Global Information Assurance Certification Paper

Implementing SPANs on Cisco Switch

Yong Hwa . Kwon
January 25, 2002

Introduction to SPAN

A SPAN, an abbreviation of Switched Port Analyzer, is a method of packet sniffing in a Cisco switch. Generally, when a user want to collect packets from a hub or swit ch using a network wiretap or sniffer without having through knowledge of the difference between a hub and switch, he would commit many errors. For more information about packet sniffer, please refer to [1].

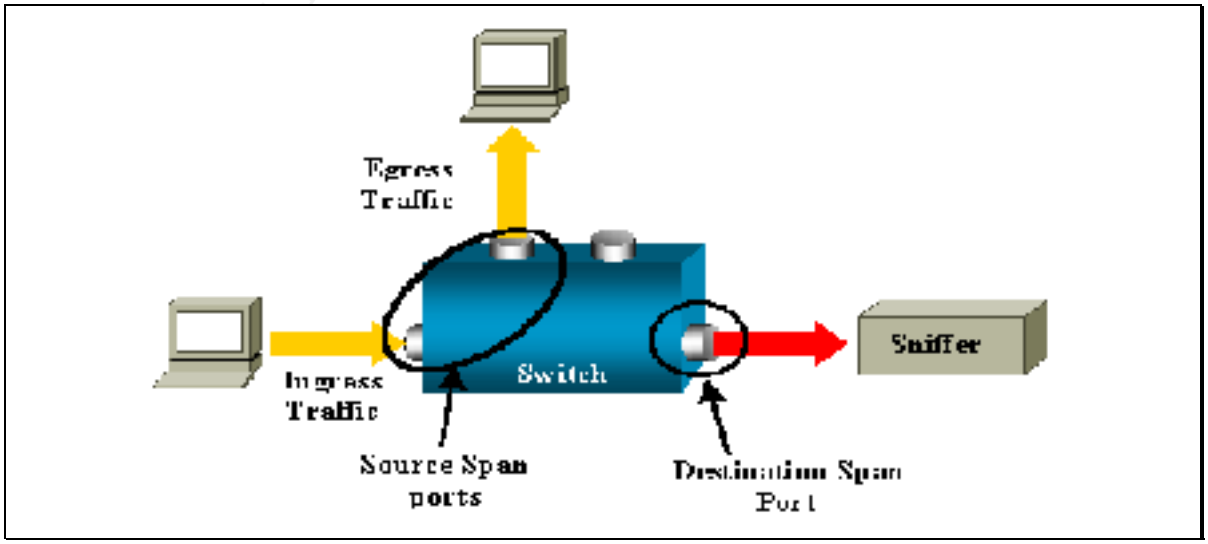
A hub and switch has a big difference as follow ing:

"The biggest difference between a switch and hub is that when a computer transmits a digital signal to a hub, it then send the signal to all ports attached to that hub, whereas a switch will send it only to the specific port where the destination MAC address is located."[2]

In a hub, all received packets are broadcasted to every ports so that a packet sniffing is possible on any ports. This characteristic of a hub involves the risks of a packet sniffing attack. However, in a switch, packets are sent on ly to a specific port. Accordingly, a sniffer only can see packets for the specific port. Thus, in a switch, to perform a packet sniffing, all packets for a target port need to be copied to a specific monitoring port. For more information about switch arch itecture, please refer to [3].

To implement the packet sniffing feature in a Cisco Catalyst Switch, a user should configure port mirroring or port monitoring feature of it, called SPAN(**S**witched **P**ort **An**alyzer). By implementing the packet sniffing feature of a switch, users can attach network analysis tools or IDSs (Intrusion Detection Systems) to the switch. This report explores some SPAN configuration methods using a couple of examples on Cisco switches.

