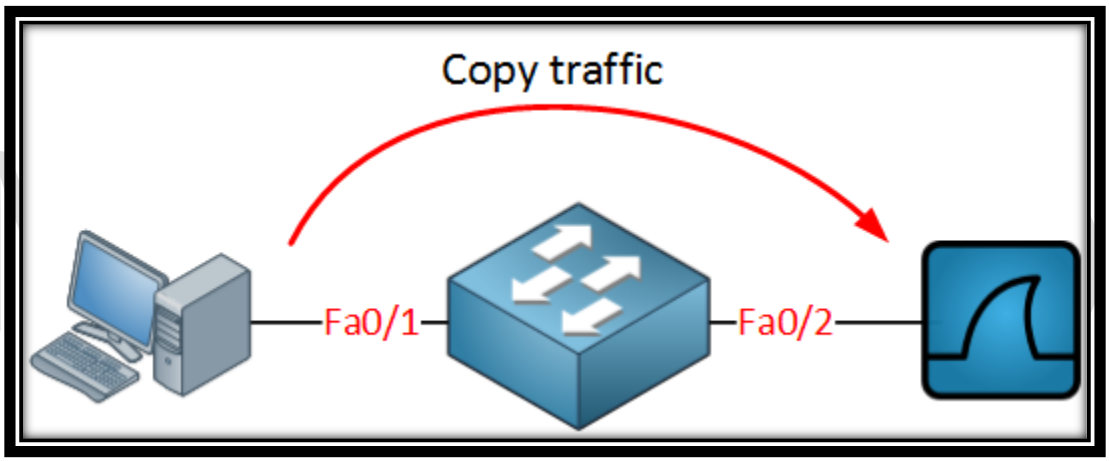

Networkforyou
Welcome
To
Network for you
SPAN, RSPAN
And
ERSPAN
Networkforyou

SPAN (Switched Port Analyzer):

- SPAN stand for Switched Port Analyzer.
- It is use to analyze the traffic for particular port.
- CISCO Catalyst Switches have this feature called SPAN.
- SPAN copy all traffic from a source port or source VLAN to a destination interface.
- SPAN is very useful for number of reasons like if you want to use Wireshark to capture traffic from an interface that is connected to a workstation, server, phone etc. or Redirect all traffic copy from that that interfaces to IDS/IPS or Redirect all VOIP calls from that interface to any call recorder.
- SPAN is also use for troubleshooting purpose and monitor network traffic etc.
- SPAN is used to monitor traffic for performing a security audit.
- SPAN is able to monitor a single interface or many interfaces.



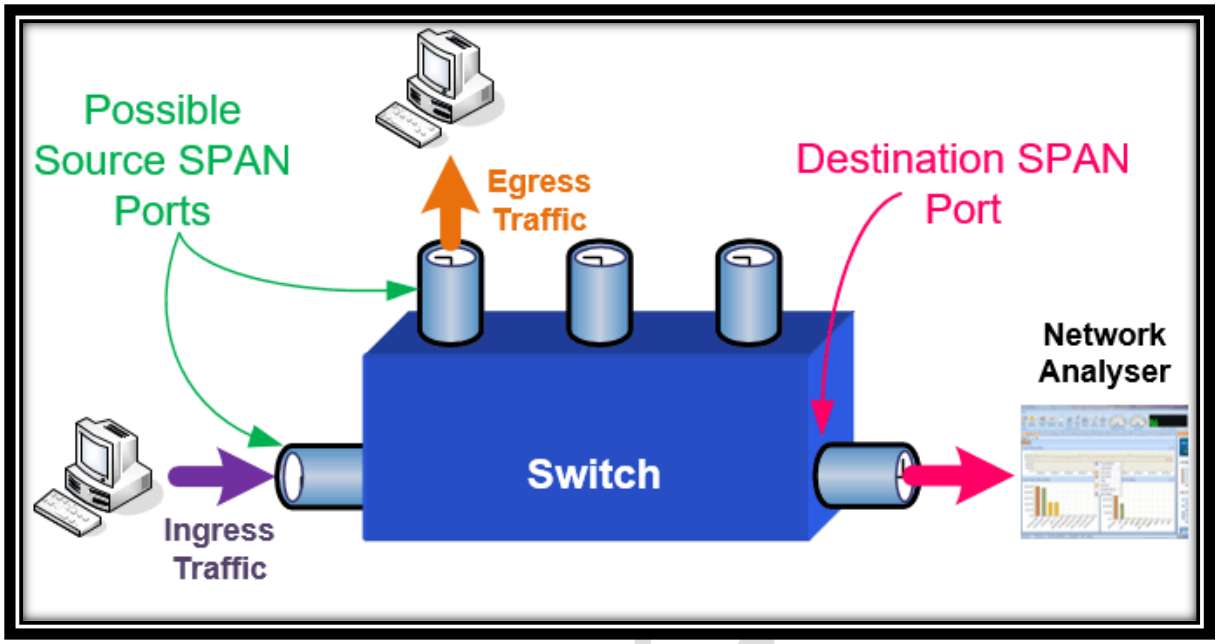
There are 3 main types of SPANs supported on CISCO Switches as given below:

