Complete the following. Please read all the way through first.

Once you complete the items below turn in any documents, spreadsheets, or diagrams used to complete this goal.

a. SNMP

i. Set up a SNMP server connected to a switch with 2 PC hosts.

1.You choose what version of SNMP and write it out and why you chose it

2.What's the difference between v1,2, 3

3.What is r/w and a community string

4.What is a MIB?

5.What are OID identifiers

b. Syslog

i. Set up a syslog server and a host or 2 on a switch. Show a syslog set up and working.

1.List some of the events available.

2.Why is this important?

3.What does this have to do with security?

c. SPAN /TAP

i. Setup a span port on a switch. If you want, put a sniffer on that port. Set up 1 monitor session.

1.What is allowed or not allowed?

2.Why would you want a core switch in a network to have a span port available to you as an engineer?

3.Is it really mirroring?

4.What is its purpose in networking and how could it be used and be helpful in security?

SNMP

SNMP configuration

The following file shows the network topology of a SNMP configuration on a router I used SNMPv3 because SNMPv3 has better security than versions 1 and 2. On SNMPv3 I can toggle a set of security levels that I may want to use, encrypt communication, and set authentication on the server by providing a username and password.

SNMP_Configuration.
pkz

Security Levels in SNMPv3

- noAuthnoPriv - Communication without authentication and privacy.
- authNoPriv - Communication with authentication and without privacy. The protocols used for Authentication are MD5 and SHA (Secure Hash Algorithm).
- authPriv - Communication with authentication and privacy. The protocols used for Authentication are MD5 and SHA; and for Privacy, DES (Data Encryption Standard) and AES (Advanced Encryption Standard) protocols can be used. For Privacy Support, you have to install some third-party privacy packages. Details about installation is dealt with in the topic "Privacy Support"

Difference between SNMPv1, v2, v3

- a community string is the only security method in the SNMPv1.
- Both SNMP version 1 and 2 provides authentication using a community string, which is a shared secret between the agent and the client that is passed in plain text over the network.
- SNMP version 3 supports user authentication and message encryption thus providing more security.
- Although SNMPV3 is the most secure SNMP version to use SNMPV2 is currently the most used version because it is easier to use than SNMPv3. the major disadvantage of SNMPv2 is that there is no security provided to a person on the network while SNMPV3 enhances the security to a person on the network.

MIB/OID Identifiers

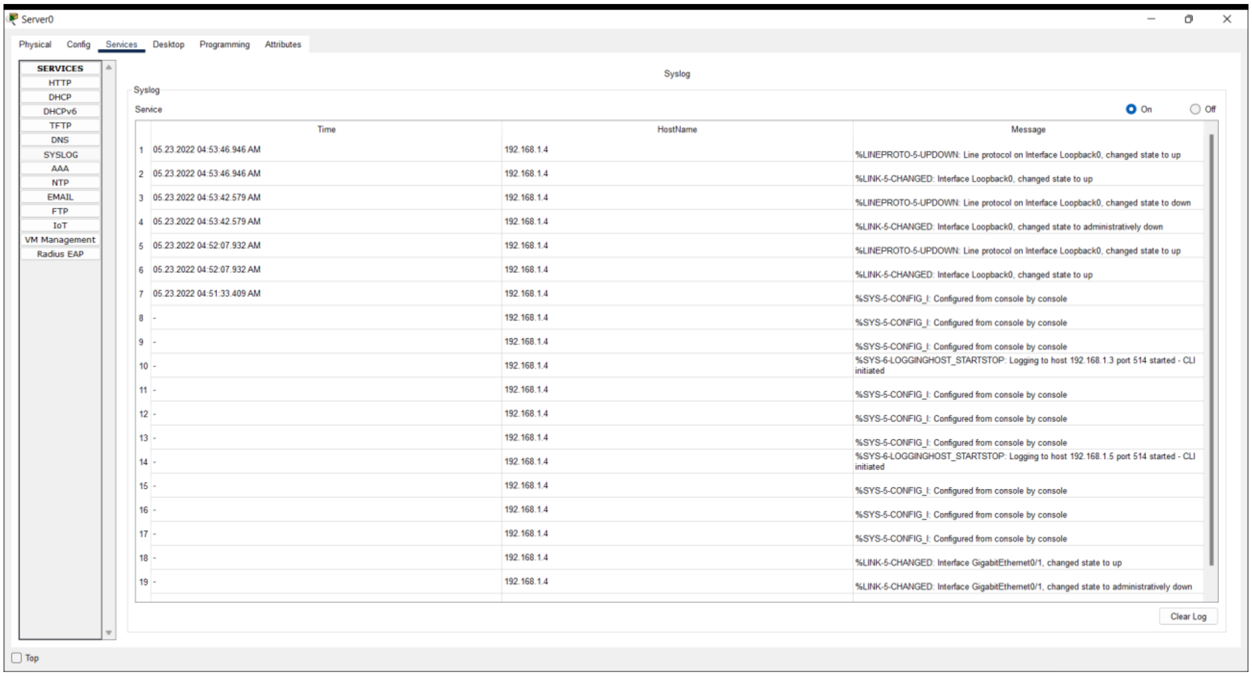
A Management Information Base (MIB) is a collection of information objects, organized as a tree. MIBs are accessed using a network-management protocol like SNMP. The following screenshot (Index.9) shows what an MIB tree looks like on CISCO Packet Tracer. The OID identifier shows the path in the MIB tree that stores information on the network. For example, the OID identifier for sysName is 1.3.6.1.2.1.1.5.0 (The path to get to sysName in the MIB Tree) The Value column displays the name that I have chosen for the system assigned with IP address 192.168.1.3. The name “Router” is what I have named the router device in the network.

