



VIT[®]
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

CSE 3502

Information Security Management

Winter Semester 2022-23

Lab Report – 4

Configuration of IOS Intrusion Prevention System (IPS)

Name: Aditya Krishna

Reg No.: 20BCE0456

Guided by: Prof. Lavanya K

24th Feb, 2023

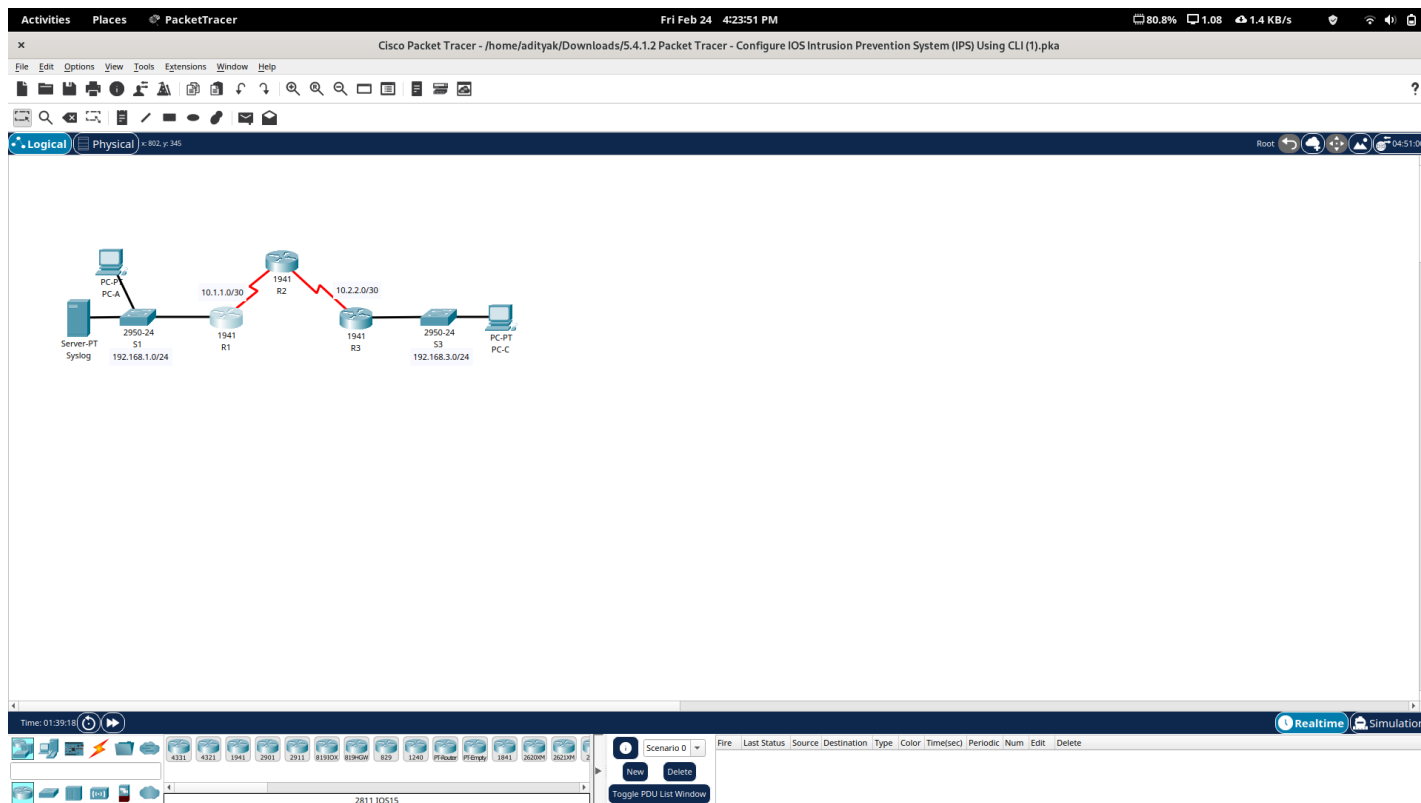
Introduction :

An IOS Intrusion Prevention System (IOS IPS) is a security technology designed to detect and prevent various types of network attacks, including network-based and application-based attacks, from penetrating and exploiting vulnerabilities in a network. It is implemented as a software module within the Cisco IOS software running on routers and switches. The IOS IPS performs real-time traffic analysis of network traffic passing through the device, compares it against predefined attack signatures, and takes action to block the traffic that matches these signatures. The IPS can operate in inline mode, where it actively blocks suspicious traffic, or in promiscuous mode, where it only monitors traffic and sends alerts to the network administrator for further analysis. By proactively identifying and blocking potential threats, an IOS IPS helps to improve the overall security posture of a network and minimize the risk of security breaches

Objectives/AIM

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

Step 0: Make the topology



IP Addressing Table

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

Assign IP's respectively & enable the connections.

