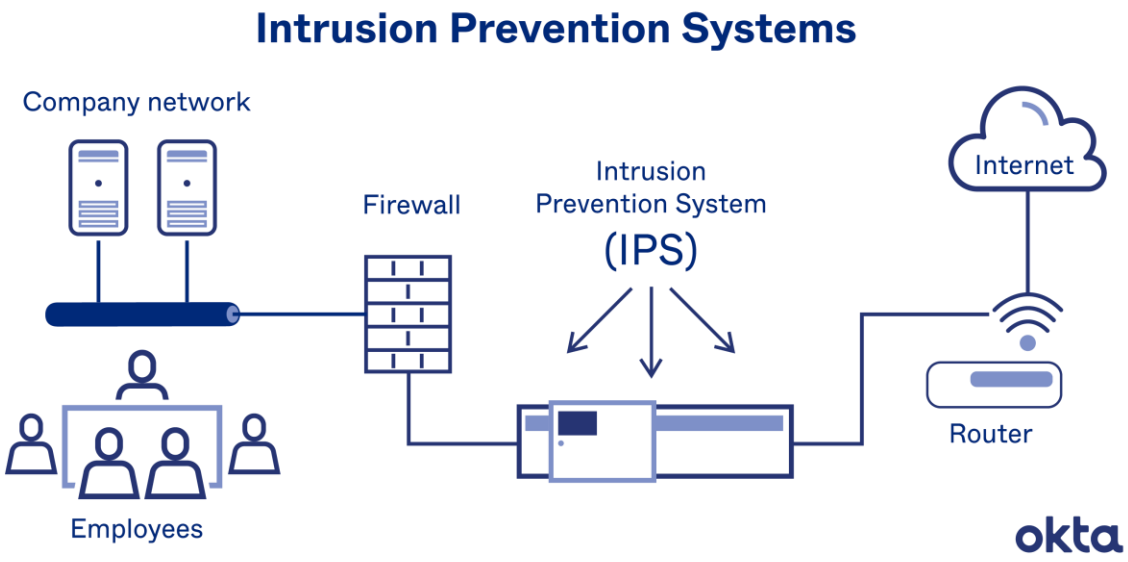
Introduction to IPS :

- ✓ Not only detects intruders, but also handles attacks.
- ✓ Has the combined abilities of IDS and Firewall.
- ✓ Active response device that works upon packets, sessions, and access controls.
- ✓ Risk of False alarm / High misclassification.



Types of IPS :

1. System memory and process protection
   Protects memory of process running on the system
2. Inline network devices
   Works in the path of communication and modify/block packets
3. Session sniping
   Terminates a TCP session by sending a TCP RST packet to both ends of the connection
4. Gateway interaction devices
   Interacts with and directs firewall to block attacks

Objectives :

- ✓ Enable IOS IPS.
- ✓ Configure logging.
- ✓ Modify an IPS signature.
- ✓ Verify IPS.

Scenario :

The task is to enable IPS on router R1 to scan traffic entering the 192.168.1.0 network.

The server labelled Syslog is used to log IPS messages. We must configure the router to identify the syslog server to receive logging messages. Displaying the correct time and date in syslog messages is vital when using syslog to monitor the network. Set the clock and configure the timestamp service for logging on the routers. Finally, enable IPS to produce an alert and drop ICMP echo reply packets inline.

The server and PCs have been preconfigured. The routers have also been preconfigured with the following:

- Enable password: ciscoenpa55
- Console password: ciscoconpa55
- SSH username and password: SSHadmin / ciscosshpa55
- OSPF 101

Configuration of IOS IPS using CISCO Packet Tracer :

Note : For all the demonstrations, timestamp is provided at the bottom-right of the screen snapshots.

Part 0 : Pre-requisites

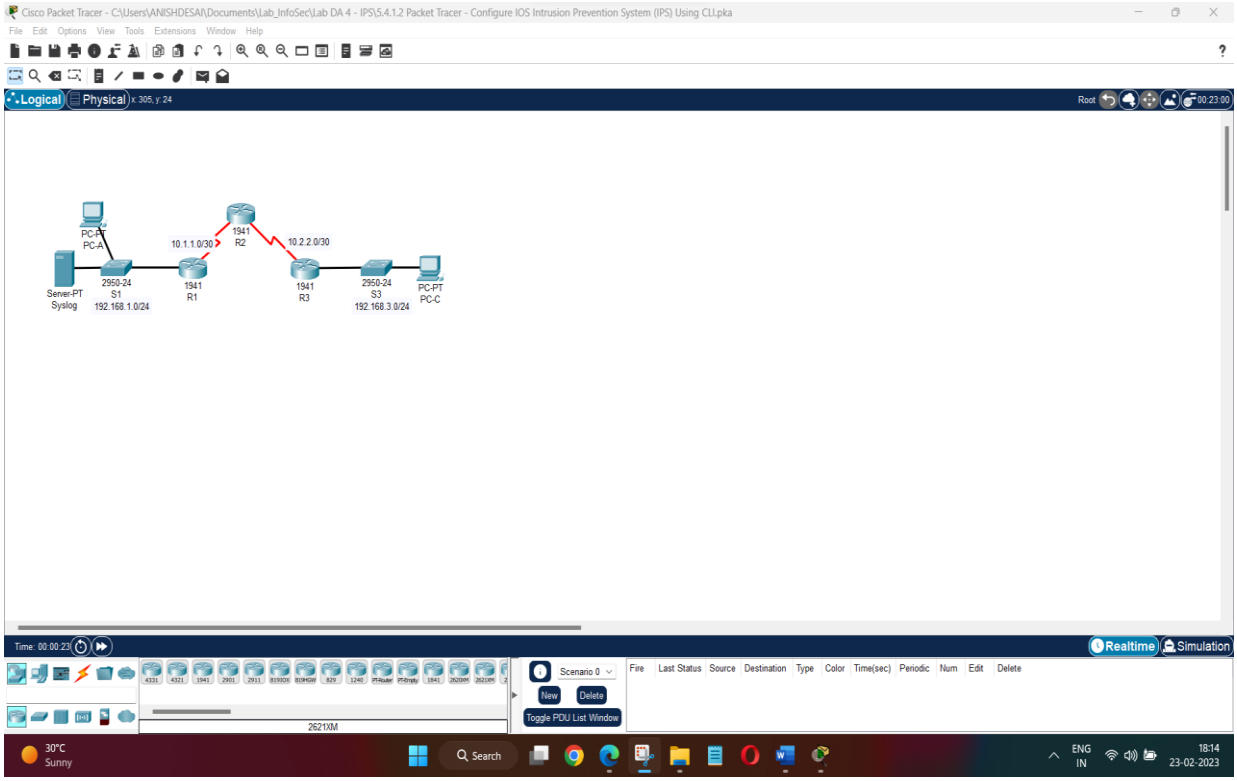
Step 1 : Outlining the components

Components used include:

1. PC-PT: PC-A and PC-C
2. Server-PT: Syslog
3. 1941-type routers: R1, R2 and R3
4. Switch 2950-24: S1 and S3

Step 2 : Topology and Initialization (pre-configured)

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/1
	S0/0/0	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/1
	S0/0/0	10.2.2.1	255.255.255.252	N/A	N/A
Syslog	NIC	192.168.1.50	255.255.255.0	192.168.1.1	S1 F0/2
PC-A	NIC	192.168.1.2	255.255.255.0	192.168.1.1	S1 F0/3
PC-C	NIC	192.168.3.2	255.255.255.0	192.168.3.1	S3 F0/2



