GIAC LevelOne Network Essentials Curriculum
Mr. Check M. Louie

Topic: Internal Network Monitoring/IDS using Gigabit Taps, 1000base-SX data collection and standalone 100Mb switches, and IDS Intel-based systems

Introduction:

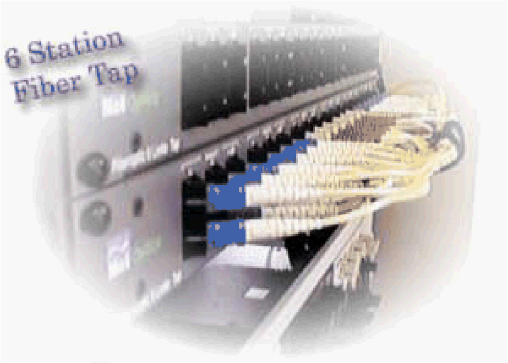
In a small organization, your network security manager recently tasked a network-monitoring research project to you. This new network security project is to monitor the current network that consists of Fiberoptic gigabit uplinks from several 10/100Mb workgroup switches to a core 100Mb switch and from this core switch to an edge router. As a network security member, we need to determine additional hardware, PC systems, Fiberoptic cabling, and software to make this a reality on the current network. This report is a summary of what is currently implemented in our network and would like to share on the design and implementation of network monitoring model to all interested network security professional.

This task mentioned that the individual switches are not to be reconfigured for VLAN port mirroring (Span) to an available port on each switch. The Network manager and NetOps personnel said that VLAN port mirroring's many to 1 would impose additional CPU load and memory resources for the individual switches along with handling the normal network traffic. Lastly, VLAN port mirroring on each switch will requires an available port for connectivity. This port in turn will transmit all local VLAN-based traffic to a data collection switch that will then be sent to networking monitoring station. Yes, host-to-host traffic can be monitored within that switch, but traffic is mainly Microsoft networking protocol such as File and Print Sharing, network print server, etc. Switch-to-switch, switch-to-VPN gateway, switch-to-backdoor RAS, switch-to-server farm switch, switch-to-network management switch, and switch-to-router traffic are of far more importance as a Network Security issue. A source packet may travel through multiple gigabit uplinks to an internal server or out on the Internet, and thus be recorded multiple times by a network monitoring station and SNORT real-time IDS.

Hardware/Software Requirements:

- NetOptics Gigabit Multi-mode Fiberoptic 6-Station Tap Device(s)
- CISCO Catalyst 4912 12-port 1000Base-SX switch
- Multimode Fiber cables
- Intel-based Snort System with
    1. Redhat Linux V6.2 OS
    2. 3Com 64-bit Gigabit Etherlink card
    3. 512Megs of Memory and 20Gig HD
- Intel-based NAI Sniffer system with
    1. Microsoft Windows NT Workstation w/sp6a
    2. 3Com 64-bit Gigabit Etherlink card
    3. 128Meg of Memory and 20Gig HD
- Intel-based Shadow IDS (Alternate IDS)

Description: NetOptics Gigabit Multi-mode Fiberoptic 6-Station Tap Device(s)



This NetOptics Gigabit Multimode 6-stations tap has SC connectors and is rack- mountable. These splitters tap will allow the networks to operate at a continuous flow while the tap is non-operational, thereby maintaining network traffic flow. If power is lost, traffic data is still passed through the tap. These taps also has passive-link integrity that is maintained whether the network monitoring devices are on or off. These splitters are used to split light with minimal loss from one to two fibers, or to combine light from two fibers into one fiber.

These Fiberoptic splitter taps provides the ability to monitor traffic flowing in either direction of a link connection. The taps we've purchased have signal ratio with a split ratio to 50/50. The main features of these taps are the 18 Duplex SC fiber connectors, compact metal enclosure, and most important is that it is passive (No need of power supply).

Each device contains four ports:
- Port A
- Port B
- Monitor Port A
- Monitor Port B

When the unit operating, Port A and Port B are connected to separate two gigabit devices, which may be workgroup switches, core switch or routers, etc. The Monitor ports are typically connected to Network Monitoring station(s). These taps are fully capable of operating in full-duplex mode. Please note that each port on the tap is rated as percent dB loss, so the distance between Gigabit uplinks should be considered. Later in this report, I will explain how to gather all the traffic, from multiple taps, collected the data using CISCO Gigabit switch and send the data back to NetOptics tap for 1 to 2 signal split. This final split will provide the ability to have 2 network monitoring/IDS systems, such as a combination of Protocol analyzer, and SNORT real-time IDS.

The benefits of using gigabit taps:

- These transparent modules provide network monitoring without downtime.
- Network traffic flows at data rates up to 1000Mbps.
- Excellent performance, high integration to current network topology, high reliability, and excellent design security.
- The lines tapped will not affect the signal integrity or loading factor.