<u>Syslog</u>

Syslog Configuration

The following file shows the network topology of a Syslog configuration on a Server. I have used NTP (Network Time Protocol) when configuring the Syslog server because it is important to have the current time across all network devices for accurate monitoring. The following screenshot shows the Syslog events of my activity on the IP address 192.168.1.4 with NTP configured on and off to show its importance.

Syslog_Configuration.pkz



Syslog

Service ● On ○ Off

	Time	HostName	Message
1	05.23.2022 04:53:46.946 AM	192.168.1.4	%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
2	05.23.2022 04:53:46.946 AM	192.168.1.4	%LINK-5-CHANGED: Interface Loopback0, changed state to up
3	05.23.2022 04:53:42.579 AM	192.168.1.4	%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to down
4	05.23.2022 04:53:42.579 AM	192.168.1.4	%LINK-5-CHANGED: Interface Loopback0, changed state to administratively down
5	05.23.2022 04:52:07.932 AM	192.168.1.4	%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
6	05.23.2022 04:52:07.932 AM	192.168.1.4	%LINK-5-CHANGED: Interface Loopback0, changed state to up
7	05.23.2022 04:51:33.409 AM	192.168.1.4	%SYS-5-CONFIG_I: Configured from console by console
8	-	192.168.1.4	%SYS-5-CONFIG_I: Configured from console by console
9	-	192.168.1.4	%SYS-5-CONFIG_I: Configured from console by console
10	-	192.168.1.4	%SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.1.3 port 514 started - CLI initiated
11	-	192.168.1.4	%SYS-5-CONFIG_I: Configured from console by console
12	-	192.168.1.4	%SYS-5-CONFIG_I: Configured from console by console
13	-	192.168.1.4	%SYS-5-CONFIG_I: Configured from console by console
14	-	192.168.1.4	%SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.1.5 port 514 started - CLI initiated
15	-	192.168.1.4	%SYS-5-CONFIG_I: Configured from console by console
16	-	192.168.1.4	%SYS-5-CONFIG_I: Configured from console by console
17	-	192.168.1.4	%SYS-5-CONFIG_I: Configured from console by console
18	-	192.168.1.4	%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
19	-	192.168.1.4	%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down

Syslog message format

The syslog message consists of three parts: PRI (a calculated priority value), HEADER (with identifying information), and MSG (the message itself).

The PRI data sent via the syslog protocol comes from two numeric values that help categorize the message. The first is the Facility value. This value is one of 15 predefined values or various locally defined values in the case of 16 to 23. These values categorize the type of message or which system generated the event.

Code	Facility description
0	Kernel messages
1	User-level messages
2	Mail System
3	System Daemons
4	Security/Authorization Messages
5	Messages generated by syslog
6	Line Printer Subsystem
7	Network News Subsystem
8	UUCP Subsystem
9	Clock Daemon
10	Security/Authorization Messages
11	FTP Daemon
12	NTP Subsystem
13	Log Audit
14	Log Alert
15	Clock Daemon
16 – 23	Local Use 0 - 7

Severity Levels

The second label of a syslog message categorizes the importance of the message in a numerical code from 0 to 7, the severity of the code, and the description of the severity.