Part 1: Enable IOS IPS

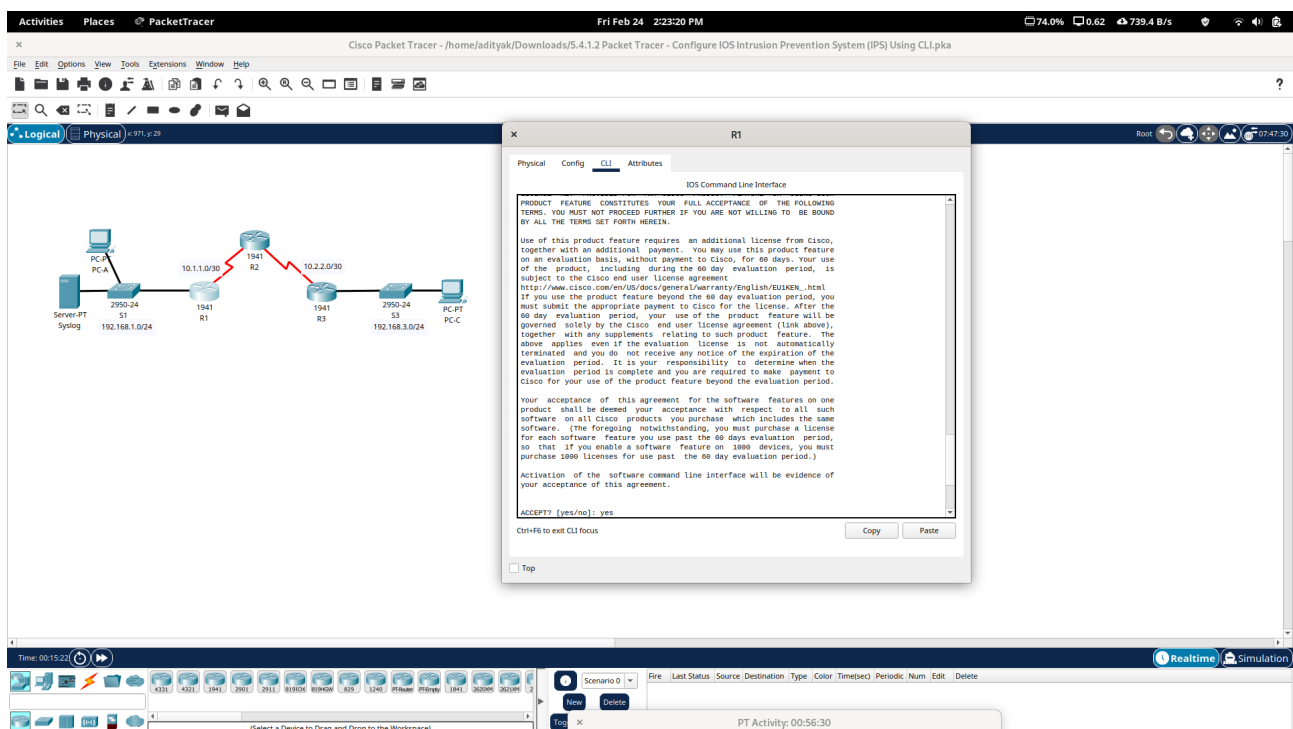
Step 1: Enable the Security Technology package.

a. On **R1**, issue the **show version** command to view the Technology Package license information.

b. If the Security Technology package has not been enabled, use the following command to enable the package.

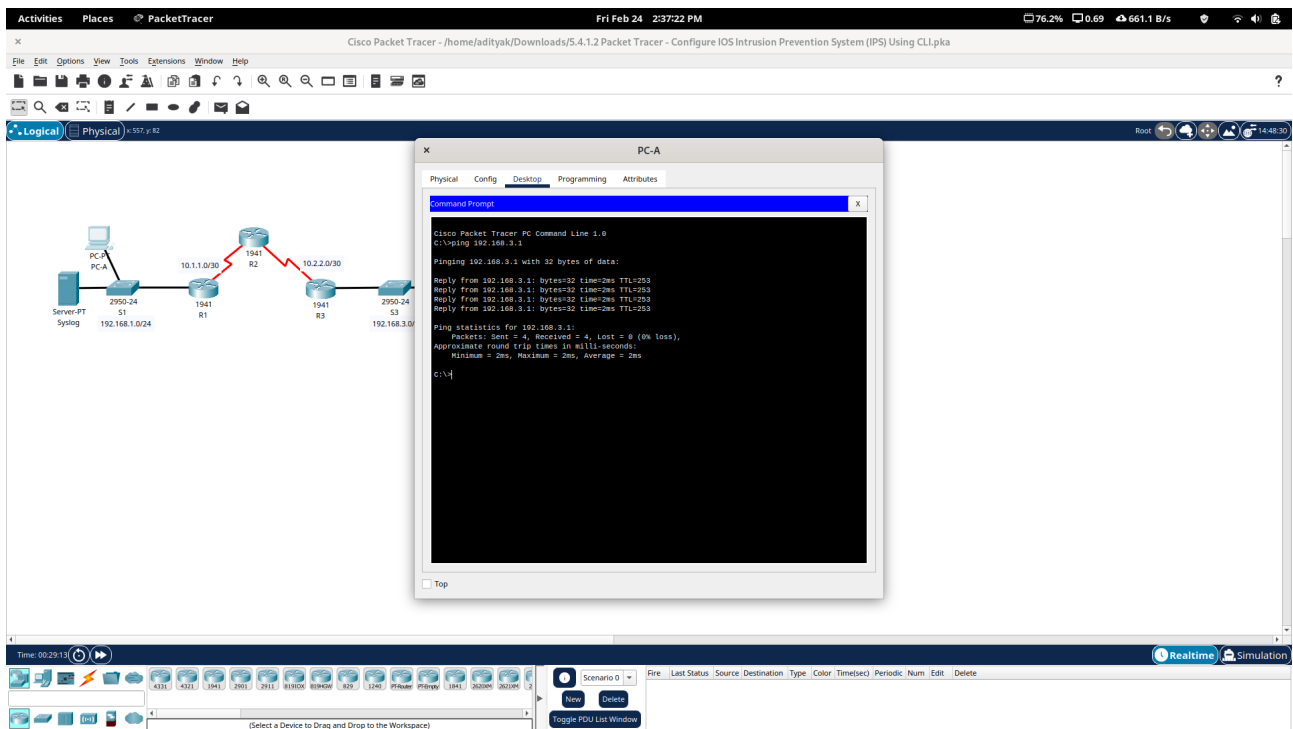
```
R1(config)# license boot module c1900 technology-package securityk9
```

c. Accept the end user license agreement.



d. Save the running-config and reload the router to enable the security license.

e. Verify that the Security Technology package has been enabled by using the **show version** command.



