- Switched Port Analyzer (SPAN) -

Traffic Monitoring

A common practice when troubleshooting network issues is to examine the headers and payload of packets, through the use of **packet sniffers** or **analyzers.**

A packet must first be **captured** before it can be analyzed. Packets can be captured and analyzed on a host using locally installed software. Wireshark and tcpdump are popular tools for this.

In legacy networks using hubs, *all traffic* on the network could be easily captured. A hub forwards a packet out *every port*, regardless of the destination. Thus, a single workstation with Wireshark could capture and analyze traffic between *any* two hosts.

This is no longer possible on modern networks that use switches. A packet will only be forwarded out the appropriate destination port. Thus, centrally analyzing all traffic on a network is more difficult.

Switch Port Analyzer (SPAN)

Cisco developed the **Switched Port Analyzer (SPAN)** feature to facilitate the capturing of packets. SPAN is supported on most Cisco switch platforms.

SPAN works by *copying* the traffic from one or more **source** ports. The copy is then sent out a SPAN **destination** port. The destination port will often be connected to a host running packet analyzing software, such as Wireshark.

Because SPAN only makes a *copy* of traffic, the source traffic is *never* affected. SPAN is an **out-of-band** process.

In addition to troubleshooting network issues and performance, SPAN is useful for intrusion detection systems (IDS) and application monitoring platforms.

SPAN is often referred to as *port mirroring*.

* * *

SPAN Sources and Destinations

A SPAN source is where traffic is mirrored *from.* A SPAN source can consist of one or more of the following:

- Access switchports
- Trunk ports
- Routed interfaces
- EtherChannels
- Entire VLANs

SPAN can mirror either **inbound** or **outbound** traffic on a source, or **both**.

A SPAN destination is where traffic is mirrored *to.* A SPAN destination port can consist of only a *single* switchport, and is completely dedicated for that purpose.

No other traffic is forwarded to or from a SPAN destination, including management traffic such as STP and CDP. A SPAN destination does not participate in the STP topology.

A SPAN destination port can only participate in one SPAN session, and cannot be a SPAN source port.

Most Cisco platforms *do not* support an EtherChannel as a SPAN destination. For the limited models that do, the EtherChannel must be manually configured as *on* – port aggregation protocols are not supported.

The traffic from the SPAN source can exceed the bandwidth capacity of the SPAN destination port. For example, a SPAN source of an entire VLAN can easily exceed the capacity of a single Gigabit Ethernet port.

In this circumstance, some packets will be dropped at the SPAN destination. **Remember:** *source* traffic is **never affected** by SPAN.

* * *

Configuring SPAN

Configuring SPAN involves two steps:

- Identifying the SPAN source or sources
- Identifying the SPAN destination

To configure SPAN sources:

Switch(config)# *monitor session 1 source interface gi0/10 rx*
Switch(config)# *monitor session 1 source interface gi0/11 tx*
Switch(config)# *monitor session 1 source vlan 100 both*

The command syntax begins *monitor session*, and assigns it a session number. In the above example, the session number is *1*. The SPAN destination must use the *same* session number.

The above example identifies three sources:

- Inbound or *rx* traffic on port *gi0/10*
- Outbound or *tx* traffic on port *gi0/11*
- *Both* inbound and outbound traffic on VLAN 100

When specifying a *trunk* port as a source, it is possible to restrict which VLANs are mirrored:

Switch(config)# *monitor session 1 filter vlan 1-5*

To configure a SPAN destination port:

Switch(config)# *monitor session 1 destination interface gi0/15*

Remember, the session number must match between the source and destination. To disable a specific monitoring session:

Switch(config)# *no monitor session 1*

To view the status of a SPAN session:

Switch(config)# *show monitor session 1*

```
Session 1
------------
Type : local
Source Ports:
    RX Only:       gi0/10
    TX Only:       gi0/11
    Both:          None
Source VLANs:
    RX Only:       None
    TX Only:       None
    Both:          100
Destination Ports: gi0/15
```

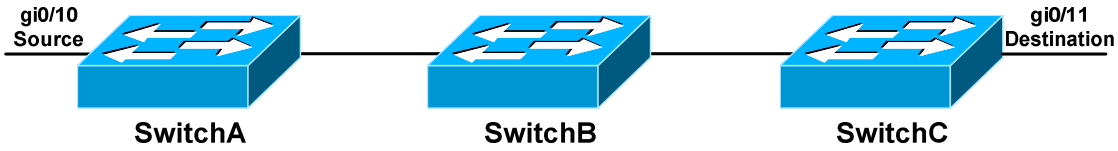
* * *

Remote SPAN (RSPAN)

The previous page describes the configuration of **Local SPAN**, where both the SPAN source and destination exist on the *same* switch.

Remote SPAN (RSPAN) allows the SPAN source and destination to exist on *different* switches. This involves configuring a RSPAN VLAN – the mirrored traffic will be carried across this VLAN from switch to switch.

Considering the following example:



The SPAN source exists on SwitchA, and the SPAN destination exists on SwitchC. Each switch must be configured with the RSPAN VLAN, including the intermediary SwitchB.

To configure RSPAN on SwitchA:

```
SwitchA(config)# vlan 200
SwitchA(config-vlan)# remote-span

SwitchA(config)# monitor session 1 source interface gi0/10
SwitchA(config)# monitor session 1 destination vlan 200
```

To configure RSPAN on SwitchB:

```
SwitchB(config)# vlan 200
SwitchB(config-vlan)# remote-span
```

To configure RSPAN on SwitchC:

```
SwitchC(config)# vlan 200
SwitchC(config-vlan)# remote-span

SwitchC(config)# monitor session 1 source vlan 200
SwitchC(config)# monitor session 1 destination interface gi0/11
```

Note that on SwitchA, the SPAN *destination* is the RSPAN VLAN, instead of a port. On SwitchC, the SPAN *source* is the RSPAN VLAN.

* * *