Code | Severity | Description

0|EMERGENCY - A "panic" condition - notify all tech staff on call? - affects multiple apps/servers/sites.

1|ALERT - Should be corrected immediately - notify staff who can fix the problem - an example is loss of backup ISP connection.

2|CRITICAL - Should be corrected immediately but indicates failure in a primary system - fix CRITICAL problems before ALERT - an example is loss of primary ISP connection.

3|ERROR - Non-urgent failures - these should be relayed to developers or admins; each item must be resolved within a given time.

4|WARNING - Warning messages, indicated that an error will occur if action is not taken, e.g. file system 85% full - each item must be resolved within a given time.

5|NOTICE - Events that are unusual but not error conditions - might be summarized in an email to developers or admins to spot potential problems - no immediate action required.

6|INFORMATIONAL - Normal operational messages - may be harvested for reporting, measuring throughput, etc. - no action required.

7|DEBUG - Info is useful to developers for debugging the app, not useful during operations.

Why is it Important?

The primary use of syslog is for systems management. Proactive syslog monitoring pays off because it can significantly reduce downtime of servers and other devices in your infrastructure.

Network alerting: Syslog is extremely helpful in identifying critical network issues. For example, it can detect fabric channel errors on a switch fabric module. This is one of many such warnings or errors that other forms of monitoring metrics cannot detect.

Server alerting: Syslog can alert on server startups, clean server shutdowns, abrupt server shutdowns, configuration reloads and failures, runtime configuration impact, resource impact, and so on. All these alerts can help detect if the servers are alive. Syslog also helps detect failed connections. Server alerts are always useful, especially when you oversee hundreds of servers.

Application alerting: You need application alerting for troubleshooting live issues. Applications create logs in different ways, some through syslog. When you run a web application, dozens of logs are written in the log folder. To get real-time monitoring, you need a syslog monitoring solution that can observe changes in the log folder.

What does this have to do with security?

Syslog messages provide detailed context of security events. Security admins can use syslog to recognize communication relationships, timing, and in some cases, an attacker’s motive, and tools.

Syslog can also help maintain data integrity although it is a difficult process using syslog. the UDP packets used to transmit the data between hosts provide no guarantee of packet delivery. The nsyslog project, syslog-ng project and the SCSC Secure Syslog project address this issue by replacing UDP packets with TCP packets. The “modular syslog” project uses one-way hashes of the data to allow an administrator to verify that that has not been modified during its transfer or storage.

Availability of the event log server to accept syslog data is important. As the syslog protocol uses UDP for network delivery of data, there is no guarantee of data receipt. If it is possible to use one of the TCP based syslog replacements in an environment. The administrator should configure the syslog server with sufficient disk space to accept large amounts of event log data. This will reduce the chance of losing event data due to exhaustion of disk space. Monitoring of disk space usage on the filesystem or disk partition where this data is stored must be setup and notification of changes in disk space usage patterns should be made the administrators who monitor the system. The data that is collected on the system should be archived on a regular basis based upon the policies in place of an organization and based upon local, state, and federal regulation.

Span/Tap

Span port Configuration

The following file shows the network topology for a Span port configuration with a sniffer configured to the switch. The following screenshot (Index.12) displays the local SPAN configuration. I tested the SPAN port configuration by sending traffic from the source IP address to the destination IP address. The ICMP packet picked up by the packet sniffer (Index.13) displays the communication between the source and destination IP addresses. the SRC IP is 10.10.100 and the destination IP is 10.1.1.200.

SPAN_Configuration.
pkz

SPAN Terminology

Ingress Traffic: Traffic that enters the switch

Egress Traffic: Traffic that leaves the switch

Source (SPAN) port: A port that is monitored

Source (SPAN) VLAN: A VLAN whose traffic is monitored

Destination (SPAN) port: A port that monitors source ports. This is usually the point to which a network analyzer is connected.

Remote SPAN (RSPAN): When Source ports are not located on the same switch as the Destination port. RSPAN is an advanced feature that requires a special VLAN to carry the monitored traffic and is not supported by all switches. RSPAN explanation and configuration will be covered in another article.

What is allowed or not allowed?

Most switches allow adding more than one source port to the SPAN configuration, meaning that you can capture multiple devices or links at the same time on a single monitor port.

Too much traffic is not allowed on SPAN so when there is a high amount of traffic the switch will drop packets. This means that your capture device will only see an incomplete set of incoming packets, and doesn’t even know that there were drops, because they happened before the network card could ever see that there was an incoming packet. The switch has no way of signaling the capture device that it had to drop packets. So, creating a SPAN port for a port where you know that the bandwidth is really high in both directions (e.g. a backbone link) is not ideal.

