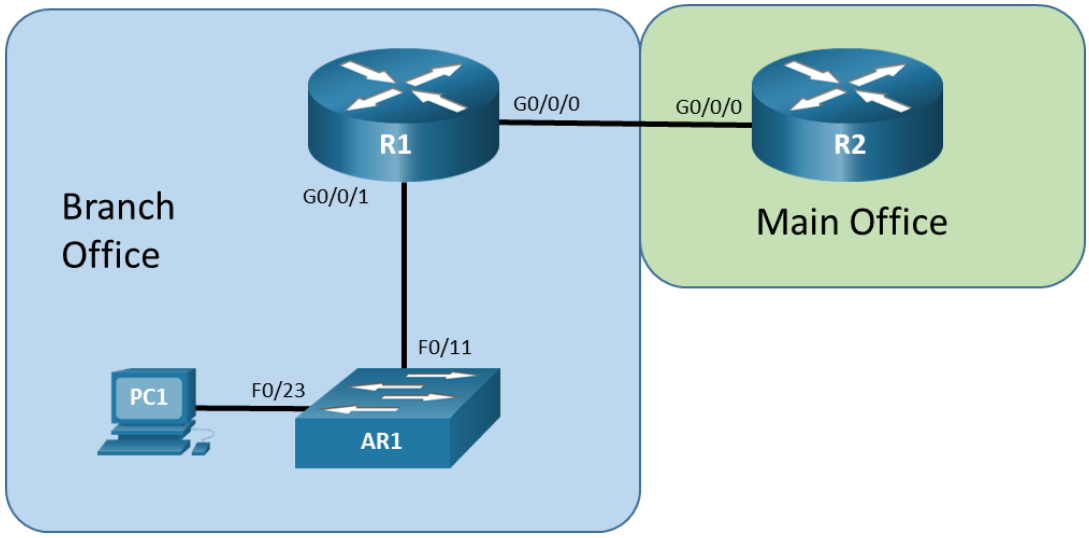
# Lab - Troubleshoot Control Plane Policing (CoPP)

## Topology




## Addressing Table

| Device | Interface | IP Address | Subnet Mask |
|---|---|---|---|
| R1 | G0/0/0 | 172.16.12.1 | 255.255.255.252 |
| | G0/0/1 | 10.10.1.1 | 255.255.255.0 |
| R2 | G0/0/0 | 172.16.12.2 | 255.255.255.252 |
| A1 | VLAN 1 | 10.10.1.4 | 255.255.255.0 |
| PC1 | NIC | 10.10.1.5 | 255.255.255.0 |

## Objectives

Troubleshoot network issues related to the configuration and operation of Control Plane Policing (CoPP).

## Background / Scenario

Control Plane Policing (CoPP) is a protection feature for the router's control plane CPU. CoPP can granularly permit, drop, or rate-limit traffic to or from the CPU using a Modular QoS CLI (MQC) policy. The CoPP policy is applied to a dedicated control-plane "interface" which protects the CPU from unexpected extreme rates of traffic that could impact the stability of the router.

**Note**: The routers used with CCNP hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.4 (universalk9 image). The switch used in the lab is a Cisco Catalyst 2960 with Cisco IOS Release 15.2(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

**Note**: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

## Required Resources

- 2 Routers (Cisco 4221 with Cisco IOS XE Release 16.9.4 universal image or comparable)
- 1 Switch ((Cisco 2960 with Cisco IOS Release 15.2(2) lanbasek9 image or comparable)
- 1 PC (Choice of operating system with a terminal emulation program and a packet capture utility installed)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

## Instructions

## Part 1: Trouble Ticket 22.1.4.1

**Scenario:**

At the main office, a decision was made to eliminate the use of Telnet for network device management. Rather than place ACLs on each interface, the main office network technician edited the existing CoPP configurations on the branch router R1, adding the restriction on Telnet by creating an ACL, class-map, and policy-map to drop all Telnet traffic to the router. The tech also added a traffic class for SSH access. While testing the new changes at the branch office, the branch network technician finds that Telnet is still possible.

