APAC SWAT

Port Mirroring Best Practice

TDA Deployment Guide

Barry Yuan/Todd Sun

08

Version History

ID	Author	Content	Comments	Date
1	Barry Yuan/Todd Sun	Port Mirroring for Cisco/H3C/HP		11/28/2008
2	Barry Yuan/Todd Sun	Added VLAN tagging removal		04/20/2009

About APAC SWAT

APAC SWAT started at 2006, providing consulting services to APAC Sales team.

We are providing services including:

- SyMac Attack
  - Competitor displacement
- Paid Deployment Service
  - Provide deployment service to customers who have signed SOW and need assistance for architecting and deploying appliance products.
- New Technology Launch
  - Support for newly released appliance products
- VLE escalations
- Document sharing and Training
  - Document creation and sharing on SWAT website

How to register for assistance:

Please go to the website below to register deal:

http://macattack.us.trendnet.org/MacAttack/Opportunity/newForm.aspx

Our Portal:

http://SWAT.trendmicro.com or http://ishare.trendmicro.com/department/ts/gsip/swat/default.aspx

If you have any question, please contact:

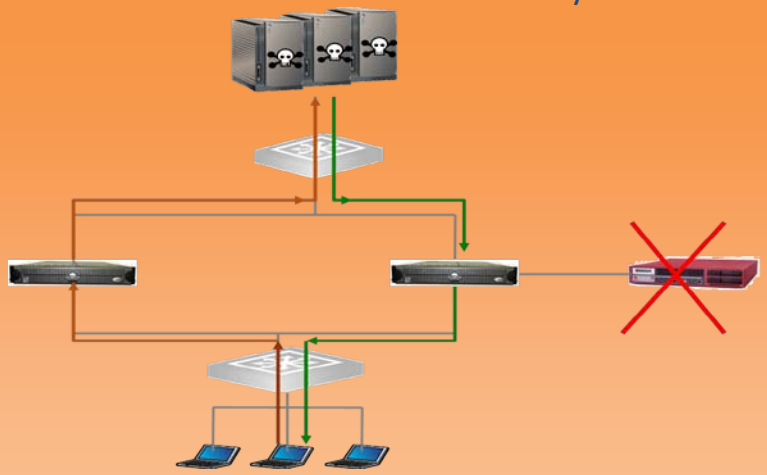
Barry_Yuan@trendmicro.com.cn

Index

1. TDA Deployment Scenarios....4
a. Customer have network TAP in place already....4
b. Need to do Port/VLAN mirror....5
   a) Typical scenario....5
   b) Need to monitor redundant network or two segments....6
   c) Need to scan selected VLANs....7
   d) Remote Port/VLAN mirroring....8
2. What is Port Mirroring (SPAN)....10
3. What is Remote Port Mirroring (RSPAN)....11
4. Configuration....12
a. Cisco....12
b. H3C....14
c. HP....16
5. Troubleshooting....17

Deployment Principals:

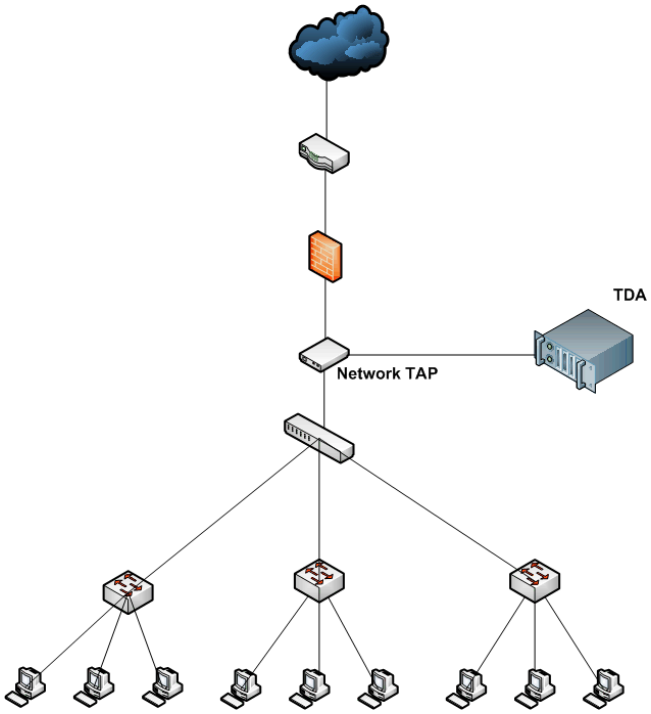
1. Port speed must match
   For port mirroring, the speed of destination port must not be smaller than source port.
   For example, if source port is Gigabit either net, and destination port is Fast either net, there will be possible data lost. See “Troubleshooting for details”
2. Must monitor complete data flow
   TDA need to monitor complete data flow, meaning data sent and received must all be mirrored to TDA.
   In some customer environment there are some asymmetric routing.