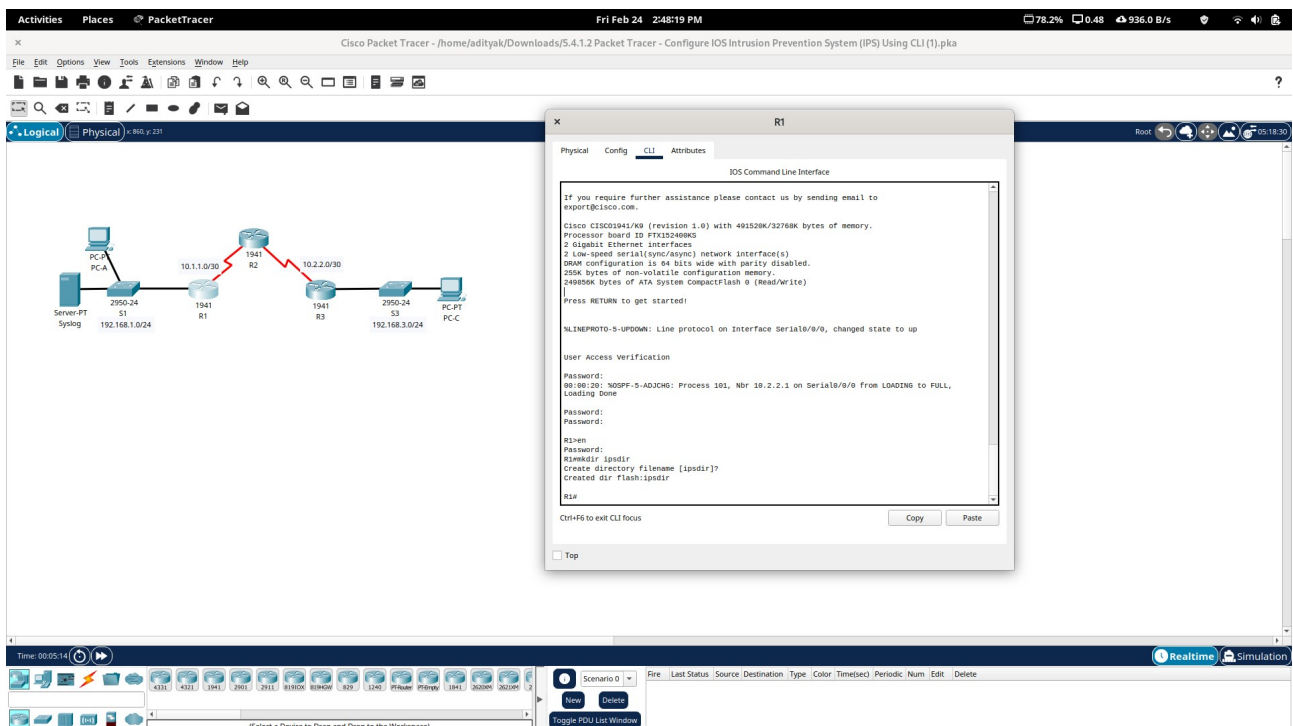
Step 3: Create an IOS IPS configuration directory in flash.

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 you just created.

```
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**.

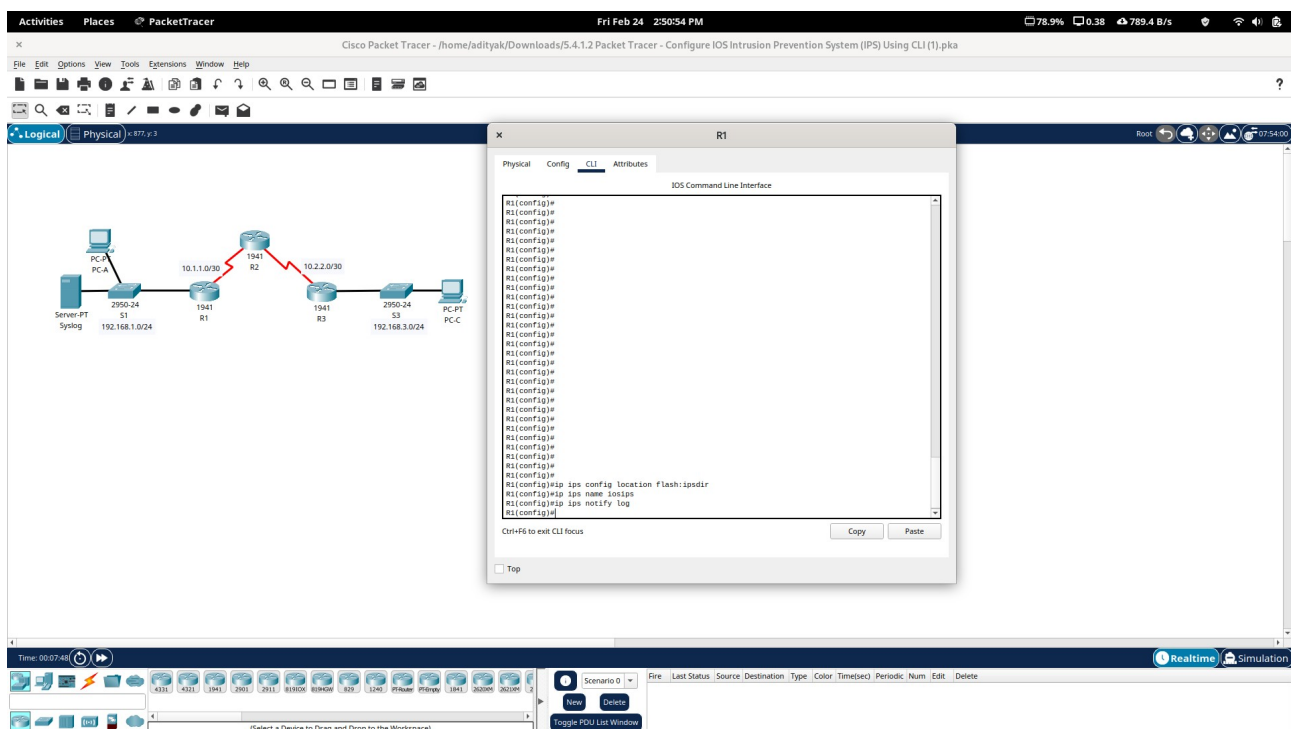
```
ip ips name iosips
```

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.

a.Enable syslog if it is not enabled