When to have a span port available on a core switch

- Access to traffic that either stays within a switch or never reaches a physical link where the traffic can be tapped.

- Limited ad hoc monitoring in locations with SPAN capabilities where a network TAP does not currently exist.
- Locations with limited light budgets where the split ratio of a TAP may consume too much light. (Another possibility here would be to use an active TAP or more powerful optics capable of longer distances.)
- Production emergencies where there is no maintenance window in which to install a TAP.
- Remote locations with modest traffic that cannot justify a full-time TAP on the link.

Unlike a network Tap the functionality is available on your switch. Compared to a network tap, port mirroring is easy and cheap to configure. You don't need any additional hardware. This makes port mirroring particularly valuable when your network configuration is constrained by physical space or when you might only need to monitor a VLAN for a short period of time you'll just need to modify your switch configuration.

Port mirroring

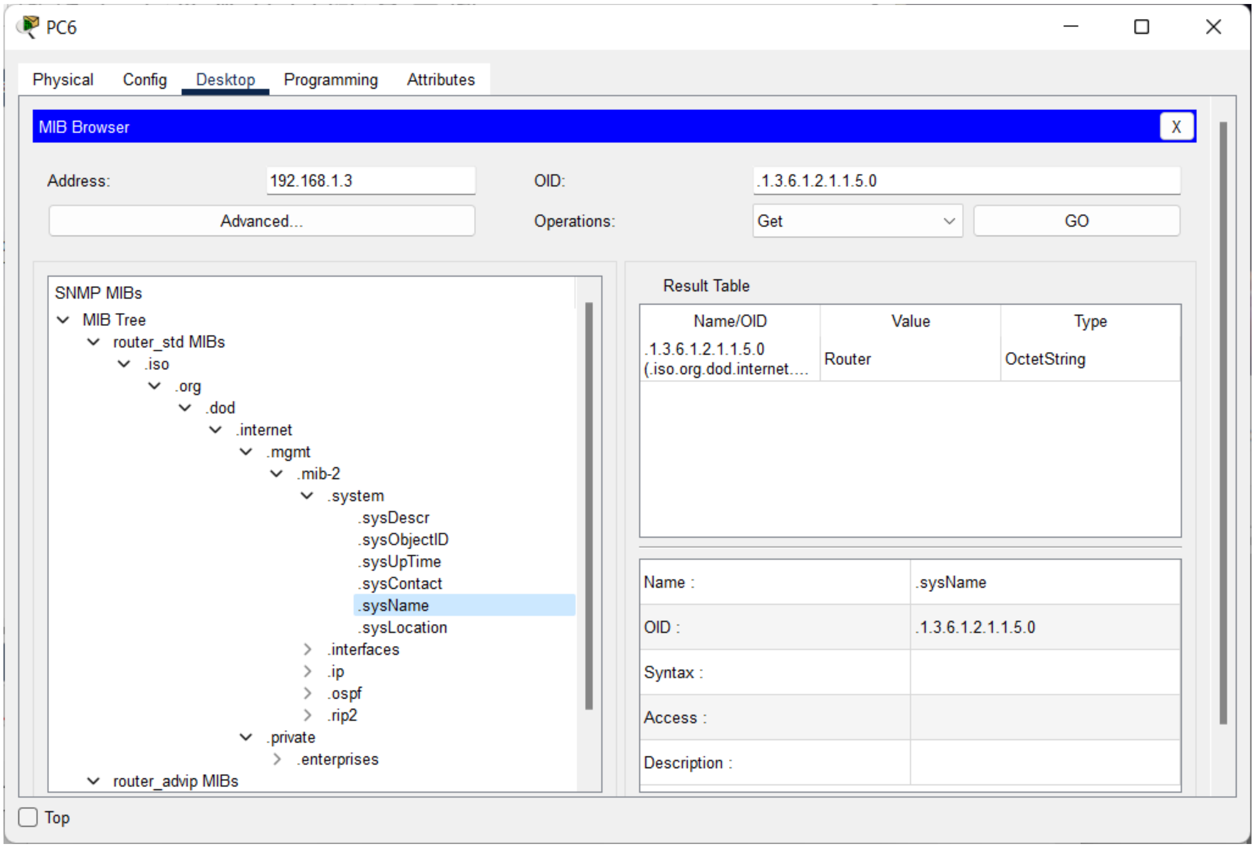
Port mirroring is used on a network switch or a router to send a copy of network packets seen on the specified ports (source ports) to other specified ports (destination ports). With port mirroring enables, the packets can be monitored and analyzed. Port mirroring is applied widely, for example, network engineers can use port mirroring to analyze and debug data or diagnose errors on their networks without affecting the packet processing capabilities of the network devices.

local port mirroring enables the network switch to forward the copy of the packet on the source port to the destination port. The monitoring device connected with the destination port can monitor and analyze the packet. The port is not actually mirroring the packets to the packet sniffer but copying the data from the source port and sending the data to the destination port to be analyzed by the packet sniffer.

