IK2215: Project guideline

1 Objective

The project aims are to:

- give you hands-on experience in designing, configuring & handling TCP/IP networks, and providing services as an Internet Service Provider (ISP) to end users by primarily using PC hardware and Unix;
- help you to gain insights into how an underlying network influences deployed services;
- learn to test and troubleshoot configurations of your network and 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 and a report containing details of your network design. During project development, you will also submit reports, including two revisions of the network design report that describes your network design in detail and a peer review report that reviews the network design report 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 go through an iterative process to improve the quality of your design and the written report based on the feedback you receive from your peers and the teacher in your final version. The network design report **must not be longer than six pages.**

2.2 Peer-review report

As a part of the peer-review process, each student will individually give constructive feedback to one network design report of another student group and produce a peer-review report as part of your deliverables. We expect you to learn from other students and improve your network design during the process. The peer-review report **must not be longer than four 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 Sections 4 and 5. Your ISP implementation must work and pass a verification test (carried out by the teaching staff) to be considered as a pass. Only those whose ISP implementation pass the test are allowed to present in the demonstration session.

IMPORTANT: You must download the project template file (i.e., `project.tgz`) from the course web to the lab VM at the /home/student/IK2215 folder and unpack it. After unpacking, you should see the `project` folder that contains multiple files. Read the README file carefully and follow the instructions to modify the Kathará configurations to your assigned group number.

2.4 Demonstration

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

You are given **2 minutes** at the start of the demonstration to summarize 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. Moreover, the teach staff will ask questions related to the ISP implementation that you submit. Concurrently, you will run the ISP implementation that you submit on your computer and demonstrate to the audience that you understand the underlying network you design and can verify your answer in practice.

IMPORTANT: Your presentation should not be longer than 2 minutes. We also impose a strict maximum of 3 minutes. **You automatically fail the presentation if you cannot finish it in 3 minutes.** We strongly recommend that you prepare your presentation properly, i.e., write down a script and practice it with a timer to ensure that you can do it within 2 minutes.

3 Working schedule

You are expected to work on the project assignment on your own time outside the course schedule. As this is group work, you need to synchronize your time with your group mate to work together. **Remember that if you have questions, the first person you ask is your group mate!** If your group cannot resolve the issue after the group discussion, you may try to ask others. We use the discussion forum on the course website as the main communication channel to ask questions. There are also some scheduled Q&A sessions that you may ask verbally and get help with issues that might be difficult to 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*X*.lab**, while a web server is named **www.isp*X*.lab**, where ***X*** is the autonomous system number (ASN). In addition, there are two public DNS servers, i.e., the root DNS and a top-level domain (TLD) DNS for the .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 ASNs. AS12 and ASX are customers of AS1, while AS21 and AS22 are customers of AS2. AS3 is a regional service provider that is connected to both AS1 and AS2.

You will run the ASX that is a customer of AS1. Besides, you will also establish a private peering with AS21 that is a customer of AS2.

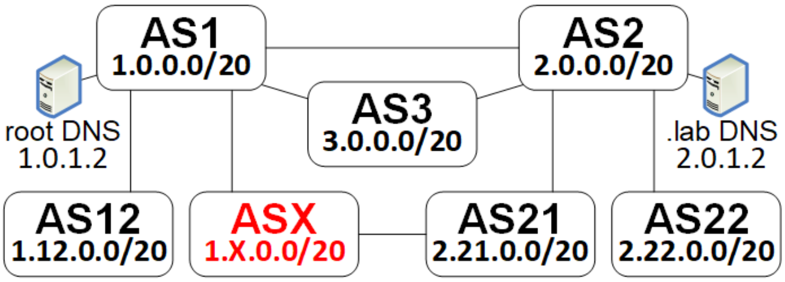

Figure 1: Overview of the Internet used in the project assignment

4.1 AS number and IP address allocation

Each ISP is assigned an 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 and you do not need to use all addresses. However, you must make sure the subnets are not overlapping! We recommend you to allocate reasonable subnets that are practical and convenient for configurations. All IP addresses that you use must come from 1.X.0.0/20, including IP addresses assigned to dummy interfaces. You can see examples of how to create dummy interfaces in the configurations of the BGP lab.

