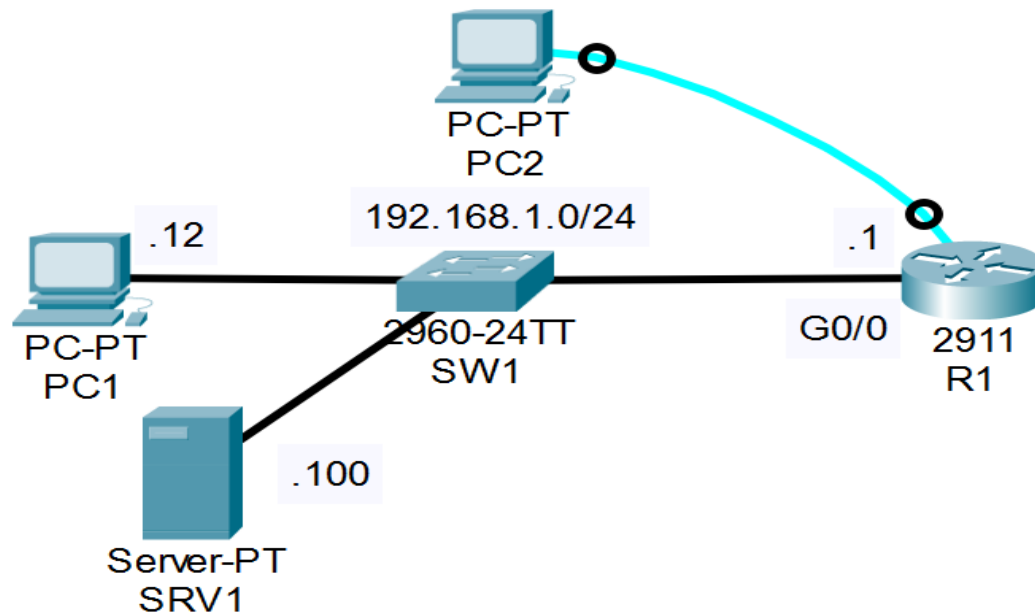


Network Topology:



Instructions and actions:

1. Connect to R1's console port using PC2. Configure username – jeremy, password – ccna.

Configured the user verification on R1 CLI using the commands:

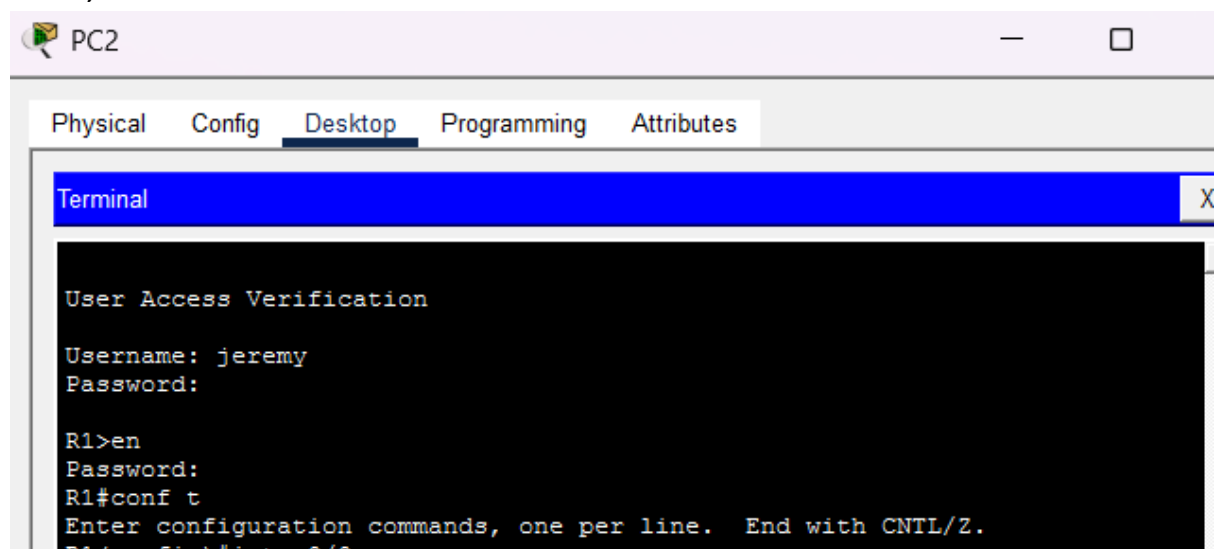
```
R1(config)#username jeremy privilege 0 password ccna
#line console 0
#login local
#exit
```

The above commands enable user verification before the user exec mode.