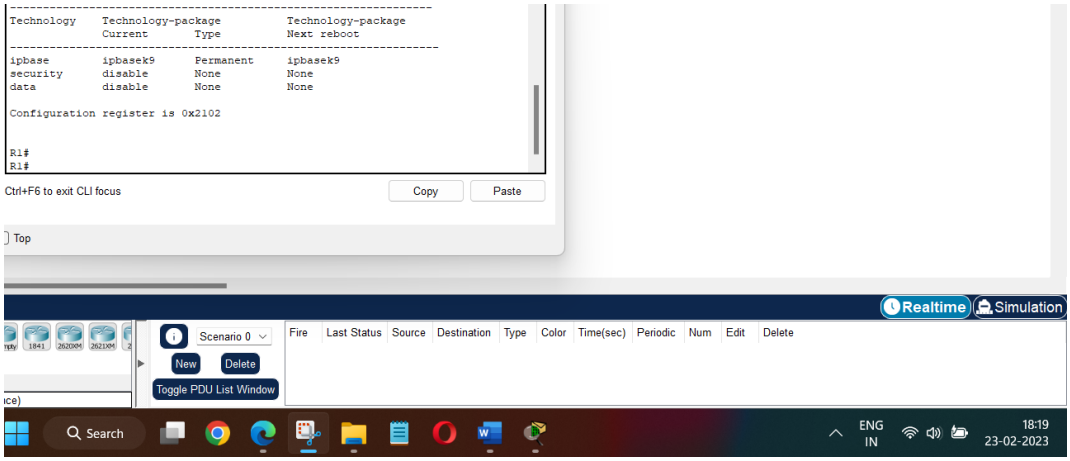
Part 1 : Enable IOS IPS

Step 1 : Enable the Security Technology Package

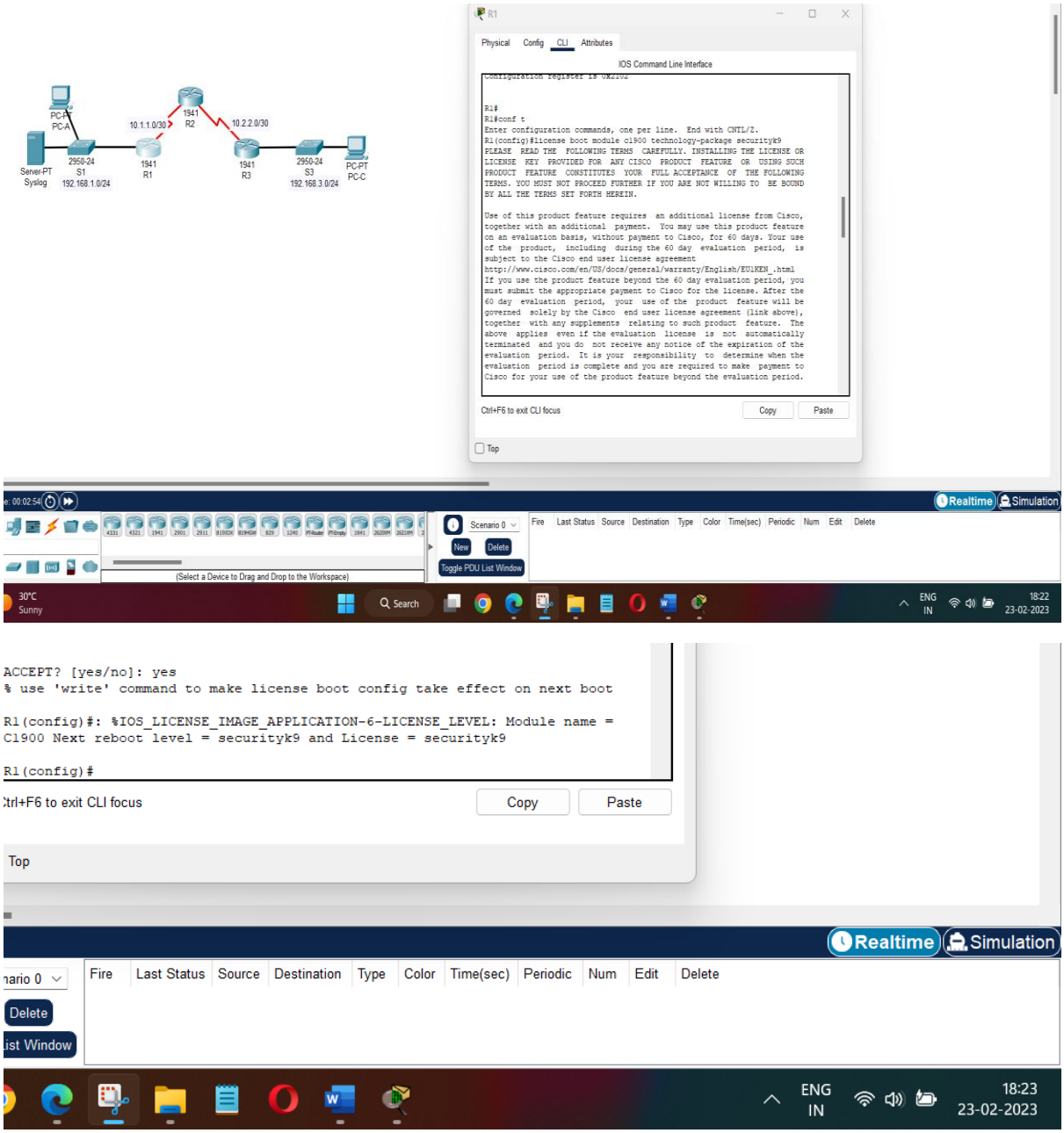
On R1, issue the show version command to view the Technology Package license information. If the Security Technology package has not been enabled, use the following command to enable the package.

R1(config)# license boot module c1900 technology-package securityk9

Accept the end user license agreement. Save the running-config and reload the router to enable the security license. Verify that the Security Technology package has been enabled by using the show version command.



As we can see, Security Technology Package isn't enabled, hence enable it.

