Data Monitoring Access
SPAN Port or Passive TAP?

What's on your Network?

Part 1

Is SPAN port a viable data access technology for today's business critical networks especially with today's access needs for Data Security Compliance and Lawful Intercept requirements?
Not really, see why !

Abstract – The idea behind this paper is to get managers thinking about today's requirements and the limitations of access methods. Part1 is focused on Taps versus port mirroring / SPAN technology. SPAN is not all bad but one must be aware of the limitations and since managed switches are part of the infrastructure one must be careful not to establish a failure point. Understanding what can be monitored with success since SPAN ports are often over used leading to dropped frames, they groom data (change timing, add delay) and extract bad frames as well as ignore all layer 1 &2 information. Most cannot handle FDX monitoring and VLAN analysis is problematic. When dealing with Data Security Compliance, SPAN access limits views, are not secure and transporting monitored traffic through the production network is not acceptable. Span is not all bad and when used within its limits and properly focused it is a valuable resource to managers and monitoring systems. However, for 100% guaranteed view of network traffic the TAP is back as a necessity for meeting many of today's access requirements and as we approach larger deployments of 10 Gigabit and up, SPAN access limitation will become more problematic.
Part 2 of this paper, to be published later, will cover Remote and Out of band access techniques to meet the needs of faster and more dynamic network monitoring and analysis requirements.

To SPAN or to TAP – That is the question!

Until the early 1990's, using a TAP or test access point from a switch patch panel was the only way to monitor a communications link. Most links were WAN so an adaptor like the V.35 adaptor from Network General or an access balum for a LAN was the only way to access a network. Most LAN analyzers had to join the network to really monitor.
As switches and routers developed, there came a technology we call SPAN ports or mirroring ports and now monitoring was off and running. Analyzers and monitors no longer had to be connected to the network; engineers would use the SPAN (mirror) port and direct packets from their switch or router to the test device for analysis. SPAN generally stands for Switch Port for ANalysis. This was a great way to effortlessly and non-intrusively acquire data for analysis. By definition, a SPAN Port usually indicates the ability to copy traffic from any or all data ports to a single unused port but also usually disallows bidirectional traffic on that port to protect against backflow of traffic into the network.

Is SPAN a passive technology – No!

Some call SPAN port a passive data access solution – but passive means "having no effect" and spanning (mirroring) does have measurable effect on the data.
First - Spanning or mirroring changes the timing of the frame interaction (what you see is not what you get),
Second - The spanning algorithm is not designed to be the primary focus or the main function of the device like switching or routing so the first priority is not spanning and if replicating a frame becomes an issue, the hardware will temporally drop the SPAN process,
Third - If the speed of the SPAN port becomes over loaded frames are dropped.
Fourth – Proper spanning requires that a network engineer configure the switches properly and this takes away from the more important tasks that network engineers have and many

times configurations can become problematic (constantly creating contention between the IT team, the security team and the compliance team).
Fifth – SPAN port drops all packets that are corrupt or those that are below the minimum size, so all frames are not passed on. All of these events can occur and no notification is sent to the user, so there is no guarantee that one will get all the data required for proper analysis
In summary, the fact that SPAN port is not a truly passive data access technology or even entirely non-intrusive, it can be a problem particularly for Data Security Compliance monitoring or lawful intercept since there is no guarantee of absolute fidelity. It is also possible and likely that evidence gathered by the monitoring process will be challenged in the court of law.

Is SPAN port a scalable technology – No!

When we had only 10Mbps links and with a robust switch (like one from Cisco) one could almost guarantee they could see every packet going through the switch. With 10Mbps fully loaded at around 50% to 60% of the maximum bandwidth, the switch backplane could easily replicate every frame. Even with 100Mbps one could be somewhat successful at acquiring all the frames for analysis and monitoring and if a frame or two here and there were lost, it was no big problem. This has all changed with Gigabit and 10 Gigabit technologies starting with the maximum bandwidth it is now twice the base bandwidth – so a Full Duplex (FDX) Gigabit link is now 2 Gigabits of data and a 10 Gigabit FDX link is now 20 Gigabits of potential data.
No switch or router can handle replicating/mirroring all this data plus handle its primary job of switching and routing. It this is difficult if not impossible to pass all frames (good and bad one) including FDX traffic at full time rate, in real time at non blocking speeds.
Furthermore, to this FDX need we must also consider the VLAN complexity and finding the origin of a problem once the frames have been analyzed and a problem detected.

From Cisco' on SPAN port usability –From Cisco's White Paper – Using the Cisco Span port for SAN analysis
"Cisco warns that the switch treats SPAN data with a lower priority than regular port-to-port data. In other words, if any resource under load must choose between passing normal traffic and SPAN data, the SPAN loses and the mirrored frames are arbitrarily discarded. This rule applies to preserving network traffic in any situation. For instance, when transporting remote SPAN traffic through an Inter Switch Link (ISL) which shares the ISL bandwidth with regular network traffic, the network traffic takes priority. If there is not enough capacity for the remote SPAN traffic, the switch drops it.
Knowing that the SPAN port arbitrarily drops traffic under specific load conditions, what strategy should users adopt so as not to miss frames? According to Cisco, the best strategy is to make decisions based on the traffic levels of the configuration and when in doubt to use the SPAN port only for relatively low-throughput situations. "

Hubs ?