Your group ASN is **100 + group number**. You can find your group number on the course website. For example, if you are group 1, your ASN is 101.

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!**

You should see that many interfaces of routers and hosts belonging to ASX are still unassigned. Moreover, the configuration folder and the startup script for routers, servers, and hosts of your AS are not included in the template. You have to create them yourself. You can see examples from the other ASes that are preconfigured and from other labs. As part of your network design, you will interconnect routers and hosts using 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 routers interconnected on the same LAN segment. 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 all routers are preassigned. R1 eth0 is connected to AS1. R2 eth0 is connected to AS21. R3 eth0 is connected to a server network. R4 eth0 is connected to a client network. Moreover, we assume that r3 and r4 do not support BGP. Therefore, **you must not run BGP on r3 and r4.**

There are three servers (s1–s3) connected to r3. 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. Instead, they must run on s2 or s3. You can choose which server runs which service. There are two clients (c1 and c2) connected to r4. They must 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.

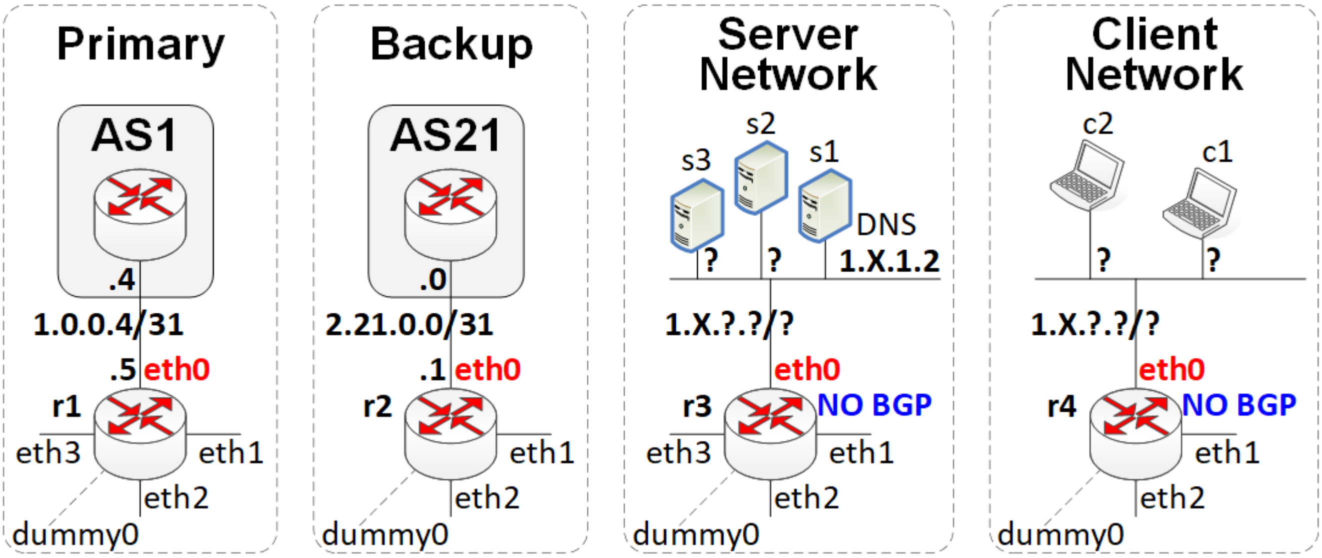

Figure 2: Routers and hosts provided for your ISP

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 **/31** subnets for the point-to-point 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 may use RIP or OSPF as your interior gateway protocol (IGP). You must show that your network has dynamic IP routing with redundant paths. All routers must have at least two disjoint paths. Your network must stay operational when one of the internal links fails (i.e., any link 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 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 the 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.