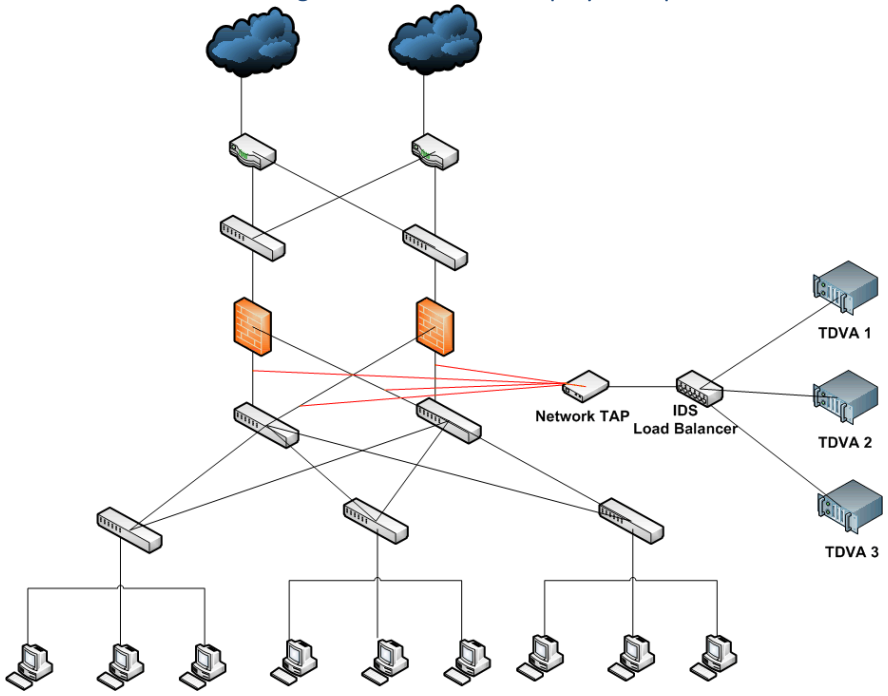
For detail please refer to 1b.

1. TDA Deployment Scenarios

a. Customer have network TAP in place already
If customer already have network TAP deployed in their network, we can simply connect TDA to the TAP.



To ensure performance, we can leverage load balancer to deploy multiple TDA.