SPAN Terminology [4]



SPAN is comprised of four components: incoming/outgoing packets to/from a switch, a source port for monitoring and a destination port(i.e. monitor port) for packet sniffing.
To study SPAN, we should understand following terminologies:

A. Ingress Traffic : incoming packets into a switch
B. Egress Traffic : outgoing traffic from a switch
C. Source Span Port : a port for monitoring through SPAN. Both ingress traffic and egress traffic will meet on this port
D. Destination Port : a port for monitoring a source port, on which a sniffer or IDS can be connected (Also, called monitor port)

Classification of SPAN

SPAN can be classified into a local SPAN or remote SPAN in accordance with the location of a source and destination port. Also, it is divided into Port-based SPAN or Vlan-based SPAN according to how to define a source span port. In a Cisco Catalyst8540, SPAN can be implemented by port snooping.
Let us examine the types of a SPAN.

A. Local SPAN : a configuration to monitor a port locally
   In a local SPAN, a source SPAN port and destination port are located on a same Switch.
B. Remote SPAN : a configuration to monitor a port remotely
   In a remote SPAN, a source SPAN port and destination port are located on the separated switches (ex. Catalyst6000 with CatOS V5.3).
C. Port-based SPAN : a configuration to monitor a specific source port or multiple source ports
D. Vlan-based SPAN : a configuration to monitor all source ports belong to a Vlan
E. Port Snooping : In a Catalyst 8540 switch, snooping means the monitoring of one or more source ports

Local SPAN

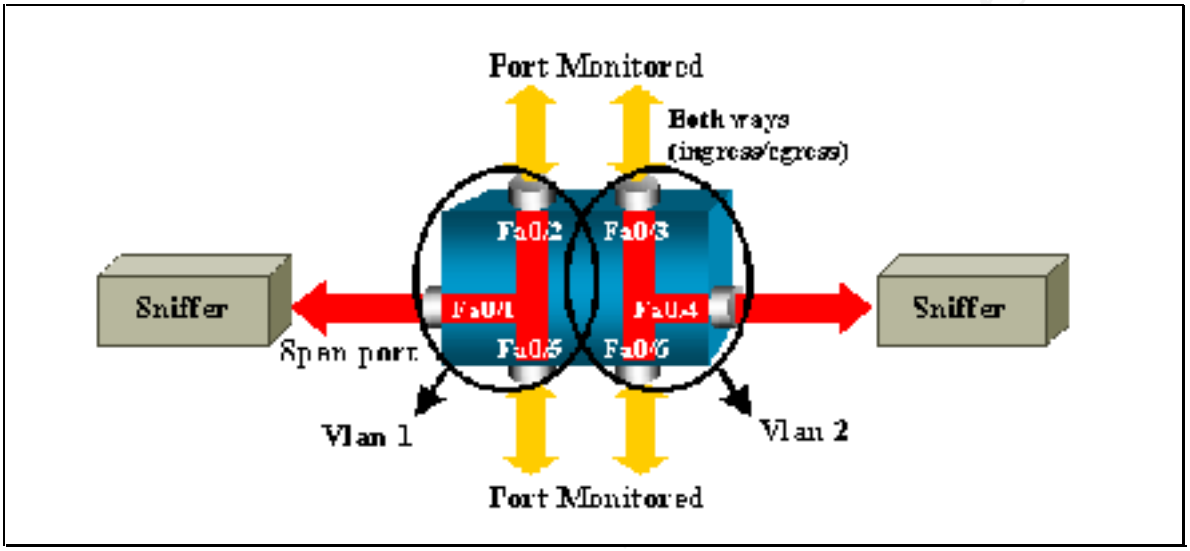
A local SPAN is a SPAN which captures packets locally because a source port (i.e. monitored port) and a destination port (i.e. monitoring port) are located on a same switch.
Cisco's switches can be further classified into IOS-based switch and Set-based switch.
Each switch has different command sets.

1. Cisco IOS-based Switch (Catalyst 2900XL/3500XL/2950)
   Users can implement a local SPAN by using port monitor <interface> command. In this case, a source and destination ports should be located on a same VLAN. Also, following ports cannot be used as a destination port (i.e. monitor port):
   - Dynamic-access port or trunk port
   - Multi-VLAN port
   - Port with port security enabled

- Port belongs to a Fast EtherChannel or Gigabit EtherChannel port group

For more information, refer to the reference [4],[5],[6].

Configuration Example – Catalyst2900XL [4]



The above figure depicts an example of monitoring ports belong to different VLANs - "Management VLAN" and other VLAN.

