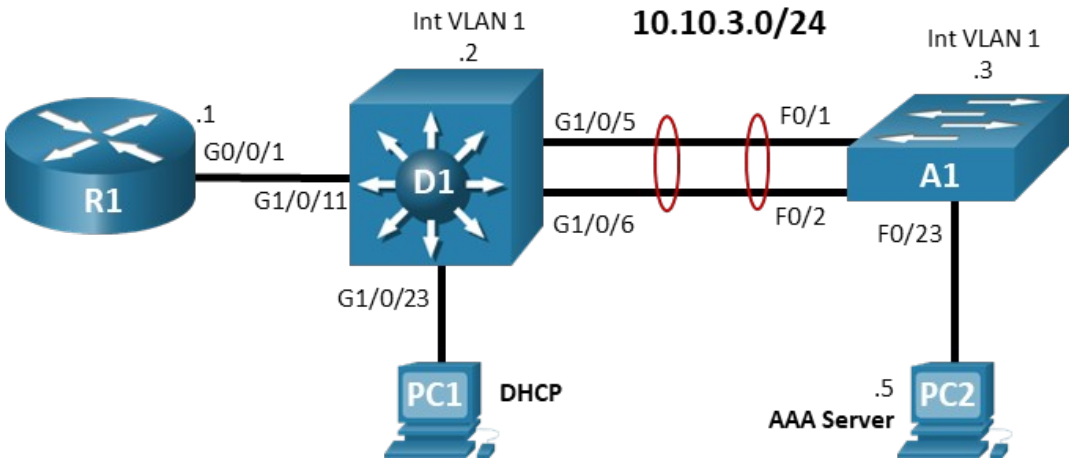
Lab – Troubleshoot IOS AAA Authentication (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

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.

Instructor Note: Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

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:

Instructor Note: Commands for uploading the configuration are provided at the end of this document

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.

Instructor Notes:

Because this activity deals with logins to the devices, students may lock themselves out of the devices. Remind them that they should not save their configurations until they have tested their access, since they may have to reboot the device if the configured settings lock them out.

This trouble ticket contains two intentional errors:

1) The console port does not have a method list configured, so it will use the default method list, which only specifies the enable password.
2) The configured CON-AUTH method list is not correct. It needs to use local authentication, instead of enable.

The commands to fix these errors should be:

```
A1(config)# no aaa authentication login CON-AUTH enable
A1(config)# aaa authentication login CON-AUTH local
A1(config)# line con 0
A1(config-line)# login authentication CON-AUTH
```

Note: Students may choose to configure local authentication directly on the console port, or to add a password on the console port to attempt to fix the problem. The requirement is to use an AAA method list to configure the login. While it is possible to edit the default method list to use local authentication, it is not recommended as it applies to all potential logins.

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:

Instructor Note: Commands for uploading the configuration are provided at the end of this document.

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.

Instructor Notes:

This trouble ticket contains two intentional errors:

1) The correct ports are not specified for the RADIUS server settings
2) The configured RAD-AUTH does not have a failover method if the specified RADIUS group is not available.

The commands to fix these errors should be:

```
D1(config)# no aaa authentication login RAD-AUTH group radius
D1(config)# aaa authentication login RAD-AUTH group radius local
D1(config)# radius server RADIUS
D1(config-radius-server)# address ipv4 10.10.3.5 auth-port 1812 acct-port 1813
D1(config-radius-server)# end
```

Note: Students may attempt to configure local authorization directly on the VTY lines, or to assign a password to the lines. The requirement is to authenticate remote access to the device using RADIUS.

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)
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.

Uploading Configuration Files

Use the commands below to create the configuration files on the lab devices for each trouble ticket in this lab. The TCL script commands help create and copy the configurations. However, the configuration commands could also be copied and pasted directly into global config mode on each device. Simply remove the TCL script commands, enter the **enable** and **configure t** commands on the device, and copy and paste the configuration commands.

