ERSPAN:

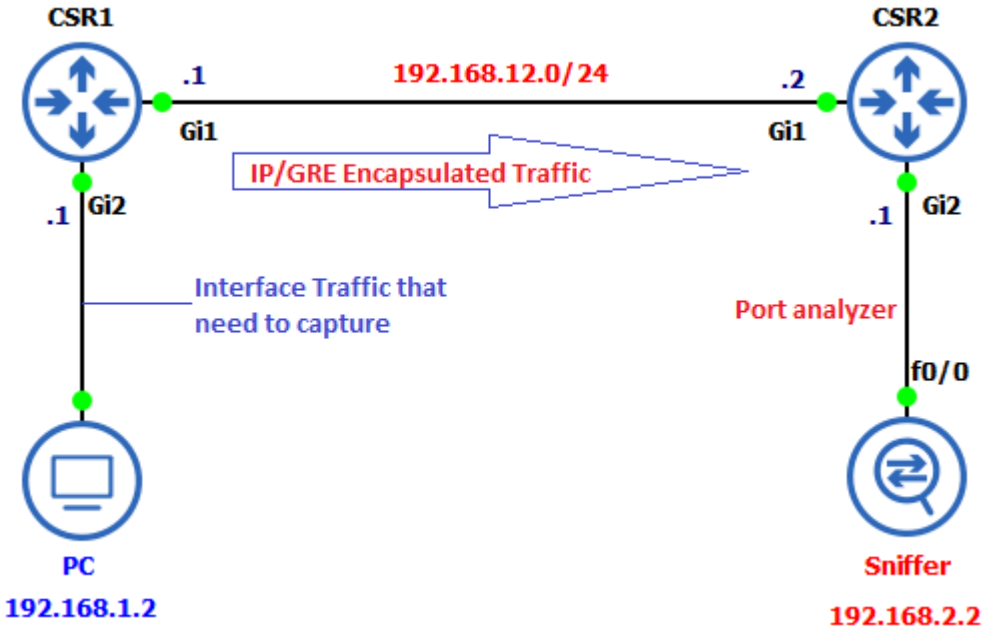
- ERSPAN is term stand for Encapsulated Remote Switched Port Analyzer.
- Feature present on new IOS-XE on ASR1000 also available on Catalyst 6500.
- ERSPAN brings generic routing encapsulation (GRE) for all captured traffic.
- ERSPAN is used to send traffic for sniffing over L3 networks using GRE tunnel.
- 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:

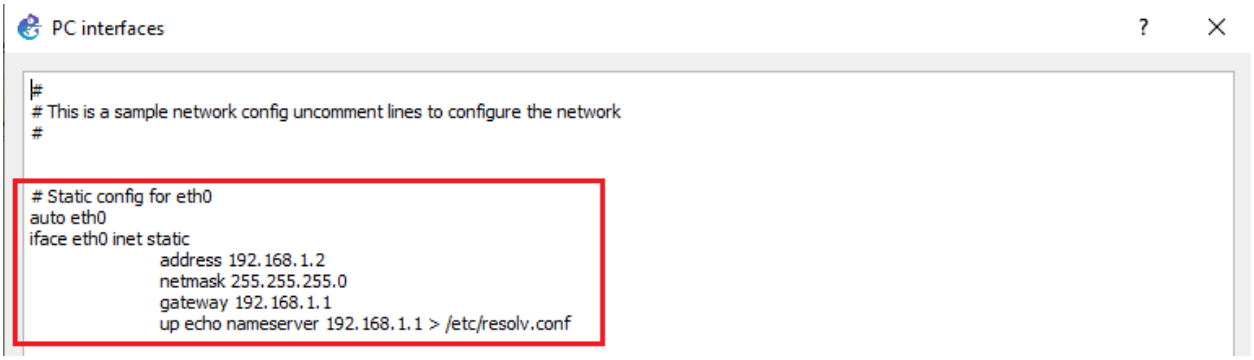
- To configure ERSPAN it requires Unique session ID, List of source interfaces or VLANs.
- What is the traffic we want to capture tx (Transmit Only), rx (Receive Only) or both.
- ERSPAN configuration require Destination IP address for the GRE tunnel to connect.
- Origin IP address which is used as source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



PC1 IP Address Configuration:



Sniffer Configuration
Sniffer(config)#interface f0/0
Sniffer(config-if)#ip address 192.168.2.2 255.255.255.0
Sniffer(config-if)#no shutdown
Sniffer(config)#ip route 0.0.0.0 0.0.0.0 192.168.2.1

