THE UNIVERSITY OF WAIKATO
COMP304-24A — Advanced Networking & Cyber Security
Assignment 2 - Routing with BGP

1 Introduction

This assignment asks you to continue adding to your network from the first assignment, which you had configured with an interior gateway protocol (OSPF), by adding an exterior gateway protocol (BGP) to connect your network to others. The aim of this assignment is that you configure and understand the operation of BGP on the Internet. This assignment gets you to configure BGP sessions with other ASes run by other students in your class on the mini-Internet to give you a feel for how the Internet works.

We continue to use the mini-Internet project and FRRouting as we did in the first assignment. For guidance on configuring BGP, refer to Richard Sanger's mini-Internet project quick start guide here: `https://github.com/rsanger/mini_internet_project/wiki/2.5.5-Configure-BGP`. The official FRRouting documentation is also available here: `http://docs.frrouting.org/en/latest/`. As with the OSPF assignment, one of the skills you will learn is becoming familiar with searching through the documentation for answers.

Check the Assignment section on Moodle if you are having trouble.

1.1 Stages

This assignment guide will help you work towards the final configuration in a series of stages:

i. Verify your OSPF configuration from assignment 1 is working correctly;

ii. Add addresses to your external network links;

iii. Configure iBGP sessions between your routers;

iv. Configure eBGP sessions with external ASes;

v. Advertise a route for your network prefix over BGP;

vi. Configure BGP communities to share routes with peers on the IXP;

vii. Configure *policy-based routing* based on whether a BGP neighbour is a peer, provider, or customer.

There are quite a few steps in this assignment. The key to successful implementation and learning is to *test each step carefully*, so you're sure it works correctly and you understand what is happening before moving on to the next one. You will find a guide to commands that you can use to test what is happening at the end of this assignment guide.

1.2 Assessment

This is a complex assignment. However, the “bar” for a pass mark is quite low. A totally correct solution with BGP sharing routes with neighbouring networks will receive a pass mark. The steps after that are more difficult and marks are allocated to the steps beyond that on a diminishing scale (not purely on effort or importance). **NOTE:** unlike the labs, **this assignment is an individual assignment. Work on your own.** You may discuss the assignment with others in general terms but do not look at anyone else’s configuration or show them yours. If you need help, ask us (the tutor and/or lecturer) or post a question on Moodle (but don’t post *any* configuration code on Moodle).

1.3 The mini-Internet

The mini-Internet is a teaching project developed by ETH Zurich[1]. As a student, you are each given your own network to manage and configure Such a network on the Internet is given the name *autonomous system (AS).*

The mini-Internet gives you access to several Docker containers. These Docker containers behave like real hosts, switches, and routers; with the main difference being that you cannot reboot or shut them down. All networks run on a single server, `mini.cms.waikato.ac.nz`.

1.4 Mini-Internet Help

Appendix A includes details of how to access the mini-Internet and should be familiar to you from the previous assignment and the labs. If you have any issues accessing your containers or any other problems, please email the lecturer/tutors as soon as possible. Also, check the Assignment section on Moodle for useful information about this assignment.

