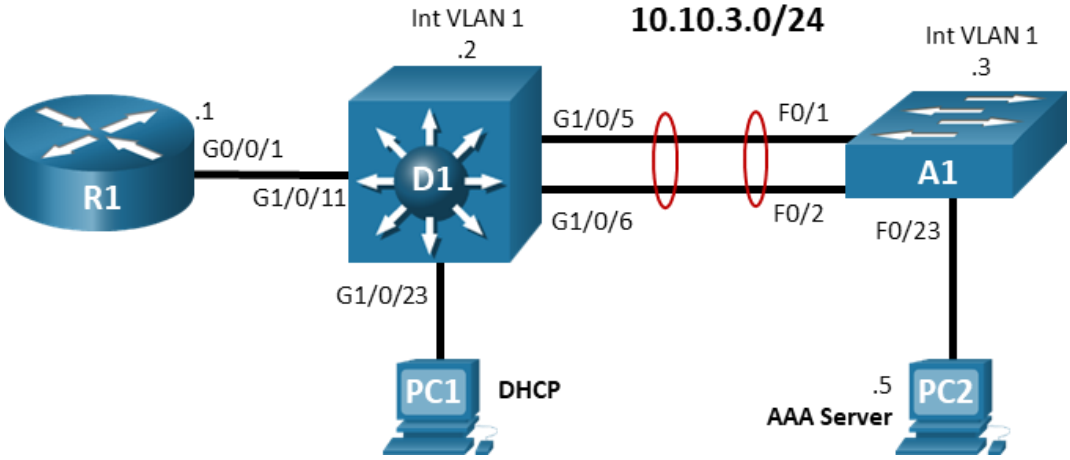
Lab – Troubleshoot IOS AAA Authentication

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
R1	G0/0/1	10.10.3.1	255.255.255.0
D1	VLAN 1	10.10.3.2	255.255.255.0
A1	VLAN 1	10.10.3.3	255.255.255.0
PC1	NIC	DHCP	
PC2	NIC	10.10.3.5	255.255.255.0

Objectives

Troubleshoot authentication issues related to the configuration and operation of AAA. Router R1 is configured for inter-VLAN routing and DHCP to provide support for PC1. You will be loading configurations with intentional errors onto the network. 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 both of the following conditions are met:

1) the complaint received in the ticket is resolved
2) the AAA process occurs as specified

Background / Scenario

Using AAA-based services allows for more granular control of access to your devices. In this lab, you will troubleshoot issues arising from the operation of local and server-based AAA.

Note: The routers used with CCNP hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.4 (universalk9 image). The switches used in the labs are Cisco Catalyst 3650 with Cisco IOS XE Release 16.9.4 (universalk9 image) and Cisco Catalyst 2960s 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

- 1 Router (Cisco 4221 with Cisco IOS XE Release 16.9.4 universal image or comparable)
- 1 Switch (Cisco 3650 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 installed)
- 1 PC (Cisco Network Academy CCNP VM running in a virtual machine client or a server with TACACS+ and RADIUS servers installed, configured and running)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Instructions

Part 1: Trouble Ticket 22.1.2.1

Scenario:

As the result of a network security audit, a policy change was implemented on the routers and switches at the branch office to force stronger access control for management of the devices. All logins were to be authenticated using AAA Method Lists. Everything appeared to go well with the change, and remote access to the devices functions as expected. About a month later, the local branch IT tech attempted to use the console connection to upgrade the IOS on **Switch A1** and was unable to gain access to the device with the local username and password combination provided (username **admin**, password **cisco1234**).

The privileged EXEC password is **cisco12345cisco**.

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

Device	Command
R1	`copy flash:/enarsi/22.1.2.1-r1-config.txt run`
D1	`copy flash:/enarsi/22.1.2.1-d1-config.txt run`
A1	`copy flash:/enarsi/22.1.2.1-a1-config.txt run`

- PC1 should be configured for and receive an address from an IPv4 DHCP server. PC2 must be statically configured with the IP address in the addressing table.
- 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 22.1.2.2

Scenario:

Recently, the RADIUS server at the main office was replaced. The previous server, which is running a standard RADIUS server on Linux, was shipped out to the branch office to be used to authenticate access to the VTY ports on the switches and routers. The server was plugged into **switch A1**. The main office technician logged into **switch D1** remotely and reconfigured it to use RADIUS authentication. As soon as the main office technician logged out of D1 to test the RADIUS authentication, the tech was no longer able to login via Telnet. The local branch office technician now needs to connect to D1 via a console connection and fix the RADIUS authentication issue. The console connection is configured to use local login. (username **admin**, password **cisco1234**). The remote access username and password is **raduser** and **upass123**.

The privileged EXEC password is **cisco12345cisco**.

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

Device	Command
R1	`copy flash:/enarsi/22.1.2.2-r1-config.txt run`
D1	`copy flash:/enarsi/22.1.2.2-d1-config.txt run`
A1	`copy flash:/enarsi/22.1.2.2-a1-config.txt run`

- PC1 should be configured for and receive an address from an IPv4 DHCP server. PC2 must be statically configured with the IP address in the addressing table.
- Passwords on all devices are **cisco1234**. If a username is required, use **admin**.
- The username and password configured on the RADIUS server is **raduser** and **upass123**.
- 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.

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)
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)

Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
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.