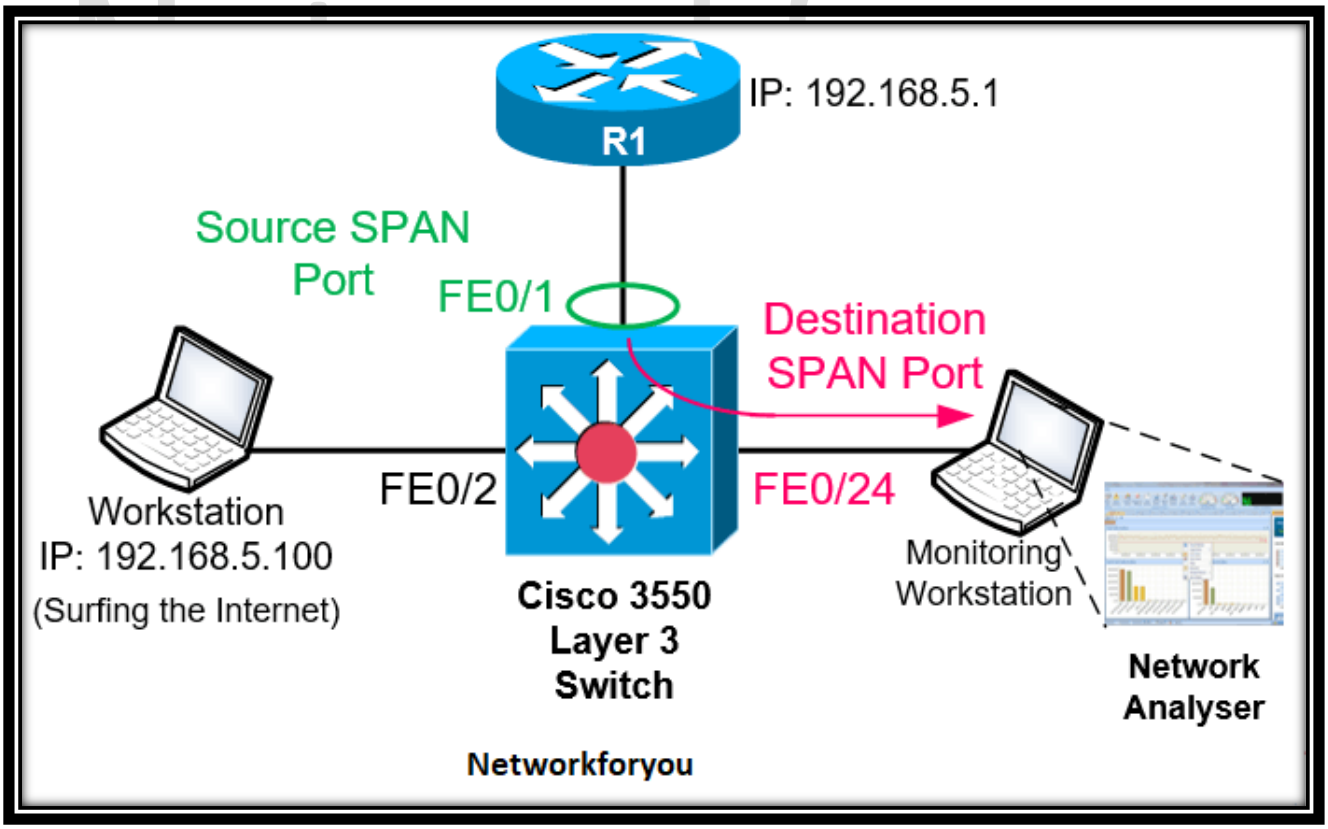
1. Local SPAN (Switched Port Analyzer)
2. RSPAN (Switched Port Analyzer)
3. ERSPAN (Switched Port Analyzer)

Local SPAN:

