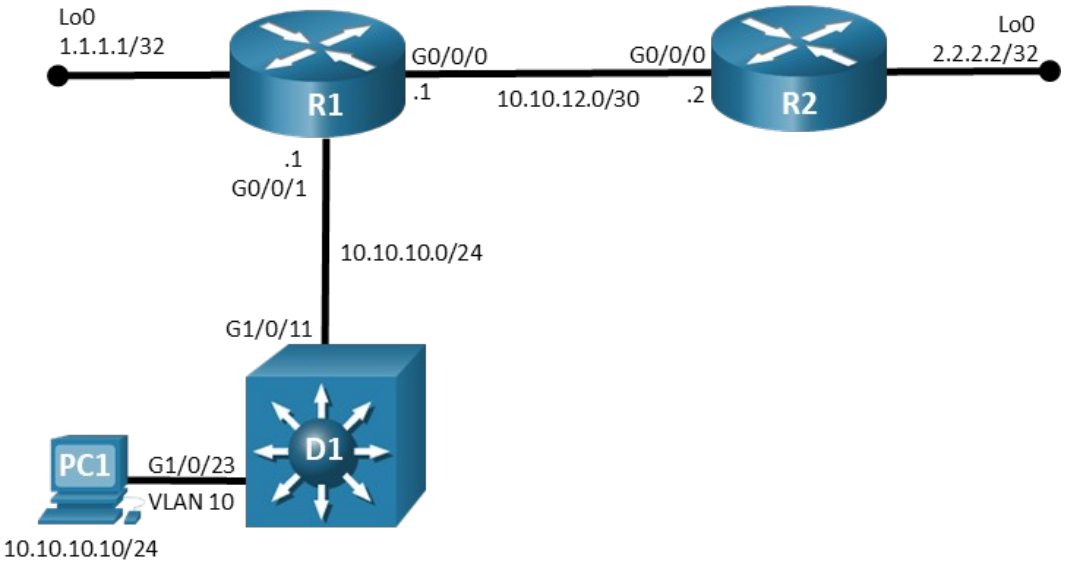
Lab - Troubleshoot SNMP and Logging Issues (Instructor Version)

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	G0/0/0	10.10.12.1	255.255.255.0
	G0/0/1	10.10.10.1	255.255.255.0
R2	G0/0/0	10.10.12.2	255.255.255.0
D1	VLAN 10	10.10.10.2	255.255.255.0
PC1	NIC	10.10.10.10	255.255.255.0

Objectives

Troubleshoot the logging issues for the devices in the topology and make the necessary corrections.

Background / Scenario

In this topology, routers R1, R2, and switch D1 are configured with logging and SNMP. 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) full functionality is restored

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). 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 devices 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

- 2 Routers (Cisco 4221 with Cisco IOS XE Release 16.9.4 universal image or comparable)
- 1 Switch (Cisco 3560 with Cisco IOS XE Release 16.9.4 universal image or comparable)
- 1 PC (Choice of operating system with terminal emulation and syslog programs installed)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Part 1: Trouble Ticket 23.1.3.1

Scenario:

SNMP messages should be coming from router R1 and switch D1. To avoid service interruption, loopback interfaces have been configured on those devices to test SNMP operation. Disabling and enabling the loopback interface should generate an SNMP trap that is displayed on the Syslog server log screen. Correct any necessary configuration issues and verify traps are being logged from both devices.

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/23.1.3.1-r1-config.txt run`
R2	`copy flash:/enarsi/23.1.3.1-r2-config.txt run`
D1	`copy flash:/enarsi/23.1.3.1-d1-config.txt run`

- PC1 should be manually configured and able to ping its default gateway, as shown in the Addressing Table.
- PC1 needs to have syslog software running. In this example, the Kiwi Syslog Server software is used and the following settings is used for all the trouble tickets in this lab.

Kiwi Syslog Server Settings:

File->Setup->Inputs – Add addresses 10.10.10.1, 10.10.10.2, and 10.10.12.2

File->Setup->Inputs->UDP – Checkbox for Listen for UDP messages checked

File->Setup->Inputs->SNMP – Checkbox for Listen for SNMP Traps checked

File->Setup->Inputs->SNMP – Add/Remove SNMP v3 Credentials dialog

User Name – USER1

Authentication Password – cisco12345

Algorithm - SHA

Private Password – cisco54321

Algorithm - AES

Security Level - Authentication & Privacy dropdown selected

Click **Add User**

Close the **Setup** dialog box.

