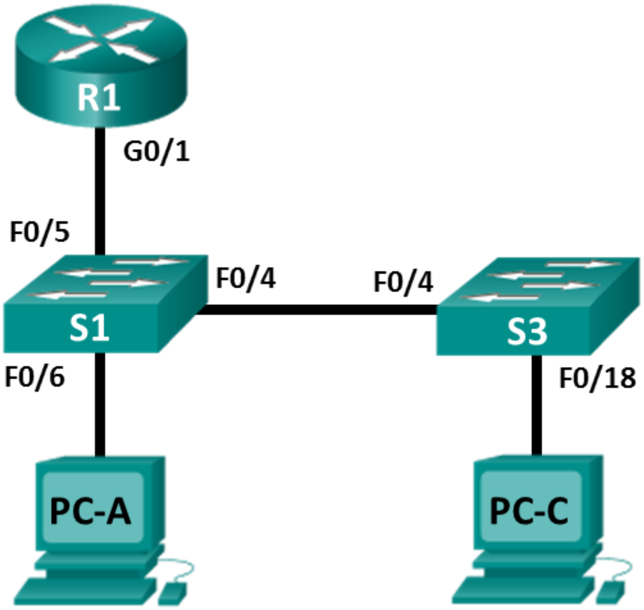
Lab – Troubleshoot LAN Traffic Using SPAN

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.2	255.255.255.0	192.168.1.1
S3	VLAN 1	192.168.1.3	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.254	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.1.10	255.255.255.0	192.168.1.1

Objectives

Part 1: Build the Network and Verify Connectivity

Part 2: Configure Local SPAN and Capture Copied Traffic with Wireshark

Background / Scenario

As the network administrator you decide to analyze the internal local area network for suspicious network traffic and possible DoS or reconnaissance attacks. To do this, you will set up port mirroring on all active switchports and mirror/copy all traffic to a designated switch port where a PC running Wireshark can analyze the captured traffic. The goal is to identify the source of suspicious traffic. To set up port mirroring you will use the Switched Port Analyzer (SPAN) feature on the Cisco switch. It is common to find a device running a packet sniffer or Intrusion Detection System (IDS) connected to the mirrored port.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.4(3) (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS

Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.4(3) universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows with a terminal emulation program, such as Tera Term or PuTTY, Wireshark, and Zenmap)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Part 1: Build the Network and Verify Connectivity

In Part 1, you will set up the network topology and configure basic settings, such as the interface IP addresses, static routing, device access, and passwords.

Step 1: Cable the network as shown in the topology.

Attach the devices as shown in the topology diagram, and cable as necessary.

Step 2: Configure PC hosts.

Step 3: Initialize and reload the routers and switches as necessary.

Step 4: Configure basic settings for the router.

a. Disable DNS lookup.

b. Configure the device name as shown in the topology.

c. Configure an IP address for the router as listed in the Addressing Table.

d. Assign **class** as the encrypted privileged EXEC mode password.

e. Assign **cisco** for the console and vty password, enable login.

f. Set the vty lines to **transport input telnet**

g. Configure **logging synchronous** to prevent console messages from interrupting command entry.

h. Copy the running configuration to the startup configuration.

Step 5: Configure basic settings for each switch.

a. Disable DNS lookup.

b. Configure the device name as shown in the topology.

c. Assign **class** as the encrypted privileged EXEC mode password.

d. Configure IP addresses for the switches as listed in the Addressing Table.

e. Configure the default gateway on each switch.

f. Assign **cisco** for the console and vty password and enable login.

g. Configure **logging synchronous** to prevent console messages from interrupting command entry.

h. Copy the running configuration to the startup configuration.

Step 6: Verify connectivity.

a. From PC-A, you should be able to ping the interface on R1, S1, S3, and PC-C. Were all pings successful?

If the pings are not successful, troubleshoot the basic device configurations before continuing.

b. From PC-C, you should be able to ping the interface on R1, S1, S3, and PC-A. Were all pings successful?

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Part 2: Configure Local SPAN and Capture Copied Traffic with Wireshark

To configure Local SPAN, you need to configure one or more source ports called monitored ports, and a single destination port, also called a monitored port, for copied or mirrored traffic to be sent out of. SPAN source ports can be configured to monitor traffic in either ingress, or egress, or both directions (default).