The following is a table of network connections that are to and from gigabit devices

NetOptics Rackmount Taps	Connection
Network 1/Port A in	← gigabit uplink device 1 (transmit)
Network 1/Port A out	→ gigabit uplink device 1 (receive)
Network 1/Port B in	← gigabit uplink device 2 (transmit)
Network 1/Port B out	→ gigabit uplink device 2 (receive)
Network 1/Port A/B B out	→ gigabit data collection switch's port 1 (receive)
Network 1/Port A/B A out	→ gigabit data collection switch's port 2 (receive)
Network 2/Port A in	← gigabit uplink device 3 (transmit)
Network 2/Port A out	→ gigabit uplink device 3 (receive)
Network 2/Port B in	← gigabit uplink device 4 (transmit)
Network 2/Port B out	→ gigabit uplink device 4 (receive)
Network 2/Port A/B B out	→ gigabit data collection switch's port 3 (receive)
Network 2/Port A/B A out	→ gigabit data collection switch's port 4 (receive)
Network 3/Port A in	← gigabit uplink device 5 (transmit)
Network 3/Port A out	→ gigabit uplink device 5 (receive)
Network 3/Port B in	← gigabit uplink device 6 (transmit)
Network 3/Port B out	→ gigabit uplink device 6 (receive)
Network 3/Port A/B B out	→ gigabit data collection switch's port 5 (receive)
Network 3/Port A/B A out	→ gigabit data collection switch's port 6 (receive)
Network 4/Port A in	← gigabit uplink device 7 (transmit)
Network 4/Port A out	→ gigabit uplink device 7 (receive)
Network 4/Port B in	← gigabit uplink device 8 (transmit)
Network 4/Port B out	→ gigabit uplink device 8 (receive)
Network 4/Port A/B B out	→ gigabit data collection switch's port 7 (receive)
Network 4/Port A/B A out	→ gigabit data collection switch's port 8 (receive)
Network 5/Port A in	← gigabit uplink device 9 (transmit)
Network 5/Port A out	→ gigabit uplink device 9 (receive)
Network 5/Port B in	← gigabit uplink device 10 (transmit)
Network 5/Port B out	→ gigabit uplink device 10 (receive)
Network 5/Port A/B B out	→ gigabit data collection switch's port 9 (receive)
Network 5/Port A/B A out	→ gigabit data collection switch's port 10 (receive)

If there are 5 pairs or less gigabit uplinks, then the following applies,

Network 6/Port A in	← gigabit data collection switch port 12 (transmit)
Network 6/Port A out	→ gigabit data collection switch port 12 (receive)
Network 6/Port B in	← Network Monitoring/IDS #1 (transmit)
Network 6/Port B out	→ Network Monitoring/IDS #1(receive)
Network 6/Port A/B B out	→ Network Monitoring/IDS #2(transmit)
Network 6/Port A/B A out	→ Network Monitoring/IDS #2(receive)

If there are more than 5 pairs of gigabit uplinks, then read the following:
The "Network 6" ports is only for directly network traffic to the Network monitoring station. Since small to medium-size network can have can have large number of Gigabit uplinks, the pairing of rack-mounted taps and data collection switches will also increase accordingly.

Description of a CISCO Catalyst 1000baseSX switch.

The Catalyst 4912G is a 12-port dedicated Gigabit Ethernet switch .The Catalyst 4912G provides high performance for Gigabit networking and delivers low-cost, high-density gigabit aggregation with modular gigabit Interface Converter (GBIC) modular protection. This unit complies with Spanning Tree Protocol: IEEE 802.1D1000BaseX (GBIC)

<u>The following is a table of network connections that are from data collection switch</u>

Catalyst Switch Port	Connection
Port 1 (receive)	← Network 1/Port A/B B out (Transmit, 1/2 Fiberoptic)
Port 1 (transmit)	not used
Port 2 (receive)	← Network 1/Port A/B A out (Transmit, 2/2 Fiberoptic)
Port 2 (transmit)	not used
Port 3 (receive)	← Network 2/Port A/B B out (Transmit, 1/2 Fiberoptic)
Port 3 (transmit)	not used
Port 4 (receive)	← Network 2/Port A/B A out (Transmit, 2/2 Fiberoptic)
Port 4 (transmit)	not used
Port 5 (receive)	← Network 3/Port A/B B out (Transmit, 1/2 Fiberoptic)
Port 5 (transmit)	not used
Port 6 (receive)	← Network 3/Port A/B A out (Transmit, 2/2 Fiberoptic)
Port 6 (transmit)	not used
Port 7 (receive)	← Network 4/Port A/B B out (Transmit, 1/2 Fiberoptic)
Port 7 (transmit)	not used
Port 8 (receive)	← Network 4/Port A/B A out (Transmit, 2/2 Fiberoptic)
Port 8 (transmit)	not used
Port 9 (receive)	← Network 5/Port A/B B out (Transmit, 1/2 Fiberoptic)
Port 9 (transmit)	not used
Port 10 (receive)	← Network 5/Port A/B A out (Transmit, 2/2 Fiberoptic))
Port 10 (transmit)	not used