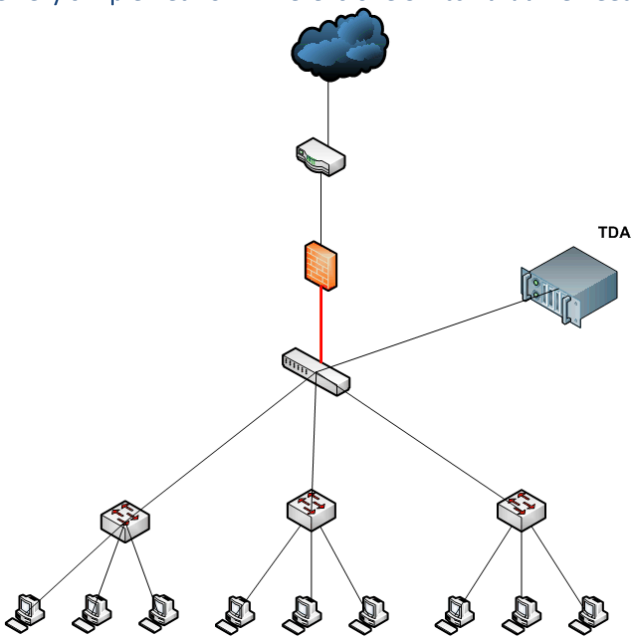


b. Need to do Port/VLAN mirror

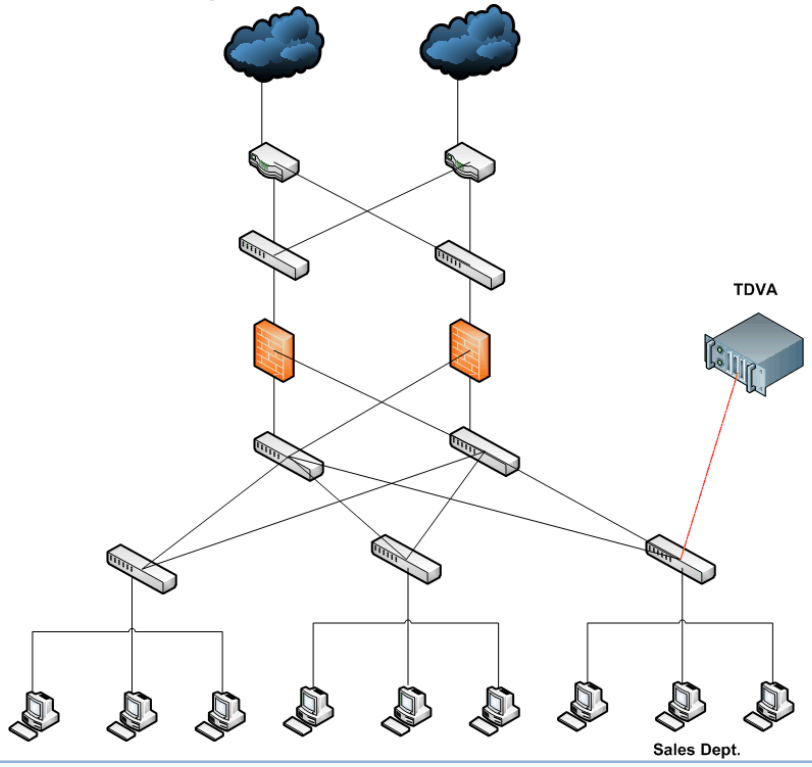
If customer doesn't have network TAP, we need to utilize their network Switches to mirror all network traffic to TDA.

a) Typical scenario

This happens in some very simple network. There is one Switch that we need to connect to.

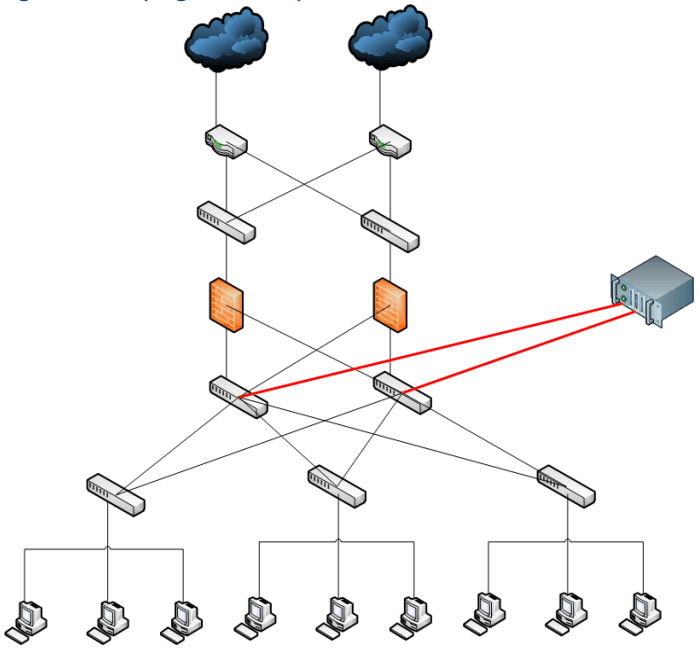


Or we only need to scan one segment.