Step 1: Configure SPAN on S1.

a. Locate the switchports that are up on S1

```
S1# show ip interface brief
```

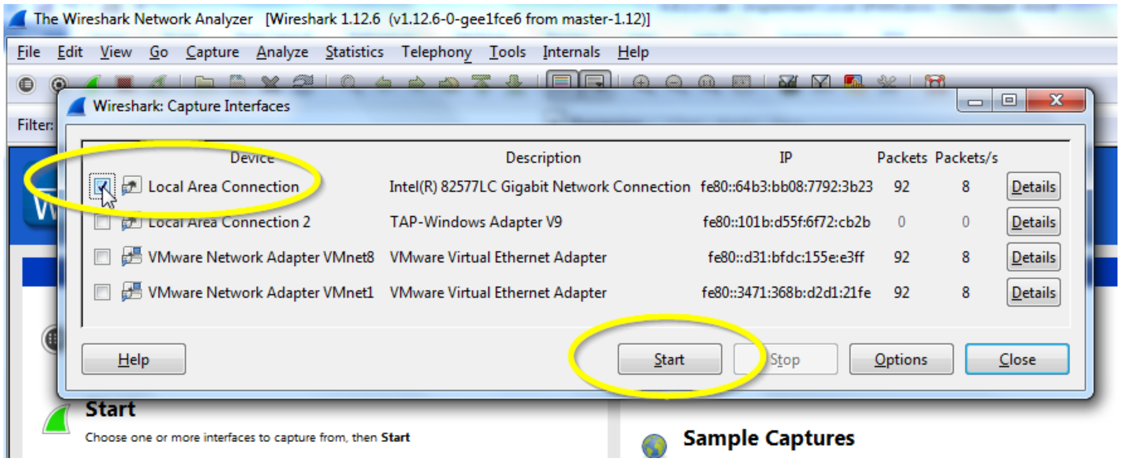
Which switchports are physically up and logically up?

On S1, F0/6 connects to PC-A which will be used for analyzing traffic with Wireshark. F0/6 will be the SPAN destination monitor port for duplicated packets. F0/4 and F0/5 will be the source monitor ports for intercepted packets. You can configure multiple source monitor ports but only one destination monitor port.

```
S1(config)# monitor session 1 source interface f0/4 - 5
S1(config)# monitor session 1 destination interface f0/6
```

Step 2: Start a Wireshark Capture on PC-A.

a. Open Wireshark on PC-A, set the capture interface to the Local Area Connection and click Start.

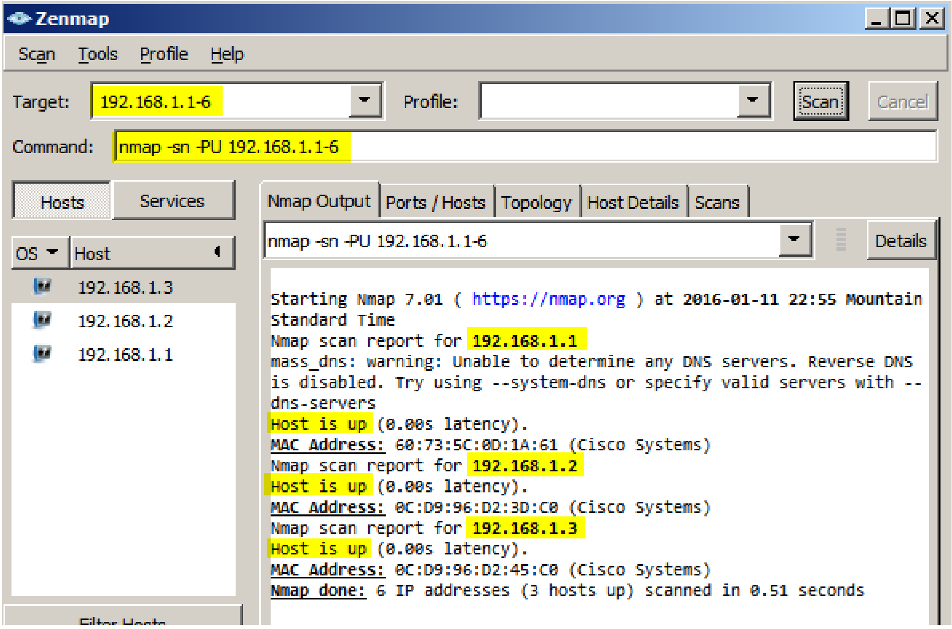

The Wireshark Network Analyzer [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Wireshark: Capture Interfaces
Help
Start
Stop
Options
Close
Start
Choose one or more interfaces to capture from, then Start
Sample Captures