A. In VLAN1(Management VLAN), F a0/2, Fa0/5 and VLAN1 can be monitored by FastEthernet 0/1.

B. In VLAN2, Fa0/3 and Fa0/6 can be monitored through FastEthernet 0/4.

For the detailed information about the management VLAN, refer to [10].

[Catalyst2900XL Sample Configuration]

Let's look at the configuration process in stages.

A. Configure the FastEthernet Port 0/1.

```
Switch(config)# int fa0/1
Switch(config)# port monitor fastEthernet 0/2
Switch(config)# port monitor fastEthernet 0/5
Switch(config)# port monitor VLAN 1
```

B. Since all ports of the switch belong to one management VLAN, we do not need specify a sepatate VLAN.

C. Assign FastEthernet Port 0/3, 0/4 and 0/6 to VLAN 2 group.

```
Switch(config)# int fa0/3
Switch(config)# switchport access VLAN 2
Switch(config)# int fa0/4
Switch(config)# s witchport access VLAN 2
Switch(config)# int fa0/6
Switch(config)# switchport access VLAN 2
```

D. Configure the port monitor on FastEthernet Port 0/4.
   Switch(config)# int fa0/4
   Switch(config)# port monitor fastEthernet 0/3
   Switch(config)# port monitor fastEtherne t 0/6
E. Check the configuration status using show port monitor command.
   Switch(config)# show port monitor

```
!
<snip>
interface FastEthernet0/1
 port monitor FastEthernet0/2
 port monitor FastEthernet0/5
 port monitor VLAN1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
 switchport access vlan 2
!
```

```
!
interface FastEthernet0/4
 port monitor FastEthernet0/3
 port monitor FastEthernet0/6
 switchport access vlan 2
!
interface FastEthernet0/5
!
interface FastEthernet0/6
 switchport access vlan 2
!
<snip>
!
interface VLAN1
 ip address 192.168.1.1 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
!
!
line con 0
 transport input none
 stopbits 1
line vty 5 15
!
end
```

The **show port monitor** command displays the status of a port monitor, as following figure shows. In the figure, you can monitor on VLAN1, Fa0/2 an d Fa0/5 through Fa0/1. For Fa0/3 and Fa0/6, you can monitor them through Fa0/4.

```
Switch#sh port monitor
Monitor Port             Port Being Monitored
-----------------------  -----------------------
FastEthernet0/1          VLAN1
FastEthernet0/1          FastEthernet0/2
FastEthernet0/1          FastEthernet0/5
FastEthernet0/4          FastEthernet0/3
FastEthernet0/4          FastEthernet0/6
Switch#
```

2. Set-based Switch(Catalyst 4000/5000/6000 Series)

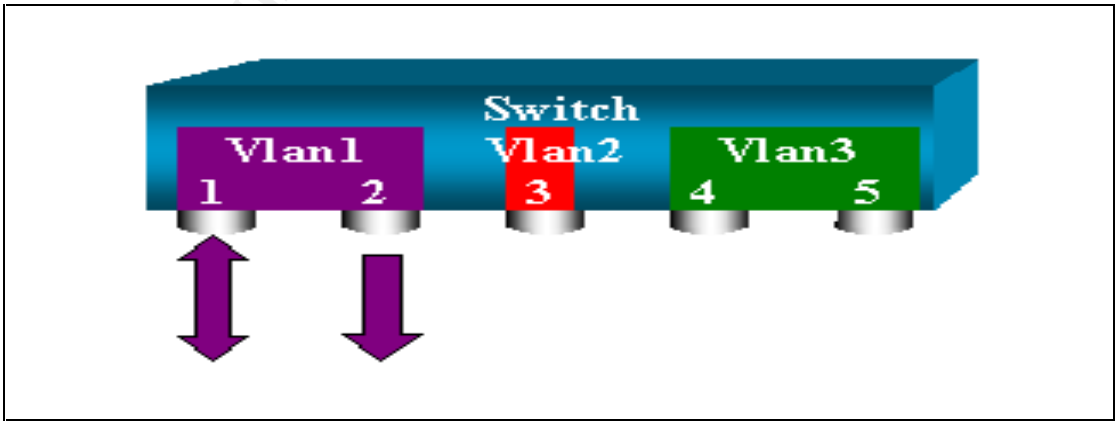
In the Catalyst 4000/5000/6000 series, users can implement port monitor using set span command. By utilizing various opt ions of the command, a user can monitor ports to meet his/her need.