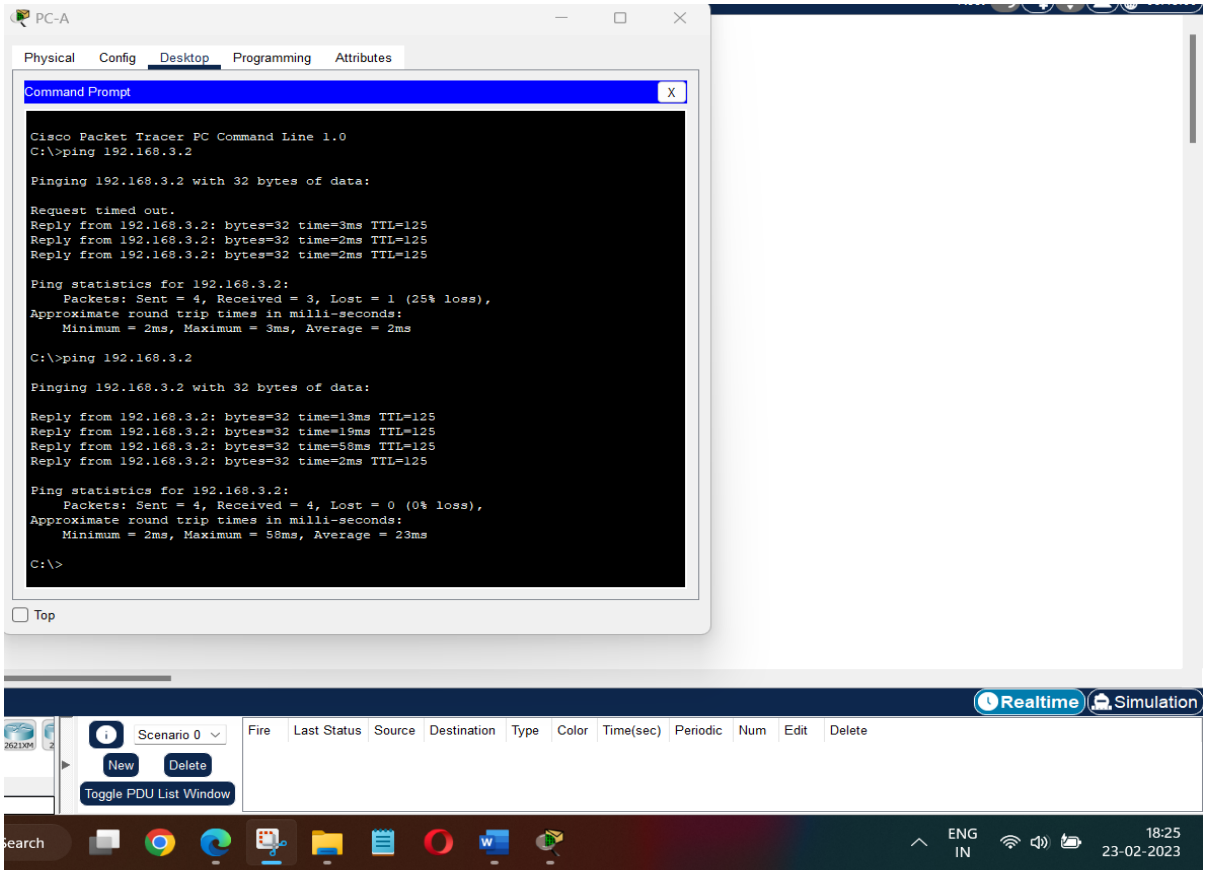


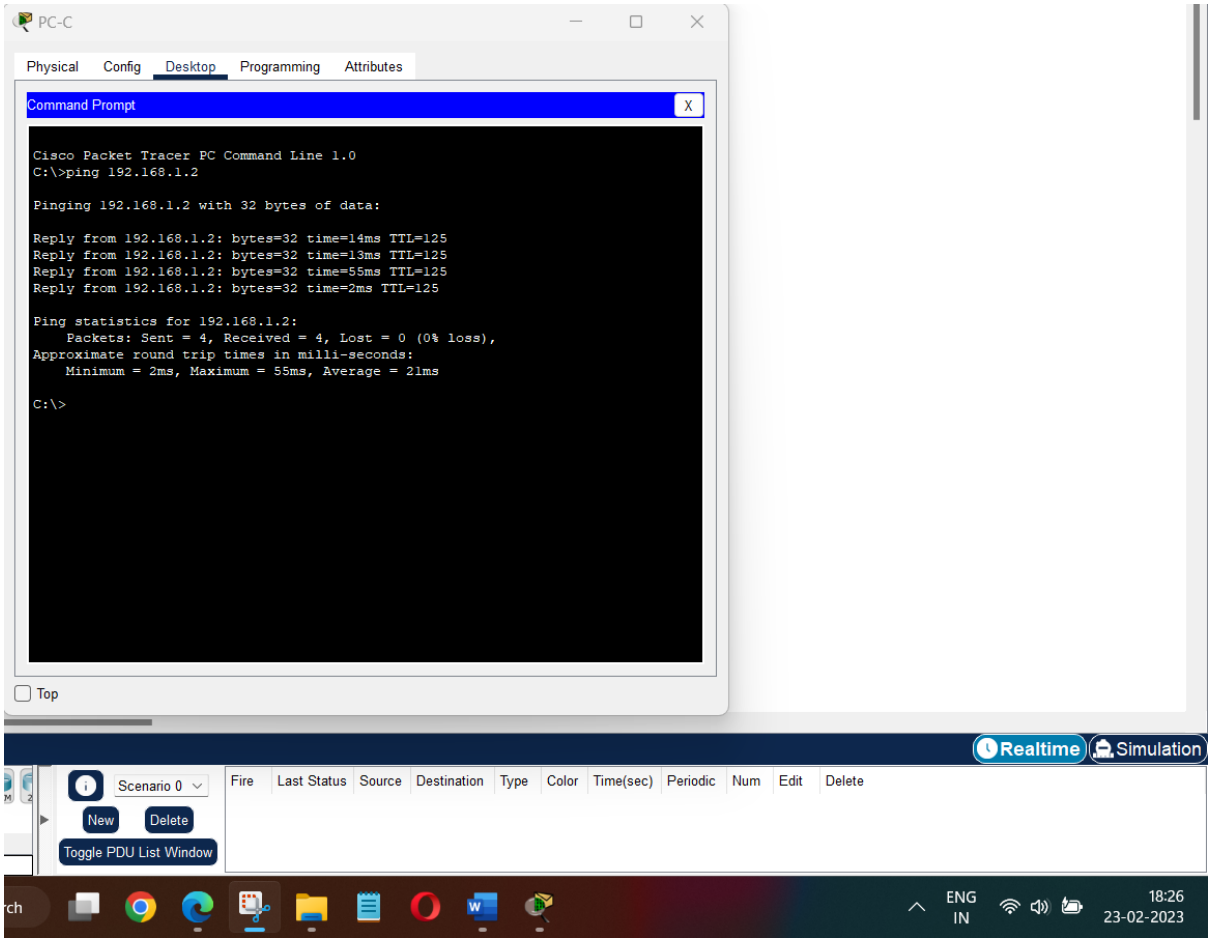
Successfully Enabled.

Step 2 : Verify Network Connectivity

Ping from PC-C to PC-A. The ping should be successful.

Ping from PC-A to PC-C. The ping should be successful.