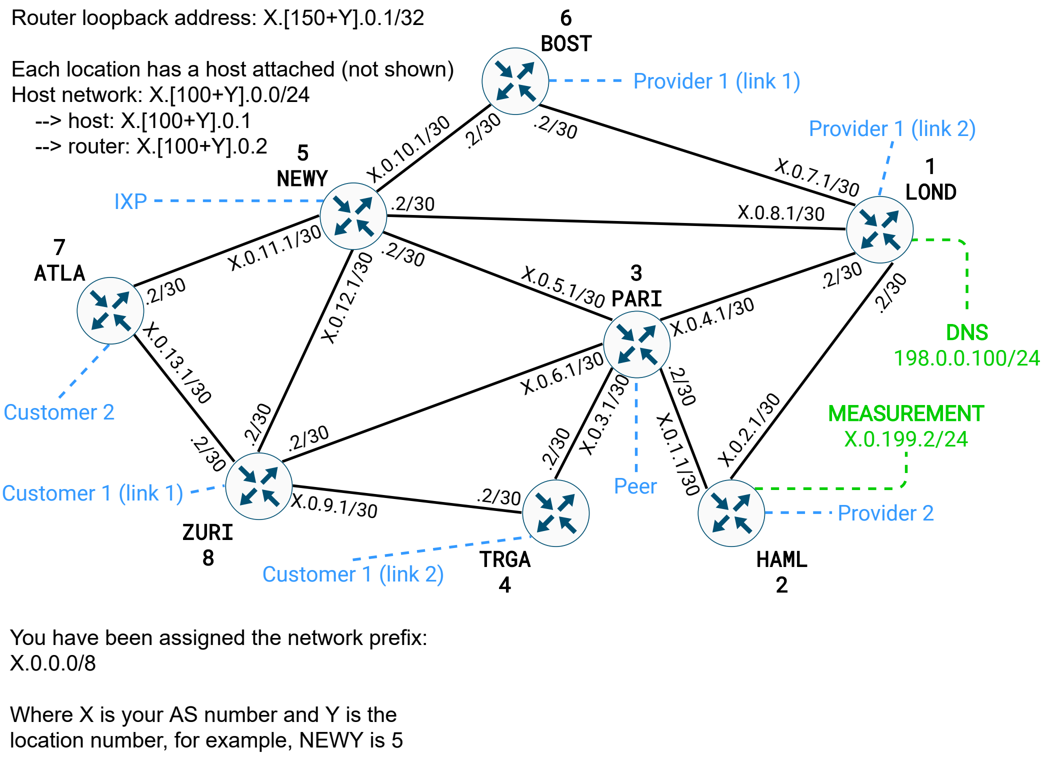
2 Network Topology

2.1 Your Internal Network Topology

Figure 1 shows the internal layout of your AS, which you configured with OSPF in Assignment 1. In Assignment 2, you will configure BGP on the inter-domain links to connect your AS with the other students in your class to form an emulated Internet. These inter-domain connections are shown in blue. Figure 2 shows exactly which other ASes your AS is connected to. Section 3.3 tells you how to assign addresses on your inter-domain links (i.e. external).

There is a DNS server attached to the LOND router. The DNS server provides you with DNS name resolution for the links and hosts in your network based

[1] The mini-Internet project `https://github.com/nsg-ethz/mini_internet_project`



Router loopback address: X.[150+Y].0.1/32

Each location has a host attached (not shown)
Host network: X.[100+Y].0.0/24
--> host: X.[100+Y].0.1
--> router: X.[100+Y].0.2

You have been assigned the network prefix:
X.0.0.0/8

Where X is your AS number and Y is the location number, for example, NEWY is 5

Figure 1: The internal layout and address plan of your AS. You have been assigned an entire /8 to number your network, X.0.0.0/8, where X is the network (autonomous system) number we have emailed to you. Each router shown has a host attached. Assignment 1 required you to configure the internal links of your network. In this assignment, you will continue from Assignment 1. All you need to do is to configure the routers to use the *external* links, shown in blue; that's all! Section 3.3 lists the addresses to use.

on the addressing we've provided. Your hosts are pre-configured to use this DNS server for commands including `traceroute`.

There is a MEASUREMENT host attached to HAML and outlined in Section 2.3.3.

2.2 The Internet Topology

Figure 2 shows the Internet topology. Every router in your AS connects to another AS network. These other ASes are either customers, providers, or peers of your AS. The NEWY router is connected to an IXP, which allows your AS to exchange routes/traffic with multiple peers.

The red ASes are Tier-1 ASes (1, 2, 15, 16, etc.), meaning that all of their neighbours are either peers or customers. The grey ASes (13, 14, etc.) have no customers and in such cases are called *stub* ASes. We have pre-configured both the Tier-1 and stub ASes; their routers will speak eBGP and exchange routes with your AS is neighbouring one of them.