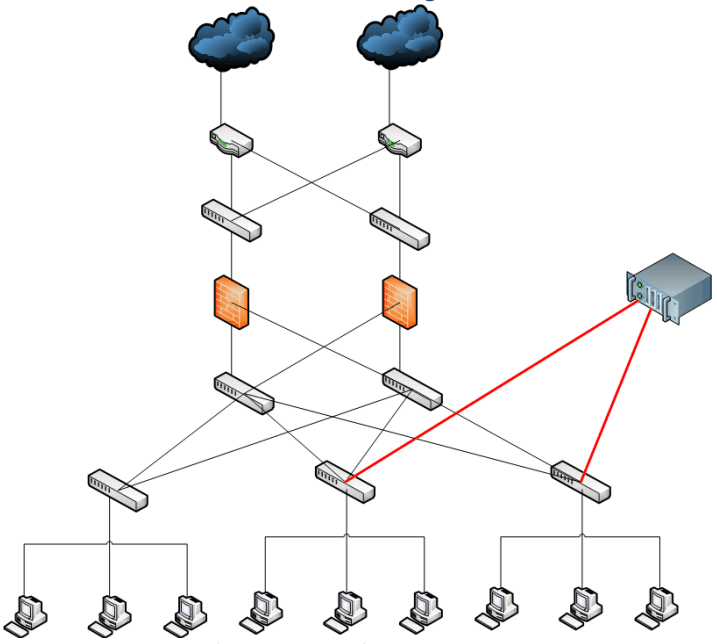


Port Mirroring Configuration Guide for these scenarios: Cisco, H3C, HP

b) Need to monitor redundant network or two segments
Redundant network is very common in enterprise environment; usually there are two switches, full mesh connecting to underlying access layer switches.



Or we need to use one TDA to monitor two network segments



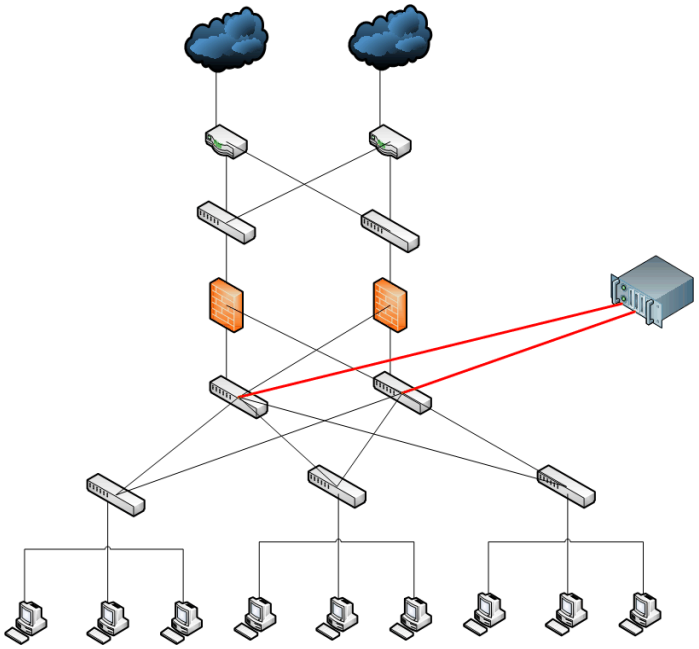
We need to enable two data ports (Data1 Data2) on TDA and connect to corresponding switch.

Port Mirroring Configuration Guide for these scenarios: Cisco, H3C, HP

c) Need to scan selected VLANs

Instead of scanning all traffic on certain ports, customer would like to only scan some selected VLANs, we don't need to mirror all traffic of each port, only need to mirror these VLANs, this can save some bandwidth and resource on TDA.

Physical connection is the same:



Configuration is different, it is VLAN based mirror.