```
ip ips notify log
```



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

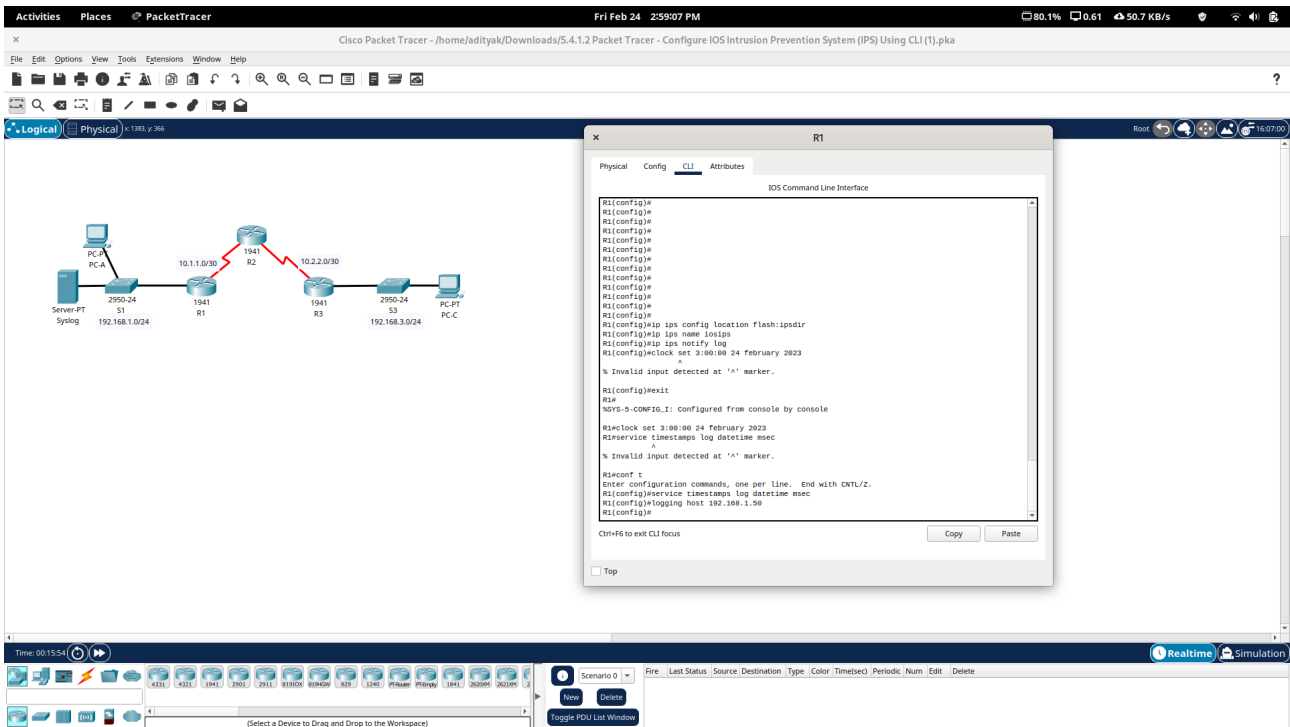
R1# clock set 10:20:00 10 january 2014

c. 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
```

d.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. Unretire the **IOS_IPS Basic** category with the **retired false** command.

```
R1(config-ips-category)# category all
```

```
R1(config-ips-category-action)# retired true
```

```
R1(config-ips-category-action)# exit
```