What is its purpose in networking and how could it be used and be helpful in security?

By using an effective port/network monitoring solution, admins can set a baseline for port activity and configure automated alerts for any suspicious activity. Admins can then close ports that have become too vulnerable, update firewall rules, and overall update the security of the network to thwart off attackers.

Index



Address: 192.168.1.3

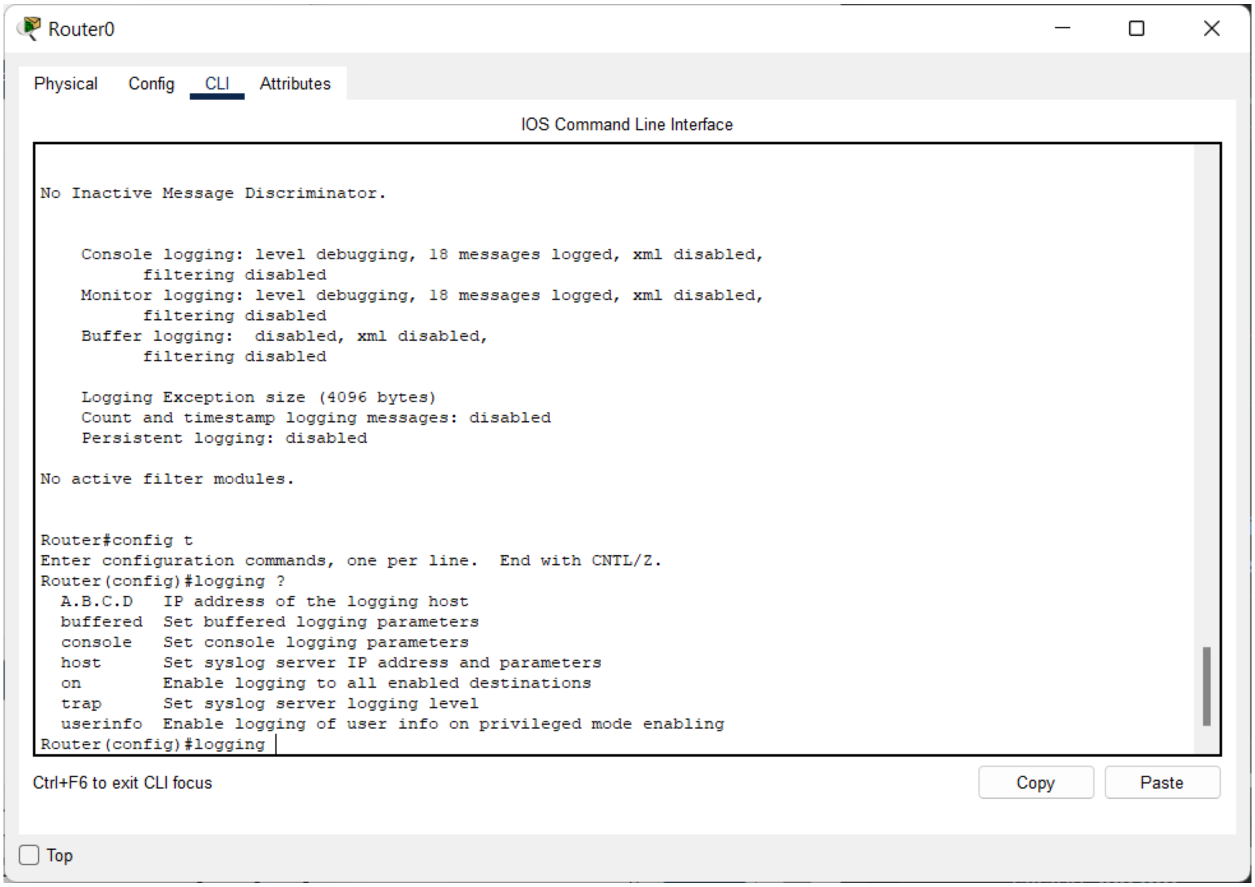
OID: .1.3.6.1.2.1.1.5.0

Operations: Get

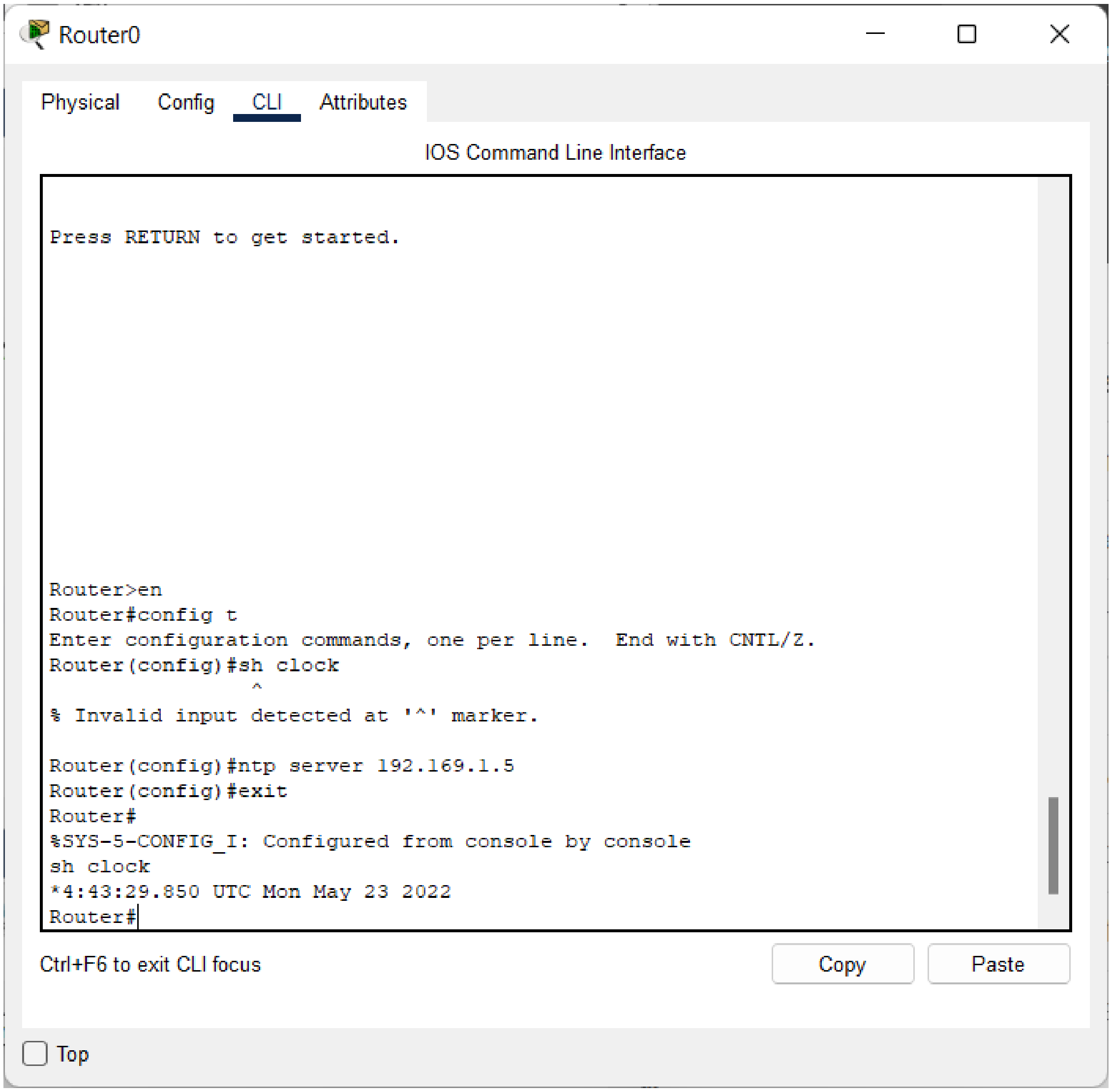
Result Table

Name/OID	Value	Type
.1.3.6.1.2.1.1.5.0 (.iso.org.dod.internet....	Router	OctetString

