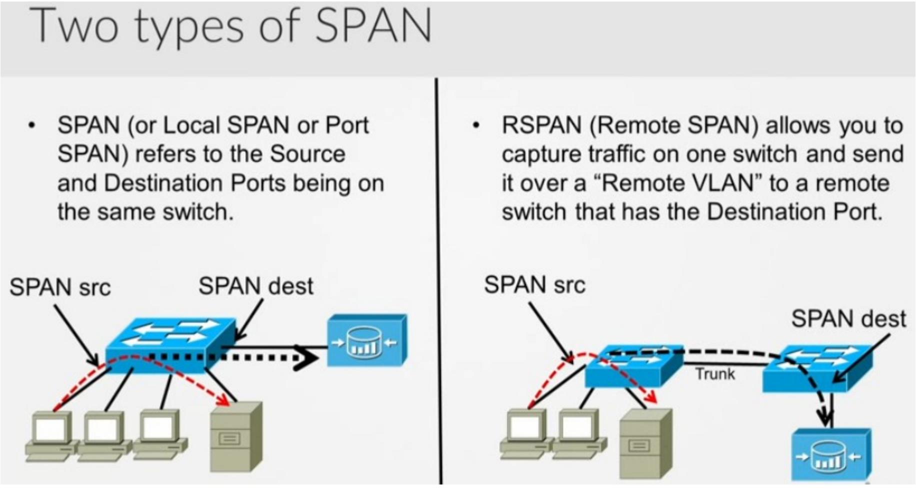
SPAN(Switch Port Analyzer)/RSPAN(Remote SPAN)/ERSPAN(Encapsulated RSPAN)

(Used for Switchport Monitoring/Port Mirroring) | SPAN (destination interface on the same switch)
RSPAN (destination interface on the another switch)
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:
1. 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.
2.Redirect all traffic from a VLAN to an IDS / IPS.
3. Redirect all VoIP calls from a VLAN so you can record the calls.
4.Traffic to/from the switch CPU.
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.
Make sure the trunks between the switches allow the RSPAN VLAN.

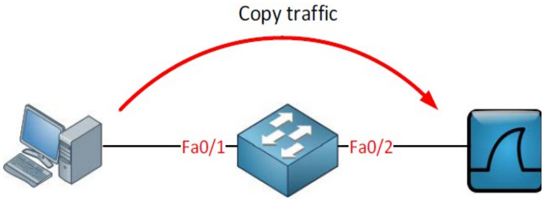
SPAN and RSPAN are great tools but there are some restrictions:
1.The source interface can be anything…switchport, routed port, access port, trunk port, etherchannel, etc.
2.When you configure a trunk as the source interface it will copy traffic from all VLANs, however there is an option to filter this.
3.You can use multiple source interfaces or a single VLAN, but you can’t mix interfaces and VLANs.
4.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.
5.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.

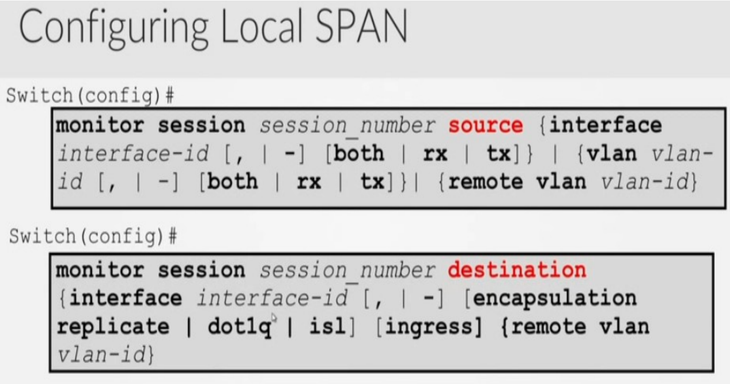


Two types of SPAN

- SPAN (or Local SPAN or Port SPAN) refers to the Source and Destination Ports being on the same switch.

- RSPAN (Remote SPAN) allows you to capture traffic on one switch and send it over a “Remote VLAN” to a remote switch that has the Destination Port.





Configuring Local SPAN

```
Switch(config)#
    monitor session session_number source {interface
    interface-id [, | -] [both | rx | tx]} | {vlan vlan-
    id [, | -] [both | rx | tx]}| {remote vlan vlan-id}

Switch(config)#
    monitor session session_number destination
    {interface interface-id [, | -] [encapsulation
    replicate | dot1q | isl] [ingress] {remote vlan
    vlan-id}
```

• 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.

Configuration:

```
Switch(config)#monitor session 1 source interface fa0/1
```

OR

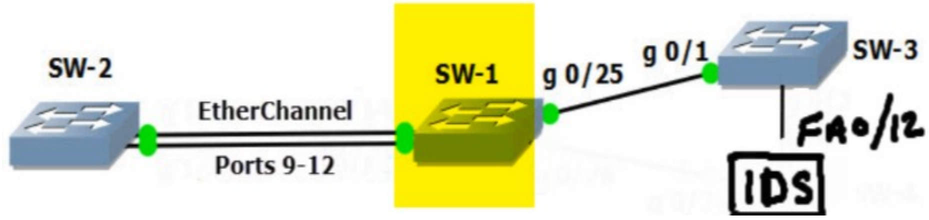
```
Switch(config)#monitor session 1 source interface fa0/1 both  !(options: both | tx | rx)
!(by default it will copy both transmitted and received traffic to the destination port)
Switch(config)#monitor session 1 destination interface fa0/2
```