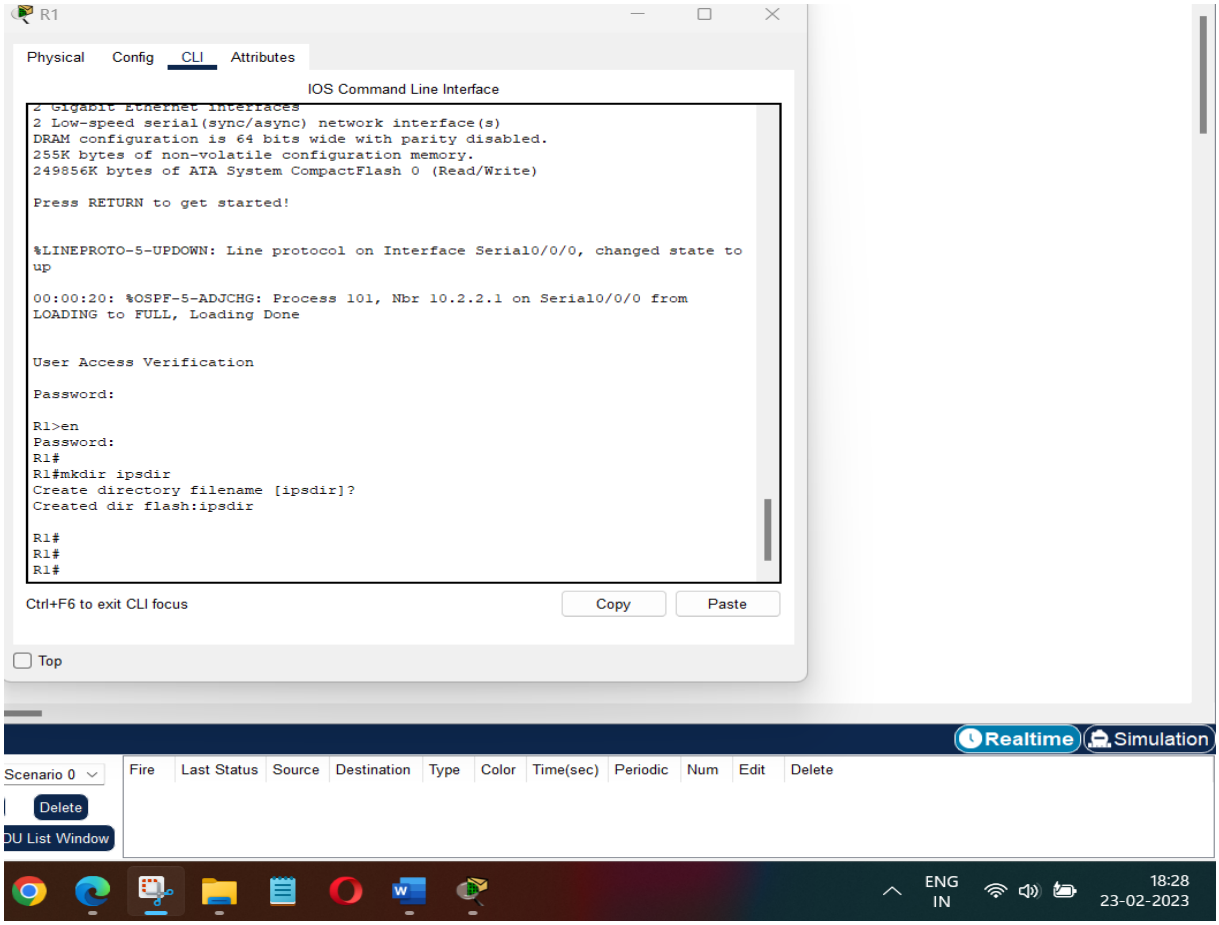

PC-A
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.2
Pinging 192.168.3.2 with 32 bytes of data:
Request timed out.
Reply from 192.168.3.2: bytes=32 time=3ms TTL=125
Reply from 192.168.3.2: bytes=32 time=2ms TTL=125
Reply from 192.168.3.2: bytes=32 time=2ms TTL=125
Ping statistics for 192.168.3.2:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 3ms, Average = 2ms
C:\>ping 192.168.3.2
Pinging 192.168.3.2 with 32 bytes of data:
Reply from 192.168.3.2: bytes=32 time=13ms TTL=125
Reply from 192.168.3.2: bytes=32 time=19ms TTL=125
Reply from 192.168.3.2: bytes=32 time=58ms TTL=125
Reply from 192.168.3.2: bytes=32 time=2ms TTL=125
Ping statistics for 192.168.3.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 58ms, Average = 23ms
C:\>
Top
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete
ENG
IN
18:25
23-02-2023


PC-C
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=14ms TTL=125
Reply from 192.168.1.2: bytes=32 time=13ms TTL=125
Reply from 192.168.1.2: bytes=32 time=55ms TTL=125
Reply from 192.168.1.2: bytes=32 time=2ms TTL=125
Ping statistics for 192.168.1.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 55ms, Average = 21ms
C:\>
Top
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete
ENG
IN
18:26
23-02-2023

Step 3 : Create an IOS IPS configuration directory in flash

On R1, create a directory in flash using the mkdir command. Name the directory ipsdir.

R1# mkdir ipsdir
Create directory filename [ipsdir]? <Enter>
Created dir flash:ipsdir



Step 4 : Configure the IPS signature storage location

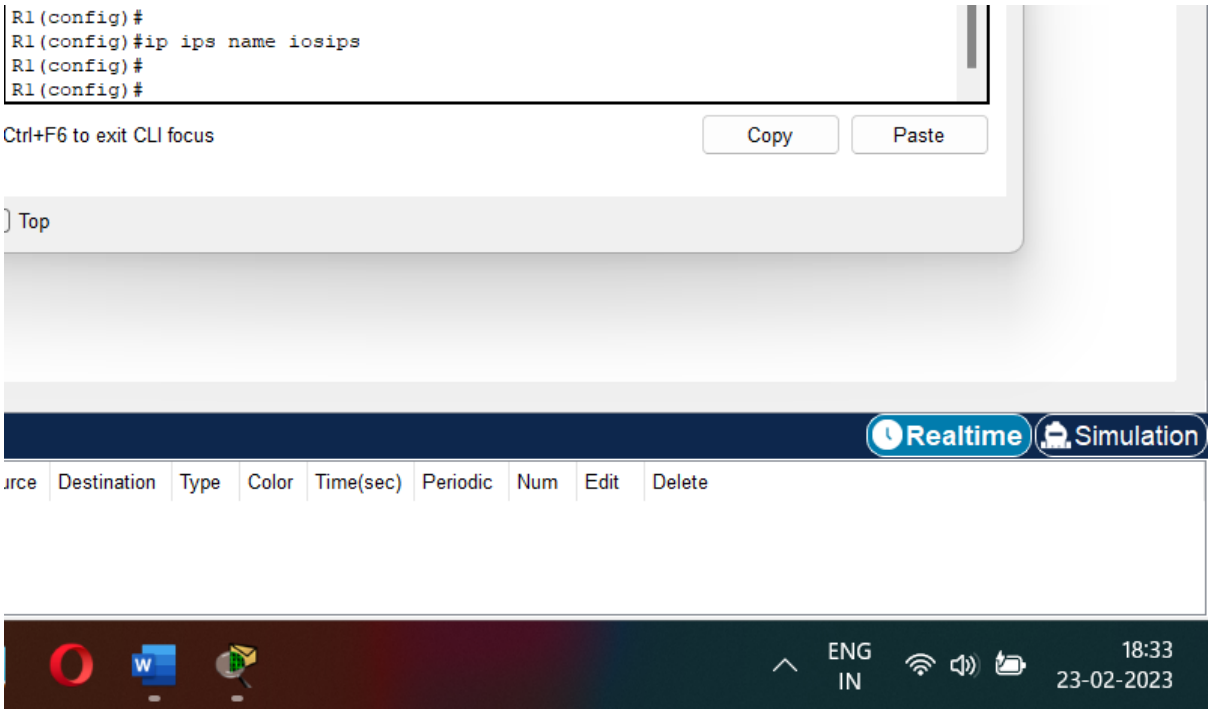
On R1, configure the IPS signature storage location to be the directory just created.

R1(config)# ip ips config location flash:ipsdir

Step 5 : Create an IPS rule

On R1, create an IPS rule name using the ip ips name name command in global configuration mode. Name the IPS rule iosips.

R1(config)# ip ips name iosips



Step 6 : Enable logging

IOS IPS supports the use of syslog to send event notification. ***Syslog notification is enabled by default***. If logging console is enabled, IPS syslog messages display.

Enable syslog if it is not enabled.

R1(config)# ip ips notify log

If necessary, use the clock set command from privileged EXEC mode to reset the clock.

