongly recommend that you prepare your presentation properly, i.e., write down a script for the presentation and practice it with timer to see that you can do it, ideally within 2 minutes.

3 Working schedule

You are expected to work on the project assignment on your own time outside the course schedule. We use the discussion forum on the course website as the main communication channel for you to ask questions. There are also some scheduled sessions that we will use as Q&A sessions that you may ask verbally and to assist you with issues that might be difficult to simply post as questions on the discussion forum. Some sessions towards the end of the course are reserved for demonstration sessions, during which you will present your final implementation.

You can find more details on the scheduled sessions on the course website.

4 Network organization

Your main task is to set up an ISP and connect to “our Internet,” as shown in Figure 1. Our Internet consists of multiples ASes. Each AS also runs basic Internet services, including DNS and Web (they are not shown in the figure). In each AS, a DNS server is named **ns.isp*N*.lab**, while a web server is named **www.isp*N*.lab**, where ***N*** is the AS number. In addition, there are two public DNS servers, i.e., the root DNS and a top-level-domain DNS for .lab domain that are connected to AS1 and AS2, respectively. AS1 and AS2 are acting as top-tier service providers. Each connects to customers that also run BGP with their own AS numbers. You will run as an ISP that is a customer of AS1 (i.e., ASX in the figure). Besides, you will also establish a private peering with AS21 that is a customer of AS2. This private peering is used for direct communication between ASX and AS21 during normal operation. It also serves as a backup for ASX and AS21, which will provide transit service when a link to the top-tier service provider fails.

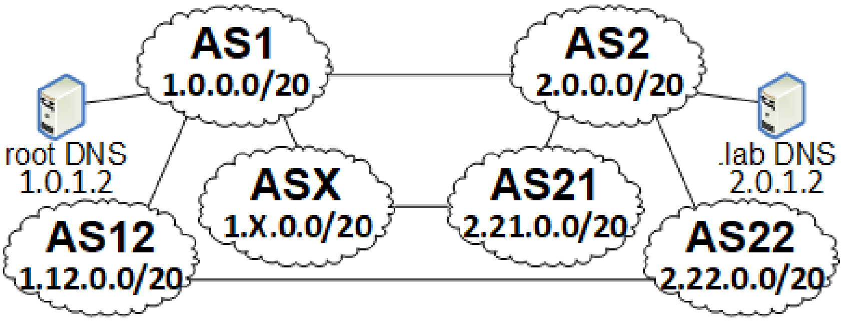

Figure 1: Overview of the Internet used in the project assignment

4.1 AS number and IP address allocation

Each ISP is assigned an AS number (ASN) and a /20 IP address block, as shown in Table 1. We also refer to the ISP using its ASN. For example, ISP 101 has an ASN 101 and 1.101.0.0/20 address block. How you allocate subnets within your ISP is entirely up to you. However, you should allocate reasonable subnets that are practical and realistic, and you don't need to use all addresses. All IP addresses that you use must come from 1.X.0.0/20.

The ASN is 100 + the group number, and you can find your group number on the course website.

ASN	/20 IP address block
101	1.101.0.0/20
102	1.102.0.0/20
X	1.*X*.0.0/20

Table 1: ASN and IP address block of each ISP

4.2 Resources

We emulate the Internet using Kathará in the lab VM. A Kathará configuration for the project assignment is available on the course website. All ASes are preconfigured except ASX that you will configure as your ISP. In the main configuration file (lab.conf), you will find a set of routers and hosts, each with a specific number of interfaces. **You are not allowed to add/remove interfaces!** Some interfaces are already assigned to a particular network. **You are not allowed to change these preassigned networks!** However, many interfaces of routers and hosts belonging to ASX are still unassigned. Moreover, you will see that the configuration folder and startup script for routers, servers, and hosts of your AS are not included in the template. You will need to create them yourself. You can see examples from labs and the other ASes that are preconfigured.

As part of your network design, you will interconnect routers and hosts using these unassigned interfaces. Therefore, you can modify these unassigned interfaces to build your ISP's internal network. When you connect these unassigned interfaces, you must use only point-to-point links, i.e., there are only two interfaces connected on the same network. You don't have to use all unassigned interfaces. But your design must fulfill the constraints and requirements of the project assignment.

There are several ways you can design the internal network of your ISP. Hardware resource is a limiting factor, which you must take into account when planning your network. Figure 2 shows all routers and hosts that you are given for the project assignment. There are four routers (r1–r4) and five hosts (three servers and two clients). The eth0 of r1 is connected to AS1 and used for the primary link to communicate with other ASes. The eth0 of r2 is connected to AS21 and used for direct communication with AS21. It also serves as a backup link for Internet access in case the primary link fails. The eth0 of r3 is connected to a server network that is connected to servers providing Internet services. There are three servers (s1–s3) that you can use. s1 must be used as your DNS server and must be assigned an IP 1.X.1.2. Furthermore, s1 must not run other Internet services. The eth0 of r4 is connected to a client network. There are two clients (c1 and c2), which should get networking information automatically from a DHCP server that resides in a server network. The clients are mainly used to verify that everything is working correctly.