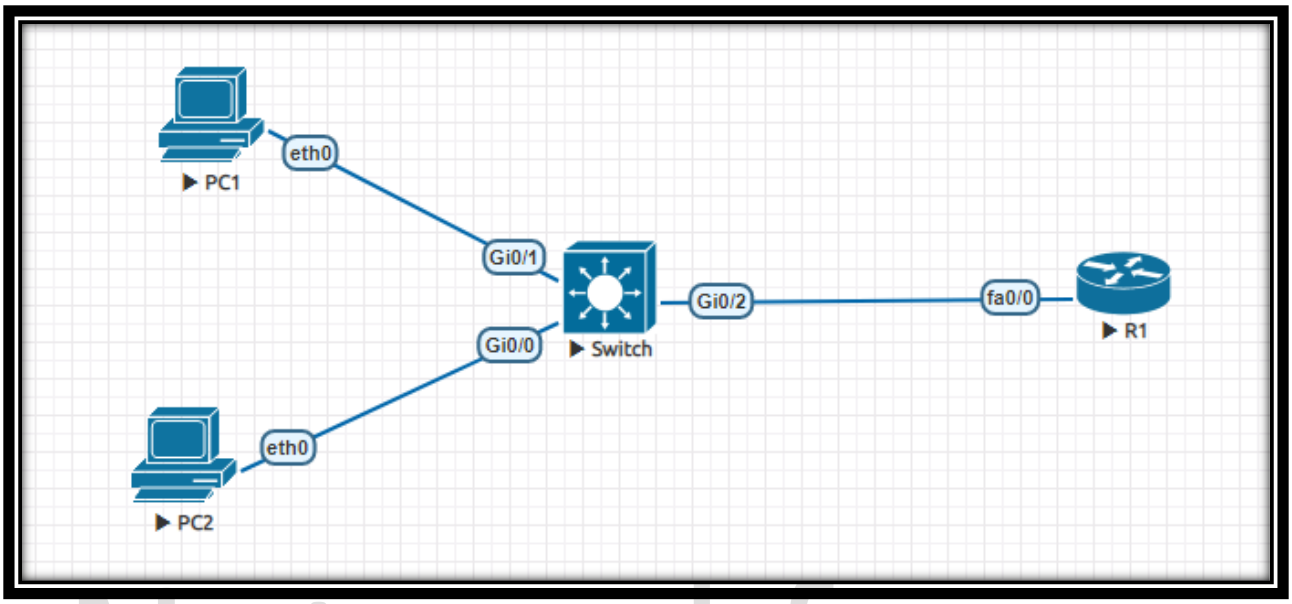
- When we use a destination interface on the same switch as your switch we called it is SPAN.
- In Local SPAN all source interface or source VLANs and destination interface are in same switch.
- In Local SPAN copies traffic from source interface to destination interface for analysis.
- When we use destination interface and source interface on same switch then it is called Local SPAN.

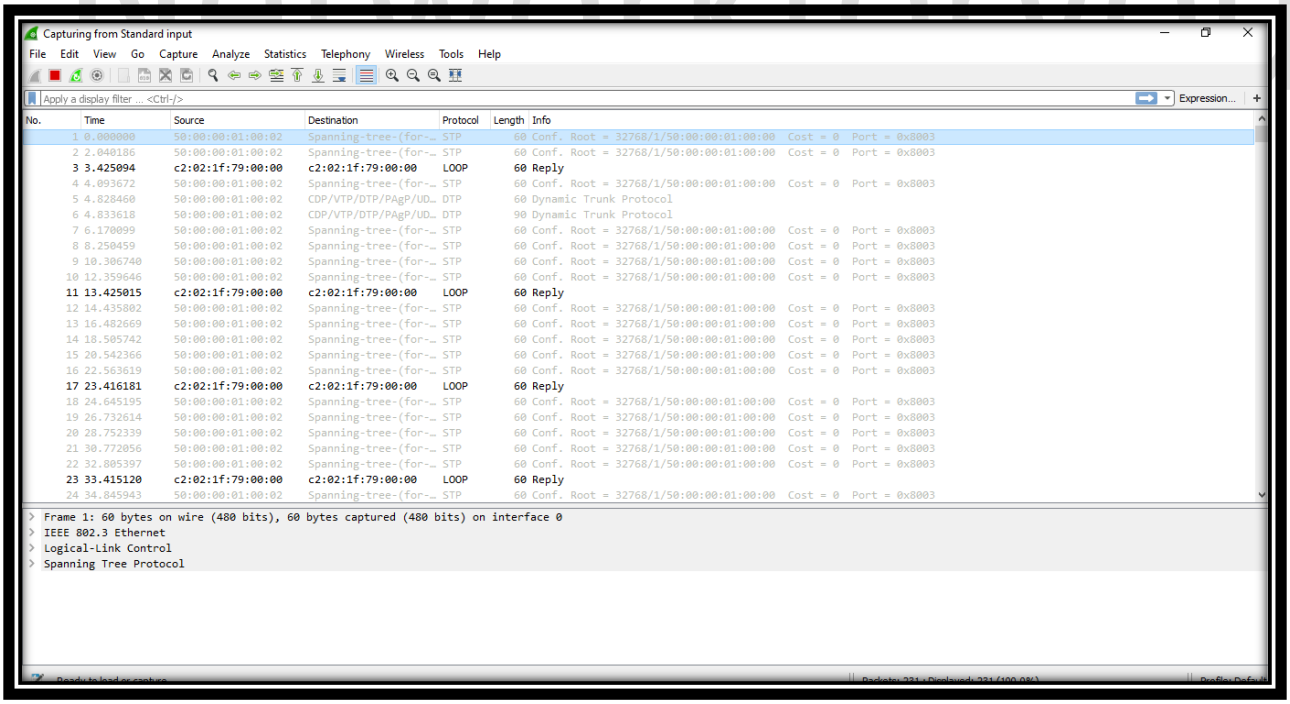
Ps: Link Shadow(https://www.linkshadow.com/) application is also we can use to analysis traffic but in lab we will use wireshark.