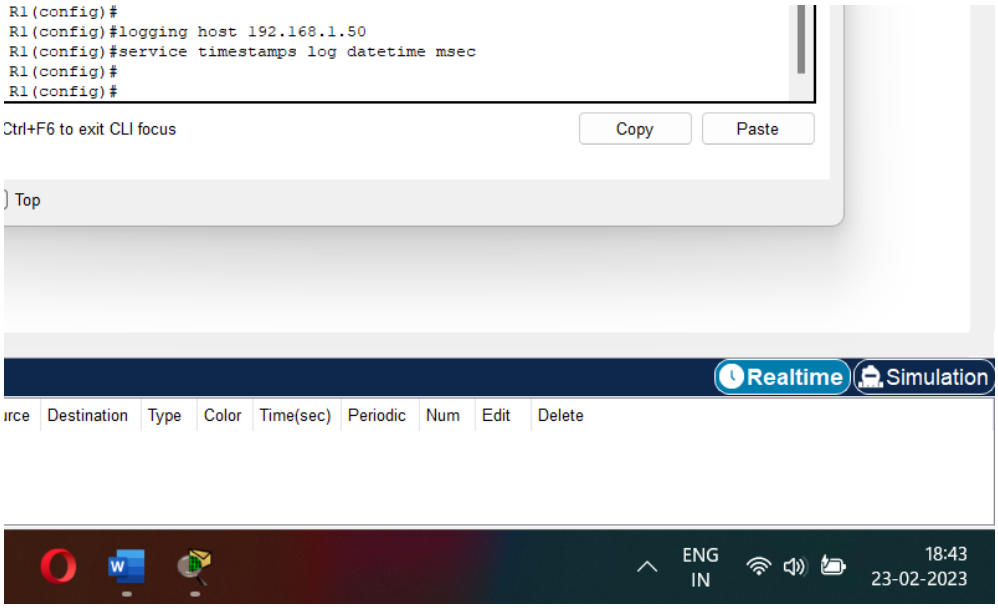
R1# clock set 10:20:00 10 january 2014

Verify that the timestamp service for logging is enabled on the router using the show run command. Enable the timestamp service if it is not enabled.

R1(config)# service timestamps log datetime msec

Send log messages to the syslog server at IP address 192.168.1.50.

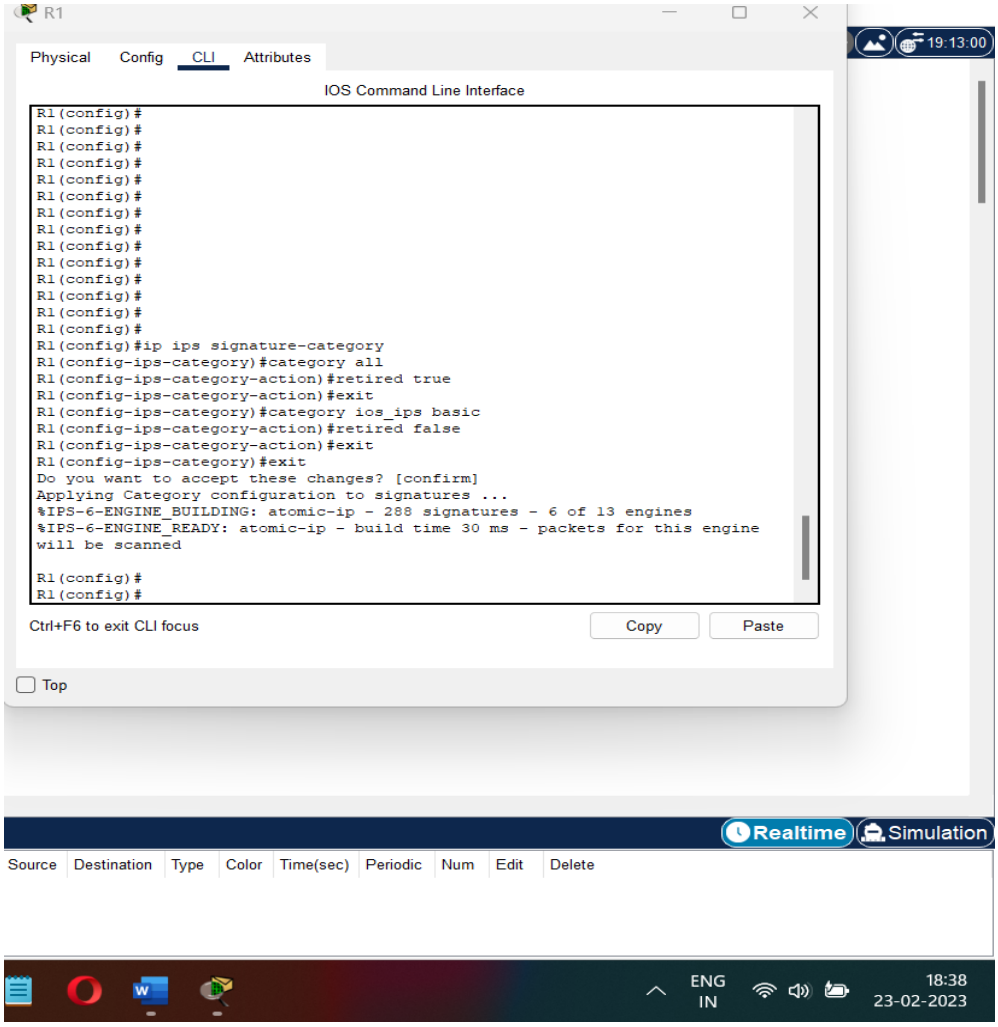
R1(config)# logging host 192.168.1.50



Step 7 : Configure IOS IPS to use the signature categories

Retire the all signature category with the retired true command (all signatures within the signature release). Unretire the IOS_IPS Basic category with the retired false command.

R1(config)# ip ips signature-category
R1(config-ips-category)# category all
R1(config-ips-category-action)# retired true
R1(config-ips-category-action)# exit
R1(config-ips-category)# category ios_ips basic
R1(config-ips-category-action)# retired false
R1(config-ips-category-action)# exit
R1(config-ips-cateogry)# exit
Do you want to accept these changes? [confirm] <Enter>

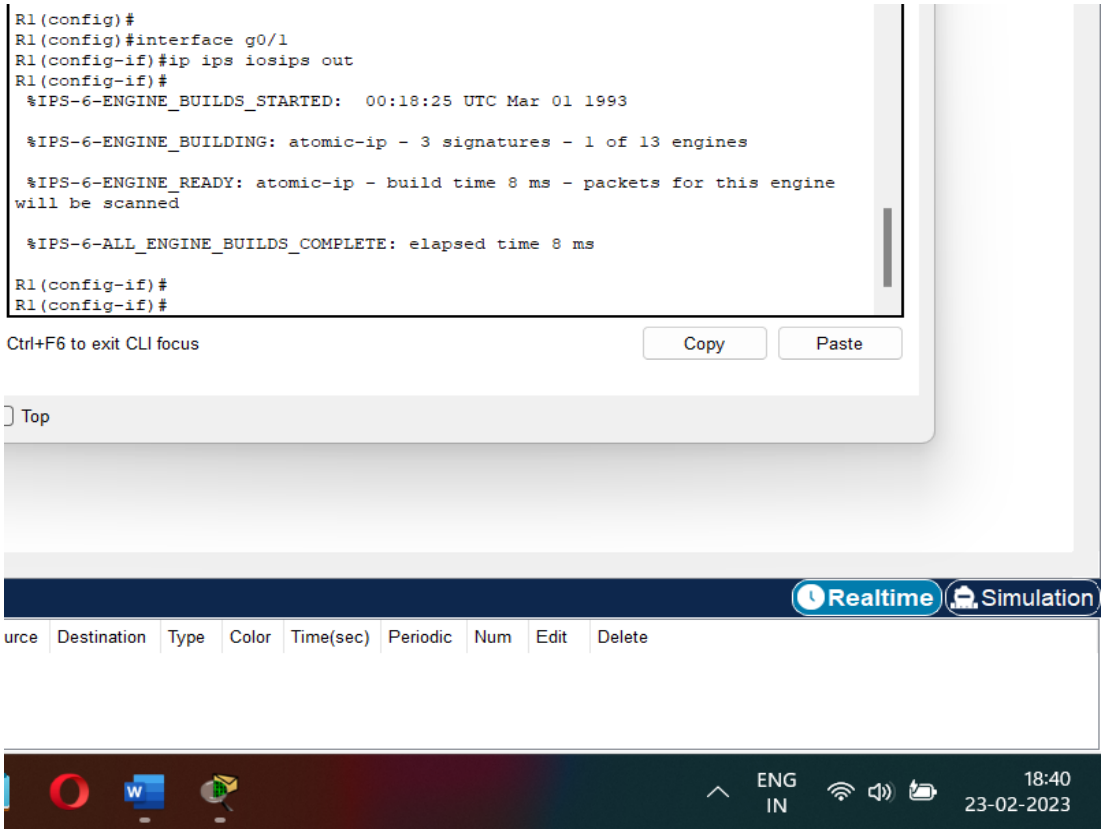


Step 8 : Apply the IPS rule to an interface

Apply the IPS rule to an interface with the ip ips name direction command in interface configuration mode. Apply the rule outbound on the G0/1 interface of R1. After you enable IPS, some log messages will be sent to the console line indicating that the IPS engines are being initialized.

