Cisco IOS SPAN and RSPAN

By : Haydar Fadel

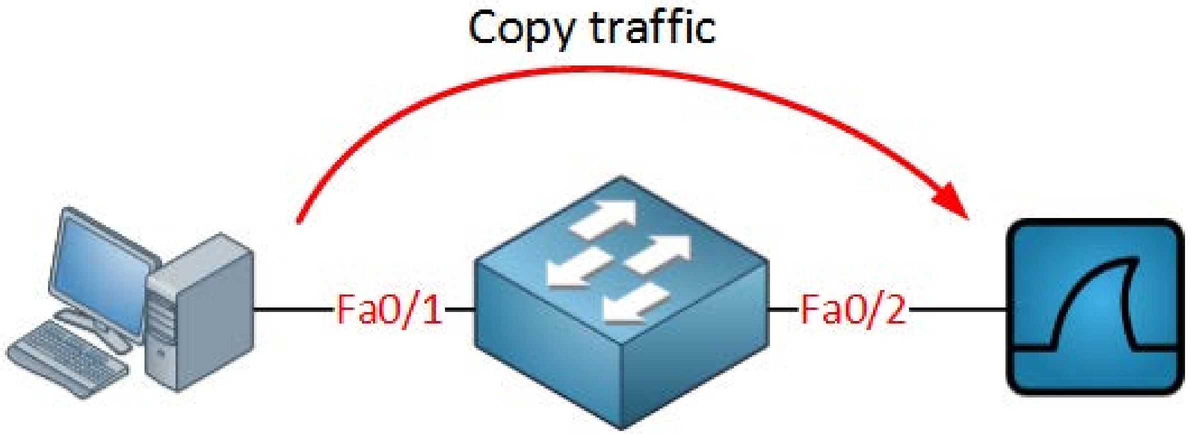
SPAN & RSPAN

Understanding and Configuring SPAN and RSPAN

Cisco IOS SPAN and RSPAN

- Cisco Catalyst Switches have a feature called SPAN (Switch Port Analyzer) that lets you **copy all traffic from a source port or source VLAN** to a destination interface.

- This is very useful for a number of reasons:
  - If you want to use Wireshark to capture traffic from an interface that is connected to a workstation, server, phone or anything else you want to sniff.
  - Redirect all traffic from a VLAN to an IDS / IPS.
  - Redirect all VoIP calls from a VLAN so you can record the calls.