Possible Source SPAN Ports
Egress Traffic
Destination SPAN Port
Network Analyser
Switch
Ingress Traffic


R1
IP: 192.168.5.1
Source SPAN Port
FE0/1
Destination SPAN Port
FE0/2
FE0/24
Workstation
IP: 192.168.5.100
(Surfing the Internet)
Cisco 3550 Layer 3 Switch
Monitoring Workstation
Network Analyser
Networkforyou

Lab Time:





Without SPAN Configuration not getting any traffic in Wire sharp.

R1 Configuration	SW1 Configuration:
en config t hostname R1 int f0/0 ip add 1.1.1.1 255.0.0.0 no sh	en config t hostname SW1 monitor session 1 source interface g0/1 both monitor session 1 destination interface g0/2 **sh monitor session 1** **sh int g0/2**

After SPAN Configuration:

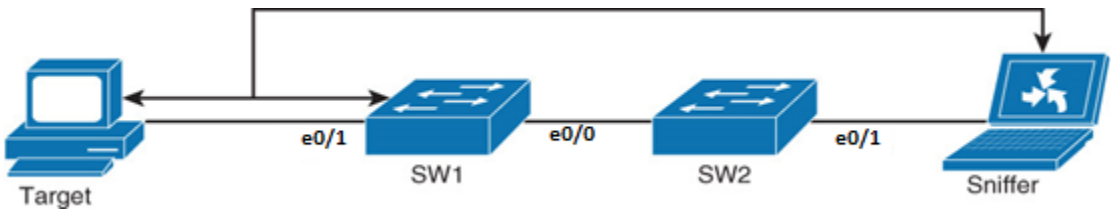
```
SW1#sh int g0/2
GigabitEthernet0/2 is up, line protocol is down (monitoring)
  Hardware is iGbE, address is 5000.0001.0002 (bia 5000.0001.0002)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto Duplex, Auto Speed, link type is auto, media type is unknown media type
  output flow-control is unsupported, input flow-control is unsupported
  Full-duplex, Auto-speed, link type is auto, media type is RJ45
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:01:02, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     4 packets output, 330 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

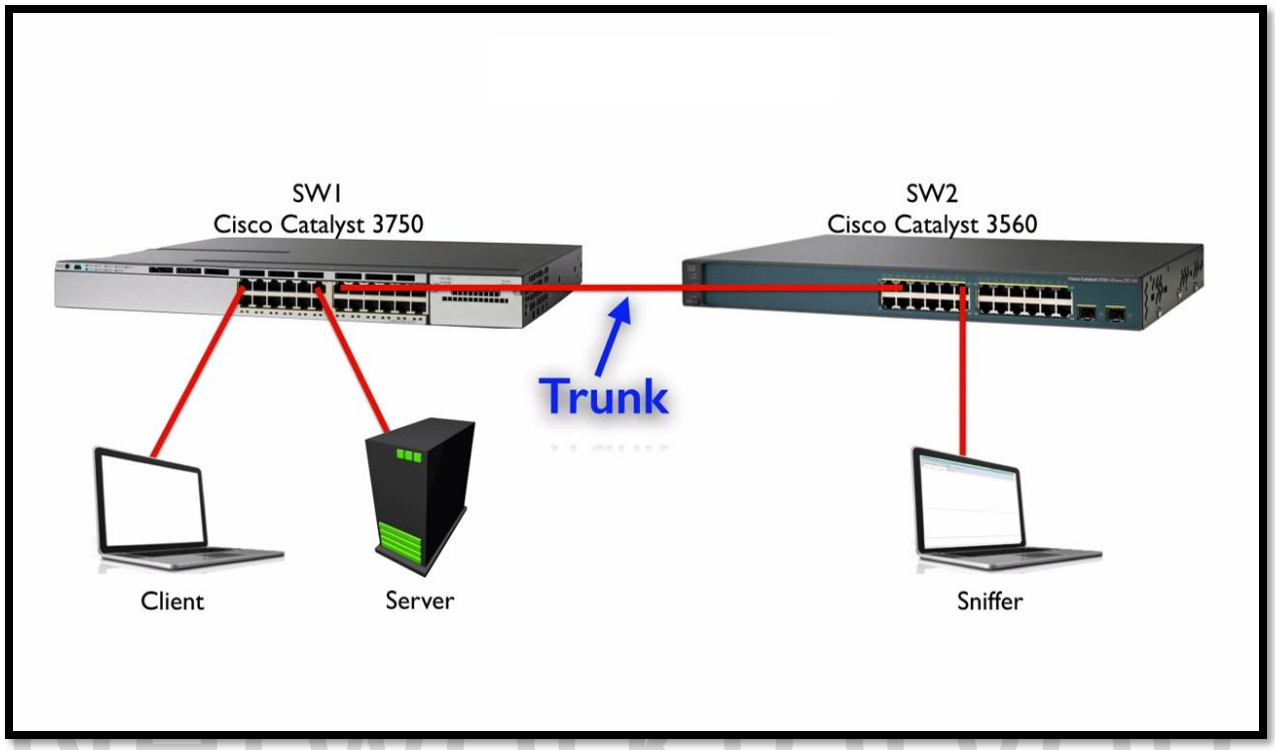
```
SW1#sh monitor session 1
Session 1
---------
Type                        : Local Session
Source Ports                :
    Both                    : Gi0/1
Destination Ports       : Gi0/2
    Encapsulation       : Native
```

No.	Time	Source	Destination	Protocol	Length	Info
525	315.436449	192.168.1.1	192.168.1.2	ICMP	98	Echo (ping) request id=0x1cfa, seq=408/38913, ttl=64 (reply in 526)
526	315.444065	192.168.1.2	192.168.1.1	ICMP	98	Echo (ping) reply id=0x1cfa, seq=408/38913, ttl=64 (request in 525)
527	316.447235	192.168.1.1	192.168.1.2	ICMP	98	Echo (ping) request id=0x1dfa, seq=409/39169, ttl=64 (reply in 528)
528	316.449623	192.168.1.2	192.168.1.1	ICMP	98	Echo (ping) reply id=0x1dfa, seq=409/39169, ttl=64 (request in 527)
529	317.455668	192.168.1.1	192.168.1.2	ICMP	98	Echo (ping) request id=0x1efa, seq=410/39425, ttl=64 (reply in 530)
530	317.459537	192.168.1.2	192.168.1.1	ICMP	98	Echo (ping) reply id=0x1efa, seq=410/39425, ttl=64 (request in 529)
531	318.463788	192.168.1.1	192.168.1.2	ICMP	98	Echo (ping) request id=0x1ffa, seq=411/39681, ttl=64 (reply in 532)
532	318.468861	192.168.1.2	192.168.1.1	ICMP	98	Echo (ping) reply id=0x1ffa, seq=411/39681, ttl=64 (request in 531)