	Device	Description	IP	Packets	Packets/s	
☑	Local Area Connection	Intel(R) 82577LC Gigabit Network Connection	fe80::64b3:bb08:7792:3b23	92	8	Details
□	Local Area Connection 2	TAP-Windows Adapter V9	fe80::101b:d55f:6f72:cb2b	0	0	Details
□	VMware Network Adapter VMnet8	VMware Virtual Ethernet Adapter	fe80::d31:bfdc:155e:e3ff	92	8	Details
□	VMware Network Adapter VMnet1	VMware Virtual Ethernet Adapter	fe80::3471:368b:d2d1:21fe	92	8	Details

Step 3: From PC-C, Use NMAP to Generate Suspicious Traffic.

a. If necessary, navigate to NMAP.org to download Zenmap. Scroll down the page to find the latest stable release for PC-C. Then following the on-screen instructions to install Zenmap with default settings.

b. Open Zenmap on PC-C and run a UDP ping scan to scan for available hosts (*nmap –sn –PU 192.168.1-6*). The scan result identifies 3 hosts on the network R1, S1, and S2 at 192.168.1.1, 192.168.1.2 and 192.168.1.3. Notice that Zenmap has also identified the MAC addresses of the three hosts as Cisco Systems interfaces. If this were a real network reconnaissance attack the scan might involve the entire range of network hosts as well as ports and OS fingerprinting.



Target: 192.168.1.1-6

Profile:

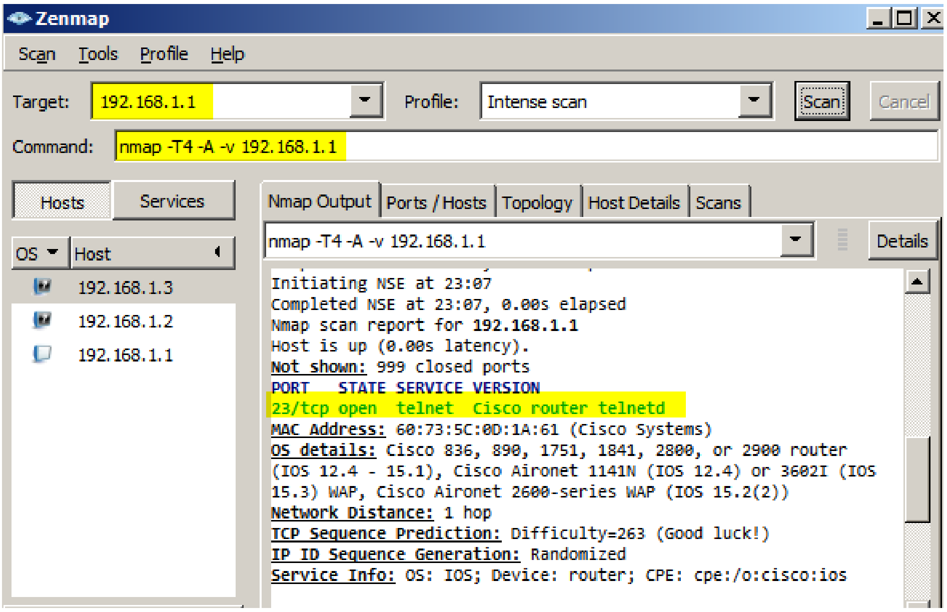
Command: nmap -sn -PU 192.168.1.1-6

192.168.1.3
192.168.1.2
192.168.1.1

nmap -sn -PU 192.168.1.1-6

```
Starting Nmap 7.01 ( https://nmap.org ) at 2016-01-11 22:55 Mountain
Standard Time
Nmap scan report for 192.168.1.1
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS
is disabled. Try using --system-dns or specify valid servers with --
dns-servers
Host is up (0.00s latency).
MAC Address: 60:73:5C:0D:1A:61 (Cisco Systems)
Nmap scan report for 192.168.1.2
Host is up (0.00s latency).
MAC Address: 0C:D9:96:D2:3D:C0 (Cisco Systems)
Nmap scan report for 192.168.1.3
Host is up (0.00s latency).
MAC Address: 0C:D9:96:D2:45:C0 (Cisco Systems)
Nmap done: 6 IP addresses (3 hosts up) scanned in 0.51 seconds
```

c. The hypothetical attacker can now issue an intense scan on R1 at 192.168.1.1 (nmap –T4 –A –v 192.168.1.1). The scan result identifies an open port 23/Telnet.