Your tasks are to FIND the error(s), document your findings and the command(s) or method(s) used to fix them, FIX the issue(s) presented here and then test the network to ensure the following conditions are met:

1) the complaint received in the ticket is resolved
2) the control-plane policy-map keeps Telnet from succeeding either from the main office or from the branch management network.

Use the commands listed below to load the configuration files for this trouble ticket:

| Device | Command |
|---|---|
| R1 | `copy flash:/enarsi/22.1.4.1-r1-config.txt run` |
| R2 | `copy flash:/enarsi/22.1.4.1-r2-config.txt run` |
| A1 | `copy flash:/enarsi/22.1.4.1-a1-config.txt run` |

- PC1 is on the management network and is configured with a static IP address from the addressing table.
- **aaa new-model** is enabled on router R1.
- Privileged EXEC password is **cisco12345cisco**.
- Passwords on all devices are **cisco1234**. If a username is required, use **admin**.
- After you have fixed the ticket, change the MOTD on EACH DEVICE using the following command:

  **banner motd # This is $(hostname) FIXED from ticket <ticket number> #**
- Save the configuration by issuing the **wri** command (on each device).
- Inform your instructor that you are ready for the next ticket.
- After the instructor approves your solution for this ticket, issue the privileged EXEC command **reset.now**. This script will clear your configurations and reload the devices.

## Part 2: Trouble Ticket 22.1.4.2

**Scenario:**

While the main office network tech was editing the CoPP configuration on the branch R1 router, the tech noticed that there was not a separate class for SSH, that it was part of the MGMT class. The tech decided to add a traffic class for SSH access, so it would be easier to troubleshoot remote access issues. The branch technician reports that after the traffic class change was added, SSH seems much slower and less responsive than before.

Your tasks are to FIND the error(s), document your findings and the command(s) or method(s) used to fix them, FIX the issue(s) presented here and then test the network to ensure the following conditions are met:

1) the complaint received in the ticket is resolved
2) SSH traffic response issues are solved

Use the commands listed below to load the configuration files for this trouble ticket:

| Device | Command |
|---|---|
| R1 | `copy flash:/enarsi/22.1.4.2-r1-config.txt run` |
| R2 | `copy flash:/enarsi/22.1.4.2-r2-config.txt run` |
| A1 | `copy flash:/enarsi/22.1.4.2-a1-config.txt run` |

- PC1 is on the management network and is configured with a static IP address from the addressing table.
- **aaa new-model** is enabled on router R1.
- Privileged EXEC password is **cisco12345cisco**.
- Passwords on all devices are **cisco1234**. If a username is required, use **admin**.
- After you have fixed the ticket, change the MOTD on EACH DEVICE using the following command:

  **banner motd # This is $(hostname) FIXED from ticket <ticket number> #**
- Save the configuration by issuing the **wri** command (on each device).
- Inform your instructor that you are finished.
- After the instructor approves your solution for this ticket, issue the privileged EXEC command **reset.now**. This script will clear your configurations and reload the devices.

## Router Interface Summary Table

| Router Model | Ethernet Interface #1 | Ethernet Interface #2 | Serial Interface #1 | Serial Interface #2 |
|---|---|---|---|---|
| 1800 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 1900 | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2801 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/1/0 (S0/1/0) | Serial 0/1/1 (S0/1/1) |
| 2811 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |

| Router Model | Ethernet Interface #1 | Ethernet Interface #2 | Serial Interface #1 | Serial Interface #2 |
|---|---|---|---|---|
| 2900 | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 4221 | Gigabit Ethernet 0/0/0 (G0/0/0) | Gigabit Ethernet 0/0/1 (G0/0/1) | Serial 0/1/0 (S0/1/0) | Serial 0/1/1 (S0/1/1) |
| 4300 | Gigabit Ethernet 0/0/0 (G0/0/0) | Gigabit Ethernet 0/0/1 (G0/0/1) | Serial 0/1/0 (S0/1/0) | Serial 0/1/1 (S0/1/1) |

**Note**: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.