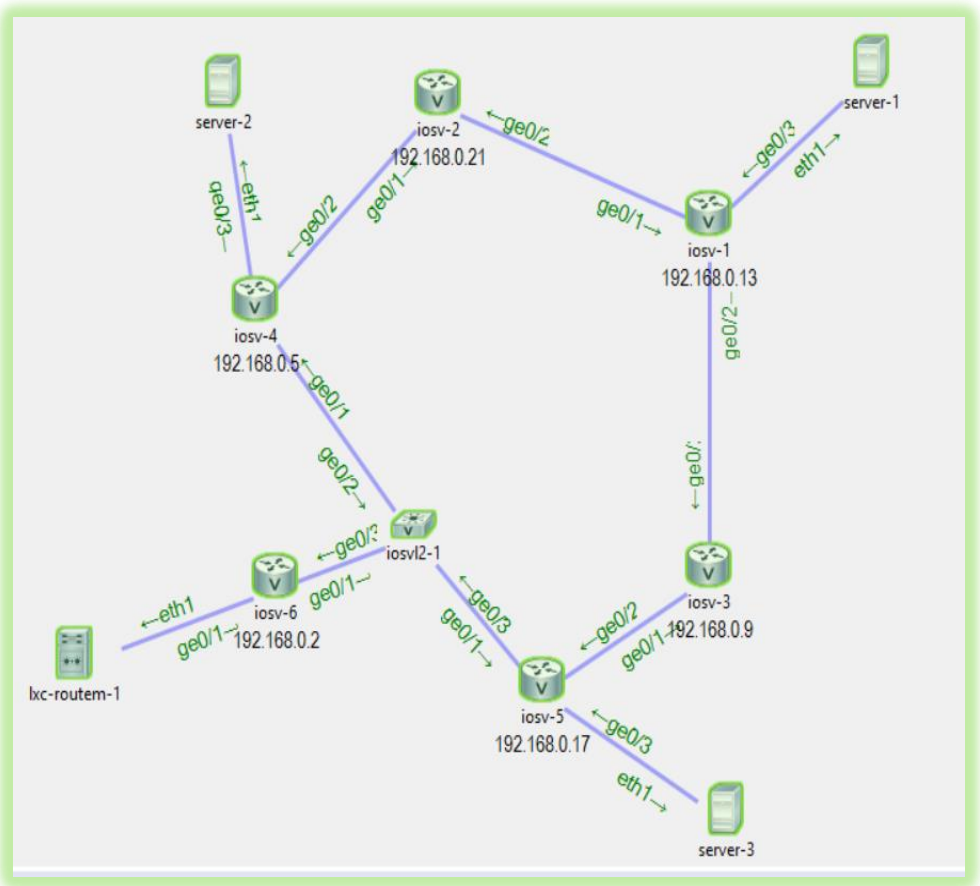
Finding unknown routing protocol deviations in routers

Abstract:

Routing protocols such as OSPF and BGP have open standards (published in RFCs), however commercial routers (e.g. Juniper and Cisco) that implement those protocols may deviate from those standards (deliberately or inadvertently). Such deviation are important to identify from a security point of view as they may be a pose a security vulnerability. We would like to discover those deviations. The problem is that commercial routers are closed-source so it is difficult to directly analyze the router's implementation.



Goals:

- Get the BlackBox Router Testing Tool (developed by Dr. Adi Sosonovich) from: https://www.dropbox.com/s/6phupjffmmoqvks/tool.zip?dl=0
- Using the tool build a reference model for the BGP protocol standard and generate tests
- Once the model is ready and tests are generated, run the tool on a virtual image of Cisco router using the VIRL Simulation. The tool will compare the tests output against the expected output.
- Extend and adapt this tool so it will be able to find deviations in the BGP implementation of Juniper virtual image router.
- The goal of the project is to discover unknown vulnerabilities in BGP protocol and report them to Cisco and Juniper.
- In addition – the outcome of the project should be a stable BlackBox testing tool that will be published to the community as Open Source.

Requirements:

Internet Networking Course, Formal verification (preferably).

Programming Languages:

C, Python

Guided by:

Dr. Adi Sosnovich, Dr. Gabi Nakibly