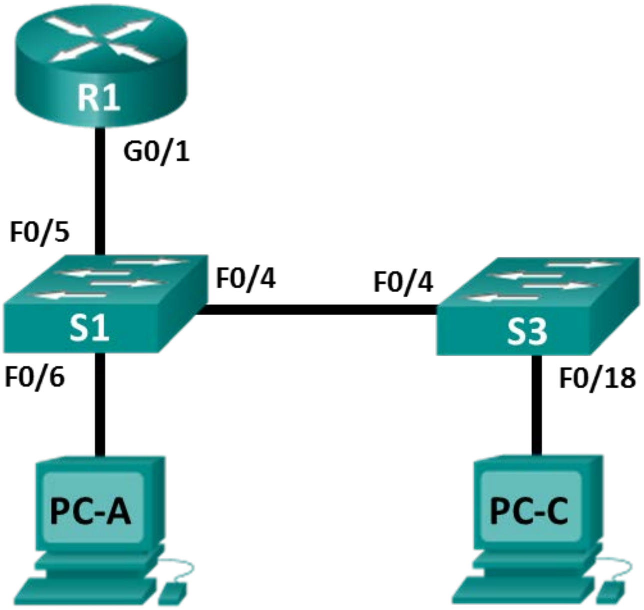
Lab – Implement Local SPAN

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 want to analyze traffic entering and exiting the local network. To do this, you will set up port mirroring on the switch port connected to the router and mirror all traffic to another switch port. The goal is to send all mirrored traffic to an intrusion detection system (IDS) for analysis. In this initial implementation, you will send all mirrored traffic to a PC which will capture the traffic for analysis using a port sniffing program. To set up port mirroring you will use the Switched Port Analyzer (SPAN) feature on the Cisco switch. SPAN is a type of port mirroring that sends copies of a frame entering a port, out another port on the same 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 terminal emulation program, such as Tera Term)
- 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 from. SPAN source ports can be configured to monitor traffic in either ingress or egress, or both directions (default).

The SPAN source port will need to be configured on the port that connects to the router on S1 switch port F0/5. This way all traffic entering or exiting the LAN will be monitored. The SPAN destination port will be configured on S1 switch port F0/6 which is connected to PC-A running Wireshark.

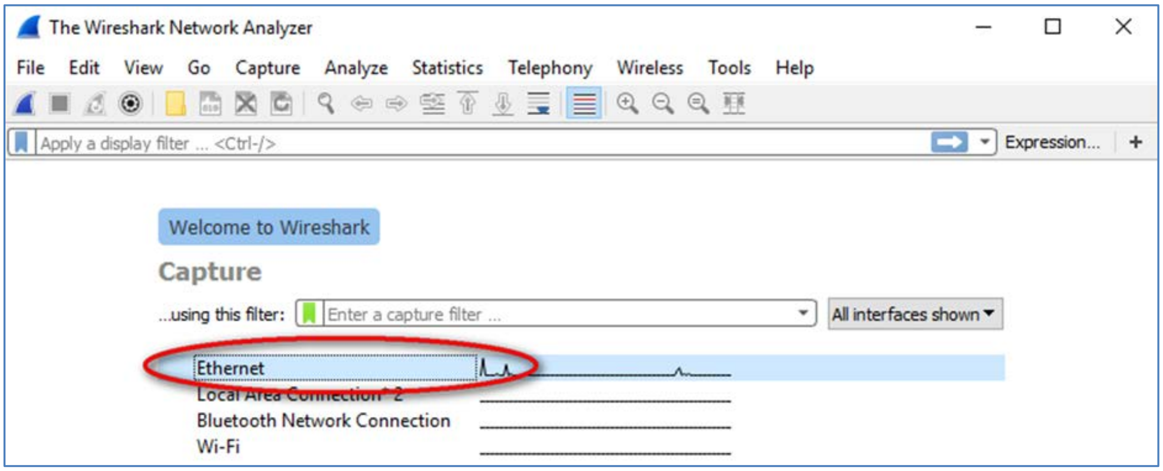
Step 1: Configure SPAN on S1.

a. Console into S1 and configure the source and destination monitor ports on S1. Now all traffic entering or leaving F0/5 will be copied and forwarded out of F0/6

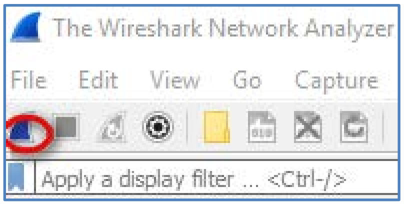
```
S1(config)# monitor session 1 source interface f0/5
S1(config)# monitor session 1 destination interface f0/6
```

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

a. Open Wireshark on PC-A, set the capture interface to **Ethernet**.



b. Click the **Wireshark** icon to start capture.