CSR1 Basic IP Configuration
CSR1(config)#interface gigabitEthernet 1
CSR1(config-if)#ip address 192.168.12.1 255.255.255.0
CSR1(config-if)#no shutdown
CSR1(config-if)#exit
CSR1(config)#interface gigabitEthernet 2
CSR1(config-if)#ip add 192.168.1.1 255.255.255.0
CSR1(config-if)#no shutdown
CSR1(config-if)#exit
CSR1(config)#ip route 0.0.0.0 0.0.0.0 192.168.12.2

CSR2 Basic IP Configuration
CSR2(config)#interface gigabitEthernet 1
CSR2(config-if)#ip address 192.168.12.2 255.255.255.0
CSR2(config-if)#no shutdown
CSR2(config-if)#exit
CSR2(config)#interface gigabitEthernet 2
CSR2(config-if)#ip add 192.168.2.1 255.255.255.0
CSR2(config-if)#no shutdown
CSR2(config-if)#exit
CSR2(config)#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 rx
CSR1(config-mon-erspan-src)#no shutdown
CSR1(config-mon-erspan-src)#destination
CSR1(config-mon-erspan-src-dst)#erspan-id 100
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 100
CSR2(config-mon-erspan-dst-src)#ip address 192.168.2.2
CSR2#show monitor session 1

Verification:

Let's ping from PC to CSR1 local interface IP which is 192.168.1.1

```
root@PC:~# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.2  netmask 255.255.255.0  broadcast 0.0.0.0
        inet6 fe80::a029:88ff:fe20:d327  prefixlen 64  scopeid 0x20<link>
        ether a2:29:88:20:d3:27  txqueuelen 1000  (Ethernet)
        RX packets 70  bytes 16072 (16.0 KB)
        RX errors 0  dropped 4  overruns 0  frame 0
        TX packets 42  bytes 3624 (3.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@PC:~# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=1.97 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=2.01 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=1.43 ms
```

```
CSR2#show monitor session 1
Session 1
---------
Type                          : ERSPAN Destination Session
Status                        : Admin Enabled
Destination Ports             : Gi2
Source IP Address             : 192.168.2.2
Source ERSPAN ID              : 100
```

```
CSR1#show monitor session 1
Session 1
---------
Type                          : ERSPAN Source Session
Status                        : Admin Enabled
Source Ports                  :
    RX Only                   : Gi2
Destination IP Address        : 192.168.2.2
MTU                           : 1464
Destination ERSPAN ID         : 100
Origin IP Address             : 192.168.12.1
```

After ping from PC to CSR1 local interface CSR1, encapsulate the traffic and send to Sniffer.

No.	Time	Source	Destination	Protocol	Length	Info
22	173.528901	192.168.1.2	192.168.1.1	ICMP	148	Echo (ping) request id=0x0268, seq=1/
23	174.513989	192.168.1.2	192.168.1.1	ICMP	148	Echo (ping) request id=0x0268, seq=2/
24	175.515633	192.168.1.2	192.168.1.1	ICMP	148	Echo (ping) request id=0x0268, seq=3/
25	176.517243	192.168.1.2	192.168.1.1	ICMP	148	Echo (ping) request id=0x0268, seq=4/
26	177.517885	192.168.1.2	192.168.1.1	ICMP	148	Echo (ping) request id=0x0268, seq=5/
27	178.517311	192.168.1.2	192.168.1.1	ICMP	148	Echo (ping) request id=0x0268, seq=6/
28	178.629621	a2:29:88:20:d3:27	0c:06:07:92:2e:01	ARP	110	Who has 192.168.1.1? Tell 192.168.1.2
29	179.517905	192.168.1.2	192.168.1.1	ICMP	148	Echo (ping) request id=0x0268, seq=7/

```
> Frame 22: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on interface -, id 0
> Ethernet II, Src: 0c:06:07:be:03:01 (0c:06:07:be:03:01), Dst: c2:01:24:ec:00:00 (c2:01:24:ec:00:00)
> Internet Protocol Version 4, Src: 192.168.12.1, Dst: 192.168.2.2
v Generic Routing Encapsulation (ERSPAN)
    > Flags and Version: 0x1000
      Protocol Type: ERSPAN (0x88be)
      Sequence Number: 0
> Encapsulated Remote Switch Packet ANalysis Type II
> Ethernet II, Src: a2:29:88:20:d3:27 (a2:29:88:20:d3:27), Dst: 0c:06:07:92:2e:01 (0c:06:07:92:2e:01)
> Internet Protocol Version 4, Src: 192.168.1.2, Dst: 192.168.1.1
> Internet Control Message Protocol
```