Advanced Network Automation

Labs 2 & 3

Streaming Telemetry and Network Monitoring (Part 1) The Power of Network Visualization (Part 2)

University of Colorado Boulder

Department of Computer Science

Network Engineering Program

Professor Levi Perigo, Ph.D.

Part 1 - Streaming Telemetry and Network Monitoring | Summary:

As a new member of RoboControl Networks, you are responsible for integrating network monitoring into the existing infrastructure. This involves configuring protocols like SNMP, gRPC, OpenConfig, Streaming telemetry, and Syslogs to enable comprehensive monitoring and alerting. By implementing these solutions, you gain visibility into network performance and can proactively identify and resolve issues. Regularly reviewing and optimizing the monitoring configuration is important to meet evolving network needs.

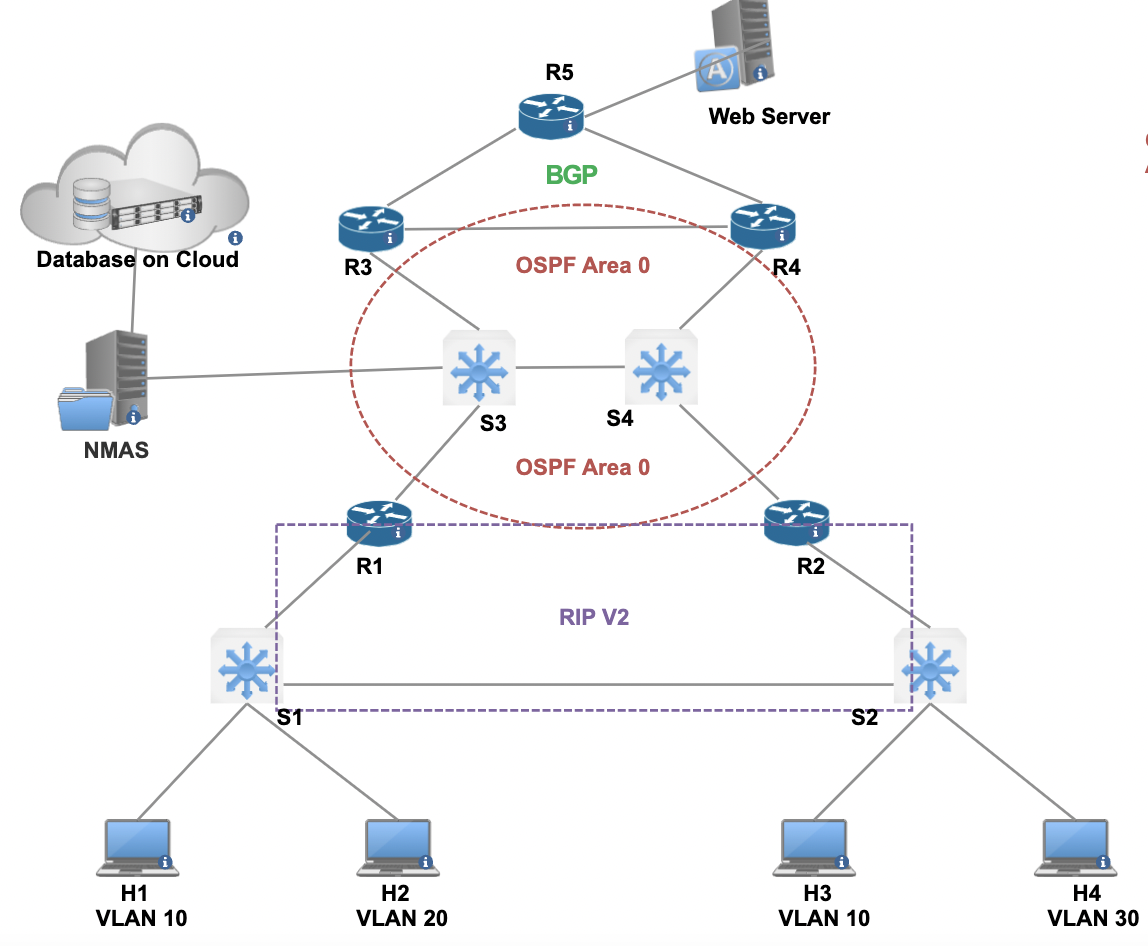
Streaming telemetry is a vital aspect of network automation and management. It continuously collects real-time network data, providing insights into behavior, performance, and health. With streaming telemetry, you can monitor performance, identify bottlenecks, and respond quickly to anomalies. It also enables enhanced network analytics, empowering data-driven decision-making for optimization, capacity planning, and resource allocation.