The direction in means that IPS inspects only traffic going into the interface. Similarly, out means that IPS inspects only traffic going out of the interface.

R1(config)# interface g0/1
R1(config-if)# ip ips iosips out

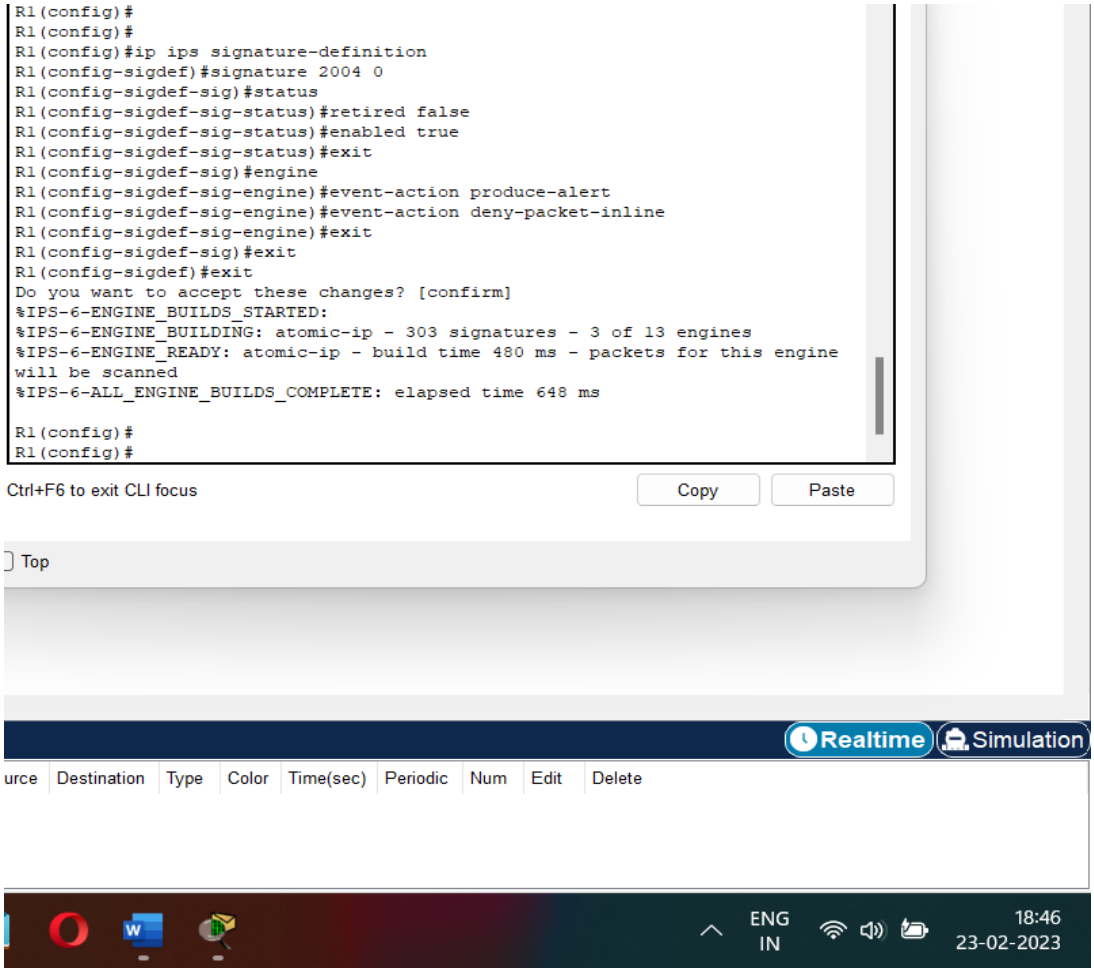


Part 2 : Modify the Signature

Step 1 : Change the event-action of a signature.

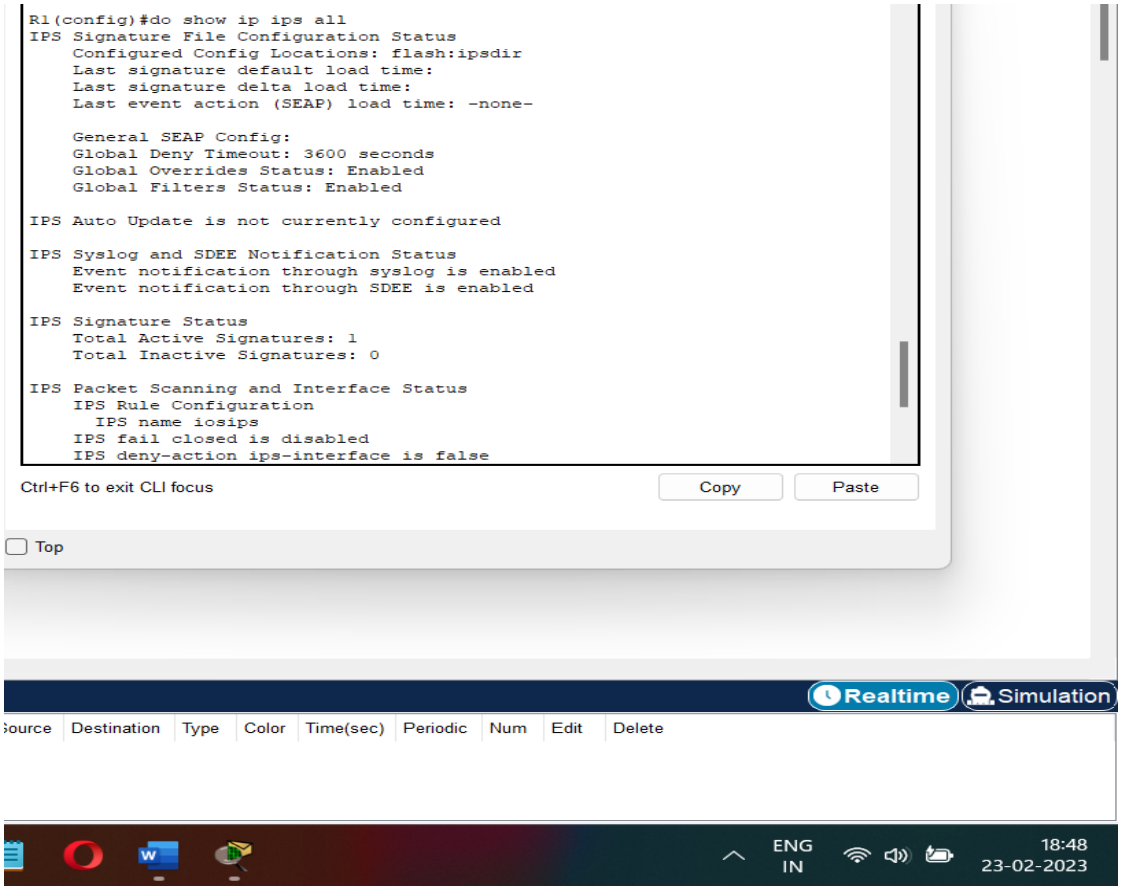
Un-retire the echo request signature (signature 2004, subsig ID 0), enable it, and change the signature action to alert and drop.

