# Lab - Configuring and Verifying SPAN (Switch Port Analyzer)

## Topology

```
[PC-A Client]----Fa0/1----[S1 Switch]----Fa0/5----[PC-B Server]
                          |
                        Fa0/24
                          |
                      [PC-C Monitor]
```

**Network Description:**

Three PCs connect to a single Cisco switch (S1):

- PC-A connects to Fa0/1 (traffic source to be monitored)
- PC-B connects to Fa0/5 (traffic destination)
- PC-C connects to Fa0/24 (SPAN destination port for monitoring)

## Addressing Table

| Device | Interface | IP Address | Subnet Mask | Default Gateway |
|---|---|---|---|---|
| PC-A | NIC | 192.168.1.10 | 255.255.255.0 | 192.168.1.1 |
| PC-B | NIC | 192.168.1.20 | 255.255.255.0 | 192.168.1.1 |
| PC-C | NIC | 192.168.1.30 | 255.255.255.0 | 192.168.1.1 |
| S1 | VLAN 1 | 192.168.1.2 | 255.255.255.0 | 192.168.1.1 |

## Skills Refreshed/Learned

- Basic switch configuration
- SPAN (Switch Port Analyzer) configuration
- Local SPAN session configuration
- SPAN traffic monitoring and analysis
- Wireshark packet capture and analysis
- Network traffic analysis
- SPAN verification commands
- Port monitoring techniques

## Objectives

**Part 1: Configure Basic Switch Settings**

- Cable the network as shown in the topology
- Configure basic switch settings
- Configure IP addressing for all devices
- Verify basic connectivity

**Part 2: Configure and Verify SPAN**

- Install and configure Wireshark on PC-C
- Configure a basic SPAN session
- Monitor traffic from PC-A to PC-B
- Verify SPAN operation
- Test different SPAN configurations

**Part 3: Advanced SPAN Configurations**

- Configure SPAN to monitor multiple ports
- Configure SPAN with traffic direction filtering
- Configure SPAN to monitor a VLAN
- Compare different SPAN configurations

## Background / Scenario

Switch Port Analyzer (SPAN) is a Cisco switch feature that mirrors traffic from one or more source ports to a destination port. This allows network administrators to monitor network traffic without impacting network performance. SPAN is commonly used with intrusion detection systems (IDS), network analyzers, and troubleshooting tools.

In this lab, you will configure SPAN on a Cisco switch to mirror traffic to a monitoring station running Wireshark. You will learn how to configure different types of SPAN sessions and verify their operation. This is an essential skill for network security monitoring and troubleshooting.

## Required Resources

- 1 Cisco Switch (2960 or similar with IOS 15.0 or later)

- 3 PCs (Windows or Linux with network capabilities)
- Console cable to configure the Cisco switch
- Ethernet cables as shown in the topology
- Wireshark software (free download from wireshark.org)

# Instructions

## Part 1: Configure Basic Switch Settings

### Step 1: Cable the network

Attach the devices as shown in the topology diagram and cable as necessary:

- Connect PC-A to S1 port Fa0/1
- Connect PC-B to S1 port Fa0/5
- Connect PC-C to S1 port Fa0/24

### Step 2: Configure basic settings on the switch

**a. Console into the switch and enable privileged EXEC mode.**

**b. Configure the hostname.**

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname S1
```

**c. Disable DNS lookup.**

```
S1(config)# no ip domain-lookup
```

**d. Configure the management VLAN interface.**

```
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.2 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# exit
```

**e. Configure all active switch ports to access mode.**

```
S1(config)# interface range fa0/1, fa0/5, fa0/24
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 1
S1(config-if-range)# no shutdown
S1(config-if-range)# exit
```

### Step 3: Configure PC IP addresses

Configure static IP addresses on all PCs:

**PC-A:**

- IP Address: 192.168.1.10
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.1.1

**PC-B:**

- IP Address: 192.168.1.20
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.1.1

**PC-C:**

- IP Address: 192.168.1.30
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.1.1

### Step 4: Verify basic connectivity

#### a. Ping from PC-A to PC-B.

```
C:\> ping 192.168.1.20
```

The pings should be successful.

#### b. Ping from PC-A to the switch.