Target: 192.168.1.1

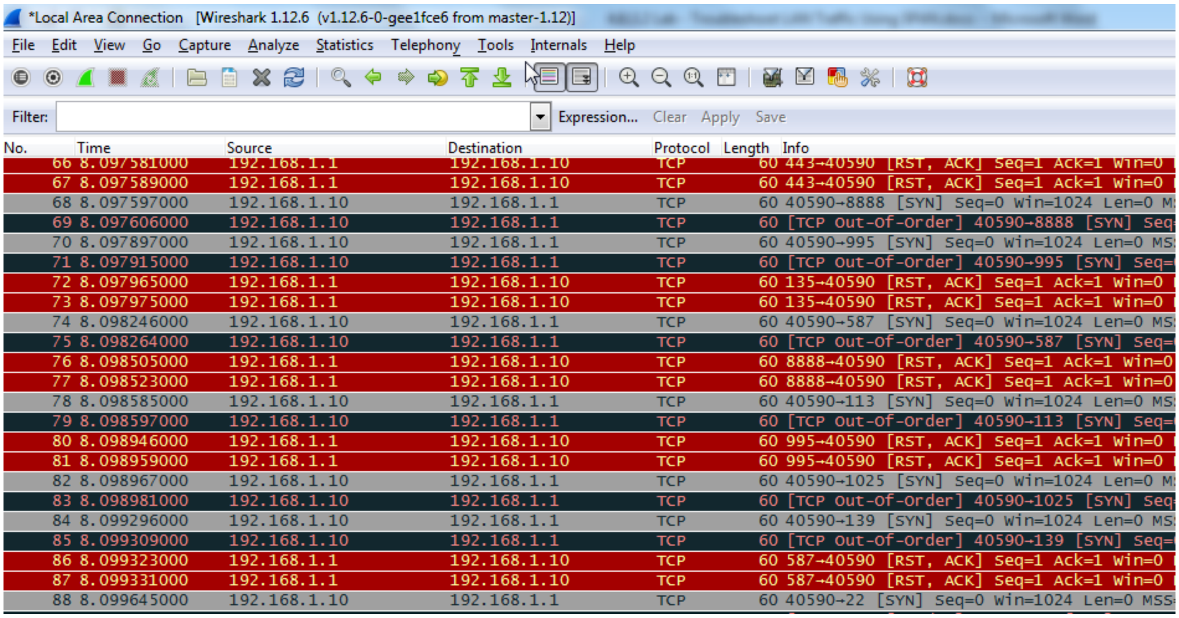
Profile: Intense scan

Command: nmap -T4 -A -v 192.168.1.1

```
Initiating NSE at 23:07
Completed NSE at 23:07, 0.00s elapsed
Nmap scan report for 192.168.1.1
Host is up (0.00s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
23/tcp open  telnet  Cisco router telnetd
MAC Address: 60:73:5C:0D:1A:61 (Cisco Systems)
OS details: Cisco 836, 890, 1751, 1841, 2800, or 2900 router
(IOS 12.4 - 15.1), Cisco Aironet 1141N (IOS 12.4) or 3602I (IOS
15.3) WAP, Cisco Aironet 2600-series WAP (IOS 15.2(2))
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Randomized
Service Info: OS: IOS; Device: router; CPE: cpe:/o:cisco:ios
```

Step 4: From PC-A Stop the Wireshark Capture and Examine the Captured SPAN Packets.

a. Return to PC-A, and stop the Wireshark capture. Notice the non-standard traffic patterns between PC-C at 192.168.1.10 and R1 at 192.168.1.1. It is filled with Out-Of-Order segments and Connection resets (RST). This packet capture identifies PC-C as sending suspicious traffic to router R1.