Port Mirroring Configuration Guide for this scenario: Cisco, H3C , HP

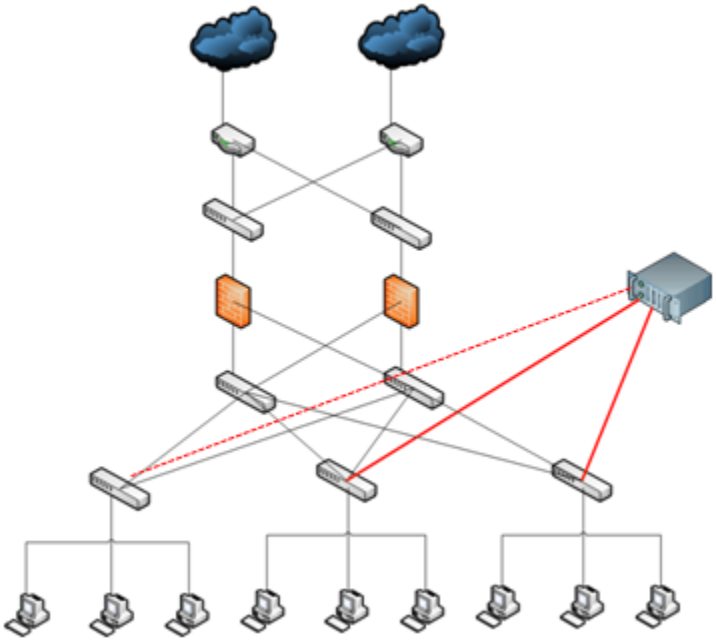
d) Remote Port/VLAN mirroring

In the following scenarios we need to use remote mirroring.

i. Does not have enough physical ports on local switch
If there's no more ports available on a switch.

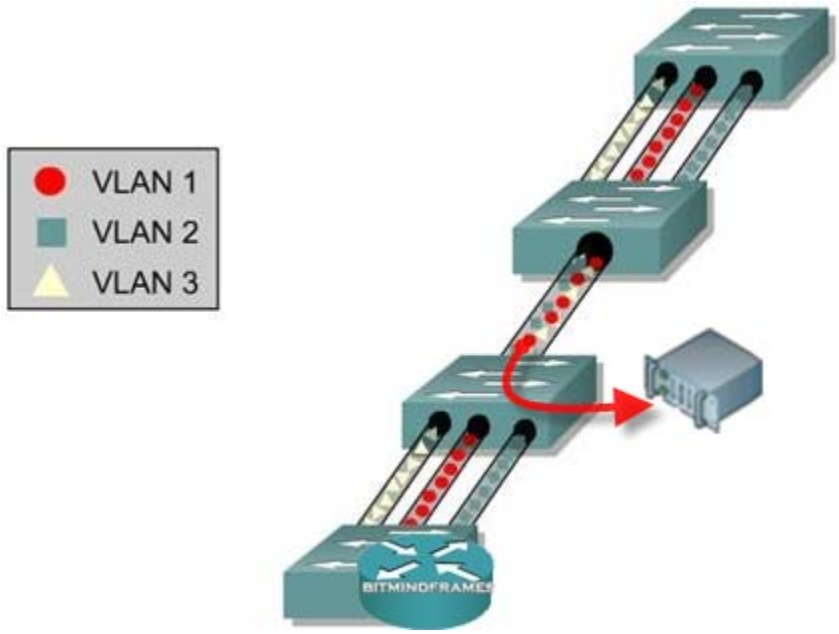
ii. Port speed on local switch does not match (Gb/Mb)
For example, there is a Cisco 3550, both Gigabit ports are used for stacking, we have no Gigabit port to do port based mirroring. (Notice we MUST use a port that matches the speed of source port)

iii. Need to monitor traffic on more than 2 switches, but TDA have only 2 data ports
For instance if we need to monitor traffic on 3 switches, we don't have data port for the 3rd switch. Then we need to consider remote port mirroring.



Port Mirroring Configuration Guide for this scenario: Cisco, H3C, HP

e) Mirroring Trunk link



There are scenarios that the source port you need to mirror is a Trunk link. (Meaning it has encapsulated multiple VLANs in the same physical link)

In this case you need to remove the VLAN tagging in order to make it understandable to TDA.

Port Mirroring Configuration Guide for this scenario: Cisco, H3C, HP

2. What is Port Mirroring (SPAN)

Port Mirroring is a method of monitoring network traffic by copying source port or VLAN specific traffic to a destination port for analysis.

Port Mirroring can be used to analyze network traffic passing through ports. This occurs by sending a copy of the traffic to a destination port on the switch that has been connected to a network analyzer or protocol analyzer. Port Mirroring can be used to mirror traffic for later analysis. Mirrored traffic is all traffic sent to and/or received from one or more Port Mirroring source ports defined in the Port Mirroring configuration.