```
C:\> ping 192.168.1.2
```

The pings should be successful.

**c. Verify all ports are up.**

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

All configured interfaces should show "up" status.

If any connectivity tests fail, troubleshoot before continuing.

## Part 2: Configure and Verify SPAN

### Step 1: Install Wireshark on PC-C

**a. Download Wireshark.**

Navigate to https://www.wireshark.org and download the appropriate version for your operating system:

- For Windows: Download the Windows Installer (64-bit or 32-bit)
- For Linux: Use your package manager (e.g., `sudo apt install wireshark` on Ubuntu)
- For macOS: Download the macOS installer

**b. Install Wireshark.**

Run the installer and follow the on-screen instructions:

- Accept the license agreement
- Install with default components (including WinPcap/Npcap for packet capture)
- Complete the installation

**c. Launch Wireshark.**

Open Wireshark on PC-C. You should see a list of available network interfaces.

**d. Identify your network interface.**

In Wireshark, identify which interface corresponds to your Ethernet connection (e.g., "Ethernet", "eth0", or "Local Area Connection").

**Note:** Wireshark is a free, open-source packet analyzer that allows you to capture and interactively browse network traffic. It's the industry-standard tool for network analysis and troubleshooting.

### Step 2: Establish baseline traffic capture (without SPAN)

**a. Start a capture on PC-C.**

In Wireshark on PC-C:

1. Double-click on your network interface to start capturing
2. You should see broadcast traffic and traffic to/from PC-C

**b. Generate traffic from PC-A to PC-B.**

From PC-A, ping PC-B:

```
C:\> ping 192.168.1.20
```

**c. Observe the capture on PC-C.**

In Wireshark on PC-C, you should NOT see the ICMP traffic between PC-A and PC-B because PC-C is not involved in that communication. You will only see:

- Broadcast traffic (ARP, etc.)
- Traffic specifically sent to or from PC-C

This demonstrates why SPAN is necessary for network monitoring.

**d. Stop the capture in Wireshark.**

Click the red square icon to stop capturing.

### Step 3: Configure a basic SPAN session

You will configure SPAN to monitor traffic on Fa0/1 (PC-A's port) and send a copy to Fa0/24 (PC-C's monitoring port).

**a. Configure the SPAN session on S1.**

```
S1(config)# monitor session 1 source interface fastethernet 0/1
S1(config)# monitor session 1 destination interface fastethernet 0/24
S1(config)# exit
```

**b. Verify the SPAN configuration.**

```
S1# show monitor

Session 1
---------
Type              : Local Session
Source Ports        :
    Both          : Fa0/1
Destination Ports   : Fa0/24
    Encapsulation   : Native
          Ingress   : Disabled
```

Verify that:

- Session 1 exists
- Source port is Fa0/1
- Destination port is Fa0/24
- Direction is "Both" (ingress and egress traffic)

**Step 4: Capture traffic with SPAN enabled**

**a. Start a new capture on PC-C.**

In Wireshark on PC-C, start a new capture on your network interface.

**b. Generate traffic from PC-A to PC-B.**

From PC-A, ping PC-B:

```
C:\> ping 192.168.1.20 -n 10
```

**c. Observe the captured traffic.**

In Wireshark on PC-C, you should now see:

- ICMP Echo Request packets from 192.168.1.10 to 192.168.1.20
- ICMP Echo Reply packets from 192.168.1.20 to 192.168.1.10
- ARP traffic between PC-A and PC-B

This traffic is being mirrored from Fa0/1 to Fa0/24 by the SPAN session.

**d. Apply a display filter in Wireshark.**

To see only the ICMP traffic, type this filter in the display filter bar:

```
icmp
```

Press Enter. You should now see only the ping traffic between PC-A and PC-B.

**e. Stop the capture.**

Click the red square to stop capturing.

### Step 5: Verify SPAN session statistics

**a. Check SPAN session details.**

```
S1# show monitor session 1
```

Review the configuration details.

**b. View interface counters.**

```
S1# show interface fa0/24
```

Note the packet counters. The destination port should show increased traffic from the mirrored packets.

## Part 3: Advanced SPAN Configurations

### Step 1: Configure SPAN to monitor multiple source ports

You will now modify the SPAN session to monitor both PC-A and PC-B ports simultaneously.

**a. Remove the existing SPAN session.**

```
S1(config)# no monitor session 1
```

**b. Configure SPAN with multiple source ports.**

```
S1(config)# monitor session 1 source interface fa0/1
S1(config)# monitor session 1 source interface fa0/5
S1(config)# monitor session 1 destination interface fa0/24
S1(config)# exit
```

**c. Verify the configuration.**

```
S1# show monitor session 1

Session 1
---------
Type              : Local Session
Source Ports        :
    Both          : Fa0/1,Fa0/5
Destination Ports   : Fa0/24
    Encapsulation   : Native
          Ingress   : Disabled
```

Both Fa0/1 and Fa0/5 should now be listed as source ports.

**d. Test the configuration.**

Start a Wireshark capture on PC-C, then:

- Ping from PC-A to the switch: `ping 192.168.1.2`
- Ping from PC-B to the switch: `ping 192.168.1.2`

You should see both sets of ICMP traffic in Wireshark because both source ports are being monitored.

**Step 2: Configure SPAN with traffic direction filtering**

SPAN can be configured to monitor only ingress (received) or egress (transmitted) traffic on the source port.

**a. Remove the existing SPAN session.**