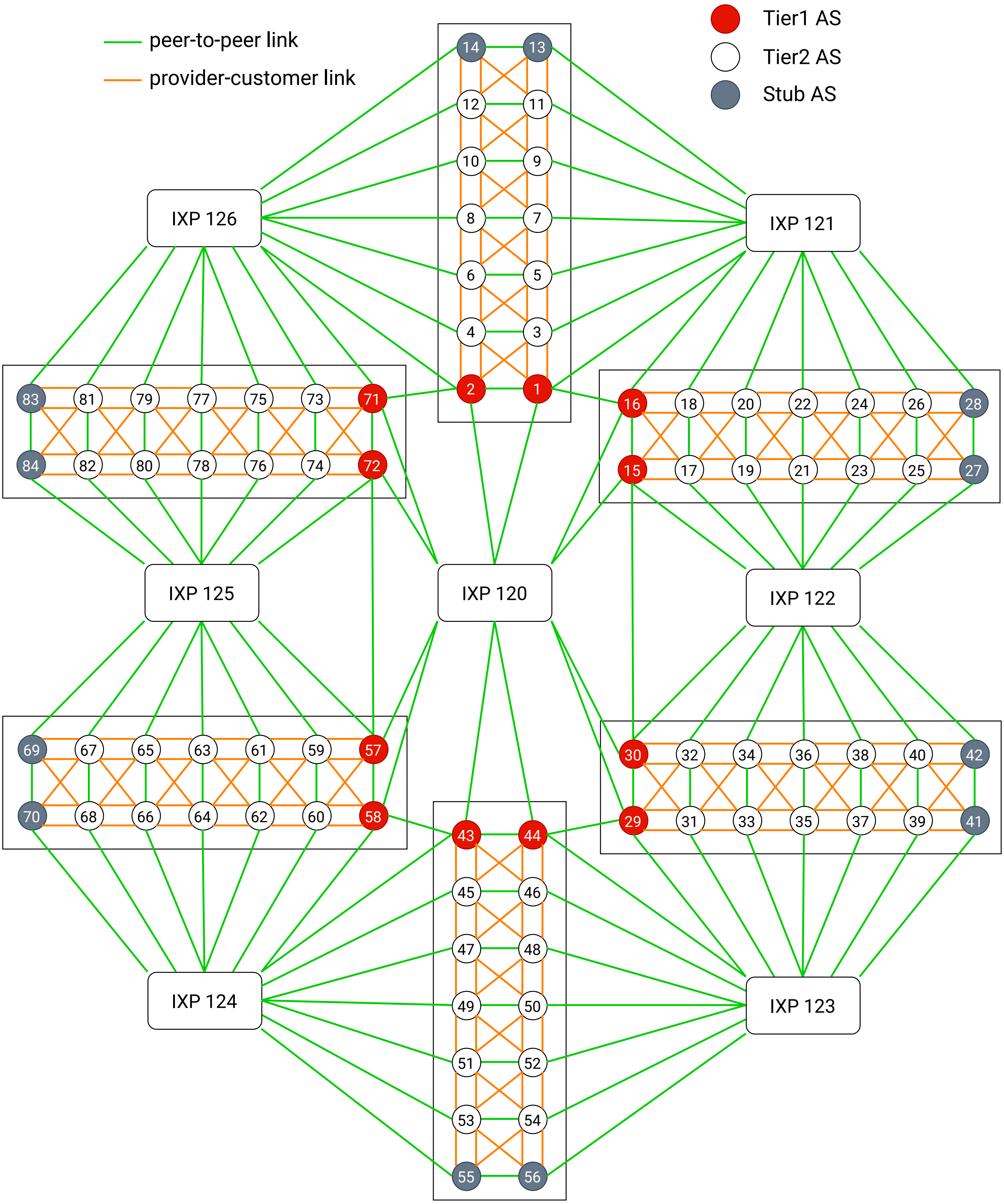


Figure 2: The topology of ASes on the mini-Internet. There are 12 Tier-1 ASes (in red), 12 Stub ASes (in grey), and 60 Tier-2 ASes. We have divided the Internet into 6 blocks, which are interconnected by tier-1 ASes and Internet eXchange Points (IXPs). Your AS has a connection to an IXP. We have assigned you one Tier-2 AS to configure, and we have pre-configured all of the Tier-1s, Stubs, and IXPs.

You are managing a Tier-2 AS, and your AS has customer, provider, and peer relationships with your neighbours. For example, if you are AS 10, you are a provider for AS 11 and AS 12; a customer of AS 7 and AS 8; and a peer of IXP 126 and AS 9. To begin with, you will focus on configuring eBGP with all of your neighbours to exchange routing information. But, at the end of the assignment, you will need to configure BGP policies to announce to your peers only your customers' routes (never your providers' routes, or you peers' routes), to avoid giving away free transit. Check the four routing leak types in the lecture slides.

The IXPs allow peering with multiple neighbours in one location and without paying a provider. Each IXP is running a BGP route server (RS) to advertise routes between all of its participants. For example, without IXPs, AS 10 would reach AS 77 via the (long) AS-path 10-8-6-4-2-71-73-75-77. However, once peered with IXP 126, AS 10 can reach AS 77 directly through the IXP.

2.3 Verifying Your Network Configuration

You can find suggestions of useful troubleshooting commands in the appendix at the end of this assignment. See Appendix B.1 for useful FRRouting commands you can run. We have also provided several tools which you can use to verify your network configuration. These are very similar to the tools actually used on the internet. You can find most of these tools linked on the main website for this project `https://mini-internet.cms.waikato.ac.nz`.

2.3.1 BGP Looking Glass

A BGP Looking Glass (LG) service is a public, read-only portal that many network operators provide to expose public routing information to other network operators to assist with network debugging. This gives you insight into the BGP routes that another network can see. The Looking Glass service for the mini-Internet provides the BGP routing database for routers. It periodically runs and saves the output of the command `show ip bgp` on all routers, grouped by the AS number.

Here is an example of LG for IXPs in NZ: `https://lg.ix.nz/`. By default, you view AKL-IX, which is the IXP in Auckland (there are other locations, such as Christchurch). There are (almost always) two route servers, for redundancy, in this case, namely rs1.akl.ix.nz and rs1.akl.ix.nz. Click on one of them. If you click on column "Routes Received", twice, you can list use descending order according to the number of routes received by the route server from the specific IXP member. Select for example ASN 32787, Akamai, by clicking on it (it has a large number of routes). Akamai is a Content Delivery Network (CDN); CDNs are like caches close to users, and are used to deliver content (e.e.g. videos) to users in a very efficient way. There you see a list of routes *accepted* by the IXP (routes can be denied during the import process). If you click on an entry, you will see the information for the route, which will have the origin of the route, local pref, next hop, may have MED, AS Path, and may have BGP communities (also Extended communities). This LG interface is called Alicia and is more sophisticated than the one we will be using.

Our own LG is here:
`https://mini-internet.cms.waikato.ac.nz/looking_glass/` It shows the routing table information organising per AS and router in the AS. For example, you can find the BGP routes for AS 1, HAML router here:
`https://mini-internet.cms.waikato.ac.nz/looking_glass/G1/HAML.txt`

2.3.2 The Connectivity Matrix

You can track your own progress towards this assignment (and the class as a whole) using the connectivity matrix. The connectivity matrix is here `https://mini-internet.cms.waikato.ac.nz/matrix/matrix.html`. The cells are coloured as follows:

- *green*: there is a working route between two ASes;
- *red*: the two networks are *not* reachable from each other;

As you and your classmates configure BGP, the matrix should turn gradually green as more of the Internet becomes reachable. After configuring OSPF in Assignment 1, your AS should have reachability to itself, i.e. the cell at row X and column X should be green. This is the diagonal green line down the middle of the matrix. NOTE: it may take over *10 minutes* for the matrix to update fully, so your BGP configurations changes will *typically not appear immediately.*

The host that helps creating this matrix, called matrix host, is connected to the PARI router. It uses a pre-configured interface (`matrix_X`) with the IP address X.0.198.2/24, where X is your AS number. It pings to the ATLA host in the target AS to check reachability (it does so for all other AS on our Internet; imagine doing so for the real Internet!). In the previous assignment, you should have configured the ATLA host with the address X.107.0.1 and a default route that allows it to respond to the matrix host. If this was not properly configured, your AS will never turn green (which will be a sad experience).