The usage of the command is following:

Usage: set span <source_mod/source_ports ….|source_vlans….|sc0>
<destination_mod/destination_ports> [rx|tx|both]
[inpkts <enable|disable>]
[learning <enable|disable>]
[multicast <enable|disable>]
[filter <vlans..>]
[create]
set span disable [destination_mod/destin ation_port|all]

For the details of command options, refer to the [4],[7] and [8].

Configuration Example – Monitoring a single port with SPAN **[4]**



This example shows the required step to monitor a single port in a Cataly st Switch. By following require steps as following, we can monitor port 9/1 through port 9/2.

A user can configure SPAN using following command:

Switch>(enable) **set span <source port> <destination port>**

Ex) switch>(enable) **set span 9/1 9/2**

```
SCP_BACKUP_SUP> (enable) set span 9/1 9/2
2002 Jan 04 11:03:02 %SYS-5-SPAN_CFGSTATECHG:local span session active for desti
nation port 9/2

Destination    : Port 9/2
Admin Source   : Port 9/1
Oper Source    : None
Direction      : transmit/receive
Incoming Packets: disabled
Learning       : enabled
Multicast      : enabled
Filter         : -
Status         : active

SCP_BACKUP_SUP> (enable) 2002 Jan 04 11:03:02 %SYS-5-SPAN_CFGSTATECHG:local span
 session active for destination port 9/2
```

The above result shows an example of a Catalyst6509. If a user want to make sure that whether the SPAN is configured to meet his/her needs or not, he/she may use **show span** command. The following results show that the configured SPAN is a port -based SPAN and local SPAN, at the same time.

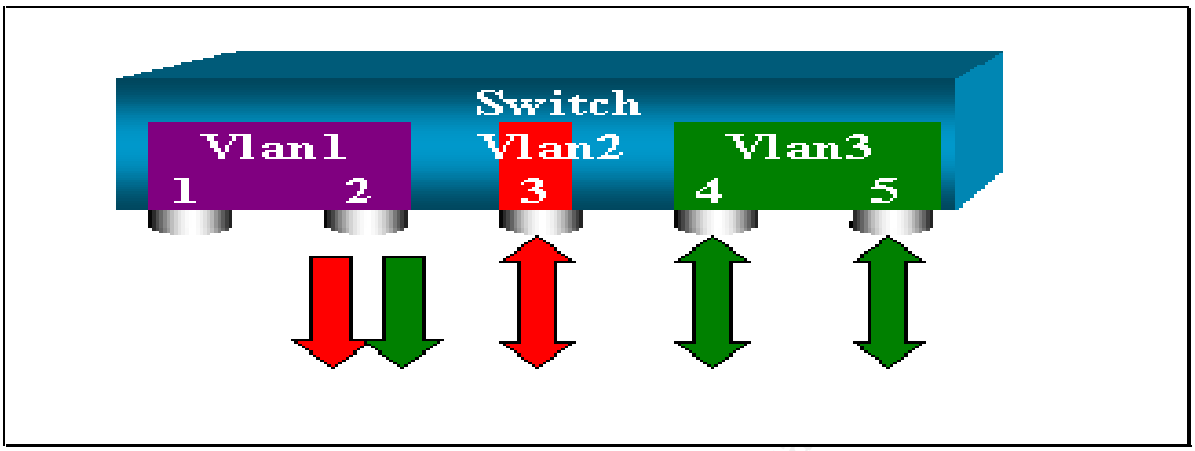
```
SCP_BACKUP_SUP> (enable) show span

Destination    : Port 9/2
Admin Source   : Port 9/1
Oper Source    : None
Direction      : transmit/receive
Incoming Packets: disabled
Learning       : enabled
Multicast      : enabled
Filter         : -
Status         : active

Total local span sessions:  1
```