- Passwords on all devices are **cisco12345**. 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> #
- Then 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 **reset.now** privileged EXEC command on each device. This script will clear your configurations and reload the devices.
- Clear the log messages on PC1 to prepare for the next ticket.

Instructor Notes:

This trouble ticket contains one intentional error:

D1 has been configured with an incorrect host IP address

The commands used to fix this error should be:

```
D1(config)# no snmp-server host 10.10.10.11 version 2c ciscolab
D1(config)# snmp-server host 10.10.10.10 version 2c ciscolab
D1(config)# end
```

Part 2: Trouble Ticket 23.1.3.2

Scenario:

A network technician notices that logging messages from the routers are not consistent. All messages should record the time the event occurs. Both routers should record when changes are made to the devices. Use the loopback interfaces on the routers to determine if messages are being recorded correctly.

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

Instructor Note: Commands for creating these files are at the end of this document.

Device	Command
R1	`copy flash:/enarsi/23.1.3.2-r1-config.txt run`
R2	`copy flash:/enarsi/23.1.3.2-r2-config.txt run`
D1	`copy flash:/enarsi/23.1.3.2-d1-config.txt run`

- PC1 should be manually configured and able to ping its default gateway, as shown in the Addressing Table.
- PC1 needs to have the Kiwi Syslog Server software running with the same setting used in Trouble Ticket 23.1.3.1.
- Passwords on all devices are **cisco12345**. 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> #

- Then 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 **reset.now** privileged EXEC command. This script will clear your configurations and reload the devices.

Instructor Notes:

This trouble ticket contains two intentional error. R1 is not configured to record timestamps. R2 is configured for an incorrect trap level.

The commands used to fix these errors should be:

```
R1(config)# service timestamps debug datetime msec
R1(config)# service timestamps log datetime msec
R1(config)# end

R2(config)# logging trap debug
R2(config)# end
```

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
```

R1 Configuration File Scripts

!R1 - Trouble Ticket # 1

```
tclsh
puts [ open "flash:/enarsi/23.1.3.1-r1-config.txt" w+ ] {
hostname R1
```

```
banner motd # This is R1, Trouble Ticket 23.1.3.1 #
enable secret cisco12345
username admin privilege 15 algorithm-type scrypt secret cisco12345
service timestamps debug datetime msec
service timestamps log datetime msec
aaa new-model
aaa authentication login default local
ip domain name ccnplab.local
crypto key generate rsa modulus 1024
ip ssh ver 2
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
interface GigabitEthernet0/0/0
 ip address 10.10.12.1 255.255.255.252
no shutdown
interface GigabitEthernet0/0/1
 ip address 10.10.10.1 255.255.255.0
 ip access-group ALLOW-TFTP out
no shutdown
router eigrp 10
 network 10.10.10.0 0.0.0.255
 network 10.10.12.0 0.0.0.3
 passive-interface GigabitEthernet0/0/1
 eigrp router-id 10.10.10.1
ip forward-protocol nd
ip access-list standard PERMIT-ADMIN
 permit 10.10.10.0 0.0.0.255
ip access-list extended ALLOW-TFTP
 permit udp 10.10.0.0 0.0.255.255 host 10.10.10.10 eq tftp
 permit udp 10.10.0.0 0.0.255.255 host 10.10.10.10 gt 1024
 permit udp 10.10.0.0 0.0.255.255 host 10.10.10.10 eq syslog
 permit udp 10.10.0.0 0.0.255.255 host 10.10.10.10 eq snmp
 permit udp 10.10.0.0 0.0.255.255 host 10.10.10.10 eq snmptrap
 permit tcp 10.10.0.0 0.0.255.255 eq 22 host 10.10.10.10
 permit icmp any any
logging trap debugging
logging host 10.10.10.10
snmp-server group ADMIN v3 priv read SNMP-RO access PERMIT-ADMIN
snmp-server view SNMP-RO iso included
snmp-server user USER1 ADMIN v3 auth sha cisco12345 pri aes 128 cisco54321
logging snmp-trap informational
snmp-server enable traps config
snmp-server host 10.10.10.10 USER1 config
line con 0
 exec-timeout 0 0
```