2.3.3 Measurement Container

We have created a measurement container that is connected to all Tier-2 networks and *allows you to run a traceroute from any of these ASes* (not necessarily your own) to any address. NOTE: it is not connected to Tier-1 or stub ASes.

You can access the measurement container using ssh

```
ssh -p 52099 root@mini.cms.waikato.ac.nz
```

The ssh password is posted on Moodle in the assignment description. Everyone in the class shares this container, so *please be careful* not to change the configuration of this container. Always close your ssh sessions cleanly, by typing `exit`.

You can launch a traceroute using the `./launch_traceroute.sh` command. For example, to ping from AS 10 to the IP 22.151.0.1 use:

```
./launch_traceroute.sh 10 22.151.0.1
```

This container is connected to every Tier-2 network via the HAML router. The interface is pre-configured with an address. From the last assignment, OSPF will be sharing the measurement network (X.0.199.0/24) to your entire AS (this does assume that OSPF is configured properly in your network).

2.3.4 BGP Analyzer

The BGP Analyzer tool helps you check your BGP policy by letting you know of routes that you are advertising to peers or providers that you are paying for. BGP Analyzer periodically updates from the live routing tables, so it can take a while (5-10 mins) until it verifies a change. Do not rely solely on this tool; recall that a change in your neighbours' policy may change the prefixes you advertise.
`https://mini-internet.cms.waikato.ac.nz/bgp_analyzer/analysis.html`

2.3.5 DNS

Your LOND router has a DNS server attached. Your hosts are pre-configured to use this DNS server. This DNS server will provide you with *reverse DNS lookups* for tools such as traceroute and ping if you run them on the host. As you have already configured OSPF, this should just work, otherwise ensure that OSPF is sharing the DNS route (198.0.0.0/24).

3 Configuration

This is where the actual assignment begins. Carefully follow the numbered steps to configure BGP on your network.

3.1 Keeping Notes

We recommend that you keep a very organised track of the commands that you use for each step in this assignment. (You can use the history command in the bash shell to show a list of commands you have used. You could redirect it to a file, e.g.

```
history > recent-commands.txt
```

You'll find you often will need to come back to them. And take note of any issues you have and submit this along with your configuration and submit them. These notes do not have to be typed: submitting photos of handwritten notes is fine.

Some steps require you to submit evidence; these are highlighted in **bold text**. Make sure you include the required information in your submission.

3.2 Verify your OSPF Configuration

From the last assignment, you should have a working OSPF configuration providing full connectivity within your AS.

1. Verify that you have full connectivity within your AS and that the corresponding square (from your AS to your AS) in the connectivity matrix is green. If not, correct your OSPF configuration so that your ATLA host can ping to X.0.198.1 and your square on the matrix turns green.

3.3 Configuring Inter-domain (External) Link Addresses

We have assigned the addresses for you to use on your inter-domain (external) links. You will find a file named `as_connections.txt` here `https://mini-internet.cms.waikato.ac.nz/as_connections.txt`.

Scroll through the file until you find your AS number in the left column. For example, if you are AS 10, you will find the following lines (not so nicely formatted):

```
10 ATLA Provider 11 HAML   Customer 179.0.76.1/30
10 BOST Customer 8   ZURI   Provider 179.0.67.2/30
10 HAML Customer 7   ATLA   Provider 179.0.65.2/30
10 LOND Customer 8   TRGA   Provider 179.0.68.2/30
10 NEWY Peer     126 IXP126 Peer     180.126.0.10/24
10 PARI Peer     9   PARI   Peer     179.0.73.2/30
10 TRGA Provider 12 LOND   Customer 179.0.75.1/30
10 ZURI Provider 12 BOST   Customer 179.0.74.1/30
```

From left to right, these are 1) your AS number; 2) your router with the inter-domain link; 3) the type of BGP relationship (your AS is either a customer/provider/peer of the neighbour AS); 4) the AS number of your neighbour; 5) the router in the neighbour AS; and 6) the address you need to configure on your interface.

For example, the following line

```
10 HAML Customer 7   ATLA   Provider 179.0.65.2/30
```

means that your router HAML is a *customer* of ATLA router *provider* in AS 7, and that you should assign the address 179.0.65.2/30 on the interface `ext_7_ATLA`, which connects to ATLA in AS 7.

The interfaces for inter-domain links are named `ext_<external AS>_<external router>`. However, you can also check on the router (`show interface brief`) and look for the `ext_*` interface. In contrast, router NEWY is always connected to an IXP and its interface is instead named `ixp_<AS>` e.g. `ixp_126`. These links match with the Internet topology, shown in Figure 2, and your internal topology, shown in Figure 1.

2. Following the guidance above and in the `as_connections.txt` file, assign an IP address to each of the interfaces with an inter-domain link (external). NOTE: you have *one* address to assign per router, for a total of eight addresses (do not overdo it!).