```
S1(config)# no monitor session 1
```

**b. Configure SPAN to monitor only ingress traffic on Fa0/1.**

```
S1(config)# monitor session 1 source interface fa0/1 rx
S1(config)# monitor session 1 destination interface fa0/24
S1(config)# exit
```

**c. Verify the configuration.**

```
S1# show monitor session 1

Session 1
---------
Type              : Local Session
Source Ports      :
    RX Only       : Fa0/1
Destination Ports : Fa0/24
    Encapsulation : Native
          Ingress : Disabled
```

Note that the direction now shows "RX Only" instead of "Both".

**d. Test ingress-only monitoring.**

Start a Wireshark capture on PC-C, then ping from PC-A to PC-B:

```
C:\> ping 192.168.1.20 -n 5
```

In Wireshark, you should see:

- ICMP Echo Request packets (these enter Fa0/1 from PC-A)
- ARP requests from PC-A
- But you should NOT see ICMP Echo Reply packets returning to PC-A (these are egress on Fa0/1)

**e. Configure SPAN to monitor only egress traffic.**

```
S1(config)# no monitor session 1
S1(config)# monitor session 1 source interface fa0/1 tx
S1(config)# monitor session 1 destination interface fa0/24
S1(config)# exit
```

**f. Test egress-only monitoring.**

Start a new Wireshark capture on PC-C, then ping from PC-A to PC-B:

```
C:\> ping 192.168.1.20 -n 5
```

Now you should see:

- ICMP Echo Reply packets (these are sent out Fa0/1 to PC-A)

- ARP replies to PC-A
- But you should NOT see ICMP Echo Request packets from PC-A (these are ingress on Fa0/1)

### Step 3: Configure SPAN to monitor an entire VLAN

Instead of monitoring specific ports, SPAN can monitor all traffic within a VLAN.

#### a. Remove the existing SPAN session.

```
S1(config)# no monitor session 1
```

#### b. Configure SPAN to monitor VLAN 1.

```
S1(config)# monitor session 1 source vlan 1
S1(config)# monitor session 1 destination interface fa0/24
S1(config)# exit
```

#### c. Verify the configuration.

```
S1# show monitor session 1

Session 1
---------
Type              : Local Session
Source VLANs      :
   Both           : 1
Destination Ports   : Fa0/24
   Encapsulation   : Native
         Ingress   : Disabled
```

Note that "Source VLANs" is now shown instead of "Source Ports".

#### d. Test VLAN monitoring.

Start a Wireshark capture on PC-C, then:

- Ping from PC-A to PC-B: `ping 192.168.1.20`
- Ping from PC-B to PC-A: `ping 192.168.1.10`

You should see traffic between any devices in VLAN 1 because the entire VLAN is being monitored.

**Important Note:** When monitoring a VLAN, you will see ALL traffic in that VLAN, which can generate a very large amount of data. Use VLAN monitoring carefully in production environments.

### Step 4: Configure SPAN using interface ranges

For efficiency, you can configure SPAN using interface ranges.

**a. Remove the existing SPAN session.**

```
S1(config)# no monitor session 1
```

**b. Configure SPAN using an interface range.**

```
S1(config)# monitor session 1 source interface range fa0/1 - 5
S1(config)# monitor session 1 destination interface fa0/24
S1(config)# exit
```

**c. Verify the configuration.**

```
S1# show monitor session 1

Session 1
---------
Type              : Local Session
Source Ports      :
    Both          : Fa0/1-5
Destination Ports : Fa0/24
    Encapsulation : Native
          Ingress : Disabled
```

This configuration monitors all traffic on ports Fa0/1 through Fa0/5.

## Part 4: Using Wireshark for Analysis

### Step 1: Analyze captured traffic

**a. Configure a basic SPAN session for this analysis.**

