Routing: Open Shortest First Path

1 Overview

This exercise introduces the Open Shortest First Path (OSPF) routing protocol, allowing students to configure OSPF-enabled routers and view their behavior. The student will use OSPF to spoof routing tables, leading to malicious mis-routing of traffic.

OSPF is an internal gateway protocol (IGP). The `bird-bgp` lab explored the Border Gateway Protocol (BGP), which is an external gateway protocol (EGP) used within the Internet backbone, e.g., between ISPs. This lab uses routers running the Bird service, 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 OSPF. 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. There are a number of web-based resources describing OSPF. Note however that many focus on Cisco command line syntax and semantics. Look for tutorials that explain concepts and not just rote steps needed to pass a certification.

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

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-ospf
```

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 topology that includes of routers implementing OSPF within an Autonomous System (AS).

In Figure 1, all of the components except those labeled *External* are within one AS. The `BR` router is the border router for the AS. The `BRX` router is the border router for the notional external system. The external system includes a web server, labeled `WX`. In addition to three internal routers, the AS has one server and three workstations.

The routers exchange routing information and traffic over the point-to-point ethernet links. Each such link 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.

This lab primarily names computers using IP addresses. Use of DNS is deliberately avoided to keep the focus on routing.

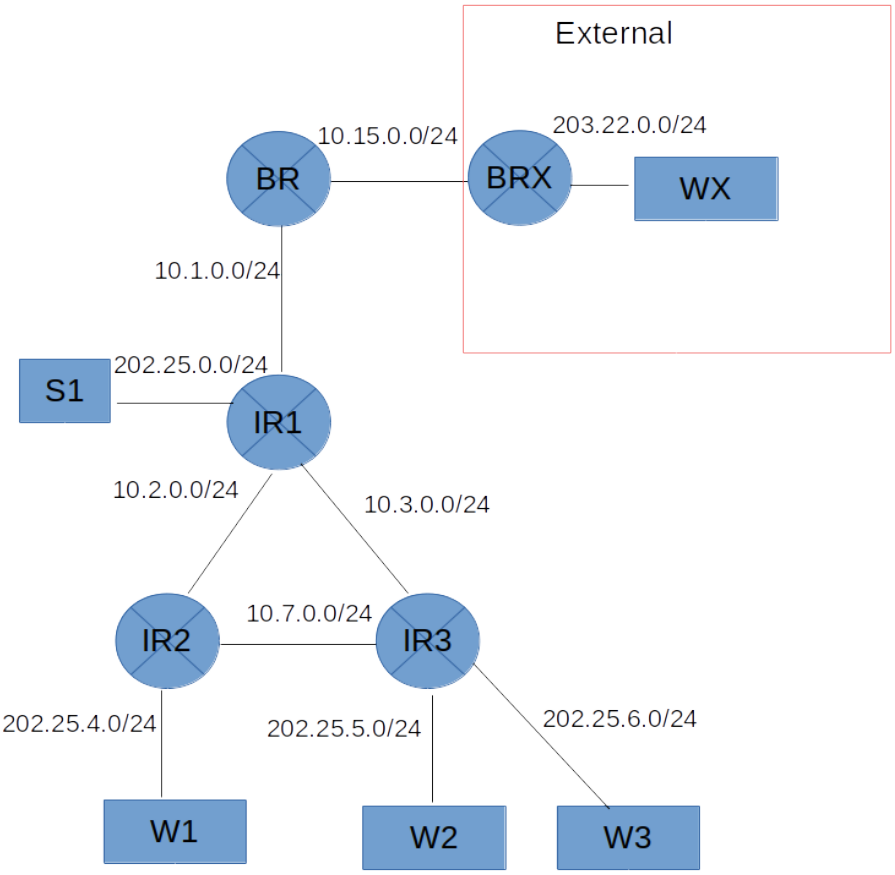

Figure 1: OSPF Routing Topology

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 computer (all components other than routers). Use that to observe the routes that traffic may take between different 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`. The remaining tasks of this lab assume the bird.conf files on each router have not been modified. If you do modify those, either restore them, or restart that lab (using the `-r` option on the `labtainer` command prior to proceeding to next steps.

4.2 Confirm connectivity

Use the `ifconfig` command (or `ip addr`) to determine IP addresses of the different computers. You should be able to ping any computer from any other. You should also be able to use `wget` to retrieve the index.html file from the WX web server.

4.3 Review authentication

Look at the `bird.conf` files and determine the type of authentication used for the OSPF protocol. Then use Wireshark on the `netmon` computer and find the plain text passwords exchanged by the routers.

4.4 Hijack the WX address

Assume you are a hostile user of the W3 workstation, and you would like to intercept traffic bound for the WX web server and replace it with your own. In this step, assume you have no access to the individual routers and have not seen their configuration files.

Playing the role of a potential victim at the W1 computer, use the `wget` command on the `W1` computer to retrieve the default web page from WX and view its content. Use `traceroute` to confirm your expectation of the route those packets will follow.

Now, by only accessing W3 – without directly modifying configuration files or Linux routes on any router – hijack traffic destined for WX and route it to a web server running on W3. Then confirm your change by going to W1 and repeating the `wget` and observe the new web content.

The following are offered as hints:

- The W3 computer contains the bird service. It can be started by running `sudo bird`.
- The loopback device on W3 (`lo` can be assigned alternate IP addresses using

```
ip addr add <addr/mask> dev lo
```

- IP packets entering W3 can be routed to the loopback device using

```
route add <addr> dev lo
```

- The W3 computer contains a simple web server program that can be started using

```
sudo ./MyHTTPServer.py
```

Too receive credit for the lab, you must use wget on W1 to retrieve the bogus web resource from W3, using the IP address of WX.

4.5 Improve authentication

Modify the router configuration files such that passwords discovered in network traffic cannot be used to corrupt routing tables. Confirm your work by restarting each router and pinging W1 from WX.

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.