In case a user wants to monitor additional ports, he may add options to the command using comma and hyphen as following:

switch>(enable) **set <source port1, source port2 -port5> <destination port>**

Ex) switch>(enable) **set 9/1, 9/3-5 9/2**

Configuration Example – Monitoring VLANs with a SPAN **[4]**



The above figure shows an example of monitoring multiple VLAN in a Catalyst Switch. Suppose a user wants to monitor VLAN2 and VLAN3 through port9/2. In this case, each SPAN belongs to a VSPAN since a port monitors multiple VLAN -based SPANs. To configure such case, a user can use the following command.

switch>(enable) **set <source vlan2, source vlan3> <destination port>**

Ex) switch>(enable) **set 2,3 9/2**

```
SCP_BACKUP_SUP> (enable) set span 41,42 9/2
2002 Jan 04 11:31:15 %SYS-5-SPAN_CFGSTATECHG:local span session active for desti
nation port 9/2

Destination     : Port 9/2
Admin Source    : VLAN 41-42
Oper Source     : None
Direction       : transmit/receive
Incoming Packets: disabled
Learning        : enabled
Multicast       : enabled
Filter          : -
Status          : active

SCP_BACKUP_SUP> (enable) 2002 Jan 04 11:31:15 %SYS-5-SPAN_CFGSTATECHG:local span
 session active for destination port 9/2
```

The above result shows a screen dump of a Catalyst6509.

We also check the configuration status by using the **show span** command as following:

```
SCP_BACKUP_SUP> (enable) sh span

Destination     : Port 9/2
Admin Source    : VLAN 41-42
Oper Source     : None
Direction       : transmit/receive
Incoming Packets: disabled
Learning        : enabled
Multicast       : enabled
Filter          : -
Status          : active

Total local span sessions:  1
```

3. Removing SPAN

To remove a SPAN, a user can use following command:

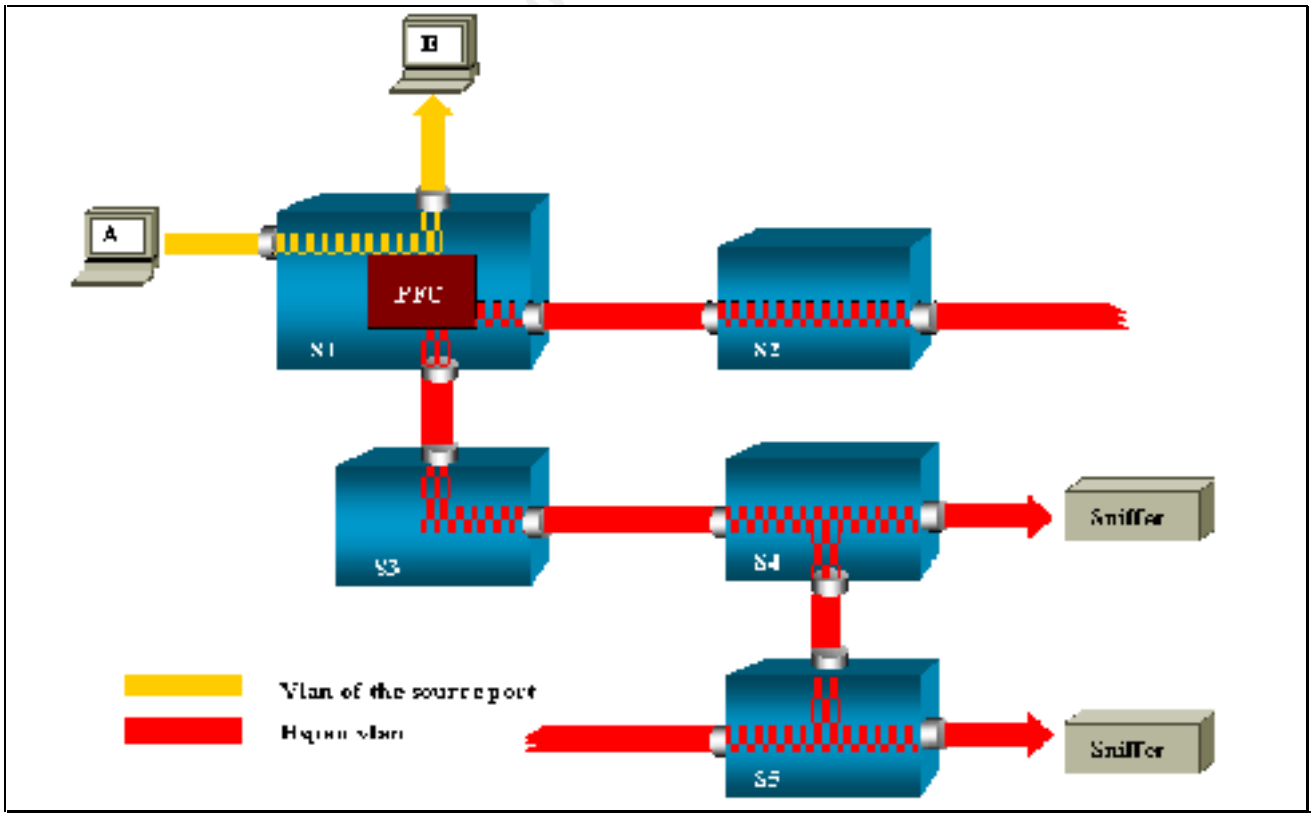
Switch>(enable) **set span disable [destination port | all]**