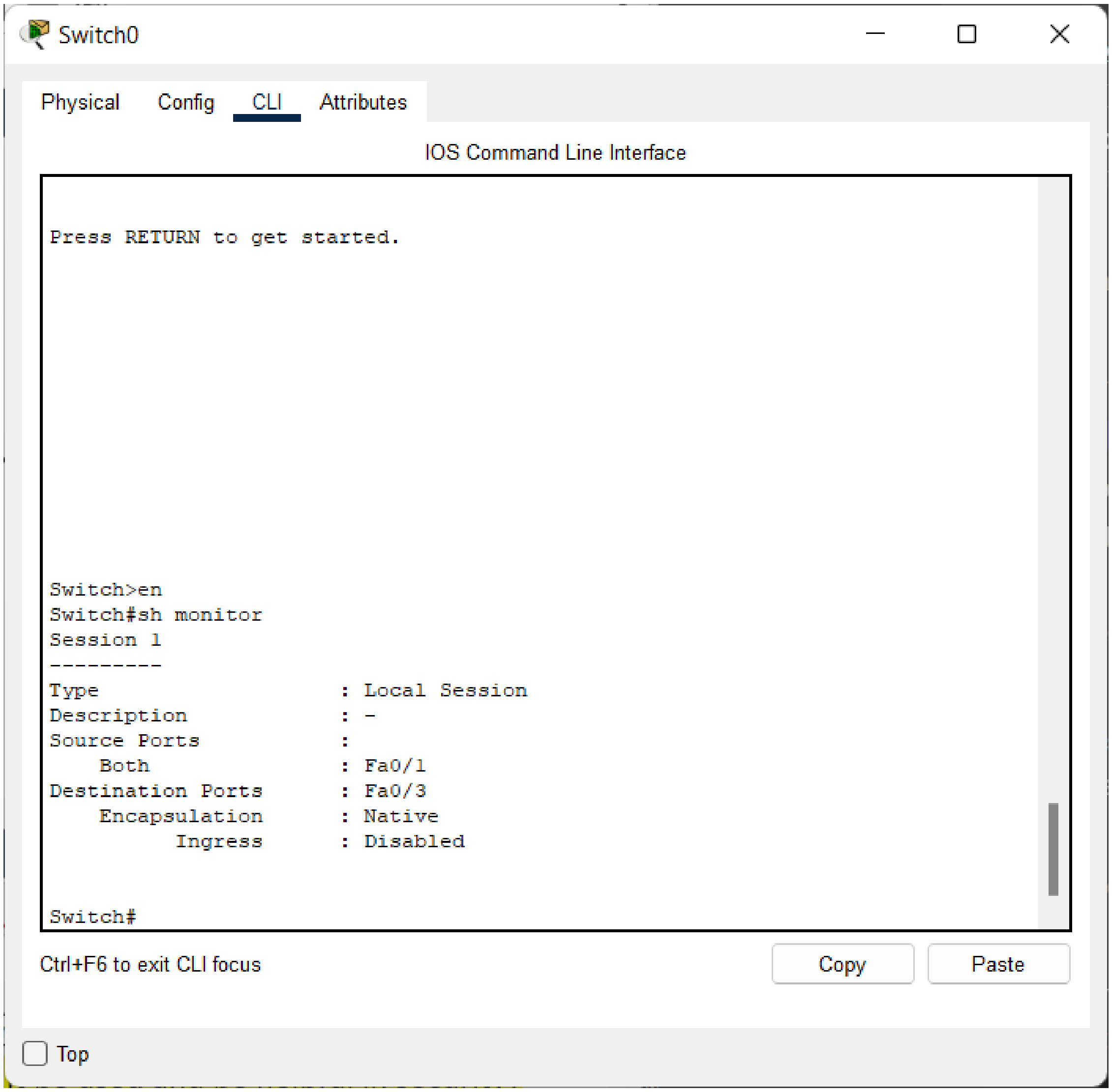
Name :	.sysName
OID :	.1.3.6.1.2.1.1.5.0
Syntax :	
Access :	
Description :	



