

The exercises are designed for students to finish in an individual capacity. The exercises are not designed to be completed in tutorial sessions but rather to give you some tasks and a starting point to continue and complete on your own.

1 Lab Tasks

Border Gateway Protocol (BGP) is the standard exterior gateway protocol designed to exchange routing and reachability information among autonomous systems (AS) on the Internet. It is the “glue” of the Internet, and is an essential piece of the Internet infrastructure. It is also a primary attack target, because if attackers can compromise BGP, they can disconnect the Internet and redirect traffics.

In this lab we are demonstrating BGP hijacking attacks. Open a terminal in your VM and run the following command to download and install the BGP project.

Run the command below on the GNS3 VM shell to download the project. If you SSH into the VM from your host OS terminal, you can simply copy and paste the command instead of typing it manually.

```
gdown 1PVQrHZM3k2JyzjmUMS_u2NSI1heHUMEq ; sudo bash ./install_BGP.sh
```

Alternatively, you can use the link below to download the same project. However, if you are connected to the **Monash Wi-Fi**, this method may not work. In that case, please use a mobile hotspot. (single command)

```
wget https://sniffnrun.com/install_BGP.sh --no-check-certificate ; \
sudo bash ./install_BGP.sh
```

BGP project should now appear in your GNS3 projects library. Open BGP project and start all nodes in the network.

1.1 Network Diagram

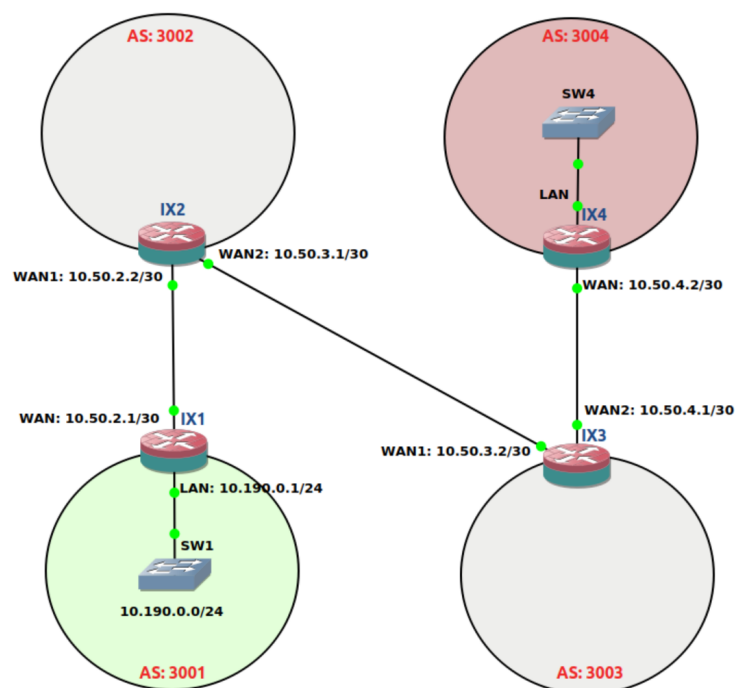


Figure 1: Network Diagram

Above is a network of 4 routers at 4 different Internet Exchanges (IXs). Run the below command on the routers to view the routing table of each router. You should only see the networks connected to each router

directly. This is because we still haven't configured BGP or any other routing protocol on these routers. Username for all routers is **admin** with blank password.

```
ip route print
```

2 Configuring BGP

Group Discussion: What are the functions of the following BGP terms? Autonomous System (AS), Autonomous System Number (ASN), AS PATH, BGP Speaker, BGP Peer.

2.1 Configure BGP Instance

A BGP instance is a single BGP process running on the router. A BGP router can run multiple BGP processes. Each BGP process corresponds to a BGP instance. Discuss with your tutor why multiple BGP instances would need to be configured on a single router.

We need to configure a BGP instance on each BGP router. Each BGP instance is configured with an ASN. Different BGP instances on the same router can have the same AS number but cannot have the same name. Instance name is unique in a router. A router ID is the unique identifier of a BGP router in an AS.