Hubs can be used for 10/100 access but they have several issues that one needs to consider.
Hubs are really Half Duplex devices and only allow one side of the traffic to be seen at a time. This effectively reduces the access to 50% of the data.
The Half Duplex issue often leads to collisions when both sides of the network try to talk at the same time. Collision loss is not reported in any way and the analyzer or monitor does not see the data.
The Big Problem is if a Hub goes down or fails the link it is on is lost.
Hubs no longer fit as an acceptable, reliable access technology for the reasons above and they do not support Gigabit or above access and should not be considered.

Today's "REAL" Data Access requirements.

To add more complexity and challenges to SPAN port as a data access technology,
1) we have entered a much higher utilization environment with many times more frames in the network
2) we have moved from 10 Mbps to 10 Gbps Full Duplex and

3) we have entered into the era of Data Security Legal Compliance and Lawful Intercept which requires that we must monitor all of the data and not just sample the data, with the exception of certain very focused monitoring technologies.
These demands will continue to grow since we have become a very digitally focused society. With the advent of VoIP and digital video we now have revenue generating data that is connection oriented and sensitive to bandwidth, loss and delay. The older methods need reviewing and the aforementioned added complexity requires that we change some of the old habits to allow for "real" 100% Full Duplex real time access to the critical data.

In summary, being able to provide "real" access is not only important for Data Compliance Audits and Lawful Intercept events, it is the law (We keep our bosses out of jail becomes a very high priority these days).

When is SPAN port methodology "OK"?

Many monitoring products can and do successfully use SPAN as an access technology. Since they are looking for low bandwidth application layer events like "conversation analysis" , "application flows" and for access VoIP reports from Call managers, etc. These use a small amount of bandwidth and grooming does not effect the quality of the reports and statistics. The reason for their success is that they keep within the parameters and capability of the SPAN port capability and they do not need every frame for their successful reporting and analysis. Spanning is a very usable technology if used correctly and the companies that use mirroring or SPAN are using it in a well managed and tested methodology.

Conclusion –

Spanning (mirroring) technology is still viable for some limited situations but as one migrates to FDX Gigabit and 10 Gigabit networks and with the demands of seeing all frames for Data Security Compliance and Lawful Intercept one must use "real" access (taps) technology to fulfill the demands of today's complex analysis and monitoring technologies.
If the technology demands are not enough, the network engineers can focus their infrastructure equipment on switching and routing and not spend their valuable resources and time setting up span ports or rerouting data access.
The big differences between Taps and port spanning/mirroring –

- Taps do not alter the time relationships of frames – spacing and response times especially important with VoIP and Triple Play analysis including FDX analysis.
  - Span ports hide any jitter or distortion as the data is groomed so this does not help in VoIP / Video analysis.
  - VLAN tags are not normally passed through the spanning port so this can lead to false issues detected and difficulty in finding VLAN issues.
- Taps do not groom data nor filter out physical layer errored packets
  - Short or large frames are not filtered
  - Bad CRC frames are not filtered out
- Taps do not drop packets regardless of the bandwidth
- Taps are not addressable network devices and therefore cannot be hacked
- Taps have no setups or command line issues so getting all the data is assured and saves users time.
- Taps are completely passive and do not cause any distortion even on FDX and full bandwidth networks. They are also fault tolerant.
- Taps do not care if the traffic is IPv4 or IPv6, it passes all traffic through.

Thoughtful usage of spanning can be successful but should be left to the professionals and changing the configuration on one's switches and routers is better left alone.

Types of Access technology (TAPS)

There are many types of access devices available that range from the just basic access, regenerative devices to out of band access devices.

However for Lawful Intercept and Data Security Compliance one must have a 100% "real" access technology. In part 2 of this article I will be reviewing remote out of band access technologies and requirements.

Comments from the Experts

Many Thanks to everyone below that reviewed and commented on this article.

Gerald Combs - Founder of Ethereal and Wireshark

This is a good article to get people thinking about what they need from the different access technologies. Compliance and Lawful Intercept is changing the dynamics of what we need from access methods.
Some switch families (e.g. the Cisco 3500 series) don't set a lower priority on SPAN traffic, and will slow down the backplane in order to deliver packets to a SPAN port.
Most vendors don't bother to document the performance characteristics of mirrored ports. Cisco is the only exception that I'm aware of.
We have a page on the Wireshark wiki that we've used to collect SPAN/monitor/mirror port configurations for different manufacturers: http://wiki.wireshark.org/SwitchReference .