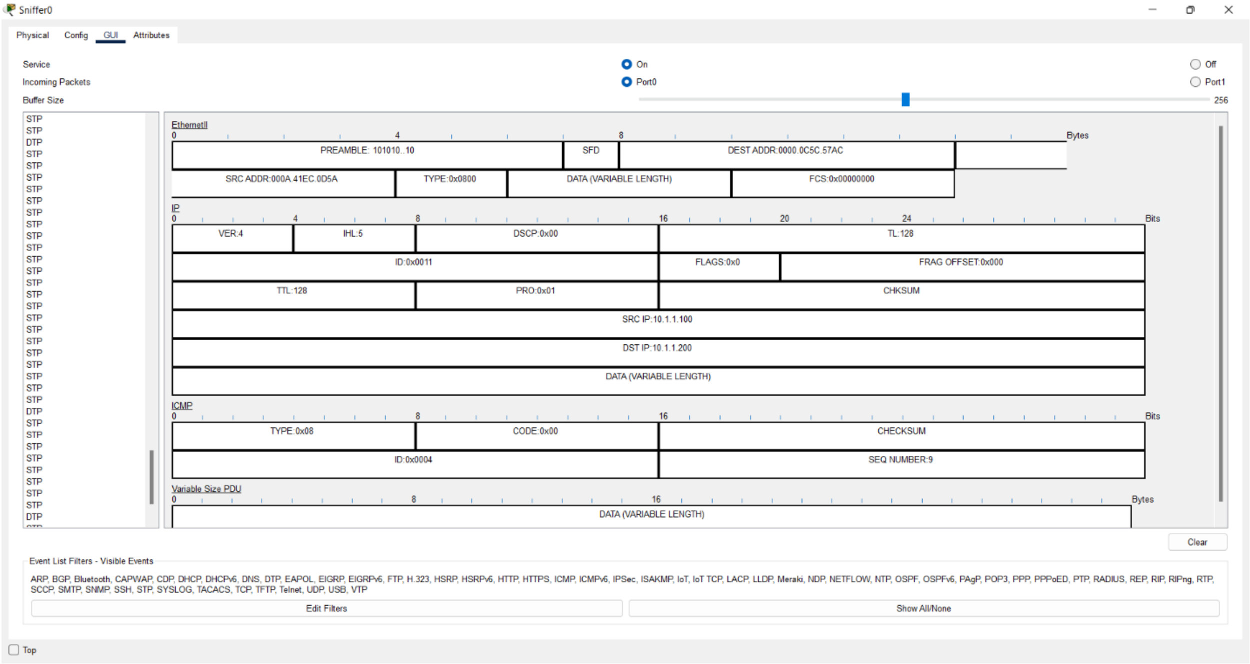
```
No Inactive Message Discriminator.


    Console logging: level debugging, 18 messages logged, xml disabled,
          filtering disabled
    Monitor logging: level debugging, 18 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.


Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#logging ?
  A.B.C.D   IP address of the logging host
  buffered  Set buffered logging parameters
  console   Set console logging parameters
  host      Set syslog server IP address and parameters
  on        Enable logging to all enabled destinations
  trap      Set syslog server logging level
  userinfo  Enable logging of user info on privileged mode enabling
Router(config)#logging 
```



```
Press RETURN to get started.









Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#sh clock
                ^
% Invalid input detected at '^' marker.

Router(config)#ntp server 192.169.1.5
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
sh clock
*4:43:29.850 UTC Mon May 23 2022
Router#
```



```
Press RETURN to get started.









Switch>en
Switch#sh monitor
Session 1
---------
Type                    : Local Session
Description             : -
Source Ports            :
    Both                : Fa0/1
Destination Ports       : Fa0/3
    Encapsulation       : Native
          Ingress       : Disabled


Switch#
```



Service ● On ○ Off

Incoming Packets ● Port0 ○ Port1

Buffer Size 256

STP
STP
DTP
STP
STP
STP
STP
STP
STP
STP
STP
STP
STP
STP
STP
STP
STP
STP
STP
STP
STP
STP
STP
STP
DTP
STP
STP
STP
STP
STP
STP
STP
STP
DTP

EthernetII (0 – 4 – 8 Bytes)

PREAMBLE: 101010..10	SFD	DEST ADDR:0000.0C5C.57AC	
SRC ADDR:000A.41EC.0D5A	TYPE:0x0800	DATA (VARIABLE LENGTH)	FCS:0x00000000

IP (0 – 4 – 8 – 16 – 20 – 24 Bits)

VER:4	IHL:5	DSCP:0x00	TL:128
ID:0x0011		FLAGS:0x0	FRAG OFFSET:0x000
TTL:128	PRO:0x01	CHKSUM	
SRC IP:10.1.1.100			
DST IP:10.1.1.200			
DATA (VARIABLE LENGTH)			

ICMP (0 – 8 – 16 Bits)

TYPE:0x08	CODE:0x00	CHECKSUM
ID:0x0004		SEQ NUMBER:9

Variable Size PDU (0 – 8 – 16 Bytes)

DATA (VARIABLE LENGTH)

Event List Filters - Visible Events

ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

□ Top