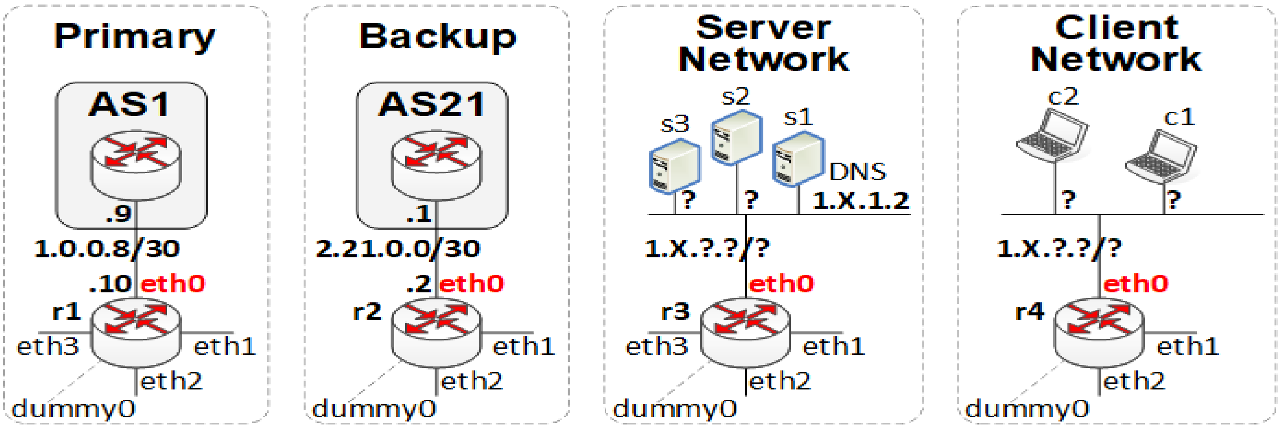

Figure 2: Routers and hosts provided for your ISP

IMPORTANT: These routers and hosts are not preconfigured. You must configure them yourself! We also put **as*X*** prefix in the name of all devices. For example, r1 of AS100 will be called as100r1 and s2 of as100 will be called as100s2. You must follow this naming convention when you create the configurations for your AS. Note that we use **/30** subnets for the links to AS1 and AS21, you must configure them accordingly.

5 Requirements

This section describes requirements that you must fulfill with your ISP implementation. We classify the requirements into two types; routing requirements and Internet service requirements.

5.1 Routing requirements

You will use different routing protocols to control how traffic traverses the internal network within your ISP (intra-domain routing) and the Internet across the ASes (inter-domain routing).

5.1.1 Intra-domain routing

You must show that your network has dynamic IP routing with redundant paths. All routers must have at least two disjoint paths and your network must stay operational when one of the internal link fails (i.e. any link that is not connected to eth0 of r1–r4 can fail without causing a permanent network disruption).

For pedagogical purpose, we would like you to configure your network so that the paths are deterministic. In particular, your network must not have equal-cost paths between two end-points, and the routers should never have to use equal-cost multi-path routing (ECMP) when forward the traffic. Instead, all traffic should always take a specific path, which we will refer to as a primary path. When the primary path fails, the traffic will take a secondary path. As a part of this task, you must identify the primary and secondary paths for the communication between two devices below.

- r1 to client network and vice versa
- r1 to server network and vice versa
- r2 to client network and vice versa
- r2 to server network and vice versa
- client network to server network and vice versa

5.1.2 Inter-domain routing

Each ISP is assigned a unique ASN, which you will use to run BGP to connect to the Internet. Your AS has two links to two different ASes; a primary link to your top-tier service provider (AS1) and a private link to a neighboring AS (AS21) that is a customer of another top-tier service provider (AS2). We expect you to set up your BGP policy, according to Figure 3.

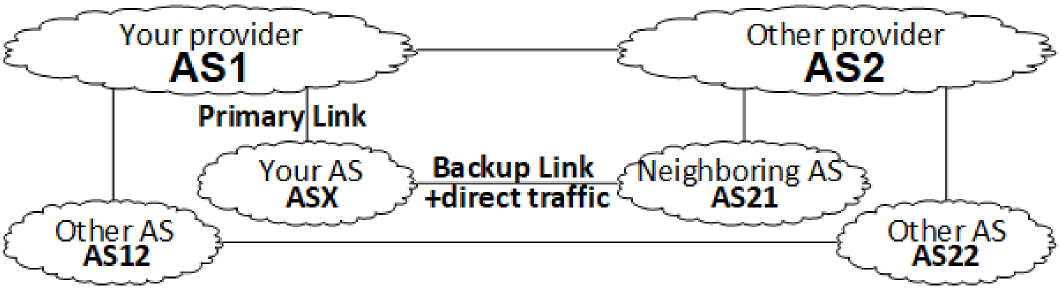

Figure 3: BGP policy

The primary link is used for all traffic (incoming and outgoing) during normal operation. However, the traffic to/from your neighboring AS (AS21) will take a direct path over the backup link. The backup link also provides Internet connectivity in case the primary link fails. This means that you and your neighboring AS provide transit for each other only when either your primary link or your neighboring AS's primary link fails.