Configurations on **IX-1**:

```
/routing bgp instance add name=DATA router-id=10.50.2.1 as=3001
```

Configurations on **IX-2**:

```
/routing bgp instance add name=DATA router-id=10.50.3.1 as=3002
```

Configurations on **IX-3**:

```
/routing bgp instance add name=DATA router-id=10.50.3.2 as=3003
```

Configurations on **IX-4**:

```
/routing bgp instance add name=DATA router-id=10.50.4.2 as=3004
```

2.2 Configure BGP Peers

To exchange routing information between two BGP systems, it is required to configure a peering on both BGP speakers first. Use the following commands to configure peering with neighbours on each BGP speaker.

Configurations on **IX-1** (one command):

```
/routing bgp peer add name=PEER_T0_IX2 remote-address=10.50.2.2 remote-as=3002 \  
instance=DATA
```

Configurations on **IX-2**(two commands):

```
/routing bgp peer add name=PEER_T0_IX1 remote-address=10.50.2.1 remote-as=3001 \  
instance=DATA  
/routing bgp peer add name=PEER_T0_IX3 remote-address=10.50.3.2 remote-as=3003 \  
instance=DATA
```

Configurations on **IX-3**(two commands):

```
/routing bgp peer add name=PEER_TO_IX2 remote-address=10.50.3.1 remote-as=3002 \  
instance=DATA  
/routing bgp peer add name=PEER_TO_IX4 remote-address=10.50.4.2 remote-as=3004 \  
instance=DATA
```

Configurations on **IX-4**(one command):

```
/routing bgp peer add name=PEER_TO_IX3 remote-address=10.50.4.1 remote-as=3003 \  
instance=DATA
```

2.3 Configure Redistribution

Route redistribution allows BGP speakers to advertise the routes learned from different routing protocols to its BGP peers. You can redistribute routes learned from OSPF, RIP, other BGP Peers, statically configured routes and routes from directly connected interfaces.

Configure the following on each BGP router to redistributed routes learned from other BGP peers and directly connected routes. Before proceeding, start packet capturing on the link connecting **IX-3** and **IX-4** to capture the BGP UPDATE messages.

Configurations on **IX-1, IX-2, IX-3, IX-4**(two commands):

```
/routing bgp instance set redistribute-other-bgp=yes 1  
/routing bgp instance set redistribute-connected=yes 1
```

2.4 Advertising Networks

You can also advertise routes directly to BGP without redistribution. Run the following command on the **IX-1** to advertise 10.190.0.0/24 network.

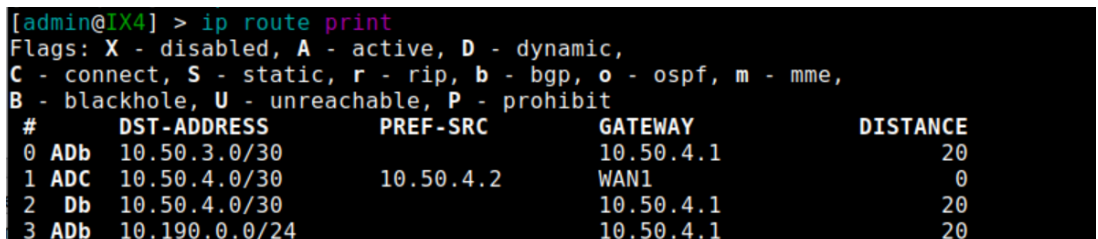
Configurations on **IX-1**:

```
/routing bgp network add network=10.190.0.0/24
```

Examine the BGP UPDATE message using Wireshark to identify the attributes and their values.

2.5 Testing

Run the following command on all routers to see if they have learned network 10.190.0.0/24 advertised from **IX-1**.



```
[admin@IX4] > ip route print  
Flags: X - disabled, A - active, D - dynamic,  
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,  
B - blackhole, U - unreachable, P - prohibit  
#    DST-ADDRESS    PREF-SRC    GATEWAY          DISTANCE  
0 ADb 10.50.3.0/30      10.50.4.1    20  
1 ADC 10.50.4.0/30      10.50.4.2    0  
2 Db  10.50.4.0/30      10.50.4.1    20  
3 ADb 10.190.0.0/24     10.50.4.1    20
```

Figure 2: Routing Table on IX-4

Configurations on **IX-4**:

```
/ip route print
```

Try pinging 10.190.0.1 from IX-4 router to confirm the routes are communicated.