3.4 Establishing iBGP Sessions

In order to become familiar with configuring BGP sessions, start by configuring iBGP sessions between your routers. As you control both routers in an iBGP session, it is easier to debug and see what is going on. By default, iBGP only shares routing information received via an eBGP session. NOTE: until you configure BGP to share your network prefix (your X.0.0.0/8), these iBGP sessions will *not* share any routing information. You will share your network prefix later in step 13. So, for the time being, you will see no actual effect apart from being able to see the connections between your routers.

3. Configure internal BGP sessions between all of your routers. You will need to establish a full-mesh in which every router has an iBGP session with every other router. You will need to configure the following to successfully establish each iBGP session:

   (a) The local AS number;

   (b) The BGP router ID (the router's loopback address, like with OSPF);

   (c) The loopback IP address of the other router;

   (d) Your ASN again (the ASN of what could be a remote AS, but for iBGP, this is again your own AS);

   (e) The local IP address or interface to use in this connection; this is known as the `update-source`. For iBGP `update-source` should be set to the router's loopback address. (If you fail to set this, BGP will connect by default from the address on the closest physical interface, which must match the remote IP address configured by the neighbour router you are connecting to. If the IP addresses were different, BGP would not establish a session.)

   NOTE: at this step, you are *not yet* sharing any routing information over BGP! You have simply established the iBGP sessions.

4. Verify your iBGP neighbours are connected by running
   `show ip bgp summary`
   Also, look at the routes being shared via BGP by running
   `show ip bgp`
   Is this what you expected?

3.5 Establishing eBGP Sessions

In this section, you will configure your eBGP sessions, starting with the IXP. You configure these in much the same way as iBGP, but you will configure a different "remote AS". NOTE: because you are establishing these connections with others in your class, they might not have configured their router yet, so the session might not be established yet despite you doing everything correctly. However, you should be able to establish the eBGP session with the IXP route server immediately, so *configure this first* and ensure it is working before you configure your other eBGP sessions. Again, thus far, we are simply establishing BGP sessions without sharing our prefix yet.

5. On the NEWY router, configure an eBGP session with your IXP route server. The IXPs are assigned the AS numbers from 121 to 126; you are connected to (*only*) one of these IXPs. You can verify the IXP you are connected to by checking Figure 2 or `as_connections.txt`. The router server in your IXP is running on the address 180.X.0.X, where X is your IXP's AS number as usual. Establish an eBGP session to that address.

   You need to set six things:

   (i) The local AS number;

   (ii) The BGP router ID (if you did not already do this when configuring iBGP);

   (iii) The IP address of the other router; for eBGP, we use the *interface address* rather than a loopback address;

   (iv) The AS number for the remote network (e.g. the IXP or another neighbour AS);

   (v) The local IP address that is used for the connection; this is known as the `update-source`. For eBGP, `update-source` should be the address we assigned to the interface with the external link. (By default, FRR will use the closest physically connected interface and will likely pick to correct one. It is always best practice to set this explicitly to avoid any surprises.)

   (vi) A `route-map` to *permit* all routes; follow step 6 next.

6. FRRouting follows RFC 4271, which states that an eBGP session should not accept or advertise routes without an explicit route-map defined. This does *not* apply to iBGP, which will accept and advertise all routes by default. For now, add a "permissive" default route-map that will accept and advertise all routes (BGP policy-agnostic). This will allow

us to import all routes announced by the peers on our IXP as well as to export our routes to the members in the IXP. This is not good, but we will fix this later in step 17.

Follow this example (considering AS 10) to install a route-map that allows all routes. The empty `ALLOW_ALL permit 10` rule matches and permits all routes.

```
NEWY_router# configure terminal
NEWY_router(config)# route-map ALLOW_ALL permit 10
NEWY_router(config-route-map)# exit
NEWY_router(config)# router bgp 10
NEWY_router(config-router)# neighbor 180.126.0.126
 ↪  route-map ALLOW_ALL in
NEWY_router(config-router)# neighbor 180.126.0.126
 ↪  route-map ALLOW_ALL out
```

7. Verify the eBGP connection with the IXP is established using
   `show ip bgp summary`
   Also, take a look at NEWY's BGP routing table using
   `show ip bgp`
   Does this show what you expect? Remember this shows the BGP routes you are *accepting* from your neighbours and not the routes you are exporting to them.

At this point, you have still not advertised routes for your own network into BGP. Let's fix that now. The easiest way to advertise our routes into BGP is to simply advertise *all* of our OSPF routes into BGP, by using `redistribute` to redistribute routes. Advertising OSPF routes into BGP is not recommended on a real network, as it fills BGP with many small prefixes rather than a single summary prefix for your entire network (this pollutes tables). Regardless, it is an easy way to advertise our network; we will fix this later.

8. Configure *only* the router NEWY to `redistribute` OSPF routes into BGP. NEWY is connected to all other routers in your AS; this will propagate over iBGP the OSPF routes to all of your routers. Do not redistribute OSPF on any other routers. You will remove this later.

9. Verify that you are exporting and importing BGP routes. Check that your iBGP mesh is carrying the routes learnt from the IXP via eBGP to the other routers on your network. Do so by checking their routing tables. Check that the IXP has imported your routes by checking its looking glass website. NOTE: the IXP will *not* advertise your routes to other AS members in the IXP until the BGP communities are added to the announcements, which is only done later in step 17 .