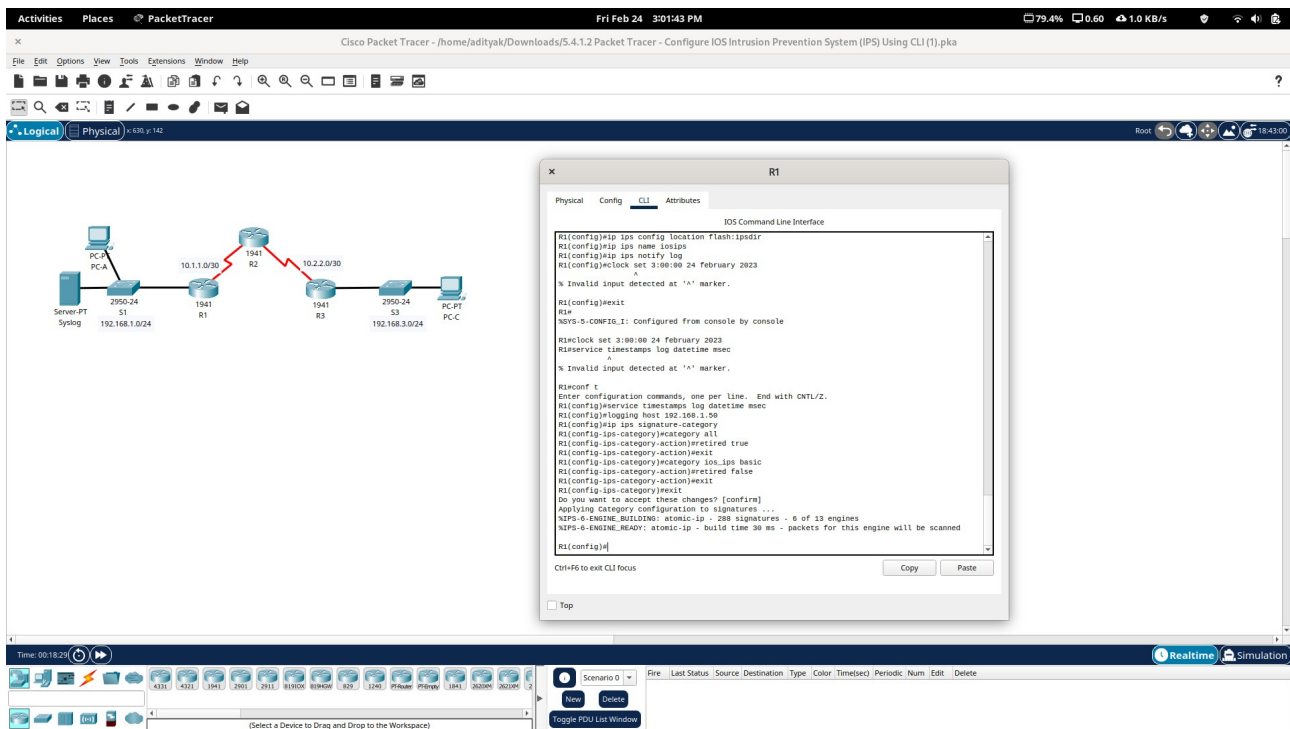
```
R1(config-ips-category)# category ios ips basic
```

```
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>

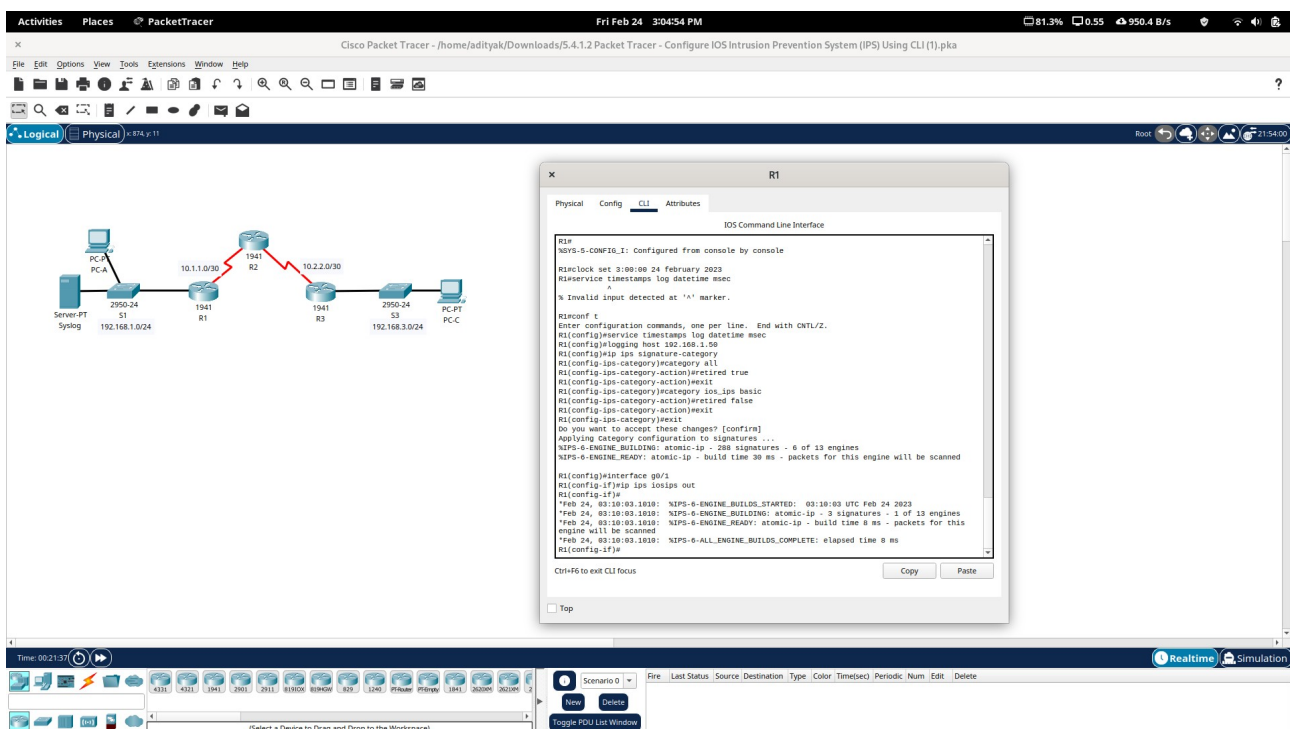


Step 8: Apply the IPS rule to an interface.

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.

R1(config)#interface g0/1

R1(config-if)#ip ips iosips out



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