You must set up BGP policy using only BGP attributes to achieve this behavior, given that the top-tier providers (AS1 and AS2) and your neighbor AS (AS21) use default BGP behavior without configuring additional BGP policy. The other customers of top-tier providers (AS12 and AS22) have a BGP policy based on AS_PATH manipulation to always use the link towards the top-tier providers as the primary link and send all traffic over this link during normal operation. In our scenario, AS12 and AS22 also have a private link that is used as a backup link when the primary link fail. Moreover, we do not enforce any transit policy among these ASes. If a link between AS1 and AS2 fails, AS12 and AS22 will provide transit for their own providers.

You will need to think about how your policy affects other ASes. In particular, you need to ensure that your policy is enforced not only for your AS but also for other ASes. For instance, AS21 shouldn't use your AS as a transit to AS1 and vice versa during normal operation. Moreover, your network must work even when either r1 or r2 is taken offline! However, you must not provide transit for other ASes, except AS21. For prefixes from your own AS, you will advertise only your aggregated prefix (i.e., 1.X.0.0/20) to other ASes and suppress other prefixes that you use for internal subnets.

IMPORTANT! Beside BGP, you must not run any dynamic routing protocol towards other ASes! For example, if you use OSPF for your internal network, you must not run OSPF on the link to your top-tier provider or your neighboring AS.

Weight is not a BGP attribute, therefore you must not use weight in your BGP policy.

5.2 Internet service requirements

As part of your ISP, you will run some basic Internet services, including DNS, web, and DHCP.

5.2.1 DNS

You must have one DNS server running in your ISP. No other services (i.e., web and DHCP) should be running on this server. Each ISP is assigned a domain **isp*X*.lab**, where ***X*** is your ASN. Your main DNS server must be named **ns.isp*X*.lab** and has an IP address **1.*X*.1.2**. Moreover, we simplify the reverse DNS zone configuration by delegating ***X*.1.in-addr.arpa** to your DNS server. The top-level-domain (TLD) DNS servers (for .lab and 1.in-addr.arpa domains) are already preconfigured with DNS delegation as described above. For example, if you are assigned ASN 100, you have isp100.lab domain. The DNS server must be named ns.isp100.lab with IP 1.100.1.2 and it is also responsible for 100.1.in-addr.arpa reverse zone.

BIND 9 is already installed on the container in the lab VM. You must use it to set up your DNS service. For your own domain configuration (i.e., for isp*X*.lab and *X*.1.in-addr.arpa), the forward lookup must work, while the reverse lookup is optional. However, both forward and reverse lookup of other domains must work correctly, i.e., servers and clients within your network must be able to perform both forward and reverse lookup of all servers residing in other domains on the Internet. All hosts and router interfaces in the server and client networks must also have names under your domain that map to their corresponding IP addresses. Hosts in other ASes must be able to resolve the names of devices in your server and client networks.

5.2.2 Web

You must have a web server running in your server network. The web server must have a name **www.isp*X*.lab**, where ***X*** is your ASN. The Apache HTTP server is already installed on the container in the lab VM. You must use it to set up your web server.

The web server main page should be a simple text-based page named **index.html** and contains the following information:

- ASN: X
- NETWORK: 1.X.0.0/20
- NAME1: <Student1 name>
- EMAIL1: <Student1 email>
- NAME2: <Student2 name>
- EMAIL2: <Student2 email>

5.2.3 DHCP

You must have at least one DHCP server running in the server network that is responsible for handing out IP address and relevant networking information (e.g., default gateway) for hosts in the client networks. The server name should be **dhcpd.isp*X*.lab**, where ***X*** is your ASN.

You also need to implement a DHCP relay since the DHCP server does not reside in the same LAN as the clients.

ISC DHCP server and relay are already installed on the container in the lab VM. You must use them to set up your DHCP server and DHCP relay.

IMPORTANT: In theory, you can simply add the DHCP client in the startup script of a client and it should automatically get IP address configuration from the DHCP server. However, docker creates the `/etc/resolv.conf` in the container as a bind mount file from the host, and the DHCP client process is unable to update `/etc/resolv.conf` (i.e., the DHCP client script fails to overwrite `/etc/resolv.conf` with `mv` command). This problem makes your clients fails to get DNS service.

Although the DHCP client process is unable to overwrite /etc/resolv.conf, it will create a temporary file called `/etc/resolv.conf.dhclient-new.XX`, where `XX` is a counter number. To resolve the problem with clients' DNS service, you can manually copy `/etc/resolv.conf.dhclient-new.XX` over `/etc/resolv.conf` with the command:

```
cp /etc/resolv.conf.dhclient-new.XX /etc/resolv.conf
```

NOTE: the DHCP client process periodically create `/etc/resolv.conf.dhclient-new.XX` files. They are identical and you can choose any one of them when you copy to `/etc/resolv.conf`.