Important: The device requires a folder in flash named **enarsi**. Use the **dir** command to verify. If the folder is missing, then create it using the **mkdir flash:/enarsi** privileged EXEC command. For all switches, make sure the vlan.dat file is set to the default. Use the **delete vlan.dat** privileged EXEC command, if necessary.

Reset scripts

These TCL scripts will completely clear and reload the device in preparation for the next ticket. Copy and paste the appropriate script to the appropriate device.

Router Reset Script

```
tclsh
puts [ open "flash:/enarsi/reset.tcl" w+ ] {
typeahead "\n"
copy running-config startup-config
typeahead "\n"
erase startup-config
puts "Reloading the router"
typeahead "\n"
reload
}
tclquit
```

D1/D2 (Cisco 3650) Reset Script - The default 3650 SDM template supports IPv6, so it is not set by this script.

```
tclsh
puts [ open "flash:/enarsi/reset.tcl" w+ ] {
typeahead "\n"
copy running-config startup-config
typeahead "\n"
erase startup-config
delete /force vlan.dat
puts "Reloading the switch"
typeahead "\n"
reload
}
tclquit
```

A1 (Cisco 2960 Script) - The default 2960 SDM template does not support IPv6, so this script includes that setting.

```
tclsh
puts [ open "flash:/enarsi/reset.tcl" w+ ] {
```

```
typeahead "\n"
copy running-config startup-config
typeahead "\n"
erase startup-config
delete /force vlan.dat
delete /force multiple-fs
ios_config "sdm prefer lanbase-routing"
typeahead "\n"
puts "Reloading the switch"
typeahead "\n"
reload
}
tclquit
```

R1 Configuration File Scripts

!R1 - Trouble Ticket # 1

```
tclsh
puts [ open "flash:/enarsi/22.1.2.1-r1-config.txt" w+ ] {
hostname R1
no ip domain lookup
enable secret cisco12345cisco
banner motd # R1, Trouble ticket 22.1.2.1 #
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
interface g0/0/1
 ip address 10.10.3.1 255.255.255.0
 no shutdown
 exit
ip dhcp excluded-address 10.10.3.1 10.10.3.5
ip dhcp pool HOST_ADDRESSING
 network 10.10.3.0 255.255.255.0
 default-router 10.10.3.1
 exit
alias exec reset.now tclsh flash:/enarsi/reset.tcl
end
}
tclquit
```

!R1 - Trouble Ticket # 2

```
tclsh
puts [ open "flash:/enarsi/22.1.2.2-r1-config.txt" w+ ] {
```

```
hostname R1
no ip domain lookup
enable secret cisco12345cisco
banner motd # R1, Trouble ticket 22.1.2.2 #
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
interface g0/0/1
 ip address 10.10.3.1 255.255.255.0
 no shutdown
 exit
ip dhcp excluded-address 10.10.3.1 10.10.3.5
ip dhcp pool HOST_ADDRESSING
 network 10.10.3.0 255.255.255.0
 default-router 10.10.3.1
 exit
alias exec reset.now tclsh flash:/enarsi/reset.tcl
end
}
tclquit
```

D1 Configuration File Scripts

!D1 - Trouble Ticket # 1

```
tclsh
puts [ open "flash:/enarsi/22.1.2.1-d1-config.txt" w+ ] {
hostname D1
no ip domain lookup
enable secret cisco12345cisco
banner motd # D1, Trouble Ticket 22.1.2.1 #
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
interface vlan 1
 ip address 10.10.3.2 255.255.255.0
 no shutdown
 exit
ip default-gateway 10.10.3.1
interface g1/0/23
 spanning-tree portfast
 switchport mode access
 no shutdown
```

```
 exit
interface g1/0/11
 spanning-tree portfast
 switchport mode access
 no shutdown
 exit
interface range g1/0/5-6
 switchport mode trunk
 channel-group 1 mode active
 no shutdown
 exit
interface range g1/0/1-4, g1/0/7-10, g1/0/12-22, g1/0/24
 shutdown
 exit
alias exec reset.now tclsh flash:/enarsi/reset.tcl
end
}
tclquit
```