R1(config)# ip ips signature-definition
R1(config-sigdef)# signature 2004 0
R1(config-sigdef-sig)# status
R1(config-sigdef-sig-status)# retired false
R1(config-sigdef-sig-status)# enabled true
R1(config-sigdef-sig-status)# exit
R1(config-sigdef-sig)# engine
R1(config-sigdef-sig-engine)# event-action produce-alert
R1(config-sigdef-sig-engine)# event-action deny-packet-inline
R1(config-sigdef-sig-engine)# exit
R1(config-sigdef-sig)# exit
R1(config-sigdef)# exit
Do you want to accept these changes? [confirm] <Enter>



Step 2 : Use show commands to verify IPS

Use the '*do show ip ips all*' command to view the IPS configuration status summary.



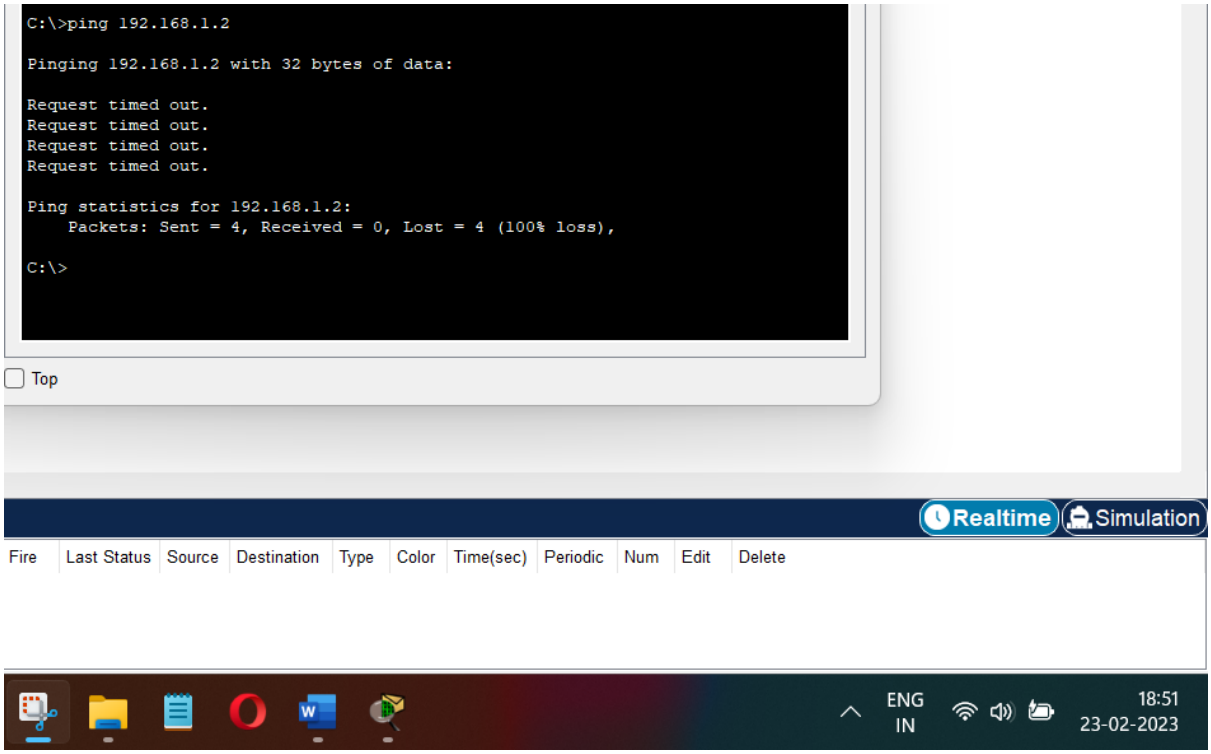
Step 3 : Verify that IPS is working properly

From PC-C, attempt to ping PC-A.

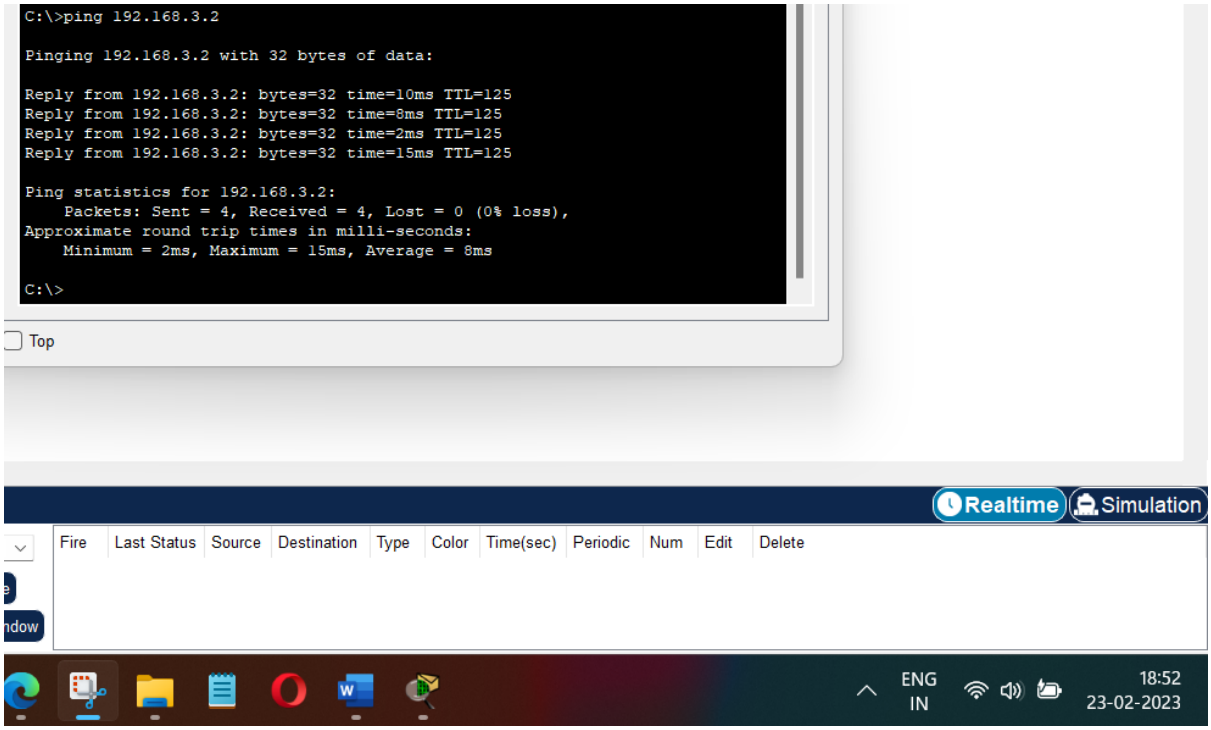
The pings should fail. This is because the IPS rule for event-action of an echo request was set to "denypacket-inline".

From PC-A, attempt to ping PC-C.

The ping should be successful. This is because the IPS rule does not cover echo reply. When PC-A pings PC-C, PC-C responds with an echo reply.