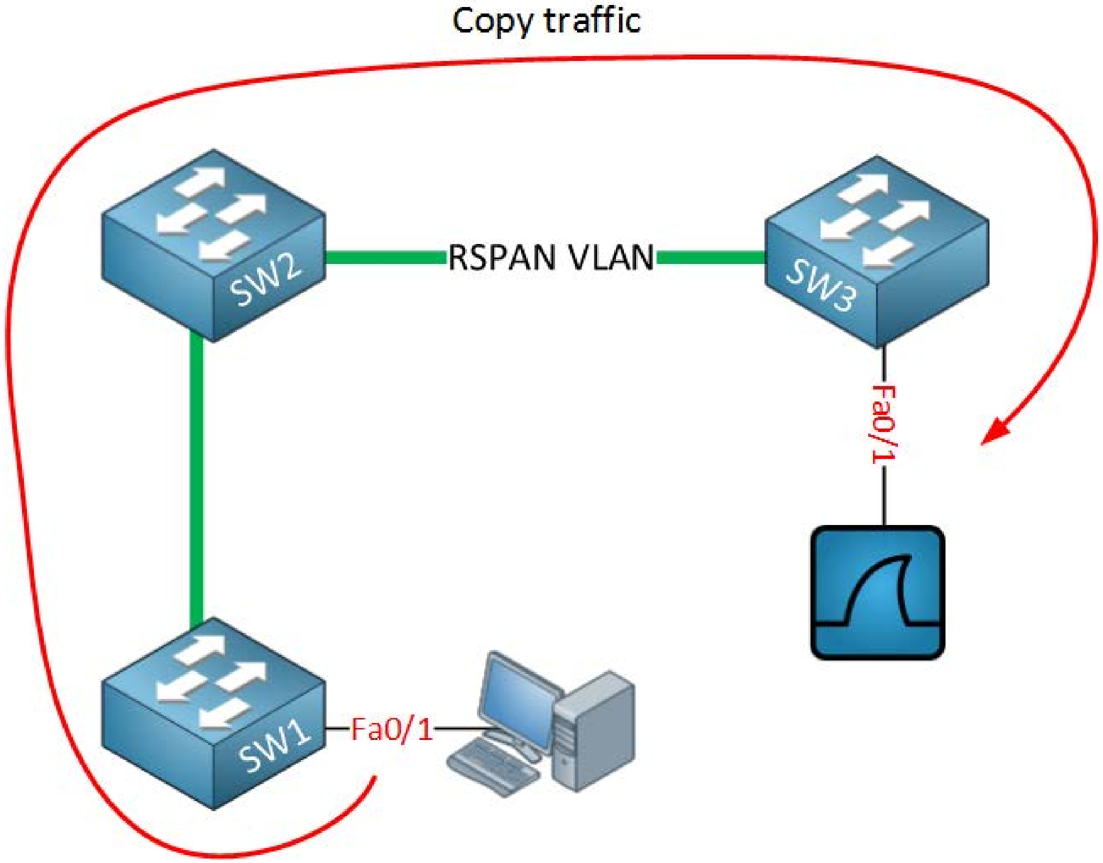
- The source can be an interface or a VLAN, the destination is an interface.

- You can choose if you want to forward transmitted, received or both directions to the destination interface.

Cisco IOS SPAN and RSPAN

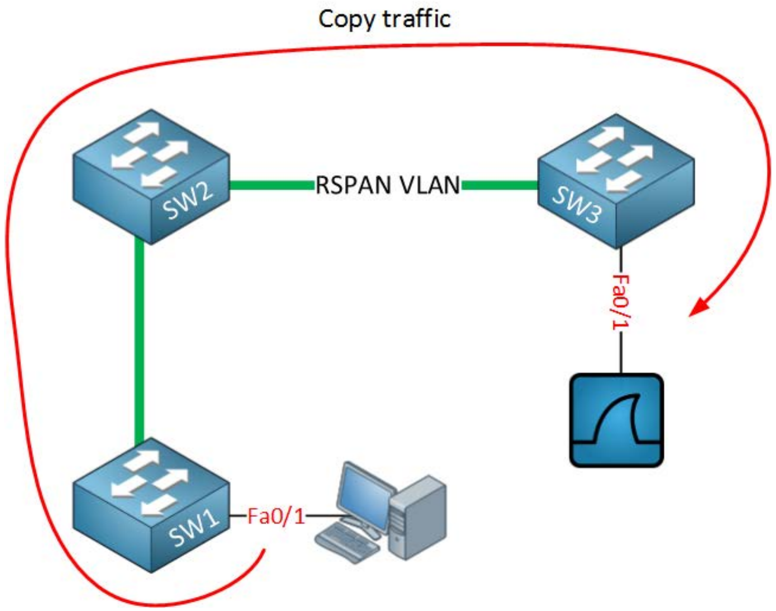
- we call it SPAN, when the destination is a remote interface on another switch we call it RSPAN (Remote SPAN).

- When using RSPAN you need to use a VLAN for your RSPAN traffic so that traffic can travel from the source switch to the destination switch.