!D1 - Trouble Ticket # 2

```
tclsh
puts [ open "flash:/enarsi/22.1.2.2-d1-config.txt" w+ ] {
hostname D1
no ip domain lookup
enable secret cisco12345cisco
banner motd # D1, Trouble Ticket 22.1.2.2 #
username admin algorithm-type scrypt secret cisco1234
username localuser algorithm-type scrypt secret letmein
aaa new-model
aaa authentication login default local enable
aaa authentication login RAD-AUTH group radius
interface vlan 1
 ip address 10.10.3.2 255.255.255.0
 no shutdown
 exit
ip default-gateway 10.10.3.1
interface g1/0/23
 spanning-tree portfast
 switchport mode access
 no shutdown
 exit
interface g1/0/11
 spanning-tree portfast
 switchport mode access
 no shutdown
 exit
```

```
interface range g1/0/5-6
 switchport mode trunk
 channel-group 1 mode active
 no shutdown
 exit
interface range g1/0/1-4, g1/0/7-10, g1/0/12-22, g1/0/24
 shutdown
 exit
radius server RADIUS
 address ipv4 10.10.3.5
 key $trongPass
 exit
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
line vty 0 4
login authentication RAD-AUTH
transport input Telnet
exit
alias exec reset.now tclsh flash:/enarsi/reset.tcl
end
}
tclquit
```

A1 Configuration File Scripts

!A1 - Trouble Ticket # 1

```
tclsh
puts [ open "flash:/enarsi/22.1.2.1-a1-config.txt" w+ ] {
hostname A1
no ip domain lookup
enable secret cisco12345cisco
banner motd # A1, Trouble Ticket 22.1.2.1 #
aaa new-model
username admin algorithm-type scrypt secret cisco1234
username localuser algorithm-type scrypt secret letmein
aaa authentication login default enable
aaa authentication login VTY-AUTH local
aaa authentication login CON-AUTH enable
aaa session-id common
interface vlan 1
 ip address 10.10.3.3 255.255.255.0
 no shutdown
 exit
ip default-gateway 10.10.3.1
```

```
interface range f0/1-2
 switchport mode trunk
 channel-group 1 mode active
 no shutdown
 exit
interface range f0/3-24, g0/1-2
 shutdown
 exit
interface f0/23
 switchport mode access
 spanning-tree portfast
 no shutdown
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
line vty 0 4
 login authentication VTY-AUTH
line vty 5 15
 exit
alias exec reset.now tclsh flash:/enarsi/reset.tcl
end
}
tclquit
```

!A1 - Trouble Ticket # 2

```
tclsh
puts [ open "flash:/enarsi/22.1.2.2-a1-config.txt" w+ ] {
hostname A1
no ip domain lookup
enable secret cisco12345cisco
banner motd # A1, Trouble Ticket 22.1.2.2 #
aaa new-model
username admin algorithm-type scrypt secret cisco1234
username localuser algorithm-type scrypt secret letmein
aaa authentication login default enable
aaa authentication login VTY-AUTH local enable
aaa authentication login CON-AUTH local enable
aaa session-id common
interface vlan 1
 ip address 10.10.3.3 255.255.255.0
 no shutdown
 exit
ip default-gateway 10.10.3.1
interface range f0/1-2
 switchport mode trunk
```

```
 channel-group 1 mode active
 no shutdown
 exit
interface range f0/3-24, g0/1-2
 shutdown
 exit
interface f0/23
 switchport mode access
 spanning-tree portfast
 no shutdown
line con 0
 login authentication CON-AUTH
 exec-timeout 0 0
 logging synchronous
 exit
line vty 0 4
 login authentication VTY-AUTH
line vty 5 15
 exit
alias exec reset.now tclsh flash:/enarsi/reset.tcl
end
}
tclquit
```