```
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
```

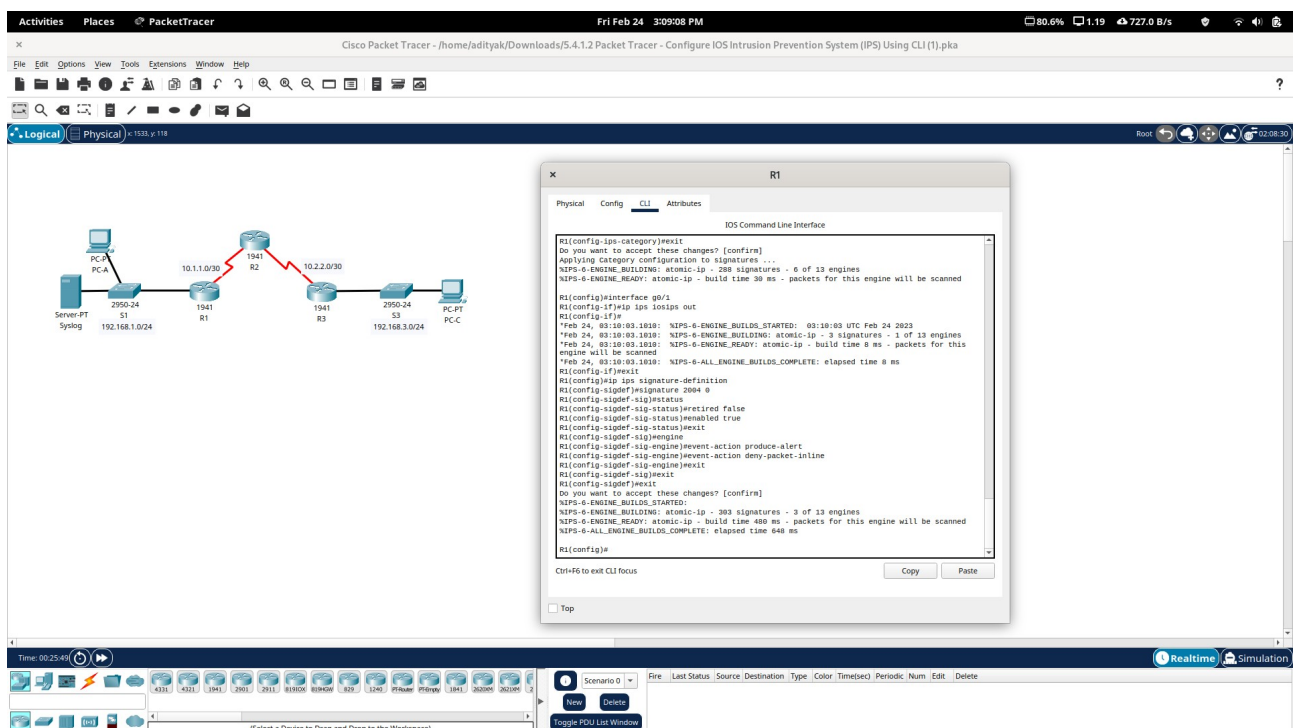
```
R1(config-sigdef-sig-engine)# event-action deny-packet-inline
```

