

OTLab 12

Fundamental Network Topologies



Prof. Dr. Luiz Fernando Freitas-Gutierrez (a.k.a. substationworm)



linkedin.com/in/lffreitas-gutierrez



github.com/substationworm/OTLab



luiz.gutierrez@ufsm.br

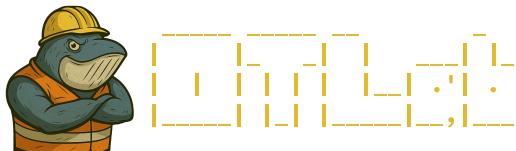
Problem Overview

Containerized Hosts

- single-pc1: 172.30.20.10, 02:12:20:00:00:01.
- single-pc2: 172.30.20.11, 02:12:20:00:00:02.
- single-pc3: 172.30.20.12, 02:12:20:00:00:03.
- ring-node1: 172.30.40.2, 172.30.40.34, 02:14:40:00:00:01.
- ring-node2: 172.30.40.3, 172.30.40.10, 02:14:40:00:00:02.
- ring-node3: 172.30.40.11, 172.30.40.18, 02:14:40:00:00:03.
- ring-node4: 172.30.40.19, 172.30.40.26, 02:14:40:00:00:04.
- ring-node5: 172.30.40.27, 172.30.40.35, 02:14:40:00:00:05.
- star-core: 172.30.30.2, 172.30.30.10, 172.30.30.18, 02:13:30:00:00:00.
- star-leaf1: 172.30.30.3, 02:13:30:00:00:01.
- star-leaf2: 172.30.30.11, 02:13:30:00:00:02.
- star-leaf3: 172.30.30.19, 02:13:30:00:00:03.

Networks

- single-net: 172.30.20.0/24.
- ring-ab: 172.30.40.0/29.
- ring-bc: 172.30.40.8/29.
- ring-cd: 172.30.40.16/29.
- ring-de: 172.30.40.24/29.
- ring-ea: 172.30.40.32/29.
- star-net-a: 172.30.30.0/29.
- star-net-b: 172.30.30.8/29.

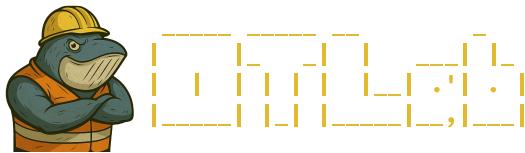


- star-net-c: 172.30.30.16/29.

Note: The `single-net` is defined as a simple, flat Layer 2 network composed of a single Ethernet segment. The ring topology, consisting of the segments `ring-ab`, `ring-bc`, `ring-cd`, `ring-de`, and `ring-ea`, is conceptual and implemented using static routes only; therefore, no reconvergence occurs in the event of a link failure. The star topology comprises a central node (`star-core`) operating as a router and three connected subnets (`star-net-a`, `star-net-b`, and `star-net-c`).

Tasks

1. Access `single-pc1` using the command `./OTLab12 -run single1` and list the ARP cache by executing `arp -a`. Then, access `single-pc2` and `single-pc3` in two additional terminal sessions. On both `single-pc2` and `single-pc3` hosts, initiate ICMP traffic monitoring using `tcpdump -i any icmp`. From `single-pc1`, perform a ping sweep across the `single-net` network: `fping -a -g <single-net_IP_range>`. After completing the sweep, run again `arp -a`. Analyze and discuss the changes observed in the ARP cache.
2. On `single-pc1`, execute a ping scan using `nmap -sn <single-net_IP_range>`. During this scan, capture ARP traffic on `single-pc2` and `single-pc3` using: `tcpdump -i any arp`. Identify and report which hosts are detected as *up*.
3. Access `ring-node1` using: `./OTLab12 -run ring1`. Evaluate the logical paths to `ring-node2`, `ring-node3`, `ring-node4`, and `ring-node5` using: `traceroute <destination_IP>`. Map the routes, evaluate the hop sequences, and draw a network topology diagram.
4. Disable one logical interface on `ring-node1`: `ip link set eth1 down`. Repeat the `traceroute` procedure to `ring-node2`, `ring-node3`, `ring-node4`, and `ring-node5`. Analyze the impact of the interface disruption on path continuity. *Note that the OTLab12 uses static routing and no automatic failover is implemented. In contrast, real-world ring topologies typically rely on dynamic routing protocols or redundancy mechanisms.*
5. Access `star-leaf1`: `./OTLab12 -run star1`. Test connectivity by sending ICMP echo requests to `star-leaf2` and `star-leaf3`. Map the routes, evaluate the hop sequences, and draw a network topology diagram.
6. Restart `OTLab12` to restore all hosts to their default configuration. In separate terminals for `single-pc2` and `single-pc3`, monitor ARP traffic: `tcpdump -i any arp`. On `single-pc1`, generate ARP broadcasts: `arping -c 3 172.30.20.11`. Document the results and identify the broadcast domains.
7. In separate terminals for `ring-node2` and `ring-node3`, monitor ARP traffic: `tcpdump -i any arp`. From `ring-node1`, execute: `arping -c 3 172.30.40.3`. Document the results and identify the broadcast domains.
8. In separate terminals for `star-leaf2` and `star-leaf3`, monitor ARP traffic: `tcpdump -i any arp`. From `star-leaf1`, execute: `arping -c 3 172.30.30.2`. Document the results and identify the broadcast domains.
9. Use the `arp-scan` utility to validate and confirm broadcast domains in each of the three network scenarios implemented in `OTLab12`.



10. For each of the three **OTLab12** network scenarios, map the Layer 3 topology using: `nmap -sn --traceroute <sequential_list_of_all_IP_addresses>`. Analyze the resulting routing paths and compare them with the expected logical topology. *Depending on the responses observed during host discovery and topology reconstruction, the following alternative command may be helpful for your analysis: `nmap -sn -PE -vv --packet-trace <sequential_list_of_all_IP_addresses>`.*

Tools

The following tools are available for completing **OTLab 12**: `arp`, `arp-scan`, `arping`, `fping`, `nmap`, `ping`, `tcpdump`, and `traceroute`.

Nomenclature

- ARP: Address resolution protocol.
- ICMP: Internet control message protocol.
- IP: Internet protocol.