Lab 5 (Updated): BGP routing

50.012 Networks

Hand-out: 6 April
eDimension hand-in: 18 April (Tuesday 23:59pm)

1 Objectives

- Get first-hand experience about how a routing protocol works.
- Get familiar with BGP.
- Discover more about mininet and learn about its basics.
- This lab is an exploratory lab, there is no extensive programming needed, only editing config files. The entirety of this lab can be done through basic command-line text editors like `vi` or `nano`, save for the occassional pcap analysis in wireshark (if you really love command line, you could even use `tshark`, the CLI equivalent). The estimated time to complete this lab is 1-2 hours.

2 Experiments

2.1 Setting up the environment

- You can either use the pre-made VM or install mininet and the frrouting package on your own linux VM.

2.1.1 Pre-made VM

- Download and import the pre-made VM into Virtualbox. Depending on your available system resources, you may need to decrease its allocated CPU and RAM resources.
- Configure port-forwarding on the Virtualbox appliance to allow yourself to SSH into the virtual machine. This is needed to open multiple terminal windows and to transfer files to/from the virtual machine. By default, it forwards host port 2222 to guest 22.
- There is no GUI/desktop environment for this VM. Transfer files using your IDE's FTP client or the command line `rsync` client in WSL/unix-like systems. If using rsync, you might need to configure your OpenSSH hosts config to direct it to use the non standard ssh port 2222. If using WSL, note that the WSL networking stack is *not* the Windows networking stack where Virtualbox is running on, so you should not be connecting to `localhost` on WSL: see this article for details on how to connect to Windows networking applications from WSL.

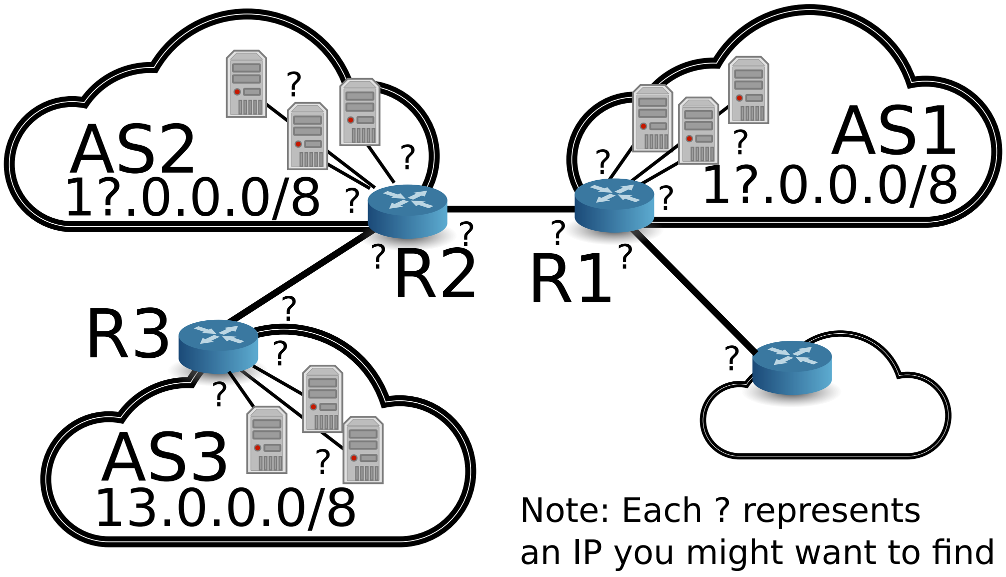
- This VM has python3 installed and all the required python packages are installed in the system wide `site-packages` directory. As with most linux distros, you need to specify `python3` instead of just `python` when running python scripts.
- While working as root user all the time is bad security practice, for the purpose of this lab, since mininet requires root you can just login as the root user and do all your work as root.
- The lab folder must be in a directory that is accessible to public (e.g. world has read permissions set) because the routing daemons switch to the non-priveleged user `frr`. This means you cannot upload/unzip the lab contents into the root user's home directory. For example, you could work in `/var/lab5` because `/var` is world-readable.

2.1.2 Building your own VM

- Review the `install.sh` file to install `mininet` and `frrouting`. Depending on your distro, you may need to build packages from source.

2.2 Getting started

- Start the mininet experiment by running the python file `bgp.py`.
- After starting mininet with the above command, try to find out more about the current topology in mininet using `nodes` and `links` (also note `help <topic>`). use `ip addr show` on the emulated nodes to figure out what interfaces each node has and what addresses they are assigned.
  - Annotate the following figure with the AS's announced prefix (network) and the IP addresses of the routers' interfaces. Please note that the "small" AS is not up yet at this stage, so you can't interact with it much.



- There are also a number of hosts in each network. They are connected to internal interfaces of the BGP routers.

- You can connect to the bgp daemons (`bgpd`) running on the nodes by running a script on the terminal (outside mininet)

```
./connect.sh R1
```

- The password for the `bgpd` is **zebra**.
- The command line interface belongs to `bgpd`, a widely used BGP routing daemon.
- Try out the different offered commands. Type `help` for a quick introduction about the bgpd (FRRouting VTY) console. Here are some common commands that might be useful for this lab:
  - `show ip bgp`
  - `show bgp neighbors`
  - Other commands available at FRRouting's bgpd documentation page

2.3 Observing BGP in action

- Using the mininet cli, use `tcpdump` to capture `.pcap` files of BGP traffic on R1. `R1 tcpdump -i R1-eth4 -s0 -w R1-bgp.pcap tcp port 179`
- Connect to R1's `bgpd` virtual terminal inside another terminal window using the `connect.sh` script. Type `enable` in the bgpd terminal (outside mininet) to enable admin mode (pw: zebra). Note that the prompt changed from `R1-bpgd>` to `R1-bgpd#`.
- Look at current routes with the `show ip bgp` command.
- Type the `clear bgp external` command to clear the exchanged routes.
- Wait for at least 5 seconds for the BGP routers to exchange new routes; then stop `tcpdump` and transfer the `.pcap` file back to your VM host for offline analysis in Wireshark.

2.4 Understanding how BGP affects host reachability

- Currently, h11 can reach h21, but it cannot reach h31. Explain why this is the case by inspecting h11's routing tables `ip route show` and the routing tables R1 received from R2 (use the `bgpd` console)
- Modify the bgpd configuration files of R2 and R3 to allow h11 to reach h31. Hint: R2 and R3 needs to add each other as peering neighbors. Reference R1's configuration file and consult the bgpd configuration section of the frr documentation
  - Tip: If `bgp.py` crashes, you can perform a "hard reset" of mininet using `mn -c`. This *does not* delete your configuration files.
- What does the `next-hop-self force` option do and why is it needed on R2 for AS1 to be able to reach AS3?

- After you ensured that the hosts in AS1 (served by R1) can reach the hosts in AS3 (served by R3), investigate if R1 itself can each the hosts in AS3 using the mininet CLI. Interestingly, invoking the ping command with different options (shown below) have different results. Explain why this is the case with reference your current understanding of the network topology, the routing tables, and the nature of the network layer.
  - `R1 ping h31` does not work, but
  - `R1 ping -I R1-eth1 h31` works.

  .

2.5 Malicious BGP abuse

2.5.1 Scenario

- Assume the following setting: a user from AS1 wants to visit a website on `13.0.1.1` (a host in AS3). A malicious attacker wants to redirect the user to its own webserver instead.
- The attacker has control over AS4, which is BGP-peering with AS1.
- How can the attacker achieve his goal by modifying `bgpd-R4.conf`?

2.5.2 Performing the attack

- Use the provided website script in a terminal (outside of mininet) like this: `./website.sh h11`
  - It will continuously contact a webserver on `13.0.1.1` from h11 (if you have successfully configured R2 and R3 to peer with each other). Leave the script running in that terminal.
- In R1's `bgpd` terminal, confirm that the route to `13.0.1.1` still goes to AS3 through As2.
- Run the `start_rogue.py` script in another terminal. Observe the results of the terminal running `./website.sh h11`
- If you have successfully configured R4:
  - the output of the website contacting script should change;
  - In R1's `bgpd` terminal, confirm that the route to `13.0.1.1` is now going to AS4.
- Running the python script `stop_rogue.py` will stop the attack.

2.5.3 [Optional] Countering the attack

- Suppose you are the owner of AS1 and have control over the `bgpd` configuration of R1. You are forced to peer with AS4 and provide connectivity to its customers due to business contacts, but you know that:
  - AS4's real customer subnet is `14.0.0.0/8`;
  - the owner of AS4 neglects cybersecurity and its R4 `bgpd` is often compromised

- What changes can you make to R1's bgpd configuration to ensure that even if R4 gets compromised again like above, you will not accept "fake" routes from R4; while still being able to provide connectivity to AS4's customers during normal operations?
- Hint: read the FRR documentation on its route-prefix and route-map features
- You can assume that only h41 is the "suspicious" host, while h42 and h43 will have `14.0.0.0/8` addresses.

3 What to Hand in

Submit your bgpd config files for all four routes, and a PDF writeup that includes the following information:

- The network topology as in the earlier figure (you could annotate the provided figure or compile a table):
  - IP addresses of all routers *and its interfaces*
  - Hosts/IPs in the ASess
- Describe in detail the BGP traffic you were able to observe during re-establishment of routes in section 2.3.
- Your answers to all the questions in sections 2.4
- Describe in detail what happened when you started the attack on BGP.
- (Optional) Describe in detail how you can counter said attack in section 2.5.