533	319.476944	192.168.1.1	192.168.1.2	ICMP	98	Echo (ping) request id=0x20fa, seq=412/39937, ttl=64 (reply in 534)
534	319.479221	192.168.1.2	192.168.1.1	ICMP	98	Echo (ping) reply id=0x20fa, seq=412/39937, ttl=64 (request in 533)
535	320.484016	192.168.1.1	192.168.1.2	ICMP	98	Echo (ping) request id=0x21fa, seq=413/40193, ttl=64 (reply in 536)
536	320.490693	192.168.1.2	192.168.1.1	ICMP	98	Echo (ping) reply id=0x21fa, seq=413/40193, ttl=64 (request in 535)
537	321.494439	192.168.1.1	192.168.1.2	ICMP	98	Echo (ping) request id=0x22fa, seq=414/40449, ttl=64 (reply in 538)
538	321.499141	192.168.1.2	192.168.1.1	ICMP	98	Echo (ping) reply id=0x22fa, seq=414/40449, ttl=64 (request in 537)
539	322.502919	192.168.1.1	192.168.1.2	ICMP	98	Echo (ping) request id=0x23fa, seq=415/40705, ttl=64 (reply in 540)
540	322.505834	192.168.1.2	192.168.1.1	ICMP	98	Echo (ping) reply id=0x23fa, seq=415/40705, ttl=64 (request in 539)

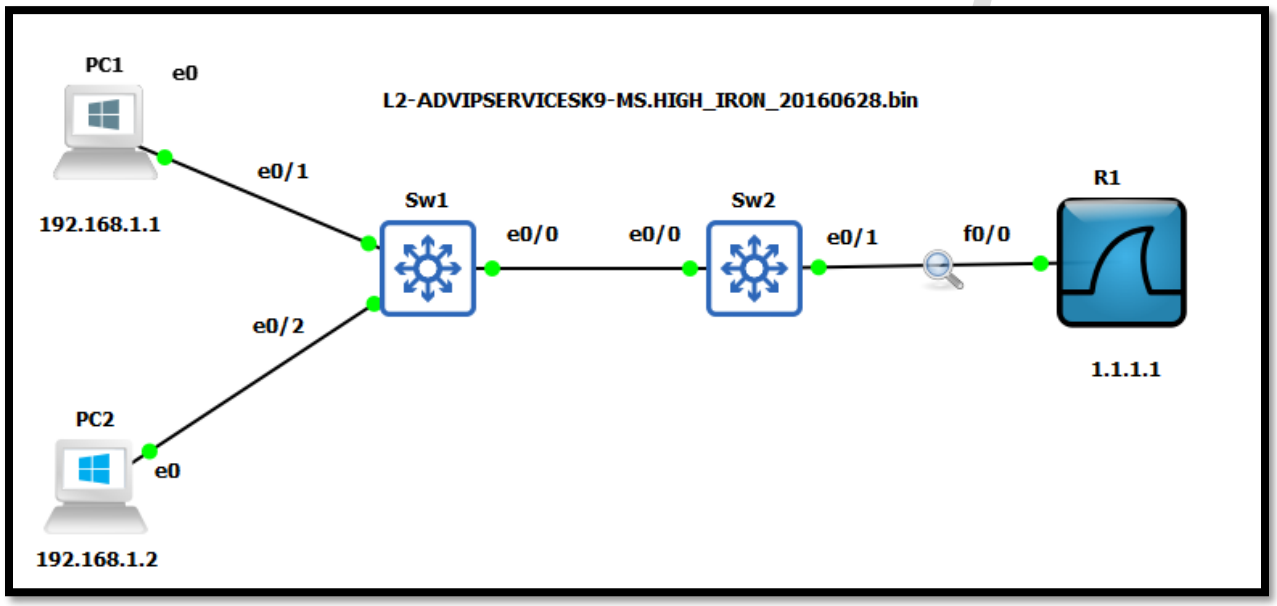
RSPAN:

- RSPAN is stands for Remote Switched Port Analyzer.
- Source port can be a routed port, switch port, trunk or ether channel.
- When destination Interface that is a remote interface on another switch then it is called RSPAN.
- Supports source ports, source VLANs & destination ports on different switches.
- Each session carries SPAN traffic over user-specified dedicated RSPAN VLAN.
- Remote Switched Port Analyzer need to use VLAN for Remote SPAN traffic.
- When we use RSPAN we need to use a VLAN that carries the traffic that you are copying.
- RSPAN need to use a dedicated VLAN that carries the traffic that are copying.
- RSPAN allows traffic that is sourced from Switch to be mirrored to a remote Switch.





Lab time RSPAN:



R1 Configuration	En Config t Hostname R1 Int f0/0 Ip add 1.1.1.1 255.0.0.0 No sh

SW1 Configuration
SW1(Config)#vlan 200 SW1(Config-vlan)#remote-span
SW1(config)#interface Ethernet 0/0 SW1(config-if)#switchport trunk encapsulation dot1q SW1(config-if)#switchport mode trunk
SW1(config)#monitor session 1 source interface Ethernet 0/1 both SW1(config)#monitor session 1 destination remote vlan 200
SW1#show monitor session all
SW2 Configuration
SW2(config)#vlan 200 SW2(config-vlan)#remote-span
SW2(config)#interface Ethernet 0/0 SW2(config-if)#switchport trunk encapsulation dot1q SW2(config-if)#switchport mode trunk
SW2(config)#monitor session 1 source remote vlan 200 SW2(config)#monitor session 1 destination interface Ethernet 0/1
SW2#show monitor session all


