Networking Academy

Virtual Internship Program 2025

Problem Statement for Networking stream

Areas it touches:

Network Topology Generation
Automatic creation of hierarchical network topology from router configuration files.
Awareness of link bandwidth and traffic load capacity.

Network Performance and Load Management
Load balancing recommendations based on link capacity and traffic demands.
Consideration of application types and expected traffic loads.

Network Configuration Validation and Optimization
Detection of missing network components (e.g., missing switch config files).
Identification of configuration flaws such as duplicate IPs, incorrect VLAN labels, wrong gateway addresses, MTU mismatches, and network loops.

Suggestions for network optimization, including node aggregation and protocol recommendations (e.g., BGP vs. OSPF).

Network Simulation and Fault Injection
Day-1 simulation of network activities like ARP, neighbour discovery, and OSPF discovery.
Simulation of link failures and their impact on endpoints and traffic.

Ability to pause and resume simulations for configuration changes and fault testing.

Implementation Architecture
Use of multithreading to represent routers and switches.
Inter-process communication (IPC) via FIFO or TCP/IP for metadata packet exchange.

Maintenance of statistics and logs at thread/node levels to simulate VLAN switches & routers.

Optional creation of real IP packets.

Problem Statement:

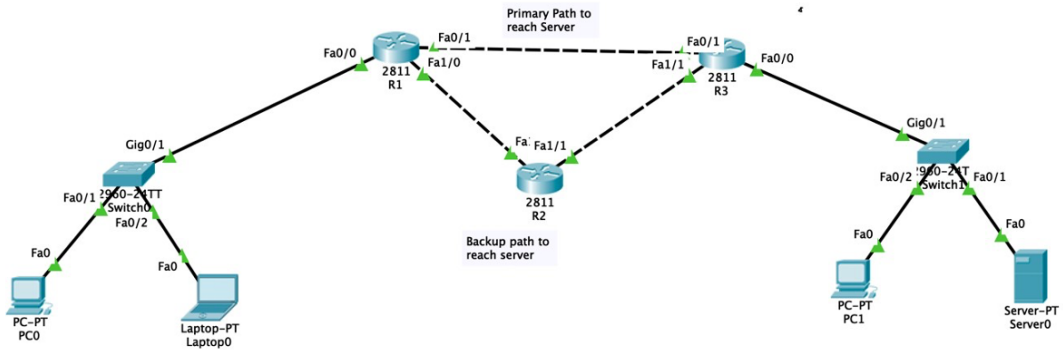
Currently, there is no existing solution to automatically generate a network topology from the configuration files of individual routers. The generated topology does not need to be highly customer-specific but should align with the concepts taught in Level 8 of the course.

Workflow:
Users will be provided with a directory containing configuration files such as:

- Conf/R1/config.dump
- Conf/R2/config.dump
- Conf/R3/config.dump
- ... and so forth.

Tool Requirements:

- The tool should construct a hierarchical network topology based on the provided configuration files.



- It must understand the bandwidth of all links and verify if the capacity is adequate for the traffic load from endpoints. Optionally, it can consider the types of applications hosted on endpoints and their expected peak and regular loads.
- The tool should recommend load balancing strategies if any link cannot handle the required traffic. For example, if R1 and R3 cannot support peak loads, it should suggest activating secondary paths for lower-priority traffic.
- It should detect and flag any missing components in the network path, such as a missing switch configuration file for an endpoint.
- The tool should identify configuration issues, including but not limited to:
  - Opportunities to optimize the network by reducing nodes through aggregation
  - Duplicate IP addresses within the same VLAN
  - Incorrect VLAN labels
  - Incorrect gateway addresses on routers like R1, R2, and R3
  - Recommendations to use BGP instead of OSPF where appropriate
  - MTU size mismatches
  - Network loops
- It should support Day-1 simulation scenarios, including:
  - Network activity when all devices are powered on (e.g., ARP, neighbour discovery, OSPF discovery)
  - Simulation of link failures at various levels, showing network behaviour such as:
  - Which endpoints are affected by link failures
  - Impact of MTU mismatches on traffic
- The tool's implementation should:
  - Use multithreading to represent routers and switches according to their roles

- Employ inter-process communication (IPC) mechanisms like FIFO or TCP/IP to exchange simple metadata packets
- Provision IPC links to handle message capacity efficiently
- Maintain statistics and basic logs at each thread/node level to simulate VLAN switches and routers operating at MAC and IP address layers
- Real IP packet creation is optional but considered a plus
- The tool should support both Day-1 and Day-2 scenarios, including the ability to pause and resume simulations after configuration changes to facilitate fault injection and network event testing.