Cisco IOS SPAN and RSPAN

- When you use RSPAN you need to use a VLAN that carries the traffic that you are copying.
- In the picture below you see SW1 which will copy the traffic from the computer onto a “RSPAN VLAN”.
- SW2 doesn’t do anything with it while SW3 receives the traffic and forwards it to a computer that has Wireshark running.
- Make sure the trunks between the switches allow the RSPAN VLAN.
- SPAN and RSPAN are great but there are a couple of things you need to keep in mind…

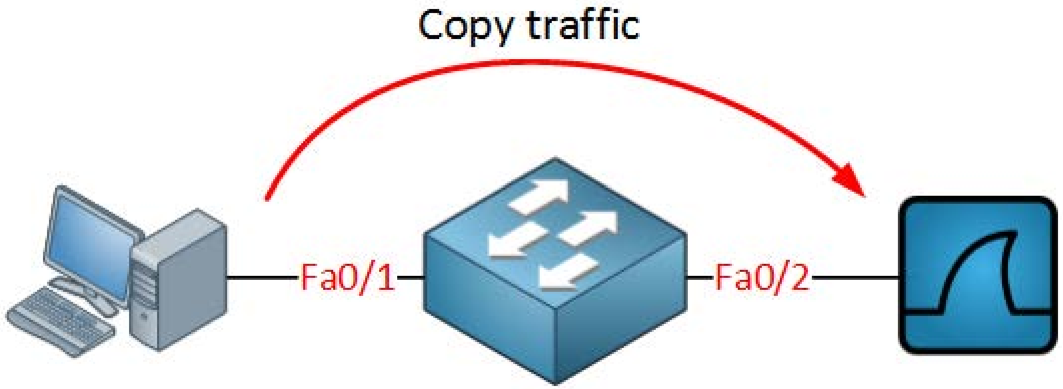


Restrictions

- Both SPAN and RSPAN have some restrictions, I'll give you an overview of the most important ones:
- The source interface can be anything…switchport, routed port, access port, trunk port, etherchannel, etc.
- When you configure a trunk as the source interface it will copy traffic from all VLANs, however there is an option to filter this.
- You can use multiple source interfaces or a single VLAN, but you can't mix interfaces and VLANs.
- It's very simple to overload an interface. When you select an entire VLAN as the source and use a 100Mbit destination interface…it might be too much.
- When you configure a destination port you will lose its configuration. When you remove SPAN, the configuration is restored.
- In short…you can't use the destination interface for anything else besides receiving traffic.
- Layer 2 frames like CDP, VTP, DTP and spanning-tree BPDUs are not copied by default but you can tell SPAN/RSPAN to copy them anyway.
- This should give you an idea of what SPAN / RSPAN are capable of. The configuration is pretty straight-forward so let me give you some examples…

SPAN Configuration

- Let’s start with a simple configuration. I will use the example I showed you earlier:



```
Switch(confg)#monitor session 1 source interface fa0/1
Switch(confg)#monitor session 1 destination interface fa0/2
```

SPAN Configuration

- You can verify the configuration like this:

```
Switch#show monitor session 1
Session 1
---------
Type : Local Session
Source Ports :
Both : Fa0/1
Destination Ports : Fa0/2
```

- As you can see, by default it will copy traffic that is transmitted and received (both) to the destination port.
- If you only want the capture the traffic going in one direction you have to specify it like this:

```
Switch(confg)#monitor session 1 source interface fa0/1 ?
, Specify another range of interfaces
- Specify a range of interfaces
both Monitor received and transmitted traffic
rx Monitor received traffc only
tx Monitor transmitted traffc only
```

SPAN Configuration

- Just add rx or tx and you are ready to go.