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

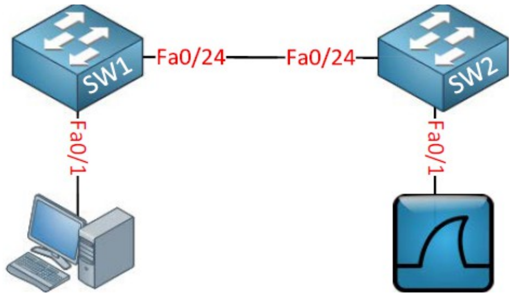
```
Switch(config)#monitor session 1 filter vlan 1 – 100 , 22
!(collecting only for VLAN 1 – 100 and 22)
```

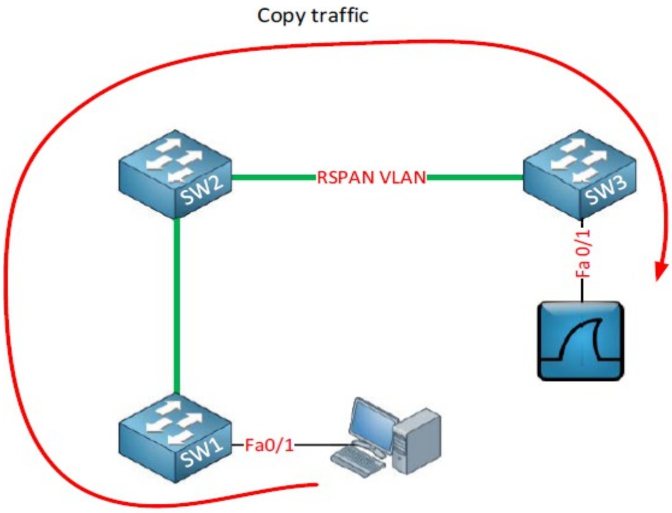
Using VLAN as a source:

```
Switch(config)#monitor session 2 source vlan 1
Switch(config)#monitor session 2 destination interface fa0/3
!(can't use the same destination interface for another session)
```



RSPAN:





```
SW1(config)#vlan 100
SW1(config-vlan)#remote-span
SW2(config)#vlan 100
SW2(config-vlan)#remote-span    !(if vtp running then it should update the remote switch)
!(Then configure the trunk port between the two switches)
SW1(config)#monitor session 1 source interface fastEthernet 0/1  !(you can also use more than one ports in one session i.e. fa0/1 – 2, but there is a limit on every switch)
SW1(config)#monitor session 1 destination remote vlan 100
```

OR

```
(3550 can't do RSPAN unless reflector port is used for it to give up ASIC capabilities. Upper end switches you don't need reflector port)
SW1(config)#monitor session 1 destination remote vlan 100 reflector-port fa 0/20
!(you have to sacrifice a port that will not be used. Any port that is not connected to anything, Note: definitely not use the trunk port as a reflector port)
SW2(config)#monitor session 1 source remote vlan 100
SW2(config)#monitor session 1 destination interface fastEthernet 0/1   !(destination switch port)
```

ERSPAN:

SPAN is however limited to one switch, RSPAN is able to send traffic between switches but this traffic can't be routed.

ERSPAN (Encapsulated Remote Switched Port Analyzer) solves this issue! It uses GRE encapsulation, this allows us to route SPAN traffic from a source to a destination.

You can use ERSPAN on IOS XE, NX-OS and the Catalyst 6500/7600 switches. Unfortunately, It's not supported on the "smaller" IOS switches and routers.

For the source session, we have to configure:

Unique session ID.

List of source interfaces or source VLANs that you want to monitor. Not all platforms support every possible source.

What traffic we want to capture: tx, rx or both.

Destination IP address for the GRE tunnel.

Origin IP address which is used as the source for the GRE tunnel.

Unique ERSPAN flow ID.

Optional: you can specify attributes like the ToS (Type of Service), TTL, etc.

For the destination we have to specify:

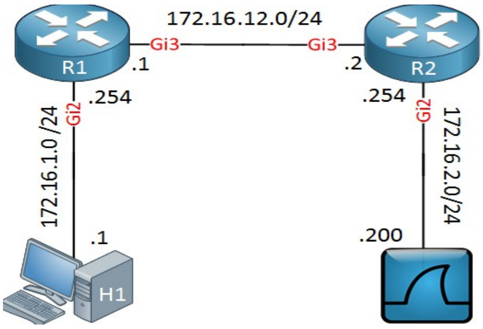
Unique session ID, doesn't have to match with the source session.

Destination interface(s) where you want to forward the traffic to.

Source IP address: has to match with the origin IP address of the source session.

Unique ERSPAN flow ID, has to match with the source session.

Let's look at an example so we can see how ERSPAN works in action.



```
R1(config)#monitor session 1 type erspan-source
R1(config-mon-erspan-src)#source interface GigabitEthernet 2 rx
R1(config-mon-erspan-src)#no shutdown
R1(config-mon-erspan-src)#destination
R1(config-mon-erspan-src-dst)#erspan-id 100
R1(config-mon-erspan-src-dst)#ip address 172.16.2.200
R1(config-mon-erspan-src-dst)#origin ip address 172.16.12.1
R2(config)#monitor session 1 type erspan-destination
R2(config-mon-erspan-dst)#no shutdown
R2(config-mon-erspan-dst)#destination interface GigabitEthernet 2
R2(config-mon-erspan-dst)#source
R2(config-mon-erspan-dst-src)#erspan-id 100
R2(config-mon-erspan-dst-src)#ip address 172.16.2.200
```

Verification and TSHOOT:

Always check if the trunk is allowing the remote-span vlan traffic through if you are using trunk to capture traffic from.

```
sh monitor     !(to see which ports are in monitoring and destination port)
sh monitor session 1
sh vlan remote-span
sh int fa0/3    !(shows if the port is in a monitoring state)
sh run | begin monitor
```