Ex) switch>(enable) **set span disable 9/2** or

switch>(enable) **set span disable all**

Remote SPAN [4]

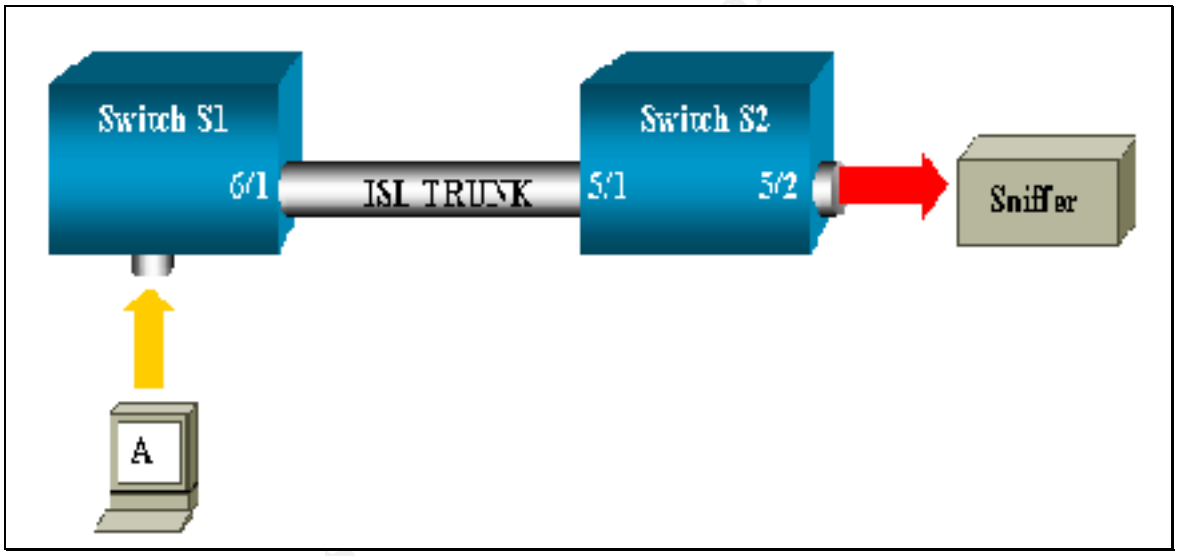
A remote span is a span that captures packets remotely because a source port (i.e. monitored port) and a destination port (i.e. monitoring Port) are located on different switches.



The description for the above network diagram is following:

A. S1 Switch: a switch with a source port
B. S2,S3 Switch: intermediate switches.
   (i.e. An Intermediate switch has n either a source port nor a destination port. As a VLAN for a RSPAN, the switches are used for packet flooding.)
C. S4,S5 Switch: a switch with a destination port
D. To prevent the packet looping in a VLAN for a RSPAN, the **Spanning-Tree Protocol** should be applied.
E. The learning option of the S2 & S3 should be disabled so that they can flood packets.
F. A user should create a specific VLAN which can be used for a RSPAN.