```
S2#sh monitor session all
Session 1
---------
Type                   : Remote Destination Session
Source RSPAN VLAN      : 200
Destination Ports      : Et0/1
    Encapsulation      : Native
```

```
S2#sh int e0/1
Ethernet0/1 is up, line protocol is down (monitoring)
  Hardware is Ethernet, address is aabb.cc00.0210 (bia aabb.cc00.0210)
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, Auto-speed, media type is RJ45
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:08:53, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 1000 bits/sec, 1 packets/sec
     127 packets input, 13457 bytes, 0 no buffer
     Received 25 broadcasts (0 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     1988 packets output, 174694 bytes, 0 underruns
 --More--
```


*- [Sw2 Ethernet0/1 to R1 FastEthernet0/0]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
63	28.109940	192.168.1.2	192.168.1.1	ICMP	98	Echo (ping) reply i
64	29.109749	192.168.1.1	192.168.1.2	ICMP	98	Echo (ping) request i
65	29.110912	192.168.1.2	192.168.1.1	ICMP	98	Echo (ping) reply i
66	30.110348	192.168.1.1	192.168.1.2	ICMP	98	Echo (ping) request i
67	30.111274	192.168.1.2	192.168.1.1	ICMP	98	Echo (ping) reply i
69	31.110954	192.168.1.1	192.168.1.2	ICMP	98	Echo (ping) request i
70	31.111293	192.168.1.2	192.168.1.1	ICMP	98	Echo (ping) reply i
71	32.111075	192.168.1.1	192.168.1.2	ICMP	98	Echo (ping) request i
72	32.111725	192.168.1.2	192.168.1.1	ICMP	98	Echo (ping) reply i
74	33.112354	192.168.1.1	192.168.1.2	ICMP	98	Echo (ping) request i
75	33.112690	192.168.1.2	192.168.1.1	ICMP	98	Echo (ping) reply i
76	34.112243	192.168.1.1	192.168.1.2	ICMP	98	Echo (ping) request i
77	34.112783	192.168.1.2	192.168.1.1	ICMP	98	Echo (ping) reply i
78	35.112209	192.168.1.1	192.168.1.2	ICMP	98	Echo (ping) request i
79	35.112714	192.168.1.2	192.168.1.1	ICMP	98	Echo (ping) reply i
80	36.113199	192.168.1.1	192.168.1.2	ICMP	98	Echo (ping) request i
81	36.114346	192.168.1.2	192.168.1.1	ICMP	98	Echo (ping) reply i