Burt Bennett – General manager of Valparaiso Broadband Communication Systems

"Looks good. One comparison that you forgot is a hub. Hubs are a fair replacement for a "tap" in the 10/100 HDX environment (none for Gigabit). Yes, there are the collision and FDX issues but it is not a bad alternative to fit a quick and temporary access requirement for user focused or end terminus analysis.
Author's Note – Burt I did leave out hubs as they do not support Gigabit or above – Thanks for pointing that out – I have added Hubs in the article to try to cover all questions.

Mike Pennacchi – Consultant, InterOp Speaker and Trainer and owner of Network Protocol Specialists.

Tim, this is a timely paper as we just came across a situation where a switch began crashing after spanning was turned on. All of the commands were entered correctly, but the switch was not stable after spanning was enabled.
Here are some of our reasons for recommending tapping to our clients:

1) Every client will change their switching infrastructure at one time or another. Chances are that the monitoring method for the new switch will be different than the old, or not exist. The troubleshooting portion of the network should not have to change every time the switches change.
2) It is assumed that the same people monitoring the network are responsible for the switch configurations. In many cases the troubleshooting groups may not have or want configuration access to the switches. By having a separate monitoring system, changes can be made to the monitoring network without affecting the switch configuration.
3) We often need multiple devices watching the same traffic. Most of the taps today support the ability to output traffic to multiple devices.

Good Paper - Best Regards - Mike

Alastair Hartrup — Network Critical, CEO and Founder

It's the most fundamental, yet often overlooked, need of any network appliance or tool — access. Before any device can collect or analyze traffic to provide its service, whether that's security, compliance, performance acceleration, etc., it must first obtain 100% visibility to this data. I started Network Critical in the 1990's with a plan to resolve the inevitable limitations of SPAN access techniques and simplify installations. At the end of the day, a switch's first priority is performance, and it will drop mirrored monitoring ports the instant they threaten priority #1. It takes dedicated monitoring solutions like TAPs to provide access, 24 hours day, 365 days a year, to help enterprise-class networks commit to today's management requirements.

To read more about permanent TAP solutions:
http://www.networkworld.com/news/tech/2007/060711-tech-update.html

Bob Morgan – Industry Specialist for over 30 years.
Thanks Tim – Great Paper - Bob

Steve Harriman – VP Marketing – NetQoS
Thanks for giving NetQoS the opportunity to review this, Tim. You have captured the facts and I look forward to Part 2 when you review the very appropriate use of SPAN technology for application and network performance monitoring.

Betty DuBois – Sniffer Expert, Course Developer, Trainer, Writer and Network Consultant
I think the things you cover are great. I would like to see the auditing/lawful intercept angle expanded on. I don't think people really think about how will an auditor approach their environment.

I would also like to add losing the vlan tag information when spanning. If there is an issue with ISL or 802.1q, how will I ever know with a span?

Another issue is duplicate copies of the packet being sent to the analyzer. If an entire VLAN is spanned (which people do, even though they shouldn't) and the traffic is destined for within the VLAN, a copy is sent both for the egress and ingress. People think they have thousands of retransmissions when they really don't. Betty Says - "you can spend twice as much time troubleshooting problems that don't exist as you do the ones that actually are happening".Real access taps solve this and other issues with spanning.

Cisco's answer to high speed capture and statistical analysis is the NAM blade. You could do an entire separate paper on the limitations and benefits of that.

Chris Bihary — Network Critical, Director for Americas
Tim, this article sheds much-needed light on today's demand for guaranteed, 100% access to properly monitor and analyze network traffic for compliance, security, QoS, and virtually any other network task. Customers come to us because they're looking for an unrestricted view into their critical network connections, with the assurance that they're seeing everything happening on the network, and that the access device is not creating a fault point in the network. This type of guarantee is only available with proper TAP solutions, or as we refer to them—Traffic Access Points. We're happy to report that businesses are turning the corner from SPAN and other access technologies, and are starting to adopt permanent TAP solutions as part of a best-practice monitoring/management infrastructure. We've seen 3X growth in TAP sales since we started operations in the U.S., and believe that it's a testament to the market being informed by thought-provoking articles like this! www.criticaltap.com

To read more about Network Access solutions:
http://www.itworldcanada.com/a/News/b5ba7558-df92-4bc7-85e5-04dcf45c332b.html

Author's info –
Tim O'Neill is an independent technology consultant. He has over 30 years experience working in the WAN, Analog, ISDN, ATM and LAN test market.
Tim has worked with companies like Navtel, Network General, Ganymede and ClearSight Networks and is now helping companies get Lab recognition and Technology verification.
Tim is acting as Chief Editor for www.lovemytool.com a website designed to help network manager's get access to valuable information and real solution stories from other customers.
Tim is a patent holding, published and degreed engineer, who has seen this technology grow from Teletype (current loop) data analysis to today's 10 Gigabit LAN's focused on Business Applications with heavy Compliance demands.