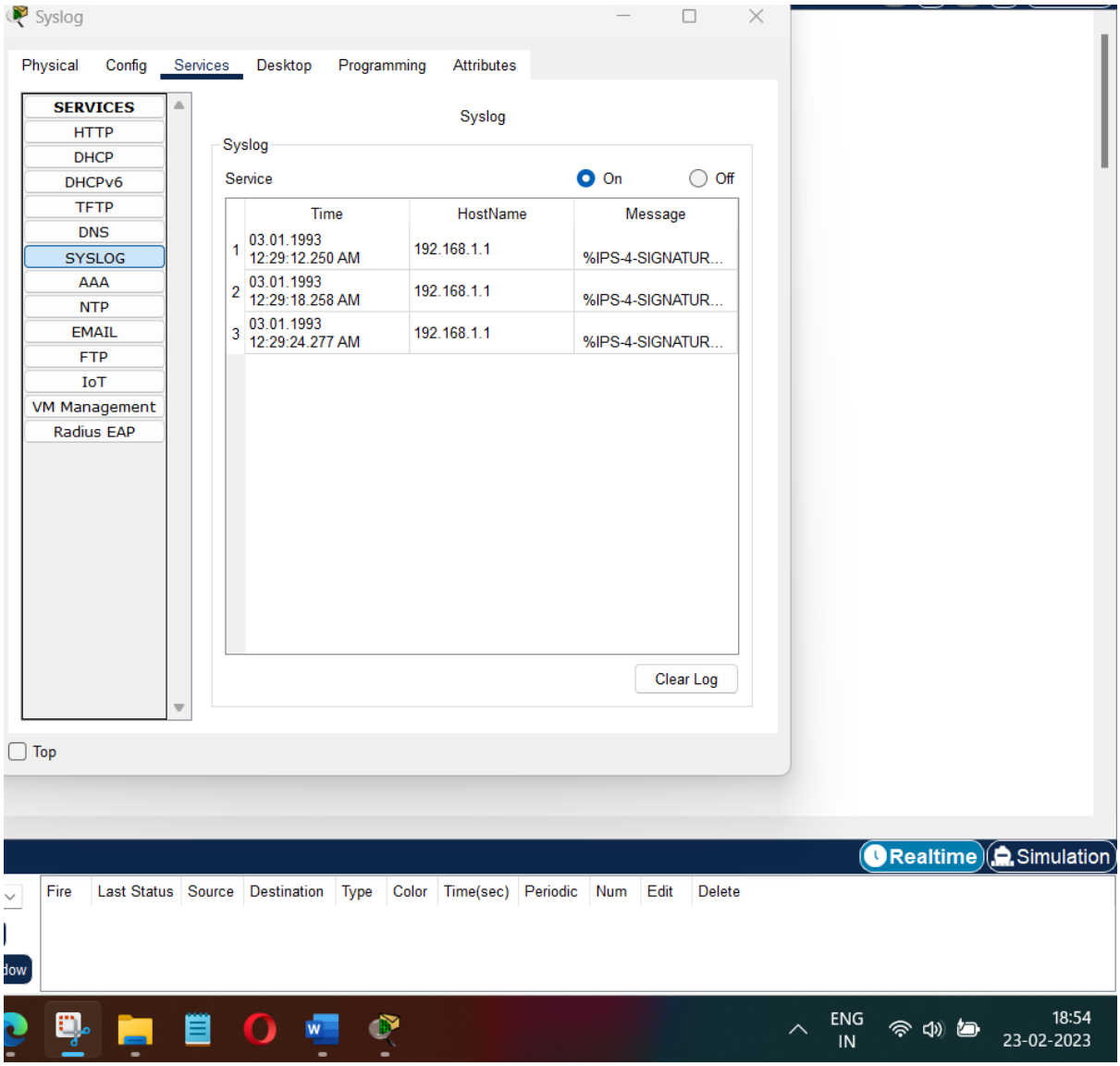
From PC-C to PC-A



From PC-A to PC-C

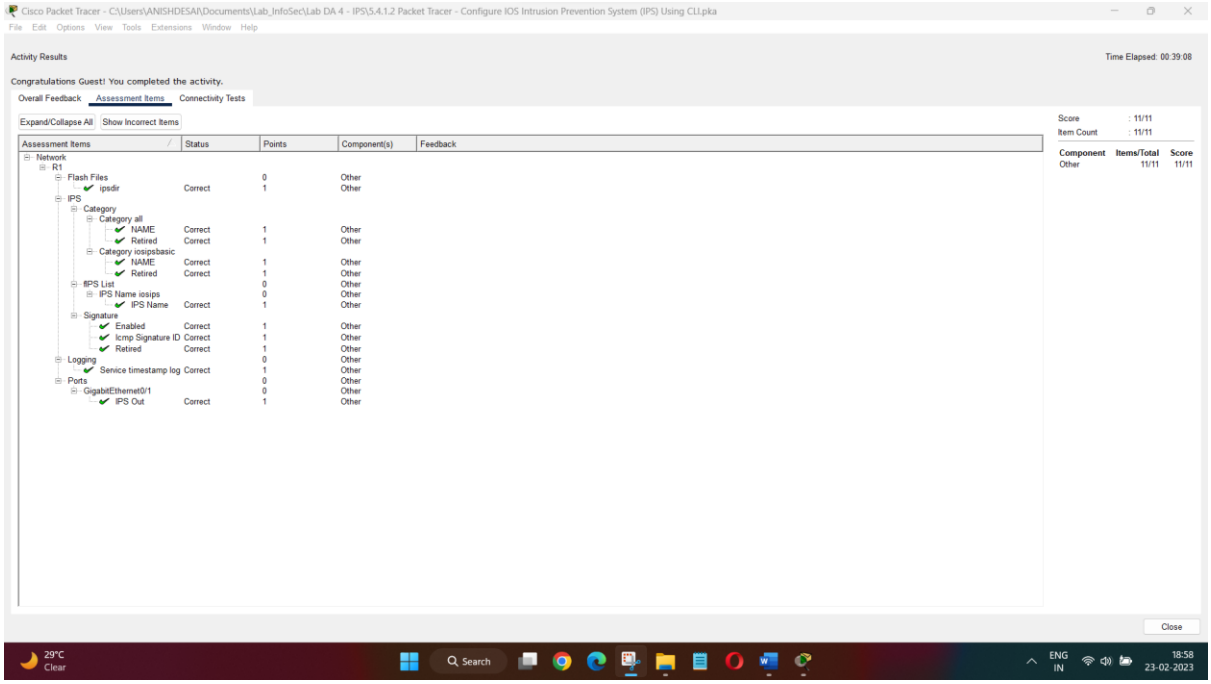
Step 4 : View the syslog messages.

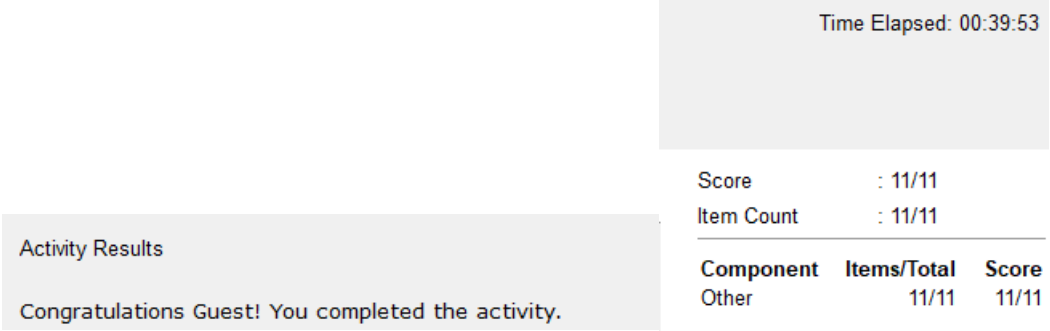
a. Click the Syslog server.
b. Select the Services tab.
c. In the left navigation menu, select SYSLOG to view the log file.



Step 5 : Check results.

Completion percentage should be 100%. Click Check Results to see feedback and verification of which required components have been completed.





As seen from the above Results, 100% completion has been achieved.
