SPAN (Switched Port ANalyzer)—a switch configuration that copies traffic passing through the switch out an additional port for analysis (troubleshooting, logging, spying, …). For example, a workstation running Wireshark could have copies of all traffic passing through the same switch sent to it. Normally, that workstation would only see its own traffic unless you're using hubs. Even with SPAN, the traffic addressing would not be changed, so Wireshark would need to listen to other people's MAC addresses. This is often called putting your NIC into "promiscuous mode" and is something that Wireshark handles by default.

SPAN Session—A collection of rules defining which port(s), including direction, should have their traffic copied to the analyzer's port. The direction can be in, out, or both (default).

VLANs—you can monitor a VLAN as a shorthand way to name all ports that carry that VLAN's traffic, including trunks. As ports are added and removed from the VLAN; the session will automatically include/exclude them. The SPAN session is still just monitoring ports, not really the VLAN itself, so the direction mentioned in a rule is applied to traffic through the individual ports.

Local SPAN—Within the same switch.

RSPAN (Remote SPAN)—can send copied traffic over a VLAN to another switch.

ERSPAN (Encapsulated RSPAN)—Uses GRE to tunnel copied traffic through routers. You'll need an L3 switch to configure GRE on.

Limitations

- Each destination port can be used with only one SPAN session at a time
- A port can't be both a destination and source at once
- Destination ports aren't switchports (no MAC learning).
- A single session can only monitor VLANs or ports, not a mixture
- A session *can* monitor multiple sources
- EtherChannels can be source ports
- Trunks can be source ports (all VLANs are copied but SPAN can filter by VLAN)

CONFIGURATION

Multiple lines of a single SPAN session are tied together by their shared session number; there is no SPAN sub-configuration mode. Usable session numbers range from 1 to 66 on the equipment you're most likely to encounter. You can have multiple source lines *and* multiple destination lines

```
S1(config)# monitor session 42 source interface gi0/1 rx
S1(config)# monitor session 42 source interface gi0/2 tx
S1(config)# monitor session 42 source interface gi0/3 - 5 both
                    Monitoring both inbound (rx) and outbound (tx) is the default, so the "both" keyword
                    won't actually appear in a "show run."
S1(config)# monitor session 42 destination interface gi0/21
S1(config)# monitor session 42 destination interface gi0/22 - 23
```

The example below shows a multi-VLAN source with an RSPAN destination (sending across a vlan to another switch). Don't worry too much about configuring an RSPAN destination; the Cert Guide doesn't.

```
1 S1(config)# monitor session 55 source vlan 22 - 44 both
2                       Range of source VLANs 22 through 44
3 S1(config)# monitor session 55 destination remote vlan 12
```

Beware, with multiple source interfaces and directions, it's easy to overload the output port, the receiving device, and/or the human analyzing the results. Monitoring both directions of all ports in a VLAN [Line 1] is especially stupid, since the session is likely to see each frame twice—entering one port and then leaving another.

VERIFICATION

Show monitor [session { # | all | local | remote | rage #-#}] [detail]

```
1  S1# show monitor detail
2  Session 42
3  ----------
4  Type                   : Local Session
5  Description            : -
6  Source Ports           :
7      RX Only            : Gi0/1
8      TX Only            : Gi0/2
9      Both               : Gi0/3-5
10 Source VLANs           :
11     RX Only            : None
12     TX Only            : None
13     Both               : None
14 Source RSPAN VLAN      : None
15 Destination Ports      : Gi0/21-23
16     Encapsulation      : Native
17           Ingress      : Disabled
18 Filter VLANs           : None
19 Dest RSPAN VLAN        : None
20
21
22 Session 55
23 ----------
24 Type                   : Remote Source Session
25 Description            : -
26 Source Ports           :
27     RX Only            : None
28     TX Only            : None
29     Both               : None
30 Source VLANs           :
31     RX Only            : None
32     TX Only            : None
33     Both               : 22-44
34 Source RSPAN VLAN      : None
35 Destination Ports      : None
36 Filter VLANs           : None
37 Dest RSPAN VLAN        : 12
```

Show monitor session { # | all | local | remote | rage #-# }

```
1  S1# show monitor session range 42-55
2  Session 42
3  ----------
4  Type                   : Local Session
5  Source Ports           :
6      RX Only            : Gi0/1
7      TX Only            : Gi0/2
8      Both               : Gi0/3-5
9  Destination Ports      : Gi0/21-23
10     Encapsulation      : Native
11           Ingress      : Disabled
12
13
14 Session 55
15 ----------
16 Type                   : Remote Source Session
17 Source VLANs           :
18     Both               : 22-44
19 Dest RSPAN VLAN        : 12
```

When you leave off the "detail" keyword, only the source port directions actually in use are listed [Lines 6-8 vs. Line 18].

One last practical note… because destination ports are not switchports, you don't want to ssh from your Wireshark workstation to the switch in order to initiate a monitor session. If you do, your ssh connection will be dropped the moment that you successfully designate your own port as the destination port for the monitor session.