10. Following the example for the IXP, configure one eBGP session to each of your 7 neighbouring ASes. You have one eBGP session per router to establish, consisting of 3 customer links, 3 provider links, and 1 peer (and peering with the IXP). Refer to the file `as_connections.txt` and

Figures 1 and 2 to find your neighbouring ASes. You need to establish your eBGP session with the IP address (part of a /30) on the other end of the external, inter-domain link. For example, if you are AS 10, you would have configured 179.0.65.2/30 locally on HAML interface ext_7_ATLA. This means the remote IP address for the eBGP session is 179.0.65.1 and the remote AS is 7. If the neighbour is a Tier-1 or Stub AS, the BGP session should establish right away as these are pre-configured. Otherwise, eBGP sessions to Tier-2 neighbours will only establish if your classmate has successfully completed this same step on their AS. Note: you will not lose marks if you cannot establish a connection because your neighbour has not configured their AS.

11. Verify your eBGP sessions are established using the
    `show ip bgp summary`
    command. Also, verify that the routes learnt from eBGP are being shared via iBGP to all of your routers by checking the routing table (recall that in an earlier step we established a mesh of iBGP connections among routers). Refer to Appendix B.6 for more information about FRR commands.

3.6 Advertising Your Network Prefix to BGP

Thus far, you have established all the BGP sessions you will need. But you are advertising your network to the Internet as many small /30 and /24 prefixes. This is inefficient and means all other routers on the Internet need to carry these routes (you are inflating all the routing tables). So, next, you will replace your BGP advertised prefixes with a single /8 network prefix for your entire network (it is what we studied in the lectures, see slides with “route aggregation”).

At this stage, we also need to create a “blackhole route” for our /8 prefix, because FRR will not advertise a route to BGP that does not exist in its routing table. A blackhole route is a way to tell the router that when it needs to forward packets that match this prefix, they should be *discarded*. At first sight, this may sound like a really bad idea, but remember that *longest prefixes match first*. So, a blackhole for your whole /8 prefix will only match packets destined for parts of your network that you do *not* have more specific (/9 or longer) routes. In other words, it will discard packets addressed to those parts of the network that do not exist. Additionally, if you don't add a blackhole route for your prefix, when the router receives a packet for an address in a subnet that is not used in your network, it could send it to another router advertising the /8 prefix. At best, this is wasteful and, at worst, it creates a routing loop!

12. Now it is the time to remove the redistribution of OSPF routes into BGP (which happens at NEWY router). You can reverse FRR configuration by putting a `no` before the command.

13. Configure BGP to advertise your /8 prefix. When you announce your /8 from one router, iBGP will carry your prefix to all other routers in your AS. This works, but for resilience, you should advertise your /8 prefix from *all* of your routers. This way you avoid the router advertising your prefix becoming a single point of failure.

    NOTE: a further step is required to advertise our prefix through the IXP. The IXP uses BGP communities to filter which peers it advertises routes to. You will address that later, in step 17.

14. On each router, add a blackhole route for your whole /8 prefix.

15. Verify your configuration has worked. First, check that the blackhole route is showing correctly in the routing table. Second, check that your /8 prefix is being advertised via BGP. You can use
    `show ip bgp neighbors <IP address> advertised-routes`
    to check.

16. (Wait some 10 minutes and then) check the connectivity matrix to see which networks have become reachable. The matrix takes some time to update; so, for a more immediate test, you might want to try running pings from a host to the router's loopback address (such as AS.151.0.1) on ASes that are connected now. It is best to ping from a host (pinging from a router might use the source IP address from an inter-domain link that you are not advertising over BGP, and it may be unreachable by the remote AS). I may be expoting my route correctly, but how do I know my neighbour has imported my route? You can use the Looking Glass (Section 2.3.1) to verify your prefix is in your neighbour's route table.

3.7 Advertising your BGP Prefix to IXP Peers

The IXPs are configured to filter which peers they announce a BGP prefix to based on the BGP community value associated with the route. Therefore, you need to specify BGP community values on the route advertisements you send to the IXP. As discussed in the lectures, a BGP community value (of default type) is comprised by two 16-bit values separated by a colon (in some communities, because ASNs are now 32 bit, the coding is different). A route can have multiple BGP community values associated with it (like multiple "tags"). To advertise your network prefix through the IXP with the AS number Z to the peer with the AS number X, you must add the community value Z:X.

Check the examples presented in the lecture and visit the links (to the right place in the FRR manual) available on the slides. Also, refer to the mini-Internet tutorial[2] on `route-maps` to help you with this step. Take a moment to read the tutorial before attempting the next steps.

[2] `https://github.com/rsanger/mini_internet_project/wiki/2.5.6-Configure-BGP-policies`

17. On NEWY router, create a route-map named `IXP_out` that *matches all routes* and *sets* a list of BGP communities that tell the route server to advertise the routes to your IXP peers. You should only advertise to your peers in the "opposite block" to your own (oposite may be 90 degrees), as within your "block", you have customer+provider relationships to honour. For example, if you are AS 10, you should set the community values 126:71, 126:73, 126:75, 126:77, 126:79, 126:81, and 126:83. AS 10 should *not* announce to AS 8 and any other in the same block via the IXP.