```
 logging synchronous
 exit
line vty 0 4
 transport input ssh
!
exit
alias exec reset.now tclsh flash:/enarsi/reset.tcl
end
}
tclquit
```

!R1 - Trouble Ticket # 2

```
tclsh
puts [ open "flash:/enarsi/23.1.3.2-r1-config.txt" w+ ] {
hostname R1
banner motd # This is R1, Trouble Ticket 23.1.3.2 #
enable secret cisco12345
username admin privilege 15 algorithm-type scrypt secret cisco12345
no service timestamps
aaa new-model
aaa authentication login default local
ip domain name ccnplab.local
crypto key generate rsa modulus 1024
ip ssh ver 2
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
interface GigabitEthernet0/0/0
 ip address 10.10.12.1 255.255.255.252
no shutdown
interface GigabitEthernet0/0/1
 ip address 10.10.10.1 255.255.255.0
 ip access-group ALLOW-TFTP out
no shutdown
router eigrp 10
 network 10.10.10.0 0.0.0.255
 network 10.10.12.0 0.0.0.3
 passive-interface GigabitEthernet0/0/1
 eigrp router-id 10.10.10.1
ip forward-protocol nd
ip access-list standard PERMIT-ADMIN
 permit 10.10.10.0 0.0.0.255
ip access-list extended ALLOW-TFTP
 permit udp 10.10.0.0 0.0.255.255 host 10.10.10.10 eq tftp
 permit udp 10.10.0.0 0.0.255.255 host 10.10.10.10 gt 1024
 permit udp 10.10.0.0 0.0.255.255 host 10.10.10.10 eq syslog
 permit udp 10.10.0.0 0.0.255.255 host 10.10.10.10 eq snmp
```

```
 permit udp 10.10.0.0 0.0.255.255 host 10.10.10.10 eq snmptrap
 permit tcp 10.10.0.0 0.0.255.255 eq 22 host 10.10.10.10
 permit icmp any any
logging trap debugging
logging host 10.10.10.10
snmp-server group ADMIN v3 priv read SNMP-RO access PERMIT-ADMIN
snmp-server view SNMP-RO iso included
snmp-server user USER1 ADMIN v3 auth sha cisco12345 pri aes 128 cisco54321
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
line vty 0 4
 transport input ssh
!
exit
alias exec reset.now tclsh flash:/enarsi/reset.tcl
end
}
tclquit
```

R2 Configuration File Scripts

!R2 - Trouble Ticket # 1

```
tclsh
puts [ open "flash:/enarsi/23.1.3.1-r2-config.txt" w+ ] {
hostname R2
banner motd # This is R2, Trouble Ticket 23.1.3.1 #
enable secret cisco12345
username admin privilege 15 algorithm-type scrypt secret cisco12345
service timestamps debug datetime msec
service timestamps log datetime msec
aaa new-model
aaa authentication login default local
aaa authorization exec default local
ip domain name ccnplab.local
crypto key generate rsa modulus 1024
interface Loopback0
 ip address 2.2.2.2 255.255.255.255
interface g0/0/0
 ip address 10.10.12.2 255.255.255.252
no shut
router eigrp 10
 network 10.10.12.0 0.0.0.3
 auto-summary
 eigrp router-id 10.10.12.2
```

```
ip forward-protocol nd
ip ssh version 2
ip scp server enable
logging trap debugging
logging source-interface gigabitEthernet0/0/0
logging host 10.10.10.10
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
line vty 0 4
 transport input ssh
!
exit
alias exec reset.now tclsh flash:/enarsi/reset.tcl
end
}
tclquit
```

!R2 - Trouble Ticket # 2