The Wireshark Network Analyzer
File Edit View Go Capture
Apply a display filter ... <Ctrl-/>

Step 3: Telnet into R1 and create ICMP traffic on the LAN.

a. Telnet from S1 to R1.

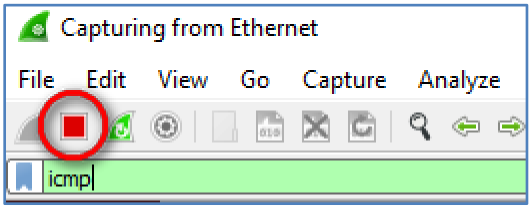
```
S1# Telnet 192.168.1.1
Trying 192.168.1.1 . . . Open

User Access Verification

Password:
R1>
```

b. From privileged mode, ping PC-C, S1 and S3.

```
R1> enable
Password:
R1# ping 192.168.1.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
R1# ping 192.168.1.2
<Output omitted>
R1# ping 192.168.1.3
<Output omitted>
```

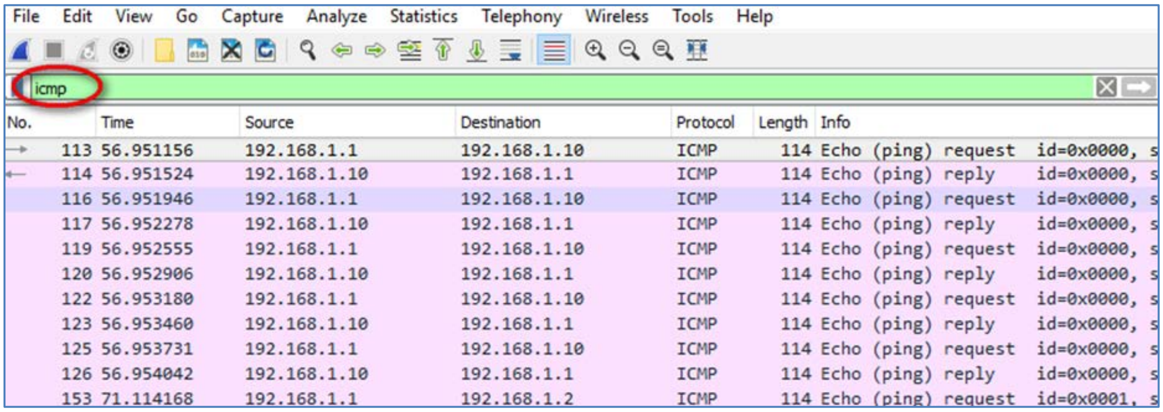
Step 4: Stop the Wireshark Capture on PC-A and Filter for ICMP.

a. Return to PC-A and stop the running Wireshark capture on PC-A.