3 BGP Prefix Attack

BGP Route Hijacking, also called prefix hijacking, is a typical attack on BGP. In this attack, the attackers' BGP routers announce the IP prefix that are not assigned to them, so the traffic to this IP prefix can get rerouted to the attackers, who can intercept or modify the traffic. Many of the incidents on the Internet are caused by such an "attack", although they are mostly caused by the mis-configured BGP routers.

3.1 Launching the Prefix Hijacking Attack from AS-3004

In this task, we will launch the prefix hijacking attack using a BGP router in AS-3004. Our goal is to hijack the IP prefix owned by AS-3001. If the attack is successful, all the packets going to AS-3001 will be maliciously rerouted to AS-3004.

We can achieve this by falsely announcing ownership of the 10.190.0.1 network but with a more specific prefix. First we will configure the LAN interface on IX-4 router with the IP 10.190.0.1/27.

Note: Before starting the attack, we will start Wireshark packet captures on 2 links. One on the link connecting IX-1 and IX-2 and the other on the link connecting IX-3 and IX-4. Start a PING from IX-3 router to the IP 10.190.0.1. You should see the ICMP packet on the first Wireshark window.

Configurations on **IX-4**: Configurations on **IX-4**:

```
/ip address add address=10.190.0.1 netmask=255.255.255.224 interface=LAN
```

Now we can advertise the subnet with a longer and more specific prefix (/27), so BGP will redistribute that subnet to it's peers as a better path to reach 10.190.0.1/27. Because we configured redistributing connected traffic in step 2.3 you may see the network advertised in BGP even without running the below command.

Configurations on **IX-4**:

```
/routing bgp network add network=10.190.0.0/27
```

If the attack is successful, ICMP traffic should switch to the second Wireshark window as traffic should be routed to IX-4 instead of IX-1.

3.2 Fighting Back from AS-3001

AS-3001 has a detection system. After the attack was launched, it immediately detected the attack. It tried to contact the operators of AS-3003, which is the upstream service provider for AS-3004, asking them to block the attack. Unfortunately, it was midnight for AS-3003's operators, so nobody could be reached. The loss of the service is very significant, so the operators of AS-3001 decide to fight back: they want to "steal" back their own network prefixes, without the help of AS-3003. Reconfigure the BGP routers of AS-3001, so you can get the traffic back.

3.3 Fixing the Problem at AS-3003

Eventually, the operators of AS-3003 are reached. Without knowing whether this is a misconfiguration on the AS-3004 side or an intentional attack, AS-3003 decides not to cut the peering with AS-3004, so the users of AS-3001,3002 and 3003 can still reach the other locations through AS-3004. However, AS-3004 must stop the propagation of the fake announcement. This can be done by removing the fake routes from its own announcement to its own peers. More specifically, AS-3003 can add some code to its filters, so the fake routes can be discarded. We need to configure prefix filters on AS-3003 to reject only the fake announcements from AS-3004.

3.4 Prefix Filtering

Using filters, we can block the prefixes with longer lengths than 24 on 10.190.0.0 network coming from IX-4 router. Use the below commands to create a filter with the name in-3004 and then attach it to the peer IX-4 configurations on IX-3 router.

Configurations on **IX-3**(three commands):

```
/routing filter add chain=in-3004 prefix=10.190.0.0/24 prefix-length=23-32 \  
action=discard  
/routing bgp peer print  
/routing bgp peer set rule_id in-filter=in-3004
```

Update the rule_id attribute in the last command to match the remote peer list entry for AS-3004.

Run the below command on **IX-1**, **IX-2**, **IX-3** routers to observe the effect of the above filter:

```
/ip route print
```

4 Group Discussion Points

1. Discuss how Resource Public Key Infrastructure (RPKI) can help to secure BGP and internet.
2. How does BGPsec differ from RPKI?

Reference: Mikrotik Documentation.