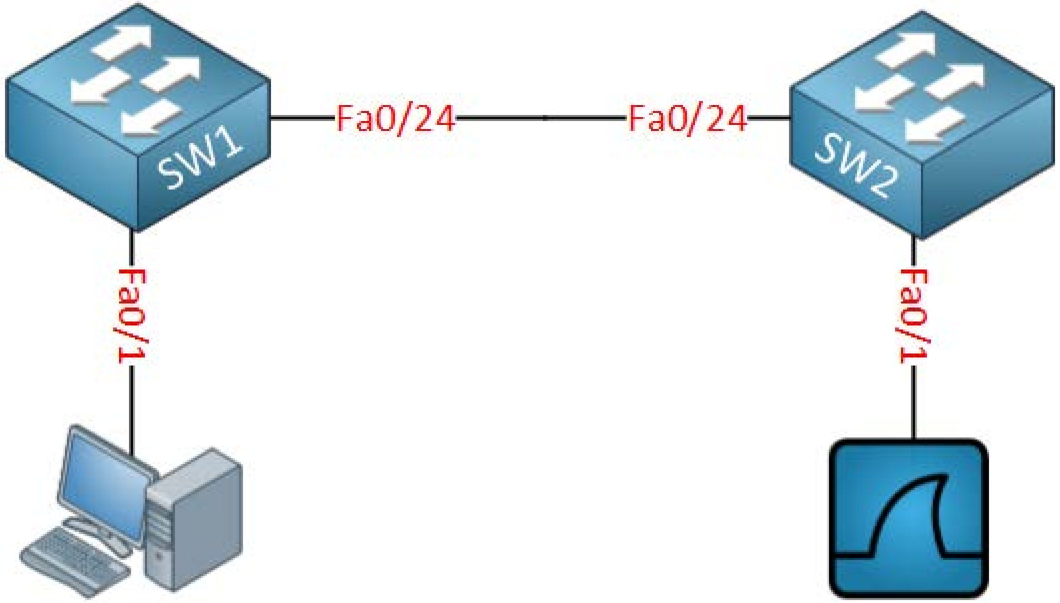
- If interface FastEthernet 0/1 were a trunk you could add a filter to select the VLANs you want to forward:

```
Switch(config)#monitor session 1 filter vlan 1 - 100
```

- This will filter VLAN 1 – 100 from being forwarded.
- If you don’t want to use an interface as the source but a VLAN, you can do it like this:

```
Switch(config)#monitor session 2 source vlan 1
Switch(config)#monitor session 2 destination interface fa0/3
```

RSPAN Configuration



- The idea is to forward traffic from FastEthernet 0/1 on SW1 to FastEthernet 0/1 on SW2.
- There are a couple of things we have to configure here:

RSPAN Configuration

```
SW1(confg)#vlan 100
SW1(confg-vlan)#remote-span
```

```
SW2(confg)#vlan 100
SW2(confg-vlan)#remote-span
```

- First we need to create the VLAN and tell the switches that it’s a RSPAN vlan.
- This is something that is easily forgotten.
- Secondly we will configure the link between the two switches as a trunk:

```
SW1(confg)#interface fastEthernet 0/24
SW1(confg-if)#switchport trunk encapsulation dot1q
SW1(confg-if)#switchport mode trunk
```

```
SW2(confg)#interface fastEthernet 0/24
SW2(confg-if)#switchport trunk encapsulation dot1q
SW2(confg-if)#switchport mode trunk
```

RSPAN Configuration

- Now we can configure RSPAN:

```
SW1(confg)#monitor session 1 source interface fastEthernet 0/1
SW1(confg)#monitor session 1 destination remote vlan 100
```

- This selects FastEthernet 0/1 as the source and VLAN 100 as the destination…

```
SW2(confg)#monitor session 1 source remote vlan 100
SW2(confg)#monitor session 1 destination interface fastEthernet 0/1
```

- And on SW2 we select VLAN 100 as the source and FastEthernet 0/1 as its destination.

RSPAN Configuration

- Here's the output of the show monitor session command:

```
SW1#show monitor session 1
Session 1
---------
Type : Remote Source Session
Source Ports :
Both : Fa0/1
Dest RSPAN VLAN : 100

SW2#show monitor session 1
Session 1
---------
Type : Remote Destination Session
Source RSPAN VLAN : 100
Destination Ports : Fa0/1
Encapsulation : Native
Ingress : Disabled
```