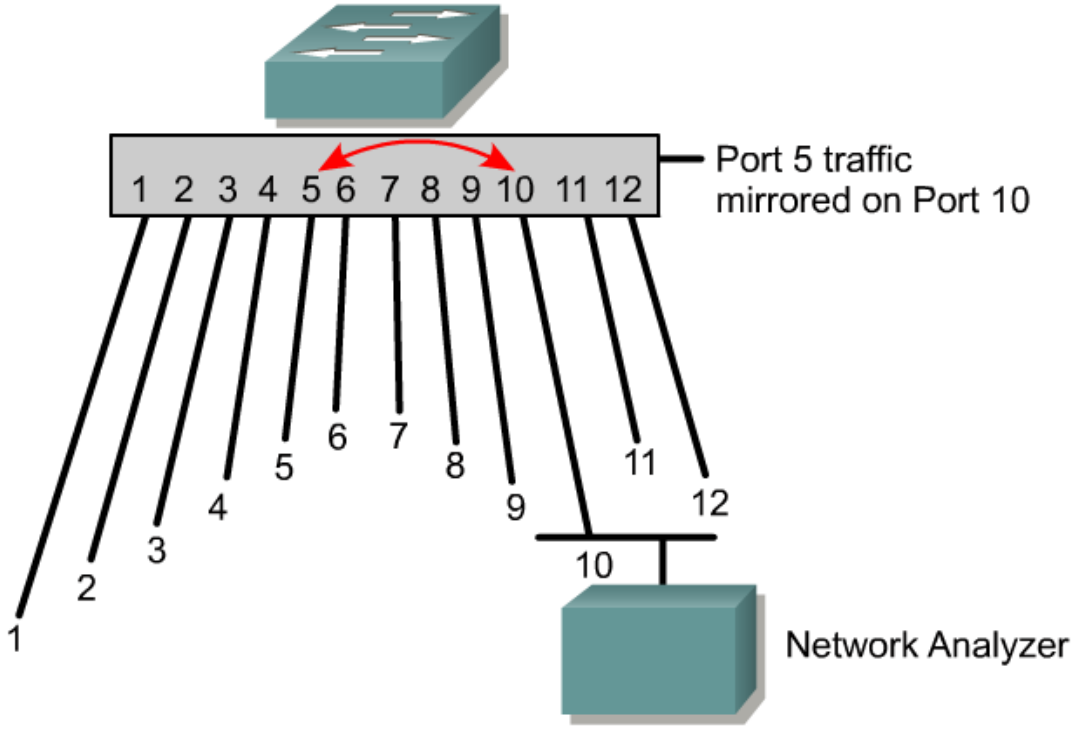


Figure 1 Port Mirroring

Port Mirroring does not affect the switching of network traffic on source ports. A copy of the packets received or sent by the source interfaces is sent to the destination interface. The only traffic sent or received by Port Mirroring destination ports is related to the Port Mirroring process.

A source port is a Layer 2 or Layer 3 port from which the Port Mirroring process copies traffic. Data forwarded from a Port Mirroring source port to a Port Mirroring destination port can include all frames transmitted by the port and/or all frames received by the port.

A Port Mirroring destination port is a Layer 2 or Layer 3 port to which the Port Mirroring process copies traffic. When a port is configured as a Port Mirroring destination port, it can no longer forward any traffic other than Port Mirroring traffic, and becomes dedicated for use by the Port Mirroring process. A Port Mirroring destination port does not forward any traffic except that required for the Port Mirroring session.

3. What is Remote Port Mirroring (RSPAN)

Remote Port Mirroring is an implementation of Port Mirroring designed to support source ports, source VLANs, and destination ports across different switches. Remote Port Mirroring allows remote monitoring of multiple switches across a network.