To enable double verification while going to privileged exec mode:

```
R1(config)#enable password ccna
#exit
```

Now, PC2 Terminal:



2. Use the shutdown and no shutdown commands for the g0/0 interface of R1 and monitor the syslog messages:

```
R1(config)#int g0/0
R1(config-if)#shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to
administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to down

R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up

R1(config-if)#exit
```

Level of Severity = 5

This is a notice/notification

3. Enable timestamps for logging messages:

```
R1(config)#service timestamps log datetime msec
R1(config)#int g0/0
R1(config-if)#shutdown

R1(config-if)#
*Feb 28, 21:24:17.2424: %LINK-5-CHANGED: Interface GigabitEthernet0/0,
changed state to administratively down
*Feb 28, 21:24:17.2424: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to down
R1(config-if)#no shutdown

R1(config-if)#
*Feb 28, 21:24:25.2424: %LINK-5-CHANGED: Interface GigabitEthernet0/0,
changed state to up
*Feb 28, 21:24:25.2424: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up
```

4. Use a Telnet connection from PC1 to R1's g0/0 interface:
I will use the Command Prompt of PC1 – The syslog messages don't appear by default on VTY lines; therefore, we will use the command:
#do terminal monitor
PC1 Command Prompt:

```

C:\>telnet 192.168.1.1
Trying 192.168.1.1 ...Open

User Access Verification

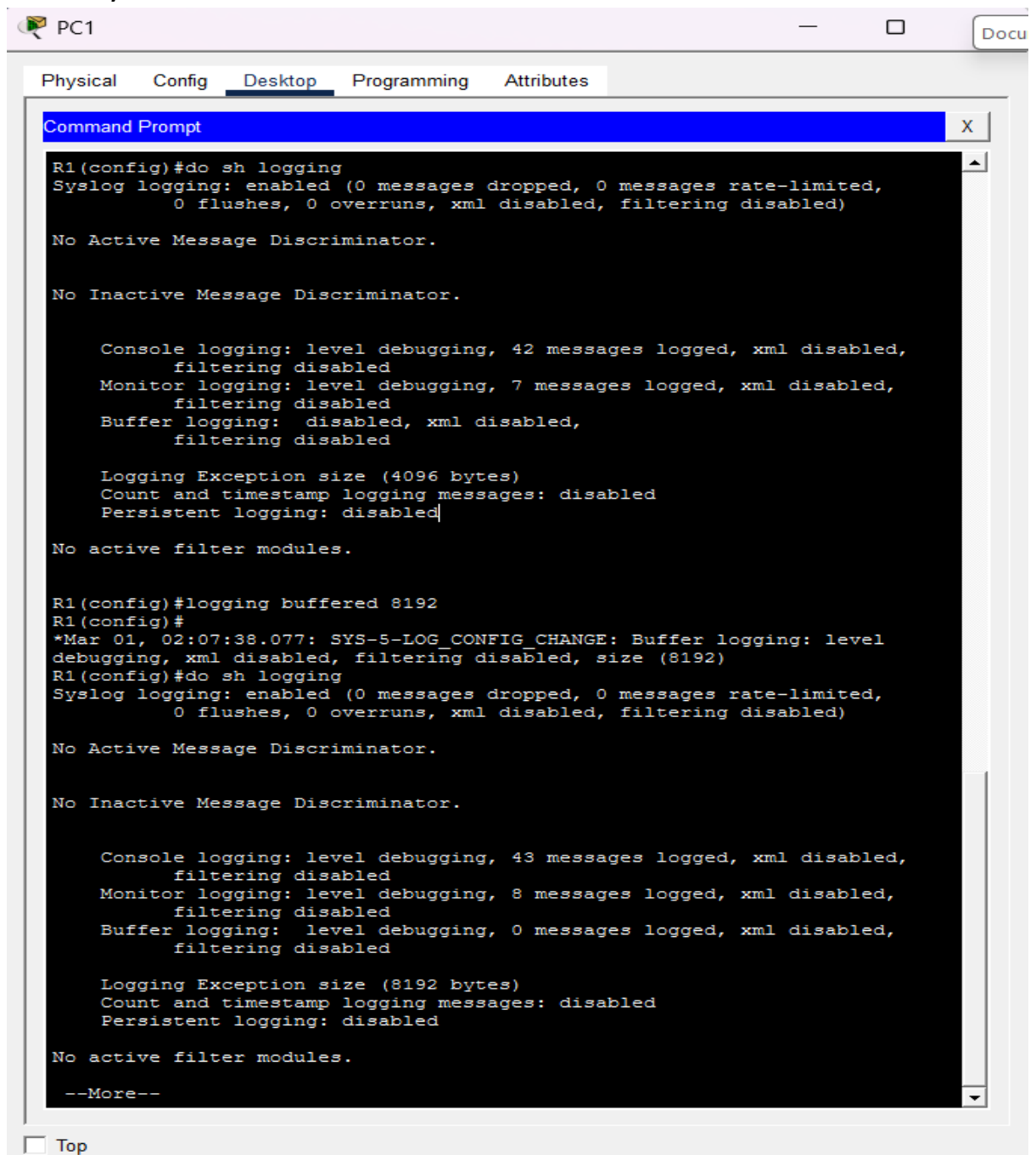
Username: jeremy
Password:
R1>en
Password:
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#do terminal monitor
R1(config)#int g0/1
R1(config-if)#no shutdown

R1(config-if)#
*Mar 01, 02:01:31.011: %LINK-3-UPDOWN: Interface GigabitEthernet0/1,
changed state to down
R1(config-if)#shutdown

R1(config-if)#
*Mar 01, 02:01:37.011: %LINK-5-CHANGED: Interface GigabitEthernet0/1,
changed state to administratively down