```
> Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
> Ethernet II, Src: Private_66:68:00 (00:50:79:66:68:00), Dst: Private_66:68:01 (00:50:79:66:68:01)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.2
> Internet Control Message Protocol
```

ERSPAN:

- ERSPAN is stand for Encapsulated Remote Switched Port Analyzer.
- Feature present on new IOS-XE on ASR1000 also available on Catalyst 6500.
- ERSPAN brings generic routing encapsulation (GRE) for all captured traffic.
- ERSPAN is used to send traffic for sniffing over L3 networks using GRE tunnel.
- ERSPAN on Cisco ASR 1000 Series Routers supports only The Layer 3 interfaces.
- Ethernet interfaces are not supported on ERSPAN configured as Layer 2 interfaces.

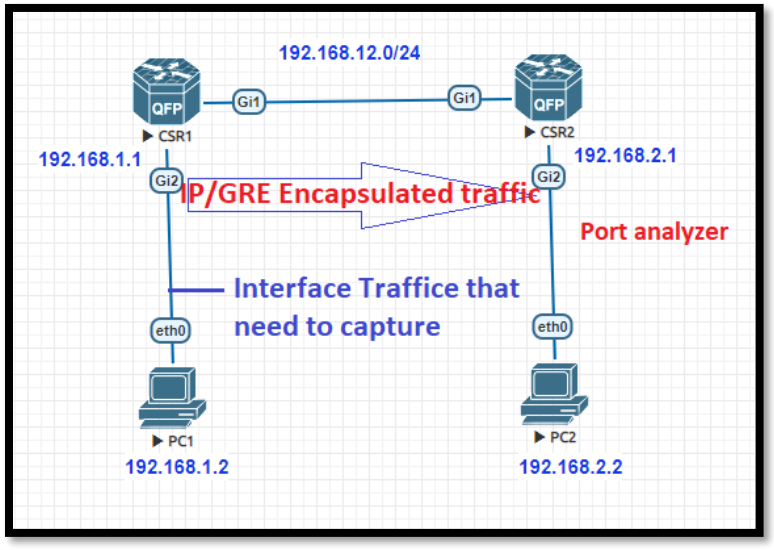
For the Source session, need to Configure:

- To configure ERSPAN it requires Unique session ID, List of source interfaces or VLANs.
- What is the traffic we want to capture tx (Transmit Only), rx (Receive Only) or both.
- ERSPAN configuration require Destination IP address for the GRE tunnel to connect.
- Origin IP address which is used as source for generic routing encapsulation tunnel.
- Unique Encapsulated Remote Switched Port Analyzer (ERSPAN) flow ID (Identity).

For the Destination need to Specify:

- For the Destination Unique session ID doesn't have to match with source session.
- ERSPAN require 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.
- ERSPAN require Unique ERSPAN flow ID, has to match with the source session.

Lab time for ERSPAN:



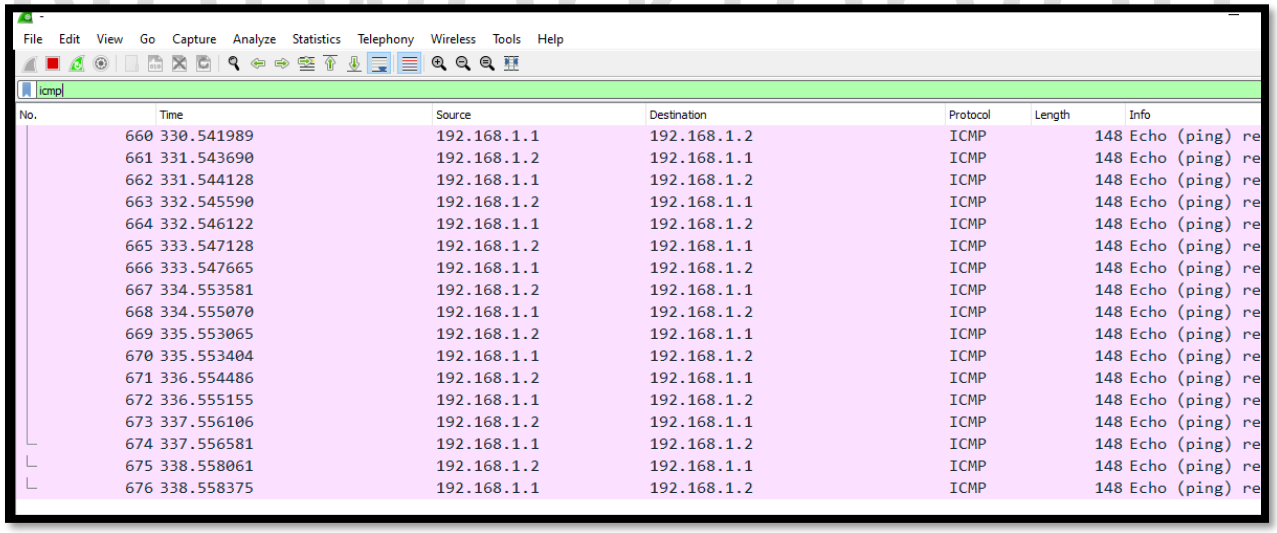
CSR1 Basic IP Configuration:	CSR2 Basic IP Configuration:
en config t hostname R1 int g1 ip add 192.168.12.1 255.255.255.0 no sh int g2 ip add 192.168.1.1 255.255.255.0 no sh exit ip route 0.0.0.0 0.0.0.0 192.168.12.2	en config t hostname R2 int g1 ip add 192.168.12.2 255.255.255.0 no sh int g2 ip add 192.168.2.1 255.255.255.0 no sh exit ip route 0.0.0.0 0.0.0.0 192.168.12.1

CSR1 ERSPAN Configuration:
CSR1(config)#monitor session 1 type erspan-source CSR1(config-mon-erspan-src)#source interface GigabitEthernet 2 both CSR1(config-mon-erspan-src)#no shutdown CSR1(config-mon-erspan-src)#destination CSR1(config-mon-erspan-src-dst)#erspan-id 200 CSR1(config-mon-erspan-src-dst)#ip address 192.168.2.2 CSR1(config-mon-erspan-src-dst)#origin ip address 192.168.12.1
CSR1#show monitor session 1

CSR2 ERSPAN Configuration:
CSR2(config)#monitor session 1 type erspan-destination CSR2(config-mon-erspan-dst)#no shutdown CSR2(config-mon-erspan-dst)#destination interface GigabitEthernet 2 CSR2(config-mon-erspan-dst)#source CSR2(config-mon-erspan-dst-src)#erspan-id 200 CSR2(config-mon-erspan-dst-src)#ip address 192.168.2.2
CSR2#show monitor session 1