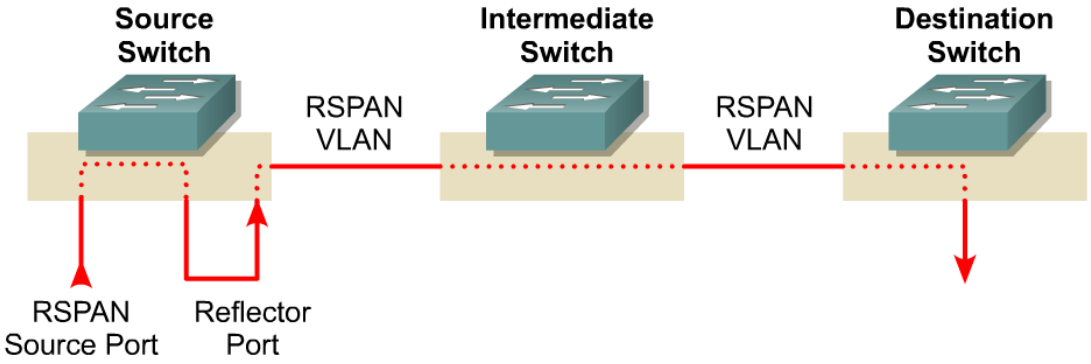


Figure 2 Remote Port Mirroring

Remote Port Mirroring traffic from source ports or source VLANs is switched to the Remote Port Mirroring VLAN, and is then forwarded to destination ports that are also in the Remote Port Mirroring VLAN. The source port or VLAN, in a Remote Port Mirroring session can be on different source switches.

Reflector Port works like a bridge between Source Port and RSPAN VLAN. Reflector ports only forward packets received or sent by source ports, and do not receive or forward any other network traffic.

Like Port Mirroring, Remote Port Mirroring does not affect the switching of network traffic on source ports.

4. Configuration

a. Cisco

Port-Base

1. Connect to switch through console port or telnet session.
2. Enter password for console port or telnet session.
3. Cisco> enable //enter Privileged mode. (You may need to enter enable password)
4. Cisco#configure terminal //enter configure mode
5. Cisco(config)#monitor session 1 source interface fastethernet 0/1 both // [both | rx | tx]
6. Cisco(config)# monitor session 1 destination interface fastethernet 0/24
7. Cisco(config)#End
8. Cisco#show monitor session 1

Vlan-Base

1. Cisco(config)# monitor session 2 source vlan 10 both
2. Cisco(config)# monitor session 2 destination interface gigabitethernet1/0/2
3. Cisco(config)# end

Remote Port Mirroring

Configuring a VLAN as an RSPAN VLAN (on every switch in the RSPAN path)

Switch(config)# vlan 901

Switch(config-vlan)# remote span

Switch(config-vlan)# end

Creating an RSPAN Source Session (on source switch)

Switch(config)# monitor session 1 source interface gigabitethernet1/0/2 rx

Switch(config)# monitor session 1 destination remote vlan 901 reflector-port

fastethernet0/1 //reflector-port can be any unused port

Creating an RSPAN Destination Session (on destination switch)

Switch(config)#interface gigabitethernet2/0/1 //destination port

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 901

Switch(config-if)#exit

Switch(config)# monitor session 1 source remote vlan 901

Switch(config)# monitor session 1 destination interface gigabitethernet2/0/1

Trunk Mirroring

For Cisco device, by default, packets appear in the untagged format at the destination port even if the source port is a Trunk, so that there is no additional configuration needed.

b. H3C

Port-Base

1. Connect to switch through console port or telnet session.
2. Enter password for console port or telnet session.
3. <H3C> system-view //Enter system view. (You may need to enter system view password.
4. [H3C] mirroring-group 1 local
5. [H3C] mirroring-group 1 monitor-port GigabitEthernet 1/1/4
6. [H3C] mirroring-group 1 mirroring-port GigabitEthernet 1/1/1 { both | inbound | outbound }
7. [H3C] display mirroring-group { all | local }

Vlan-Base

Do not support on S3xxx

Remote Port Mirroring

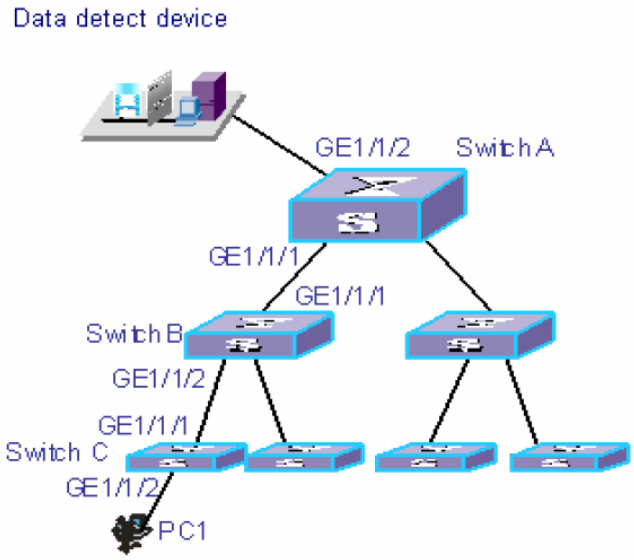


Figure 3 Configuration example

Configuring a VLAN as an remote-probe VLAN (on Switch A,B,C)