When developing a network monitoring solution at RoboControl Networks, ensure device compatibility and programmability. Select devices that support the solution and can be programmatically managed in the future. Compatibility with protocols like SNMP, gRPC, OpenConfig, and Streaming telemetry enables comprehensive insights into network performance. Prioritizing programmable devices allows efficient automation of management tasks and future-proofs the infrastructure for scalability. Consider both compatibility and programmability to establish a robust monitoring solution that meets current needs and adapts to future advancements.

Prerequisites:

Before beginning this lab, you should have the network infrastructure built and make yourself familiar with network monitoring protocols such as SNMP, gRPC, OpenConfig, Streaming telemetry, and Syslogs.

# Topololgy:



Objective 1: Network Monitoring | SNMP & Syslog

1. The NMAS should be configured as the SNMP NMS and data/log collector
2. Configure/enable SNMP on all devices
   1. The NMS should be able to monitor CPU of the devices via OIDs
   2. The NMS should receive a trap if a link goes down
3. Configure network devices with syslog
   1. Devices should report critical errors to the NMAS
      1. The files should be stored only for a time period and then deleted

Deliverables:

1. A write-up with instructions for installing and configuring SNMP on all devices in the lab environment.
2. A list of OIDs that NMAS should poll on each device.
3. Verification tests to demonstrate that NMAS can poll all devices for the appropriate OIDs and receive SNMP trap notifications for link status and CPU usage.

Objective 2: Network Monitoring | gRPC & NetConf

1. Configure gRPC and NetConf for streaming telemetry
   1. The devices should stream to the NMAS which will be the data collector

Deliverables:

1. A write-up with instructions for installing and configuring gRPC | NetConf on all devices in the lab environment.
2. A list of data to be streamed via gRPC or NetConf from each device to its respective host.
3. Verification tests to demonstrate that devices are successfully streaming telemetry data to the NMAS.

Objective 3: Viewing Logs | SNMP, Syslog, gRPC & NetConf

1. All monitoring systems should store information in a data lake

Deliverable:

1. Submit a Video explaining and demonstrating functionality of the network such as:
   1. Verification tests to demonstrate SNMP polls/traps are working; gRPC updates are stored in a data lake and can be retrieved, and Syslog files show critical alerts.

Part 2 - The Power of Network Visualization |Summary:

When developing a network visualization solution at RoboControl Networks, the focus is on leveraging Grafana, Telegraph, and InfluxDB to provide comprehensive insights into network performance. Grafana is a powerful visualization platform that allows the creation of interactive and customizable dashboards, making it an ideal tool for visualizing network data. By integrating Grafana with Telegraph and InfluxDB, network administrators can gather real-time data from various network devices and store it in the InfluxDB time-series database.

Telegraph serves as the collection agent, gathering network data from devices and sending it to InfluxDB for storage. This data includes metrics such as network bandwidth, latency, error rates, and packet loss. InfluxDB, a high-performance time-series database, efficiently stores and organizes the collected data, enabling fast and flexible retrieval for visualization purposes.