```
R1#sh monitor session all
Session 1
---------
Type                          : ERSPAN Source Session
Status                        : Admin Enabled
Source Ports                  :
    Both                      : Gi2
Destination IP Address        : 192.168.2.2
MTU                           : 1464
Destination ERSPAN ID         : 200
Origin IP Address             : 192.168.12.1
```

```
R2#sh monitor session all
Session 1
---------
Type                          : ERSPAN Destination Session
Status                        : Admin Enabled
Destination Ports             : Gi2
Source IP Address             : 192.168.2.2
Source ERSPAN ID              : 200
```

No.	Time	Source	Destination	Protocol	Length	Info
660	330.541989	192.168.1.1	192.168.1.2	ICMP	148	Echo (ping) re
661	331.543690	192.168.1.2	192.168.1.1	ICMP	148	Echo (ping) re
662	331.544128	192.168.1.1	192.168.1.2	ICMP	148	Echo (ping) re
663	332.545590	192.168.1.2	192.168.1.1	ICMP	148	Echo (ping) re
664	332.546122	192.168.1.1	192.168.1.2	ICMP	148	Echo (ping) re
665	333.547128	192.168.1.2	192.168.1.1	ICMP	148	Echo (ping) re
666	333.547665	192.168.1.1	192.168.1.2	ICMP	148	Echo (ping) re
667	334.553581	192.168.1.2	192.168.1.1	ICMP	148	Echo (ping) re
668	334.555070	192.168.1.1	192.168.1.2	ICMP	148	Echo (ping) re
669	335.553065	192.168.1.2	192.168.1.1	ICMP	148	Echo (ping) re
670	335.553404	192.168.1.1	192.168.1.2	ICMP	148	Echo (ping) re
671	336.554486	192.168.1.2	192.168.1.1	ICMP	148	Echo (ping) re
672	336.555155	192.168.1.1	192.168.1.2	ICMP	148	Echo (ping) re
673	337.556106	192.168.1.2	192.168.1.1	ICMP	148	Echo (ping) re
674	337.556581	192.168.1.1	192.168.1.2	ICMP	148	Echo (ping) re
675	338.558061	192.168.1.2	192.168.1.1	ICMP	148	Echo (ping) re
676	338.558375	192.168.1.1	192.168.1.2	ICMP	148	Echo (ping) re