<H3C> system-view

[H3C] vlan 10

[H3C-vlan10] remote-probe vlan enable

[H3C-vlan10] quit

Creating an Source Session (on source switch C)

[H3C] mirroring-group 1 remote-source

[H3C] mirroring-group 1 mirroring-port GigabitEthernet 1/1/2 //source port

[H3C] mirroring-group 1 reflector-port GigabitEthernet 1/1/3 //can be any unused port

[H3C] mirroring-group 1 remote-probe vlan 10

[H3C] display mirroring-group remote-source

Creating an Destination Session (on destination switch A)

[H3C] mirroring-group 1 remote-destination

[H3C] mirroring-group 1 monitor-port GigabitEthernet 1/1/2 //destination port

[H3C] mirroring-group 1 remote-probe vlan 10

[H3C] display mirroring-group remote-destination

Trunk Mirroring

Assume we have 3 vlan's (10, 20, 30) traffic on the Trunk port which we need to monitor, then we need to add the following configuration on the destination port which connect to TDA. The purpose is to set the destination port type to "hybrid" and remove the vlan tag of vlan 10, 20, 30.

interface GigabitEthernet1/1/2 //destination port

port link-type hybrid

port hybrid vlan 10 20 30 untagged

c. HP

Port-Base

1. Connect to switch through console port or telnet session.
2. Enter password for console port or telnet session.
3. ProCurve> **enable** //enter Privileged mode. (You may need to enter enable password)
4. ProCurve#configure //enter configure mode
5. ProCurve(config)# mirror-port a6 //assign port A6 as the destination port
6. ProCurve(config)# interface ethernet a5 monitor
7. show monitor

Vlan-Base

Do not support

Remote Port Mirroring

Do not support

5. Troubleshooting

a. Speed doesn't match

Symptom:

==========

TDA will see a lot of damaged files due to the data collected are not complete.

When you run "show interface" on the port mirror destination interface, you will see:

1366659376 packets output, 3190358519 bytes, 61441916 underruns
0 output errors, 0 collisions, 1 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 PAUSE output
61441916 output buffer failures, 0 output buffers swapped out

Root Cause:

==========

For port mirroring, the speed of destination port must not be smaller than source port.

For example, if source port is Gigabit either net, and destination port is Fast either net, there will be possible data lost.

Solution:

==========

Find a destination interface that can match the speed of the source interface.

b. Asymmetric route

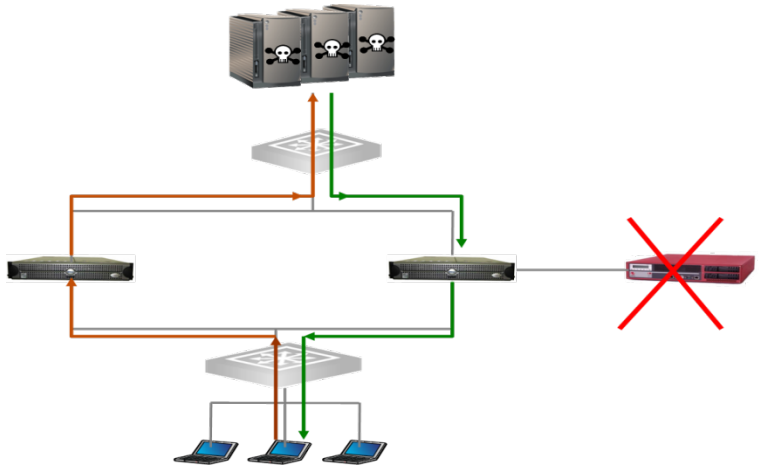
Symptom:

==========

TDA will not be able to analyze traffic.

Root Cause:

==========



As shown in the chart above, traffic doesn't flow through the same switch when it's sent and received from the clients.

Solution:

==========

We need to enable two data ports (Data1 Data2) on TDA and connect to corresponding switch.