```
S1(config)# no monitor session 1
S1(config)# monitor session 1 source interface fa0/1
S1(config)# monitor session 1 destination interface fa0/24
S1(config)# exit
```

**b. Generate various types of traffic.**

Start a Wireshark capture on PC-C, then from PC-A:

- Ping PC-B: `ping 192.168.1.20 -n 10`
- Use a web browser to attempt to connect to PC-B (this will fail but generate TCP traffic)
- Generate continuous pings: `ping 192.168.1.20 -t` (press Ctrl+C to stop)

**c. Stop the capture and analyze the data.**

In Wireshark, explore the captured packets:

1. Click on any packet to see detailed information
2. Expand the protocol layers in the middle pane
3. Observe the hex dump in the bottom pane

**d. Use Wireshark statistics.**

Explore Wireshark's built-in analysis tools:

- Click **Statistics > Protocol Hierarchy** to see a breakdown of protocols
- Click **Statistics > Conversations** to see communication between hosts
- Click **Statistics > IO Graph** to visualize traffic over time

**e. Apply useful display filters.**

Try these display filters in Wireshark:

- Show only ARP traffic: `arp`
- Show only traffic to/from PC-B: `ip.addr == 192.168.1.20`
- Show only ICMP traffic: `icmp`
- Show only TCP traffic: `tcp`
- Show only broadcast traffic: `eth.dst == ff:ff:ff:ff:ff:ff`

**Step 2: Identify network issues using SPAN and Wireshark**

SPAN combined with Wireshark is a powerful troubleshooting tool.

**a. Look for ARP requests.**

Apply the filter `arp` in Wireshark. ARP traffic helps you:

- Verify devices are communicating at Layer 2
- Identify IP address conflicts
- Detect ARP spoofing attempts

**b. Analyze ping (ICMP) traffic.**

Apply the filter `icmp`. Look for:

- Echo Request and Echo Reply pairs
- Time-to-Live (TTL) values
- Response times in the Info column

**c. Observe the three-way TCP handshake.**

Apply the filter `tcp`. Look for sequences of:

- SYN packet (initiates connection)
- SYN-ACK packet (acknowledges connection)
- ACK packet (confirms connection)

This shows successful TCP connection establishment.

## Part 5: SPAN Best Practices and Limitations

### Step 1: Understanding SPAN limitations

SPAN has several important limitations:

**a. Destination port is receive-only.**

The SPAN destination port (Fa0/24 in this lab) can only receive mirrored traffic. It cannot transmit normal network traffic. This is why we use it exclusively for the monitoring PC.

**b. Potential for packet loss.**

If the source ports generate more traffic than the destination port can handle, packets may be dropped. This is called oversubscription.

**c. No Layer 1 error visibility.**

SPAN operates at Layer 2 and above. It will not show you Layer 1 errors like CRC errors or physical link issues.

**d. CPU impact on switch.**

Excessive SPAN configurations can impact switch CPU performance. Monitor switch CPU usage when using SPAN.

### Step 2: SPAN best practices

Follow these best practices when using SPAN:

**a. Match bandwidth appropriately.**

Ensure the destination port speed is equal to or greater than the combined speed of all source ports. For example:

- If monitoring two 100 Mbps ports, use a 1 Gbps destination port
- Never monitor a 1 Gbps port with a 100 Mbps destination port

**b. Use SPAN selectively.**

Only monitor the ports or VLANs you need. Excessive monitoring can:

- Overwhelm your monitoring tools
- Generate too much data to analyze effectively
- Impact switch performance

**c. Document your SPAN sessions.**

Keep a record of:

- Which session numbers are in use
- What each session monitors
- Why each session was created
- When to remove temporary sessions

**d. Remove unused SPAN sessions.**

Clean up SPAN sessions when monitoring is complete:

```
S1(config)# no monitor session 1
```

**e. Consider Remote SPAN (RSPAN) for distributed monitoring.**

If you need to monitor traffic across multiple switches, consider using RSPAN, which extends SPAN across the network.

## Part 6: Verification and Documentation

### Step 1: Final verification

**a. Verify your SPAN configuration is removed.**

If you created multiple sessions during the lab, remove them all:

```
S1(config)# no monitor session 1
S1(config)# no monitor session 2
S1(config)# no monitor session 3
S1(config)# exit
```

**b. Verify no SPAN sessions remain.**

```
S1# show monitor
```

You should see no active sessions.

**c. Verify all interfaces are operational.**

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

All interfaces should show "up" status.

# Lab Submission

To complete this lab, submit the switch running configuration:

1. **Display the running configuration:**

```
S1# show running-config
```

2. **Copy the output to a text file named `S1-running-config.txt`**
3. **Submit your configuration file** according to your instructor's directions.

## Additional Resources

**Wireshark Resources:**

- Official Wireshark website: https://www.wireshark.org
- Wireshark User's Guide: https://www.wireshark.org/docs/wsug_html_chunked/
- Wireshark Display Filters: https://wiki.wireshark.org/DisplayFilters

**Alternative Open-Source Tools:**

- **tcpdump** (Linux/macOS command-line): Lightweight packet capture
- **tshark** (Wireshark's CLI version): Command-line packet analysis
- **Ettercap**: Network security tool with packet capture capabilities
- **ntop/ntopng**: Network traffic probe and monitoring

**Cisco SPAN Documentation:**

- Search Cisco.com for "Configuring SPAN and RSPAN" for your specific switch model

## End of Lab