```
tclsh
puts [ open "flash:/enarsi/23.1.3.2-r2-config.txt" w+ ] {
hostname R2
banner motd # This is R2, Trouble Ticket 23.1.3.2 #
enable secret cisco12345
username admin privilege 15 algorithm-type scrypt secret cisco12345
service timestamps debug datetime msec
service timestamps log datetime msec
aaa new-model
aaa authentication login default local
aaa authorization exec default local
ip domain name ccnplab.local
crypto key generate rsa modulus 1024
interface Loopback0
 ip address 2.2.2.2 255.255.255.255
interface g0/0/0
 ip address 10.10.12.2 255.255.255.252
no shut
router eigrp 10
 network 10.10.12.0 0.0.0.3
 auto-summary
 eigrp router-id 10.10.12.2
ip forward-protocol nd
ip ssh version 2
ip scp server enable
logging trap critical
```

```
logging source-interface gigabitEthernet0/0/0
logging host 10.10.10.10
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
line vty 0 4
 transport input ssh
!
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/23.1.3.1-d1-config.txt" w+ ] {
hostname D1
banner motd # This is D1, Trouble Ticket 23.1.3.1 #
enable secret cisco12345
username admin privilege 15 algorithm-type scrypt secret cisco12345
service timestamps debug datetime msec
service timestamps log uptime
aaa new-model
aaa authentication login default local
ip domain name ccnplab.local
crypto key generate rsa modulus 1024
interface Loopback0
 no ip address
interface range g1/0/1 - 24
 switchport mode access
 shutdown
 exit
interface g1/0/11
 switchport mode access
 switchport access vlan 10
 no shutdown
 exit
interface range g1/0/23-24
 switchport mode access
 switchport access vlan 10
 no shutdown
 exit
```

```
interface Vlan10
 ip address 10.10.10.2 255.255.255.0
no shut
ip default-gateway 10.10.10.1
ip http server
ip http secure-server
ip access-list standard SNMP_ACL
 permit 10.10.10.10
snmp-server community ciscolab RO SNMP_ACL
snmp-server location snmp_manager
snmp-server contact ciscolab_admin
snmp-server enable traps snmp authentication linkdown linkup coldstart
warmstart
snmp-server enable traps transceiver all
snmp-server enable traps tty
snmp-server enable traps fru-ctrl
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps power-ethernet police
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps port-security
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps energywise
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps stpx inconsistency root-inconsistency loop-
inconsistency
snmp-server enable traps syslog
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 10.10.10.11 version 2c ciscolab
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
line vty 0 15
 transport input ssh
!
```

```
exit
alias exec reset.now tclsh flash:/enarsi/reset.tcl
end
}
tclquit
```

!D1 - Trouble Ticket # 2

```
tclsh
puts [ open "flash:/enarsi/23.1.3.2-d1-config.txt" w+ ] {
hostname D1
banner motd # This is D1, Trouble Ticket 23.1.3.2 #
enable secret cisco12345
username admin privilege 15 algorithm-type scrypt secret cisco12345
service timestamps debug datetime msec
service timestamps log uptime
aaa new-model
aaa authentication login default local
ip domain name ccnplab.local
crypto key generate rsa modulus 1024
interface Loopback0
 no ip address
interface range g1/0/1 - 24
 switchport mode access
 shutdown
 exit
interface g1/0/11
 switchport mode access
 switchport access vlan 10
 no shutdown
 exit
interface range g1/0/23-24
 switchport mode access
 switchport access vlan 10
 no shutdown
 exit
interface Vlan10
 ip address 10.10.10.2 255.255.255.0
no shut
ip default-gateway 10.10.10.1
ip http server
ip http secure-server
ip access-list standard SNMP_ACL
 permit 10.10.10.10
snmp-server community ciscolab RO SNMP_ACL
snmp-server location snmp_manager
snmp-server contact ciscolab_admin
```

```
snmp-server enable traps snmp authentication linkdown linkup coldstart
warmstart
snmp-server enable traps transceiver all
snmp-server enable traps tty
snmp-server enable traps fru-ctrl
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps power-ethernet police
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps port-security
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps energywise
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps stpx inconsistency root-inconsistency loop-
inconsistency
snmp-server enable traps syslog
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 10.10.10.10 version 2c ciscolab
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
line vty 0 15
 transport input ssh
!
exit
alias exec reset.now tclsh flash:/enarsi/reset.tcl
end
}
tclquit
```