How to Configure Cisco SPAN – RSPAN – ERSPAN

Having visibility in the traffic flowing through your network from specific hosts is an excellent way to troubleshoot problems or gather useful information and data. Cisco switches offer the capability to copy packets from specific ports or VLANs and send them to other ports for capturing and analyzing. The traffic can be captured and analyzed using for example Wireshark. This is also useful when you want to send traffic to an Intrusion Detection System (IDS) for security purposes. In Cisco environments you can use a feature called SPAN (Switch Port Analyzer) for this purpose.

There are three kinds of SPAN modes that are available for different scenarios: SPAN, RSPAN & ERSPAN all of them having the following key features:

- Require a source port or vlan and a destination port where the traffic will be collected.
- Source port can be a routed port, switchport, trunk or etherchannel.
- Destination port does not support 802.1x, private vlan, CDP, STP, VTP.

Something to keep in mind also is that you can monitor three kinds of traffic:

1. Incoming (rx) – monitored traffic is sent towards the destination port before any policy modification (ACL, QoS, Policy-Map etc)
2. Transmitting (tx) – monitored traffic is sent towards the destination port after any policy is applied.
3. Encapsulation replicate – Forwards CDP, STP, VTP traffic that usually is ignored by SPAN.
Basic SPAN configuration

I have published a basic SPAN tutorial in this post here in the past, but let’s revisit this configuration to refresh our memory.

Basic SPAN captures traffic from one source port or VLAN and sends the traffic to another port on the same switch. On the diagram shown below, we will capture traffic from source port fa0/1 (connected to a user computer) and send the traffic to destination port fa0/5.

![SPAN Topology](image)

Configuration

Switch# configure terminal
Switch(config)# monitor session 1 source interface fa0/1
Switch(config)# monitor session 1 destination interface fa0/5

With this simple configuration, traffic sourced from interface fa0/1 will be mirrored to interface fa0/5 where you will be able to capture it.
Basic RSPAN configuration

RSPAN (Remote SPAN) feature allows traffic that is sourced from a switch to be mirrored to a remote switch within a layer 2 network over trunk ports. To accomplish this you will have to configure the destination VLAN across the entire path between the switches.

In the diagram below, we want to capture traffic from Switch1 (port fa0/1) and send the traffic to Switch2 (port fa0/5). Although here we show a direct connection with a Layer2 trunk port between Switch1-Switch2, you can have multiple switches between them with no problem (the capturing vlan must be active on the whole path though).

![RSPAN Topology](image)

**Configuration**

Switch1# config term
Switch1 (config)# vlan 100 < —This is the capturing VLAN
Switch1 (config-vlan)# remote span
Switch1(config-vlan)# exit
Switch1 (config)# monitor session 10 source interface fa0/1
Switch1 (config)# monitor session 10 destination remote vlan 100

Switch2_Remote# config term
Switch2_Remote (config)# vlan 100 < —This is the capturing VLAN
Switch2_Remote (config-vlan)# remote span
Switch2_Remote (config-vlan)# exit
Switch2_Remote (config)# monitor session 11 source remote vlan 100
Switch2_Remote (config)# monitor session 11 destination interface fa0/5
All traffic sourced from interface fa0/1 on switch 1 will be forwarded using vlan 100 towards the destination port on remote switch2 where you can sniff the traffic.

**Basic ERSPAN configuration**

ERSPAN (Encapsulated Remote Switched Port Analyzer) is a feature present on the new IOS-XE on ASR1000 but is also available on Catalyst 6500 or 7600. It is used to send traffic for sniffing over layer3 networks and it works by encapsulating the traffic using a GRE tunnel.

On the diagram below, there is a GRE tunnel between Switch1 (again this is usually an ASR1000 or 7600 etc) and remote Switch2. The GRE tunnel is established between IP address **172.16.10.10** (on switch1) and **10.10.10.10** (on switch2). We want to send traffic from fa0/1 on Switch1 to fa0/5 on Switch2.
Configuration

Switch1

Switch1(config)# monitor session 1 type erspan-source
Switch1 (config-mon-erspan-src)# source interface fa0/1
Switch1 (config-mon-erspan-src)# destination
Switch1 (config-mon-erspan-src-dst)# erspan-id 110 < — This ID must be the same on Switch2
Switch1 (config-mon-erspan-src-dst)# ip address 10.10.10.10 < — ip address on switch2
Switch1(config-mon-erspan-src-dst)# origin ip address 172.16.10.10 < — ip address on switch 1

Switch2

Switch2_Remote (config)# monitor session 1 type erspan-destination
Switch2_Remote (config-mon-erspan-dst)# destination interface fa0/5
Switch2_Remote (config-mon-erspan-dst)# source
Switch2_Remote (config-mon-erspan-dst-src)# erspan-id 110
Switch2_Remote (config-mon-erspan-dst-src)# ip address 172.16.10.10 < — source IP from switch 1

Some final notes:

- You can monitor specific vlan traffic using the command:

“monitor session 1 source vlan 10”

- You can monitor incoming or outgoing traffic using

“monitor session 1 source vlan 10 rx/tx”

- Verification is done issuing:

“show monitor session 1”
About the Author

Harris Andrea is a Cisco Certified Professional with more than 18 years of experience working with Cisco network technologies. He is the author of two Cisco Books ("Cisco ASA Firewall Fundamentals" and "Cisco VPN Configuration Guide") which have been embraced by thousands of Cisco professionals all over the world. You can find more Cisco configuration guides and tutorials on his blog here http://www.networkstraining.com