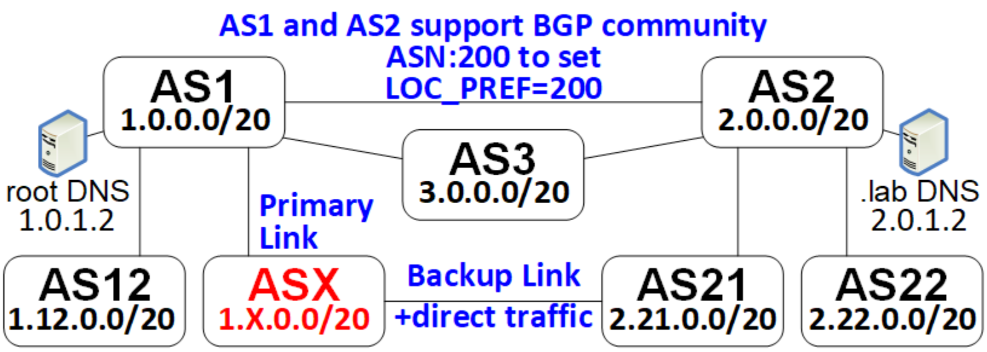

Figure 3: BGP policy

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 only provide transit for each other when either your primary link or your neighboring AS's primary link fails. Moreover, your ISP must **advertise only the aggregated prefix 1.ASN.0.0/20** in all BGP routing updates, i.e., your ISP must not advertise more-specific prefixes that you use for internal subnets such as 1.ASN.x.x/24, 1.ASN.x.x/30, and 1.ASN.x.x/31.

In our setup, all other ASes use default BGP behavior without any BGP manipulation. Thus, the data traffic will not be taking the correct paths. In this assignment, you must set up a BGP policy to **manipulate BGP routing updates using solely BGP attributes** so that the traffic of all ASes would take the correct paths. One exception is that AS1 and AS2 have configured to support a BGP community value for setting local preference attribute. AS1 supports a BGP community value of **1:200**, while AS2 supports a BGP community value of **2:200**. When they receive a routing update with such a community value, they will set the local preference of the received prefix to 200. Once the value is set, the BGP community attribute is also removed from the routing information. For instance, if AS1 receives a prefix 1.2.3.0/24 with community 1:200, it will set a local preference of the prefix 1.2.3.0/24 to 200 and remove the BGP community attribute from the 1.2.3.0/24 prefix. When AS1 advertises 1.2.3.0/24 to other ASes, the prefix will no longer contain the BGP community value of 1:200. Note that AS1 will not do anything to the BGP community value that it does not recognize. For example, if AS1 receives a prefix 4.5.6.0/24 with a community value 2:200, it will accept the prefix as normal and include the community value when it advertises the prefix to other ASes (it does not set the local preference to 200).

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 to 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.ASN.0.0/20) to other ASes and suppress other prefixes that you use for internal subnets.

IMPORTANT! You must not run any dynamic routing protocol towards other ASes except BGP! 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.

Moreover, you must not run BGP on r3 and r4.

One caveat in Quagga is that the BGP community will not work correctly if you set multiples BGP community values on a prefix. Thus, **you must use only one BGP community value per prefix.**

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 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. The forward lookup must work for your own domain configuration (i.e., for isp*X*.lab and *X*.1.in-addr.arpa), 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 lookups of all servers residing in other domains on the Internet. All router interfaces and hosts in the server and client networks must 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 the 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> (if your group has two members)
- EMAIL2: <Student2 email> (if your group has two members)

5.2.3 DHCP

You must have at least one DHCP server running in the server network that is responsible for handing out IP addresses 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. For your information, **dhcpd** represents the **DHCP d**aemon, which is the DHCP server process.

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.

IMPORTANT: In theory, you can simply add the DHCP client in the startup script of a client, and it should automatically get the 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 fail 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 creates `/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`.

5.3 Additional configuration requirements

There are some additional requirements that you must follow:

- All router interface IP addresses must be configured via Quagga.
- You must not use any static route in your router configuration, including a static route to the Null0 interface.
- You must not use more than one BGP community value of ASN:value per prefix.
- You must use a default route in your IGP so that non-BGP routers can communicate with other ASes. You may redistribute AS21's prefix from BGP into your IGP. However, you are not allowed to redistribute other BGP prefixes into IGP.
- All servers' IP address and default route must be configured via the startup script using the `ip` command.
- All clients' startup script must contain only one command line to start DHCP client on eth0.
- All active IP addresses of router and host interfaces must have domain names mapped to them, including the dynamic IP addresses for the clients.