18. Now you have created the route-map you need to apply it to your BGP session with the IXP. Apply the route-map in the `out` direction to apply it to all routes that you advertise to the IXP.

19. Check that you are advertising your prefix to the stub and Tier-1 ASes (and any other BGP sessions which you have established) in the opposing block. You can use the looking glass, connectivity matrix, and ping to confirm.

20. **Save a backup of your configuration at this step (see Appendix A.3). Name the archive `step-20-config.zip` and include it in your submission.**

3.8 Applying Policy

Currently, you are not filtering the routes which you are advertising through BGP. By not filtering routes, you will be paying to carry traffic for networks that are not paying you (i.e. your peers) over links that cost you money (i.e. your providers). Remember that in BGP routing decisions are often made based on financial relationships rather than the best path.

The goal of this section is to only advertise your network prefix and customer routes to all of your BGP neighbours. You must advertise to your customers *all* routes you learnt from the Internet. However, do not advertise routes learnt from peers or providers to each other, including between two providers or peers. This would provide your peer free transit using your upstream which you are paying for. Recall the route leaks discussed in the lectures. Note that the ASes connected through the IXP are all considered peers. You can use the BGP Analyzer (§ 2.3.4) to help.

One way to apply this policy is to tag incoming routes with an "informational" BGP community value indicating if they are a customer, peer, or provider (check BGP communities in the slides). Then, filter outgoing routes based on where they were learnt from (e.g. do not announce to peer a route learnt from another peer). To implement this policy, you will need to use route-maps. This new route-map will replace your `ALLOW_ALL` and `IXP_out` route-map, so ensure they also include that existing behaviour such as advertising communities to the IXP.

21. Apply BGP policy so that you only carry traffic through your network on behalf of your customers. But, don't carry traffic through your network on behalf of your peers or providers as this just costs you money.

    Include a short report named `bgp-policy.txt` or `bgp-policy.pdf` with a brief description of how you applied this policy. Include a before and after snapshot of `show ip bgp neighbors <address> advertised-routes` (or a looking glass snapshot) that shows that your configuration has worked.

22. You are done. Look over your configuration by using the `show running-config` command and clean up anything extra. Remember that you can use the `no` command to delete blocks of configuration.

    Include a copy of your router configuration (see Appendix A.3) and name it `final-config.zip` in your submission.

4 Assessment

This assignment is assessed entirely on success and correctness. Though you will not be penalised for not being able to connect to a neighbour if they have not configured their network. The marks will be allocated as shown in table 1.

Steps	Description	Marks
1 – 2	Interfaces and OSPF configured	1
3 – 4	Established iBGP sessions	2
5 – 11	Established eBGP sessions	1
13 – 15	Advertise your prefix over BGP	1
17 – 20	IXP communities	3
21 – 22	Policy-based routing	2
		10

Table 1: Distribution of Marks

Your assignment must be submitted electronically using Moodle. You may submit either a set of files or an archive containing multiple files made using `tar` or `zip`. Please do not use a different archive program (like 7z for example).

Your submission **must** include:

- A note of which steps you completed and any issues you encountered. Put this note in a separate file called `steps-done.txt`.
- Final, full and unmodified router configurations for all routers saved using `./save_configs.sh` as described in Appendix A.3. Rename the archive to `final-config.zip` before uploading.
- Router configuration after configuring BGP communities to advertise your prefix to your IXP peers from step-20, named `step-20-config.zip`.
- A description of how you applied BGP policy in a file named `bgp-policy.txt` or `bgp-policy.pdf`, with an example of the policy working.
- *Optionally*, incomplete configuration. Include a note in `steps-done.txt` as to what this covers. Name this `ic-config.zip`
- *Optionally*, a `notes.txt` or `notes.pdf` file containing any notes you have taken.

5 Final Checklist

Check you have:

- □ Used the correct IP addresses on your external links as described in Section 3.3.

- □ Submitted, via Moodle, which steps you completed in a text document named `steps-done.txt`.

- □ Submitted, via Moodle, router configuration files after connecting to the IXP with the name `step-20-config.zip`

- □ Submitted, via Moodle, your final router configuration with the name `final-config.zip`

- □ Submitted, via Moodle, a description of how you have applied policy in a file named `bgp-policy.txt` or `bgp-policy.pdf`

- □ *Optionally*, submitted, via Moodle, incomplete router configuration with the name `ic-config.zip`. Make sure you detail in `steps-done.txt` how far you got

- □ *Optionally*, submitted, via Moodle, a file named `notes.txt` or `notes.pdf`

- □ Reread the submission instructions above

Appendices

A The mini-Internet

A.1 Accessing the mini-Internet

These are the same instructions as before. You can access the mini-Internet using the secure shell (ssh) command either from home or the lab. One host within your network is pre-configured with a secure shell server which is exposed on a unique port on `mini.cms.waikato.ac.nz`. Your unique port number is 52000 added to your AS number. We have sent out an email to everyone individually with corresponding AS number and password. Don't share your password with anyone else. Don't change this password. If you want to simplify access, please set up an SSH key instead, details of which are included in the first lab.