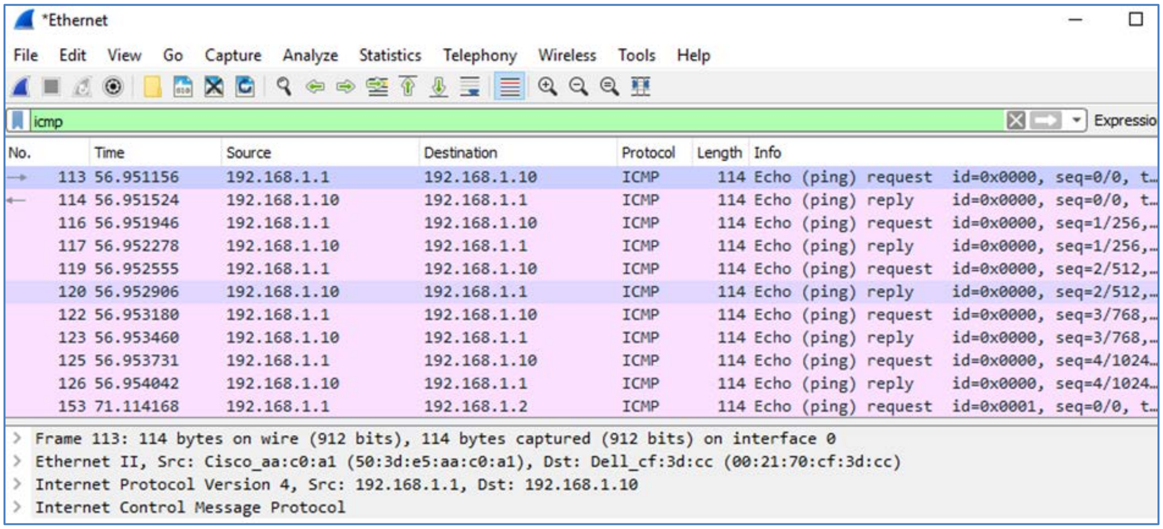
icmp

b. Filter the Wireshark capture for ICMP packets. Type in icmp and press **Enter**.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp

```
No.   Time        Source         Destination    Protocol  Length Info
  113 56.951156   192.168.1.1    192.168.1.10   ICMP      114 Echo (ping) request  id=0x0000, s
  114 56.951524   192.168.1.10   192.168.1.1    ICMP      114 Echo (ping) reply    id=0x0000, s
  116 56.951946   192.168.1.1    192.168.1.10   ICMP      114 Echo (ping) request  id=0x0000, s
  117 56.952278   192.168.1.10   192.168.1.1    ICMP      114 Echo (ping) reply    id=0x0000, s
  119 56.952555   192.168.1.1    192.168.1.10   ICMP      114 Echo (ping) request  id=0x0000, s
  120 56.952906   192.168.1.10   192.168.1.1    ICMP      114 Echo (ping) reply    id=0x0000, s
  122 56.953180   192.168.1.1    192.168.1.10   ICMP      114 Echo (ping) request  id=0x0000, s
  123 56.953460   192.168.1.10   192.168.1.1    ICMP      114 Echo (ping) reply    id=0x0000, s
  125 56.953731   192.168.1.1    192.168.1.10   ICMP      114 Echo (ping) request  id=0x0000, s
  126 56.954042   192.168.1.10   192.168.1.1    ICMP      114 Echo (ping) reply    id=0x0000, s
  153 71.114168   192.168.1.1    192.168.1.2    ICMP      114 Echo (ping) request  id=0x0001, s
```

c. Examine the Wireshark capture filtered for ICMP packets.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
Expressio

```
No.   Time        Source         Destination    Protocol  Length Info
  113 56.951156   192.168.1.1    192.168.1.10   ICMP      114 Echo (ping) request  id=0x0000, seq=0/0, t…
  114 56.951524   192.168.1.10   192.168.1.1    ICMP      114 Echo (ping) reply    id=0x0000, seq=0/0, t…
  116 56.951946   192.168.1.1    192.168.1.10   ICMP      114 Echo (ping) request  id=0x0000, seq=1/256,…
  117 56.952278   192.168.1.10   192.168.1.1    ICMP      114 Echo (ping) reply    id=0x0000, seq=1/256,…
  119 56.952555   192.168.1.1    192.168.1.10   ICMP      114 Echo (ping) request  id=0x0000, seq=2/512,…
  120 56.952906   192.168.1.10   192.168.1.1    ICMP      114 Echo (ping) reply    id=0x0000, seq=2/512,…
  122 56.953180   192.168.1.1    192.168.1.10   ICMP      114 Echo (ping) request  id=0x0000, seq=3/768,…
  123 56.953460   192.168.1.10   192.168.1.1    ICMP      114 Echo (ping) reply    id=0x0000, seq=3/768,…
  125 56.953731   192.168.1.1    192.168.1.10   ICMP      114 Echo (ping) request  id=0x0000, seq=4/1024…
  126 56.954042   192.168.1.10   192.168.1.1    ICMP      114 Echo (ping) reply    id=0x0000, seq=4/1024…
  153 71.114168   192.168.1.1    192.168.1.2    ICMP      114 Echo (ping) request  id=0x0001, seq=0/0, t…

> Frame 113: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
> Ethernet II, Src: Cisco_aa:c0:a1 (50:3d:e5:aa:c0:a1), Dst: Dell_cf:3d:cc (00:21:70:cf:3d:cc)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.10
> Internet Control Message Protocol
```

d. Were the pings from R1 to PC-C, S1 and S3 successfully copied and forwarded out f0/6 to PC-A?

e. Was the traffic monitored and copied in both directions?

Reflection

In this scenario, instead of using PC-A, and a packet sniffer, would an IDS or an IPS be more appropriate?

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.				