Port 11 (receive)	←"daisy-chained" collection switch B (if required)
Port 11 (transmit)	→"daisy-chained" collection switch B (if required)
Port 12 (receive)	← NetOptics "Network 6" port for 1-to-2 split
Port 12 (transmit)	→ NetOptics "Network 6" port for 1-to-2 split

Here is a list of important gigabit uplinks that can be monitored:

- Between network DMZ and firewall
- Between workgroup switches and core switch
- Between edge router and the core or central switch.
- Between switch and the server farm switch (web, ftp, mail, etc.)
- Between switch and network management farm switch (VLAN manager, etc.)
- Between switch and print server farm switch (HP printer)
- Between VPN gateway and the internal network
- Between RAS and internal network

Since Gigabit Fiberoptic uplinks are full-duplex mode, the taps captured data traffic in both directions. All traffic is tapped using NetOptics gigabit taps and light signal is split from one to two paths. Each pair of Fiberoptic tap is then redirected to a receive port on the data collection switch. The end result is that capturing network traffic in both directions required two receive ports on the data collection switch. Since 12-port data collection switch can handle a maximum of 10 ports (11th for daisy chaining and 12th is for network-monitoring system), therefore, a maximum of 5 uplink taps can be deployed. The 11th gigabit port is available, if required, for connecting or "daisy-chaining" from similar gigabit switches. Each individual port is "span" or "VLAN port-mirroring" to the 12th port on the data collection switch. The result is the 12th will see full-duplex traffic from all NetOptic taps. This mirroring concept is "many ports-to-1". The transmitting 12th port of the data collection switch then sends all the collected data to NetOptics' "Network 6/Port A In" connection. This concept is "1-to-2 split" and is used when more than 1 network monitoring/IDS device is used to read the same set of network traffic. The two connections are connected to Redhat Linux V6.2 system running SNORT and a Sniffer system. Shadow IDS' sensor can also be used as an alternate means of packet capturing running along with Shadow Analysis and WEB server. Note that if the Snort system has an Active Defense running, a pair of reset signals can only be sent out from a second NIC card due to the gigabit NIC card is in promiscuous mode and does not an assigned IP address. Also the data collection switch cannot transmit is not connected to the taps. In short, this will prevent a reset signal from reaching the network.

In summary, This network monitoring capability provided us with all of critical gigabit uplink network data that we can process, analyze, and react accordingly.

Work Cited:

"Sniffing (network wiretap, Sniffer) FAQ" Version 0.3.3, September 14, 2000
<http://www.robertgraham.com/pubs/sniffing-faq.html>

"Fiber Optics Basics" Ohio University - School of Communications
<http://www.tcomschool.ohiou.edu/its_pgs/fiber.html>

"Gigabit Ethernet Enterprise Solution" Amy Hanson. Enterasys Networks Incorporated Online <http://www.enterasys.com/gigabit/>

"Matrix E6 formerly SmartSwitch 6000" Enterasys Network Incorporated Online
<http://www.enterasys.com/technologies/switching/6000/>

"Tap into your Network, Network Monitoring Made Easy." NetOptics Inc. Online
<http://www.netoptics.com/station-tap.html>

"For Your Information" NetOptics Incorporated Online
<http://www.netoptics.com/9.html>

"Customer Drawing for Network Tap Modules for 12 nodes " Dennis Carpo and Tara Danz of NetOptics Incorporated Online
<http://www.netoptics.com/96153.pdf>

"Catalyst 4912G — 12-Port Dedicated Gigabit Ethernet" Cisco System Inc. Online
<http://www.cisco.com/univercd/cc/td/doc/pcat/ca4912.htm>

"Gigabit EtherLink Server" 3COM Incorporated Online
<http://www.3com.com/products/nics/3c985bsx.html>

"What is Snort?". Mr. Martin Roesch Online
<http://www.snort.org/what_is_snort.html>

"Sniffer Portable". Network Associates Inc. Online
<http://www.sniffer.com/products/dssrmon-gigabit/default.asp?A=2>

"Shadow IDS ". Naval Surface Warfare Center, Dahlgren Division Dahlgren Laboratory Online <http://www.nswc.navy.mil/ISSEC/CID/index.html>