```
R1(config-sigdef-sig-engine)# exit
```

```
R1(config-sigdef-sig)# exit
```

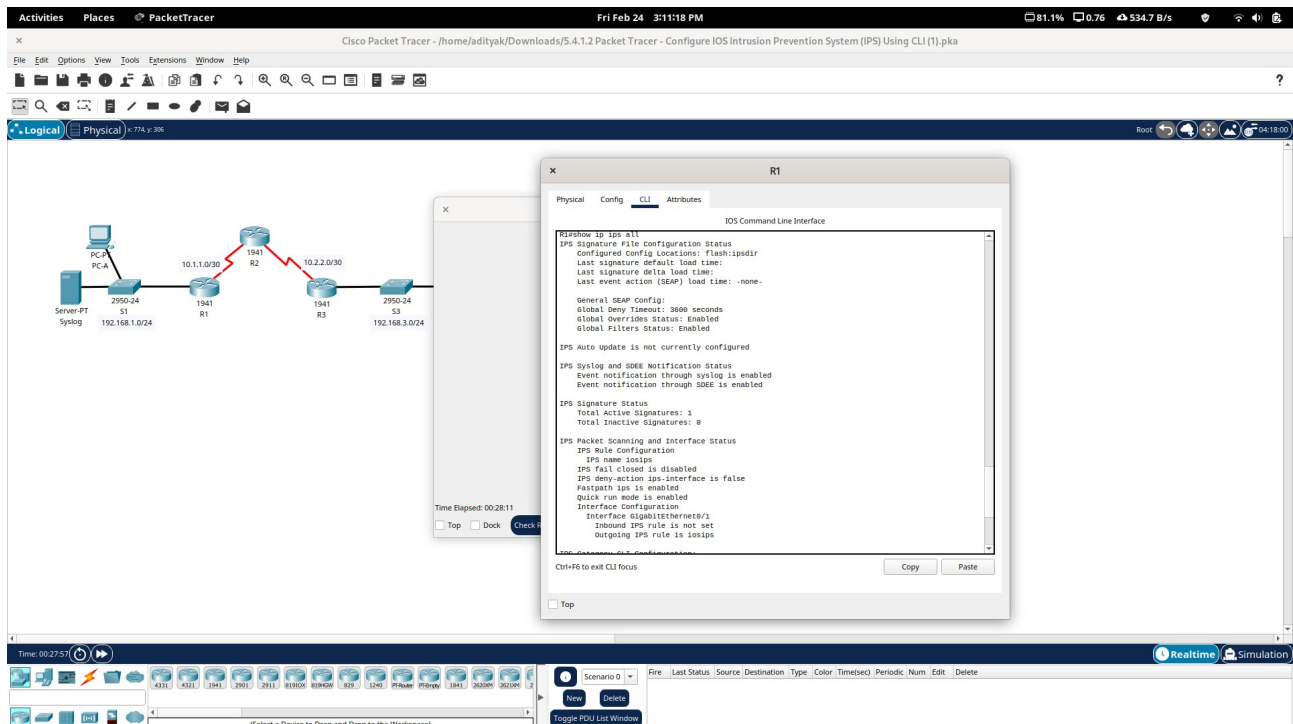
```
R1(config-sigdef)# exit
```

Do you want to accept these changes? [confirm] <Enter>



Step 2: Use show commands to verify IPS.

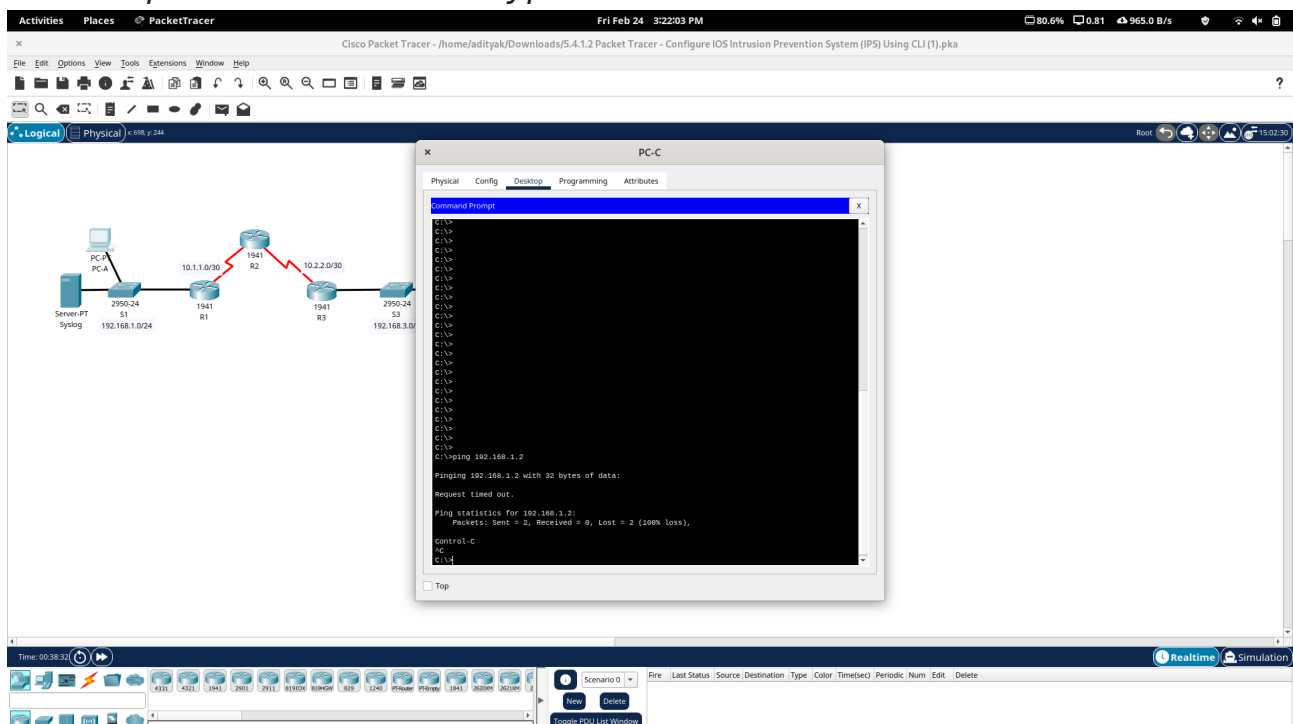
Use the **show ip ips all** command to view the IPS configuration status summary.



Step 3: Verify that IPS is working properly.

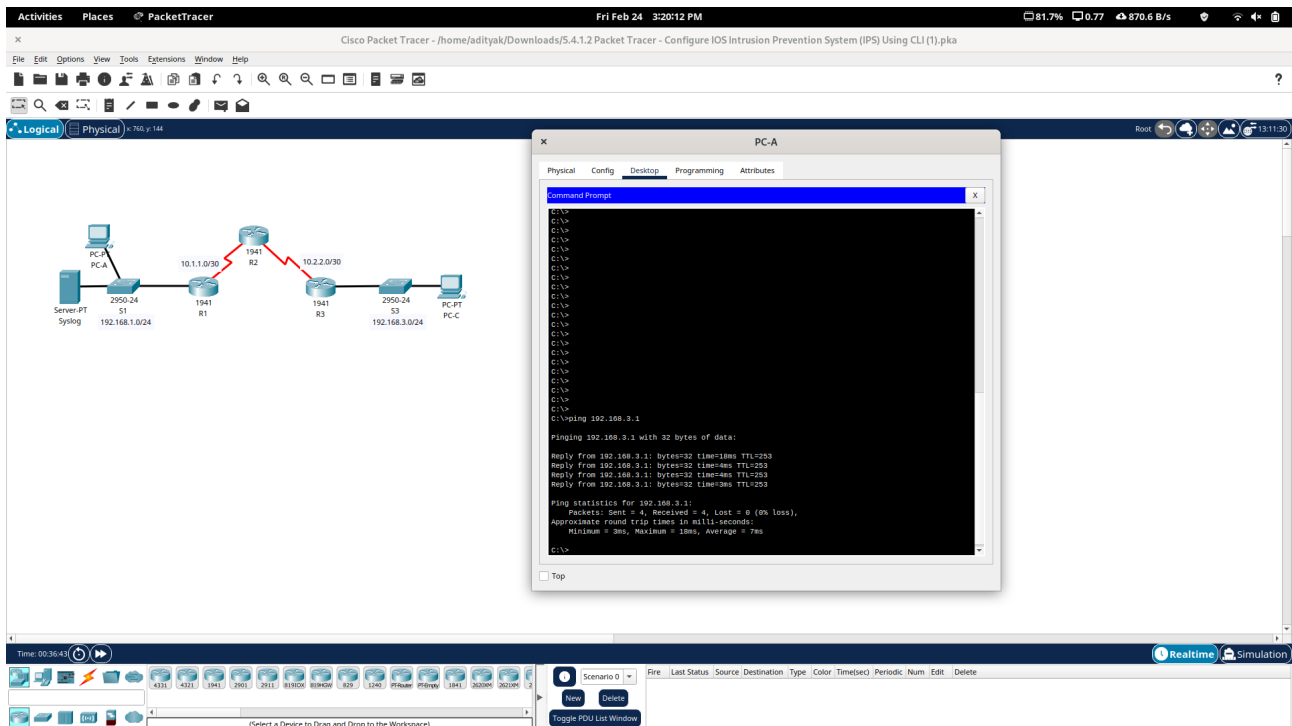
a. From **PC-C**, attempt to ping **PC-A**.

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



b. 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.

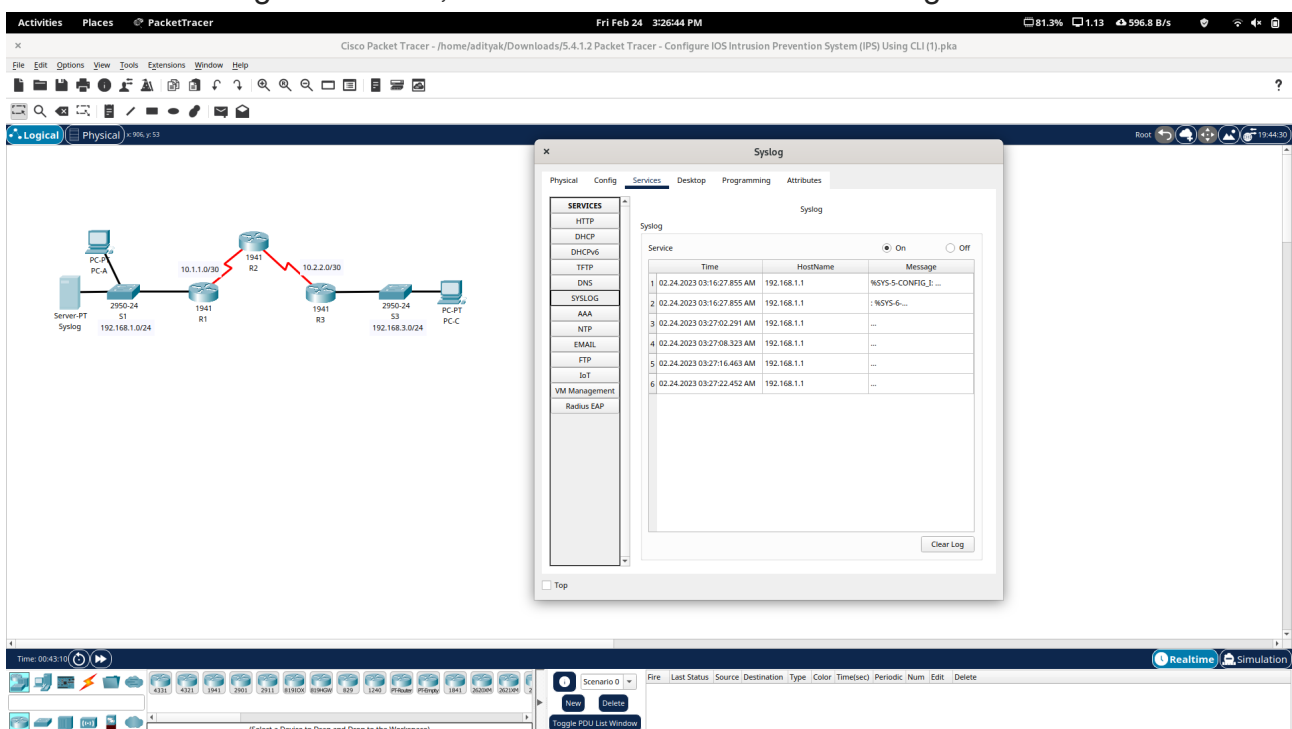


Step 4: View the syslog messages.

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.

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

Activities Places PacketTracer Fri Feb 24 3:30:53 PM 84.3% 1.28 636.5 B/s

Cisco Packet Tracer - /home/adityak/Downloads/5.4.1.2 Packet Tracer - Configure IOS Intrusion Prevention System (IPS) Using CLI (1).pka

File Edit Options View Tools Extensions Window Help

Activity Results Time Elapsed: 00:47:45

Congratulations Guest! You completed the activity.

Overall Feedback Assessment Items Connectivity Tests

Expand/Collapse All Show Incorrect Items

Assessment Items	Status	Points	Component(s)	Feedback
Network				
R1				
Flash Files		0	Other	
✓ ipdir	Correct	1	Other	
IPS				
Category				
Category all				
✓ NAME	Correct	1	Other	
✓ Retired	Correct	1	Other	
Category iospsbasic				
✓ NAME	Correct	1	Other	
✓ Retired	Correct	1	Other	
RPS List		0	Other	
RPS Name help		0	Other	
✓ RPS Name	Correct	1	Other	
Signature				
✓ Enabled	Correct	1	Other	
✓ Signature ID	Correct	1	Other	
✓ Retired	Correct	1	Other	
Logging		0	Other	
✓ Service timestamp log	Correct	1	Other	
Ports		0	Other	
GigabitEthernet0/1		0	Other	
✓ IPS Out	Correct	1	Other	

Score : 11/11
Item Count : 11/11

Component	Items/Total	Score
Other	11/11	11/11

Close