Configuration Example – Remote SPAN **[4]**



In this case, a user remotely monitors port 6/1 in swic h1 through port 5/2 in switch2. Two switches have a trunk port in between them.

To implement the above configuration, a user should follow following steps:

A. Configure a VTP domain so that the VLAN information is shared.
   Switch2>(enable) **set vtp domain cisco**
B. Create a TRUNK LINK between two switches
   Switch2>(enable) **set trunk 5/1 desirable**
C. Create a VLAN for RSPAN
   Switch2>(enable) **set vlan 100 rspan**
D. Configure a destination port and VLAN for a RSPAN on Switch2
   Switch2>(enable) set rspan destination 5/2 100
E. Configure a source port on Switch1
   Switch2>(enable) set rspan source 6/2 100

For the details of VTP and Trunk port setup, please refer to the reference[11].

```
SCP_MASTER_SUP> (enable) sh conf
This command shows non-default configurations only.
Use 'show config all' to show both default and non-default configurations.
<snip>
#time: Fri Jan 4 2002, 14:09:52 UTC
!
#version 6.1(1b)

<snip>
#vtp
set vtp domain datacenter            ; VTP Domain  => datacenter
<snip>
#port channel
set port channel 1/1-2 10
set port channel 6/1-4 30
set port channel 9/17-20 31
set port channel 2/1-2 74
set port channel 7/15-16 75
<snip>
!
#module 1 : 2-port 1000BaseX Supervisor
set port name       1/1  SCP Backup Switch
set port name       1/2  SCP Backup Switch
set trunk 1/1  on isl 1-1005,1025-4094      ; Trunk Port
set trunk 1/2  on isl 1-1005,1025-4094
set port channel 1/1-2 mode on
```

The above figure shows a real configuration example of a Catalyst6509.
In this example, the vtp domain is a datacenter and both port 1/1 and 1/2 are used for the trunk link between two switches.

[Creation of a VLAN 100 for RSPAN]

```
SCP_BACKUP_SUP> (enable) set vlan 100 rspan
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 100 configuration successful
```

[Switch <SCP_BACKUP_SUP> Destination Port Configuration]

```
SCP_BACKUP_SUP> (enable) set rspan destination 9/2 100
2002 Jan 04 14:48:03 %SYS-5-SPAN_CFGSTATECHG:remote span destination session act
ive for destination port 9/2

Rspan Type     : Destination
Destination    : Port 9/2
Rspan Vlan     : 100
Admin Source   : -
Oper Source    : -
Direction      : -
Incoming Packets: disabled
Learning       : enabled
Multicast      : -
Filter         : -
Status         : active

SCP_BACKUP_SUP> (enable) 2002 Jan 04 14:48:03 %SYS-5-SPAN_CFGSTATECHG:remote spa
n destination session active for destination port 9/2
```

[Switch <SCP_BACKUP_SUP> Source Port Configurat ion]

```
SCP_MASTER_SUP> (enable) set rspan source 9/1 100
2002 Jan 04 14:51:18 %SYS-5-SPAN_CFGSTATECHG:remote span source session active
for source port 9/1

Rspan Type      : Source
Destination     : -
Rspan Vlan      : 100
Admin Source    : Port 9/1
Oper Source     : Port 9/1
Direction       : -
Incoming Packets: disabled
Learning        : enabled
Multicast       : -
Filter          : -
Status          : active

SCP_BACKUP_SUP> (enable) 2002 Jan 04 14:51:18 %SYS-5-SPAN_CFGSTATECHG:remote spa
n source session active for source port 9/1
```

[Switch <SCP_BACKUP_SUP> Disabling RSPAN]

```
SCP_BACKUP_SUP> (enable) set rspan disable ?
  destination            Set rspan disable destination [<mod/port>|all]
  source                 Set rspan disable source [<rspan_vlan>|all]
SCP_BACKUP_SUP> (enable) set rspan disable destination 9/2
This command will disable your span session.
Do you want to continue (y/n) [n]?y
Disabled monitoring of remote span traffic on port 9/2
```

For the detailed information for RSPAN, refer to the [4].