```

5. Enable logging to the buffer, and configure the buffer size of 8192 bytes



The screenshot shows a PC1 window with a Command Prompt open. The Command Prompt displays the output of several Cisco IOS commands. The first set of commands shows the current logging status, including Syslog, Console, Monitor, and Buffer logging. The second set of commands shows the configuration of buffer logging with a size of 8192 bytes.

```

PC1
Physical Config Desktop Programming Attributes
Command Prompt
R1(config)#do sh logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited,
0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.

No Inactive Message Discriminator.

Console logging: level debugging, 42 messages logged, xml disabled,
filtering disabled
Monitor logging: level debugging, 7 messages logged, xml disabled,
filtering disabled
Buffer logging: disabled, xml disabled,
filtering disabled

Logging Exception size (4096 bytes)
Count and timestamp logging messages: disabled
Persistent logging: disabled

No active filter modules.

R1(config)#logging buffered 8192
R1(config)#
*Mar 01, 02:07:38.077: SYS-5-LOG_CONFIG_CHANGE: Buffer logging: level
debugging, xml disabled, filtering disabled, size (8192)
R1(config)#do sh logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited,
0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.

No Inactive Message Discriminator.

Console logging: level debugging, 43 messages logged, xml disabled,
filtering disabled
Monitor logging: level debugging, 8 messages logged, xml disabled,
filtering disabled
Buffer logging: level debugging, 0 messages logged, xml disabled,
filtering disabled

Logging Exception size (8192 bytes)
Count and timestamp logging messages: disabled
Persistent logging: disabled

No active filter modules.

--More--

```

☐ Top

6. Enable logging to the syslog server SRV1 with a level of 'debugging'

The default level in Cisco Packet Tracer is debugging, and it doesn't allow for configuring higher levels.

Trying this command on the external server SRV1 from PC1:

```
R1(config)#logging host 192.168.1.100
R1(config)#logging trap ?
    debugging  Debugging messages                (severity=7)
    <cr>
R1(config)#logging trap debugging
```

Observation:

Changes made using the command prompt of PC1 can be observed under the services option of SRV1.

PC1:

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int g0/1
R1(config-if)#no shutdown

R1(config-if)#shutdown

R1(config-if)#|
```

SRV1:

The screenshot shows the SRV1 configuration window with the 'Services' tab selected. The 'Syslog' service is enabled (radio button selected). A table displays the Syslog messages received from the router.

	Time	HostName	Message
1	03.01.1993 02:19:10.737 AM	192.168.1.1	%SYS-5-CONFIG_I: Configured from ...
2	03.01.1993 02:19:10.737 AM	192.168.1.1	: %SYS-6- LOGGINGHOST_S...
3	03.01.1993 02:19:45.023 AM	192.168.1.1	%LINK-3-UPDOWN...
4	03.01.1993 02:19:54.782 AM	192.168.1.1	%LINK-5-CHANGE...