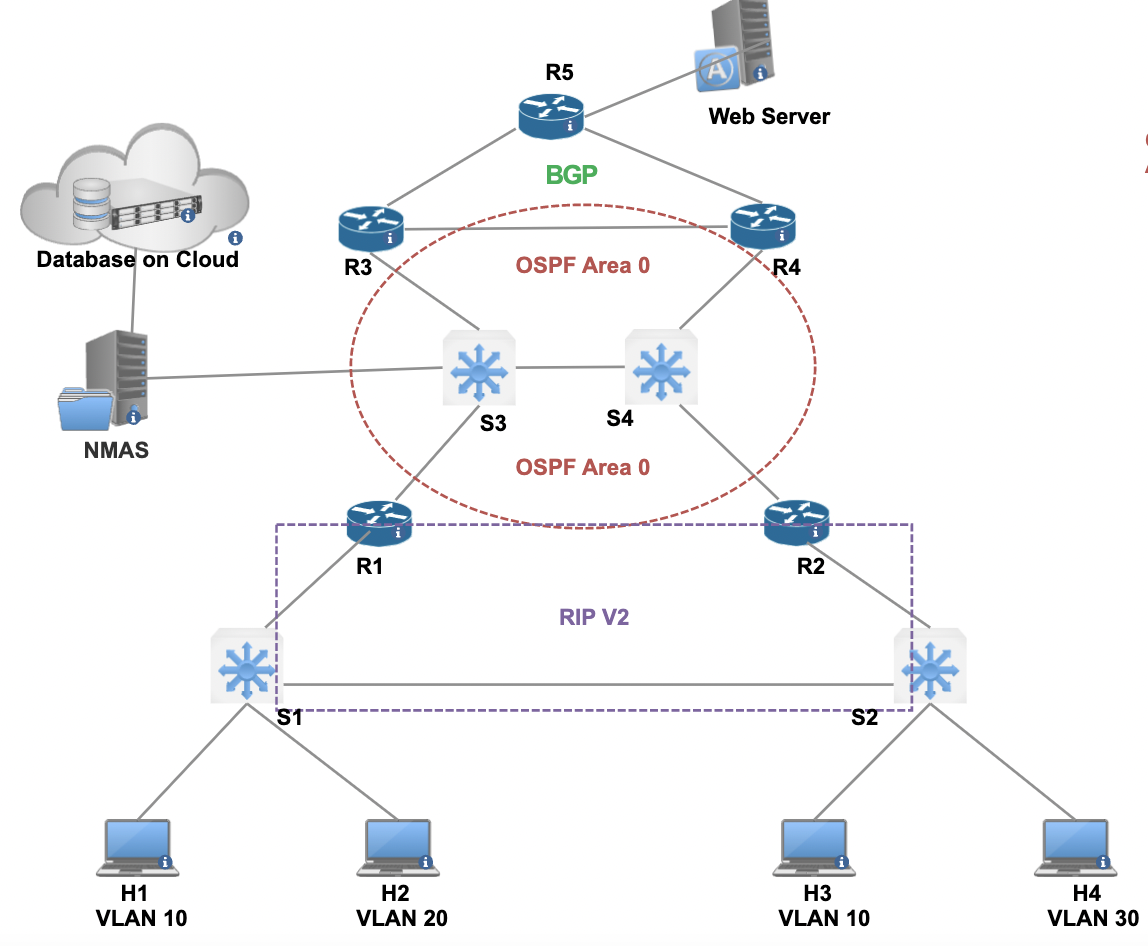
With the combination of Grafana, Telegraph, and InfluxDB, network administrators can create visually appealing and insightful dashboards. These dashboards can display real-time network metrics, historical trends, and key performance indicators (KPIs), allowing for in-depth analysis and monitoring. Visualizing network data through Grafana enables network administrators to identify bottlenecks, anomalies, and areas of improvement, facilitating proactive network management and optimization.

By investing in network visualization using Grafana, Telegraph, and InfluxDB, RoboControl Networks can gain a holistic view of its network performance. This empowers network administrators to make data-driven decisions, enhance troubleshooting capabilities, and ensure optimal network performance and reliability. Regularly reviewing and fine-tuning the visualization setup will help maintain accurate and actionable network insights for effective management and decision-making.

Prerequisites:

Before beginning this lab, you should have the network infrastructure built, and network monitoring should be configured. You should make yourself familiar with network visualization tools such as protocols such as Grafana, Telegraph, and InfluxDB.

# Topololgy:



Objective 1: Network Visualization | SNMP, ST, & Syslog (Grafana & Telegraph)

1. Configure a network visualization tool to visualize relevant SNMP, ST, and Syslog information captured on your NMAS data lake
   1. (Note: an example would be to add Telegraph and InfluxDB to your monitoring solution (gRPC, SNMP, & Syslog) to act as a bridge between the network devices and the storage backend with a time-series database; then incorporate a visualization tool such as Grafana)
   2. This data visualization provided to the user via a dashboard (such as Grafana) should grant the user actionable insights, proactively identify issues, and optimize network performance.
   3. The visualization should enhance decision-making and streamline troubleshooting which can be automated in the future
2. Extra Credit:
   1. Visualize the network with a dynamic and real-time network diagram (For example, the NetworkX library can be used)

Deliverables:

1. A write-up with instructions for installing and configuring the network visualization tool in the lab environment.
2. Submit a Video explaining and demonstrating functionality of the network visualization such as:
   1. Verification tests to demonstrate the dashboard is accurately representing the network
   2. Failures are displayed in real-time to the dashboard