SPAN Feature and Limitation

Feature [4]	Catalyst4000	Catalyst5000	Catalyst6000
Inpkts enable/disable option	4.4	4.2	5.1
Multiple sessions, Ports in different Vlans	5.1	5.1	5.1
SC0 Option	X	5.1	5.1
Multicast enable/disable option	X	5.1	5.1
Learning enable/disable option	5.2	5.2	5.3
RSPAN	X	X	5.3

The above table shows the relationship between SPAN options and Catalyst OS Version[4] [7] [8]. A concise descriptions are:

A. To prevent from Bridging Loops, a user should apply the enable/disable option for input packet to the Catalyst switch. Default setting is disabled.
B. For CatOS v.5.1 or later, the multiple SPAN sessions and ports are allowed.
C. For Catalyst5000/6000 with CatOS 5.1 or later, the traffic monitoring for Management Interface SC0 and Multicast Traffic is allowed.
D. CatOS 5.2 or later provides the learning option which is used when a destination port learns a Mac address from in coming packets.
E. As noted earlier, RSPAN features are only provided in the Catalyst6000 with CatOS 5.3 or later.

Since the number of SPAN in a Catalyst switch affects to the performance of a switch, the number of optimal SPAN is limited as following:

Feature [4]	Catalyst4000	Catalyst5000	Catalyst6000
Rx or Both SPAN sessions	5	1	2
Tx SPAN sessions	5	4	4
Rx, Tx, or both RSPAN source sessions	X	X	1
RSPAN destination	X	X	24

For more information, refer to the reference [4], [7] and [8].

A compact description for the above table is following:

A. In a Catalyst 4000, the maximum allowed number of SPAN sessions for both Transmit/Receive traffic is five.

B. In a Catalyst 5000, the maximum number of SPAN session for the Transmit traffic is four. However, the maximum allowed number of SPAN session for both Transmit/Receive traffic is one.

C. In a Catalyst 6000, for the local SPANs, the numbers of session are allowed from two to four. For the RSPAN, the number for source session is one but the number for destination session is allowed upto twenty -four.

To maintain optimal switch performance, users should consider recommended number of SPAN sessions.

Conclusion

To utilize various network analysis and security tools in a switched network environment, we should understand the architecture and characteristics of a switch and its configuration methods. In this report, as the door to understand network and switch monitoring, we have explored SPAN and its various configurations. Since the importance of Internet is increasing everyday, the accurate network analysis is key factor for network security.

On the basis of the precise network analysis, we are able to identify the potential problems and deal effectively with tense situations.

Reference

[1] “Sniffing(Network wiretap, sniffer)
http://www.robertgraham.com/pubs/sniffing -faq.html

[2] “The Difference between a hub and a switch ”
SYBEX “Cisco Certified Network Associate, Study Guide . Exam (640-407) (p.7~8)

[3] “Switch Architecture”
http://www.anixter.com/techlib/whiteppr/network/d0504p06.htm

[4] “Configuring the Cisco Catalyst SPAN Feature ”
http://www.cisco.com/warp/public/473/41.html

[5] “Catalyst 2900XL/3500XL Release ”
http://www.cisco.com/univercd/ cc/td/doc/product/lan/c2900xl/29_35wc2/1331203.htm

[6] “Catalyst 2950 Release ”
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2950/1216ea2/ol164401.h tm

[7] “Catalyst 5000/5500 Release ”
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat5000/index.htm
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat5000/rel_6_2/ config/span.htm

[8] “Catalyst 6000/6500 Release ”
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/index.htm
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sft_6_1/configgd/span.htm

[9] “Configuring VTP and VLANs ”
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sft_6_1/configgd/vlans.htm
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat5000/rel_6_2/ config/vlans.htm

[10] “Management VLAN ”
http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/29_35xu/olhelp/mgmtvlan.htm

[11] “Configuring Cisco Switch ”
Cisco Systems “Building Cisco Multilayer Switched Networks Student Guide Ver1.1 ”

Last Updated: July 22nd, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor