Border Gateway Protocol

1 Overview

This exercise introduces Border Gateway Protocoal (BGP) fundamentals, allowing students to configure BGP routers and view their behavior. The lab uses Bird routers, which is an open source Linux-based router implementation.

1.1 Background

This exercise assumes the student has received instruction on functions of network routers, and BGP. A tutorial on BGP can be found at: `http://www.cs.fsu.edu/~xyuan/cis6930/APRICOT2004-BGP00.pdf`. It is also assumed that the student is familiar with basic Linux routing, e.g., as explored in the routing-basics and routing-basics2 labs.

This lab exercise only touches on some of the most basic elements of BGP.

2 Lab Environment

This lab runs in the Labtainer framework, available at http://my.nps.edu/web/c3o/labtainers. That site includes links to a pre-built virtual machine that has Labtainers installed, however Labtainers can be run on any Linux host that supports Docker containers.

From your labtainer-student directory start the lab using:

```
labtainer bird-bgp
```

A link to this lab manual will be displayed, along with a link to the Bird router user guide.

3 Lab topology

The lab presents a simplified view of Internet routers implementing BGP. Each router is connected to one or more notional enterprises, respresented by a single computer. In Figure 1, the routers are labled R1-R4. Enterprises are labeled E1-E5. The routers exchange routing information and traffic over point-to-point ethernet links. Each of these links has a network tap that forwards copies of traffic to the `netmon` component (not pictured), which collects network traffic in files within its `/taps` directory.

Note that E2 and E5 share router R2. This might reflect that R2 belongs to an ISP, whose customers include enterprise E2 and enterprise E5.

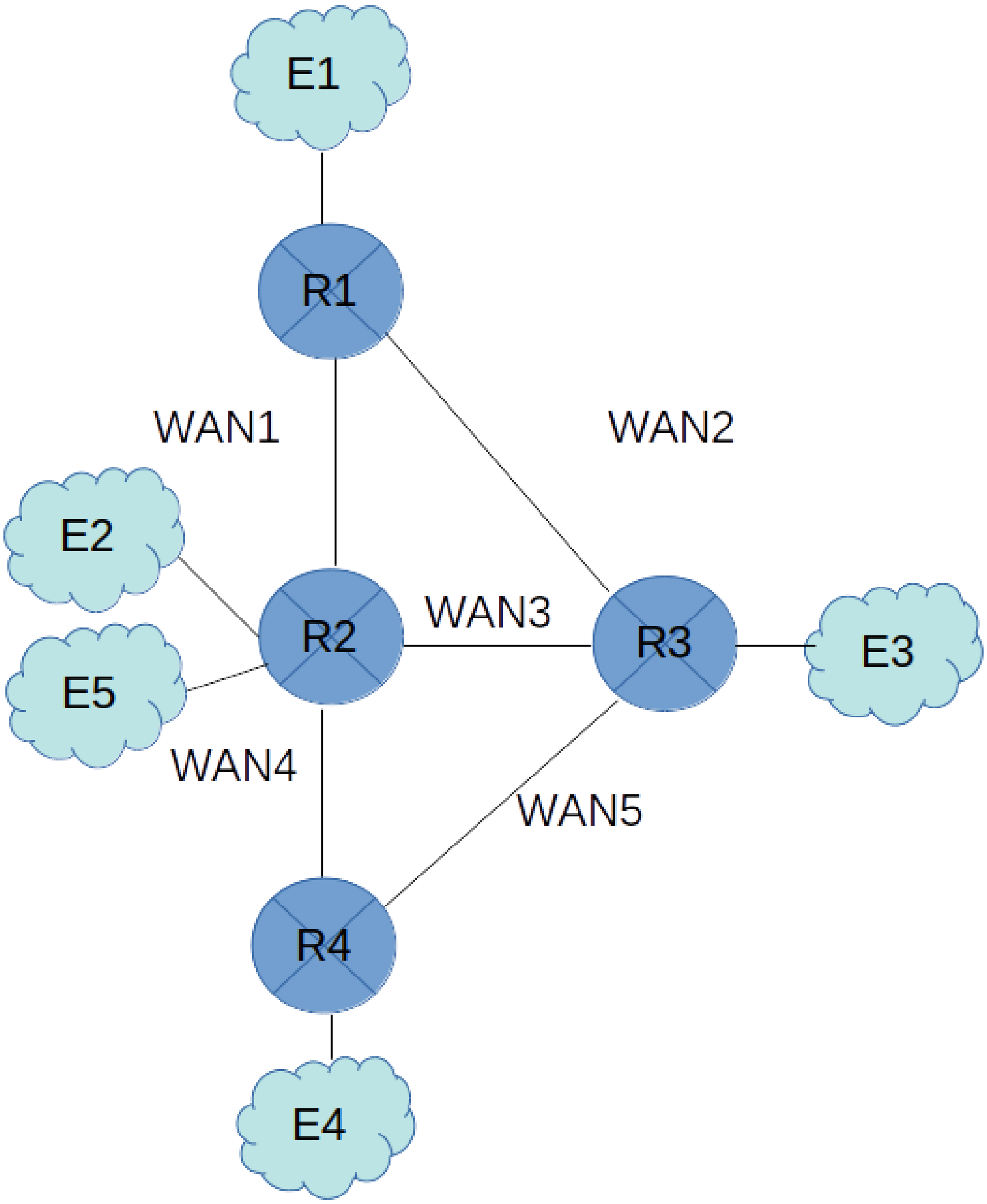

Figure 1: BGP Routing Topology

4 Tasks

4.1 Explore

The following items (among other), are available to explore the network:

- Wireshark and tcpdump are installed on the `netmon` computer, use them to review the PCAP files found in the `/taps` directory. When using Wireshark, if you encounter black or otherwise corrupt pulldown windows, try resizing the window, or restarting the application. The `ctrl-r` key sequence will cause Wireshark to reload the PCAP file that is currently being viewed, i.e., to see the latest traffic.

- The `traceroute` program is install on each enterprise computer. Use that to observe the routes that traffic may take between different enterprise computers.

- Each router includes the Bird client, which you can start using `sudo birdc`. Use it to view routes and protocol definitions. Bird is configured via use of configuration files found at `/usr/local/etc/bird.conf`. The bird service runs under systemd. If you modify a configuration file, you may rstart bird using `systemctl restart bird`.

4.2 Configure routers for R4

By now you should have noticed that E4 cannot be reached from the other enterprise computers. If not, go back and explore!

You are the network administrator for E4, and your task is to configure its router so that it will announce the route to E4 to the other routers. All the other routers are already configured to talk to R4, so you need not modify their configurations. Use the Bird user guide and the existing bird.conf files as examples to modify the R4 bird.conf file.

To demonstration you have configured R4, you must successfully ping E1, E2 and E3 from E4.

Use Wireshark to observe the BGP routing information propagate to the other routers.

5 Submission

After finishing the lab, go to the terminal on your Linux system that was used to start the lab and type:

```
stoplab
```

When you stop the lab, the system will display a path to the zipped lab results on your Linux system. Provide that file to your instructor, e.g., via the Sakai site.

This lab was developed for the Labtainer framework by the Naval Postgraduate School, Center for Cybersecurity and Cyber Operations under sponsorship from the DoD CySP program. This work is in the public domain, and cannot be copyrighted.