*Local Area Connection [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression...
Clear
Apply
Save

```
No.  Time          Source         Destination    Protocol Length Info
  66 8.097581000   192.168.1.1    192.168.1.10   TCP      60 443→40590 [RST, ACK] Seq=1 Ack=1 Win=0
  67 8.097589000   192.168.1.1    192.168.1.10   TCP      60 443→40590 [RST, ACK] Seq=1 Ack=1 Win=0
  68 8.097597000   192.168.1.10   192.168.1.1    TCP      60 40590→8888 [SYN] Seq=0 Win=1024 Len=0 M
  69 8.097606000   192.168.1.10   192.168.1.1    TCP      60 [TCP Out-Of-Order] 40590→8888 [SYN] Seq
  70 8.097897000   192.168.1.10   192.168.1.1    TCP      60 40590→995 [SYN] Seq=0 Win=1024 Len=0 MS
  71 8.097915000   192.168.1.10   192.168.1.1    TCP      60 [TCP Out-Of-Order] 40590→995 [SYN] Seq=
  72 8.097965000   192.168.1.1    192.168.1.10   TCP      60 135→40590 [RST, ACK] Seq=1 Ack=1 Win=0
  73 8.097975000   192.168.1.1    192.168.1.10   TCP      60 135→40590 [RST, ACK] Seq=1 Ack=1 Win=0
  74 8.098246000   192.168.1.10   192.168.1.1    TCP      60 40590→587 [SYN] Seq=0 Win=1024 Len=0 MS
  75 8.098264000   192.168.1.10   192.168.1.1    TCP      60 [TCP Out-Of-Order] 40590→587 [SYN] Seq=
  76 8.098505000   192.168.1.1    192.168.1.10   TCP      60 8888→40590 [RST, ACK] Seq=1 Ack=1 Win=0
  77 8.098523000   192.168.1.1    192.168.1.10   TCP      60 8888→40590 [RST, ACK] Seq=1 Ack=1 Win=0
  78 8.098585000   192.168.1.10   192.168.1.1    TCP      60 40590→113 [SYN] Seq=0 Win=1024 Len=0 MS
  79 8.098597000   192.168.1.10   192.168.1.1    TCP      60 [TCP Out-Of-Order] 40590→113 [SYN] Seq=
  80 8.098946000   192.168.1.1    192.168.1.10   TCP      60 995→40590 [RST, ACK] Seq=1 Ack=1 Win=0
  81 8.098959000   192.168.1.1    192.168.1.10   TCP      60 995→40590 [RST, ACK] Seq=1 Ack=1 Win=0
  82 8.098967000   192.168.1.10   192.168.1.1    TCP      60 40590→1025 [SYN] Seq=0 Win=1024 Len=0 M
  83 8.098981000   192.168.1.10   192.168.1.1    TCP      60 [TCP Out-Of-Order] 40590→1025 [SYN] Seq
  84 8.099296000   192.168.1.10   192.168.1.1    TCP      60 40590→139 [SYN] Seq=0 Win=1024 Len=0 MS
  85 8.099309000   192.168.1.10   192.168.1.1    TCP      60 [TCP Out-Of-Order] 40590→139 [SYN] Seq=
  86 8.099323000   192.168.1.1    192.168.1.10   TCP      60 587→40590 [RST, ACK] Seq=1 Ack=1 Win=0
  87 8.099331000   192.168.1.1    192.168.1.10   TCP      60 587→40590 [RST, ACK] Seq=1 Ack=1 Win=0
  88 8.099645000   192.168.1.10   192.168.1.1    TCP      60 40590→22 [SYN] Seq=0 Win=1024 Len=0 MSS
```

b. The attacker on PC-C knowing that the router has an open port on 23 could attempt an additional brute force attack or DoS style attack, like a LAND attack. A LAND attack is a TCP SYN packet with the same source and destination IP address and port number. Using Zenmap, the command **nmap –sS 192.168.1.1 –S 192.168.1.1 –p23 –g23 –e eth0** is an example. Notice how the LAND attack sets both the source and destination IP addresses to 192.168.1.1 and both the source and destination port numbers to the open port at 23. Although R1 with IOS15 is not vulnerable to this older type of DoS attack, many older systems and servers are still vulnerable. This attack will crash vulnerable systems, by setting them into an infinite loop.

Reflection

In this scenario, SPAN was used to troubleshoot and identify the source of suspicious activity on the network? What other troubleshooting scenarios might SPAN be useful for?

Router Interface Summary Table

Router Interface Summary				
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)

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.