TIM O'NEILL

CHIEF CONTRIBUTING EDITOR FOR LOVEMYTOOL.COM

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 is now helping companies get lab recognition and technology verification. Tim is a patent holding, published and degreed engineer. Tim is currently Chief Contributing Editor for LoveMyTool.com.

WWW.LOVEMYTOOL.COM

Is SPAN port a viable data access technology for today's business critical networks, especially with today's ever increasing pressure to satisfy Data Security Compliance and Lawful Intercept requirements? In today's world we now have the GDPR requirements that "Require" 100% data inspection and retention! So TAPs are even more in demand!

► **Authors Note:** This article goes back to the late 90's when we at Network General needed a TAP to allow access to the network for our portable and distributed sniffers. In the mid 1970's I helped build the first RS-232 and V.35 TAPs to support the Telcom's data monitoring needs.

This article comes from all those experiences and wanting people to see all their data and not waste their time looking at a portion of their network through corrupted data.

This article has been stolen by some companies who have put their name on it or removed my name and the origin from www.lovemytool.com. I am not sure why, so I would steer clear of unethical companies that do such things.

Full permission has been given to the Profitap Team to reprint and post this article as they wish.

The Profitap Team is one of the Best and you should consult with them for your Visibility Needs!

SPAN OR TAP - SEE WHY!

► **Abstract:** Network engineers and managers need to think about today's compliance requirements and the limitations of conventional data access methods. This article is focused on taps versus port mirroring / SPAN technology.

SPAN is not all bad but one must be aware of its limitations and since managed switches are integral part of the infrastructure, one must be careful not to establish a failure point. Understanding what can be monitored is important for success since SPAN ports are often overused leading to drop frames, all due to the fact that LAN switches are designed to groom data (change timing, add delay) and extract bad frames as well as ignore all layer 1 & 2 information. Furthermore, typical implementations of SPAN ports cannot handle FDX monitoring and analysis of VLAN is also problematic.

Moreover, when dealing with Data Security Compliance, the combination of the facts that SPAN ports limit views, are not secure and transporting monitored traffic through the production network could prove itself to be unacceptable in the court of law.

When used within its limits and properly focused, SPAN is a valuable resource to managers and monitoring systems. However, for 100% guaranteed view of network traffic, passive network TAP is 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 of an issue.

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 and 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 PORT 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 a political issue (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 can be a problem particularly for Data Security Compliance monitoring or Lawful Intercept. Since there is no guarantee of absolute fidelity, it is possible or even likely that evidence gathered by this 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 fact that maximum bandwidth 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 handling its primary job of switching and routing. It 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's own White Paper – On SPAN port usability and using the SPAN port for LAN 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 (RSPAN) 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."

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.
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 (e.g., application performance monitoring).

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 (keeping our bosses out of jail has become 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 monitoring requirements utilize 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. In other words, SPAN port 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

IN SUMMARY, THE ADVANTAGES OF TAPS COMPARED TO SPAN PORTS ARE ...

◉ Taps do not alter the time relationships of frames – spacing and response times especially important with VoIP and Triple Play analysis including FDX analysis.

◉ Taps do not introduce any additional jitter or distortion which is important in VoIP / Video analysis.

◉ VLAN tags are not normally passed through the SPAN 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.

◉ 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.

I wish everyone Great Success and when looking at your data with a TAP you will see everything clearly and without distortion if you use a Quality TAP. DO NOT GO TO CHEAP – Quality is a TOP requirement, especially when one is in the Fiber Optic/Glass/Photonic arena!

IT ALL STARTS WITH VISIBILITY

PROFI TAP

Profitap develops a wide range of state-of-the-art and user-friendly network monitoring tools for both SMEs and the enterprise sector. Our wide range of high-density network TAPs, field service troubleshooters and network packet brokers are extremely performant, providing complete visibility and access to your network, 24/7.

We've been creating monitoring solutions for network analysis and traffic acquisition for more than 33 years. Therefore, we are experts in our field and our award-winning ProfiShark® 1G stands to prove it. This lightweight, advanced and portable network TAP is one the most innovative products on the market.

With more than 1,000 clients from 55 countries, PROFITAP has become a must-have solution for many important businesses, many of which are among Fortune 500 companies.

PROFITAP HQ B.V.

HIGH TECH CAMPUS 9

5656 AE EINDHOVEN

THE NETHERLANDS

sales@profitap.com

www.profitap.com

f Profitap

t @Profitap

in profitap-international