The command to connect to the mini-Internet is:

```
ssh root@mini.cms.waikato.ac.nz -p <your ssh port number>
```

A.2 Accessing Routers and Hosts

Using the `./goto.sh` script in the proxy container you can access any router or host you wish. You can always see the container you are logged into by looking at the hostname on the left of your terminal. To exit any container back to the proxy you can press `ctrl+d` or type `exit`. You can (should) log in to multiple hosts or routers at once, or even the same one twice.

Accessing routers: Access a router using `./goto.sh <router name> router`. For example to access the router HAML:

```
root@gXX-proxy:~# ./goto.sh HAML router
```

Now you are in the FRRouting CLI on the router HAML.

Accessing hosts: Each location shown in Figure 1 has a host attached directly to the router. To access the host attached to a router, use the command `./goto.sh <router> host`. For example, to access the host directly connected to the NEWY router, use:

```
root@gXX-proxy:~# ./goto.sh NEWY host
```

Now you are in a standard Linux shell, where you can run commands like `ip` just as you have done in the lab exercises.

A.3 Backing Up Your Configuration

You can create a backup of the running configuration on your routers using the `./save_configs.sh` command on the proxy host. `./save_configs.sh` will create a folder configs_[date]_[time] and a zipped version of that folder. You should keep regular backups of your configuration. You will also need to submit this zip file as the final version of your configuration.

You can copy this off the proxy host by running at the linux-labs host the `scp` command. For example on your home or lab machine run:

```
linux-labs$ scp -P <port number> \
    root@mini.cms.waikato.ac.nz:<config name>.zip ./dst/path/
```

Note: you supply the port number to `scp` using the capital '-P' option, rather than the lowercase '-p' like with `ssh`. In the command above, '\' splits this long line across two, a terminal will remove the '\' and run the command as if it was on a single line.

B Testing and Troubleshooting

B.1 Useful FRRouting Debugging Commands

Troubleshooting in FRRouting is run from enable mode (not configuration mode) most often using commands beginning with `show`.

? View the commands available to you, in any mode

<tab> Try and auto-complete a command, will list known options like interfaces names or addresses etc.

show running-config Show your configuration

show ip route Show all routes learnt from any source

show ip bgp Show all routes learnt from BGP

show ip ospf Show all routes learnt from OSPF

show ip bgp summary Shows the status of your BGP neighbours

show ip bgp neighbors <address> routes Show the routes received, after route-map filtering, from this neighbour

show ip bgp neighbors <address> advertised-routes Show the routes you are advertising to this neighbour, after route-map filtering

show ip bgp route-map <name> shows the result of applying this route-map to your routing table, i.e. what this route-map would advertise.

ping + traceroute Like the Linux tools, without option support (e.g. -n)

B.2 Ping and Traceroute

`Ping` and `traceroute` are often the starting point of debugging. For example, what can you reach and what can't you? Can you ping to each interface along the path you expect the packets to follow.

`Traceroute` is also very helpful. Remember, though, that traceroute shows the forward path only and that a failure at a particular hop may be because the *reply* packets can not get back to the source. You may find that some machines do not reply to the traceroute itself even though you can ping them.

B.3 Forwarding and Route Information

The command (from enable mode) `show ip route` shows the routers forwarding table. This includes the routes that have been selected from the various routing protocols, static routes and directly connected networks. The selection is done, in part, using the *administrative distance* which is a priority. See the last few slides of the BGP lecture notes for a discussion of how routes are selected for inclusion in the forwarding table. Note that the source of the route is included in the output.

The command
`show ip route bgp`
shows the routes in the forwarding table that have come from BGP (but not all of the routes that BGP knows about…see the BGP Information section below for that). Similarly,
`show ip route ospf`
shows routes selected from OSPF.

B.4 Traffic monitoring

You can run `tcpdump` on any of your hosts to capture traffic. This is, of course, limited to only seeing traffic arriving at that host (or departing from).

B.5 OSPF Information

A few useful commands:

- `show ip ospf`: prints information about the OSPF area;
- `show ip ospf neighbor`: shows what neighbours OSPF is communicating with. It is a good quick check if something seems not to be working with OSPF.
- `show ip ospf interface`: shows the instance of OSPF that is communicating over the subnet attached to that interface. It includes, for

example, the number of neighbours found and the identity of the DR and BDR.

- `show ip ospf route` and `show ip ospf database`: show the information that OSPF knows about the network, including all the prefixes that it has learned.

B.6 BGP Information

- `show ip bgp summary`: shows what neighbours BGP is communicating with and statistics about the connection. It is a good quick check if something seems not to be working with BGP.
- `show ip bgp neighbors`: shows more detail than the previous command.
- `show ip bgp summary`: check the number in the `State/PfxRcd` column; if the column shows a state of `Idle` then you likely have a mismatch with your neighbour. If you see `Active` if your neighbour has not configured BGP yet.

Probably the most important BGP information is given by the command
`show ip bgp`
which shows the list of BGP paths that the route is seeing, including the AS path. For example the entry:

```
*  172.16.128.0/21  192.168.127.246           0 64999 65001 i
*>                  10.254.254.253            0 65111 65001 i
```

means that BGP knows two ways to reach the 172.16.128.0/21 subnet. One is via AS65001 then AS64999, the other is via AS65001 then AS65111. The route chosen by BGP is marked with `>` at the left, which in this case is the second one.

The command
`show ip bgp regexp 65111`
will show just those paths that include AS65111.