White paper

Tap vs SPAN

Real Network Visualization Considerations for Professionals

by Tim O'Neill - OLDCOMMGUY™

GARLAND TECHNOLOGY

See every bit, byte, and packet®

Abstract

This paper is an in-depth study of network visualization access requirements. Today's requirements for security, monitoring, management, compliance, deep or historic captures and auditing of our networks requires full and real time access to the packets that flow through our network. Today network, security and management personnel must have full access and using TAP (test access points) technology is the only viable and reliable technology for that job.

This paper will cover the value TAP access will provide and remove all the misinformation about SPAN or Monitor access through switches and false products.

This paper should be read by every network and security professional as well as management.

Not using a real TAP will lead to misinformation about your network, servers and applications not to mention several legal aspects to consider, like CALEA and lawful capture.

The goal of Network, Security, Compliance and Application managers requires full visualization of the Network and the packets therein.

Real Visualization is Everything

If you cannot see an issue, like an attack, misusage, inefficiency, etc., then how are you going to understand it and resolve it?

Some Fundamental Considerations for REAL Network Visualization Requirements

1. Any active device that touches a frame has changed the frame timing, even if nothing more than changing its absolute timing reference to the network. The only viable exception is a real TAP.

2. It is essential to keep all changes by a device, linear. If the frame offset was 10ms then all frames should have the same offset, if not, the device is interfering with the Real Time Analysis Capability of that access point. SPAN access is a great example of variable offset and the impossibility of doing authentic time based analysis from a SPAN/Monitor port. A good TAP with a tested algorithm handles the Send and Receive integration with consistent timing for the best visualization.

3. All access devices can change the frame and its environment. Consideration No. 1. However as long as the company providing it and the operator understands this, then one can get relevant data and facts from the devices as long as they do not get into the weak areas of the access device/ technology. A TAP is the only reliable access device, see Consideration No. 4.

4 A TAP is the only device that will pass every bit, byte, nibble and octet, including the interframe gap, bad, large, small and other error packets. Even if one uses a higher technology filtering device, I strongly suggest that you stick with using a TAP as your media access. A standalone TAP, not an integrated one.

- *There is significant debate about the viability of passing bad packets for capture and post capture analysis. I feel that just counting the bad packets/types are acceptable and a requirement for base lining analysis.*

5 Before one deploys an access technology, one should do two things and study a lot more:

a) Test more than one device to make sure you are getting what you really need for your tools and that you (and your company) can really use the device and the data it provides.

b) Be sure to test the network before and after the access device to compare and get a real baseline of the Access device effects on the frames.

c) Always buy quality. My mind jumps to 100% made and supported in the U.S.A.

e) No matter the temptation, never mix physical media when using rack mount platforms.

One major and important consideration about access technology – Please do not forget that any access device can be called into question in civil and criminal cases. When using the data captured as the evidence in employee misuse or for CALEA/Lawful capture type situations a TAP is your very best ally, as it just presents the evidence with NO CHANCE of changing anything and with a solid time reference, we call this forensically sound data/evidence and is a MUST for when using for court evidence! Another plus to consider in our security conscious world - a real TAP cannot be hacked so any evidence gathered is as pure as it can get.

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/Monitor ports or mirroring ports and now monitoring was off and running. Analyzers and monitors no longer had to be connected to the network directly; 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. The SPAN or nMonitor port was originally a Quality Assurance Test point for their manufacturers and became a visualization access point as an afterthought.

Is a 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 packets themselves as well as all the packet timing is affected.

Is a SPAN port a scalable technology? – No

When we had only 10Mbps links and with a robust switch (like ones from Cisco) one could almost guarantee they could see every packet going through the switch, except for bad frames. With 10Mbps fully loaded at around 50% to 60% of the maximum bandwidth, the switch backplane could easily replicate every good frame. Even with 100Mbps one could be somewhat successful at acquiring all the good 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 1, 10, 40 and 100 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 flows.

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 ones) including FDX traffic at full time rate with the interframe gap, in real time at non-blocking speeds. All this times 16 ports is a whole lot of data to go through one port. 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.

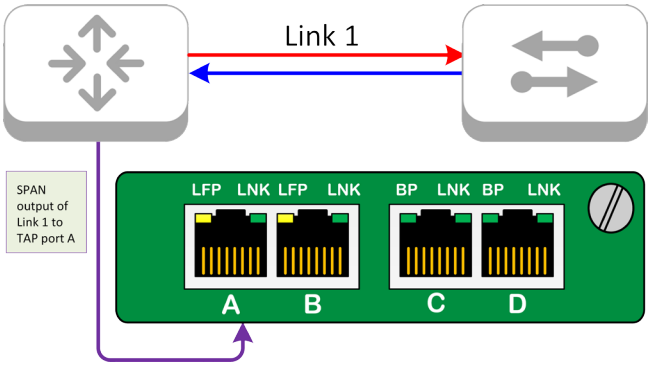

Figure 1: SPAN port sends a mirrored output

The SPAN/Mirrored output of the switch is the aggregation of the "send" and "receive" traffic of the Link as illustrated in Figure 1.

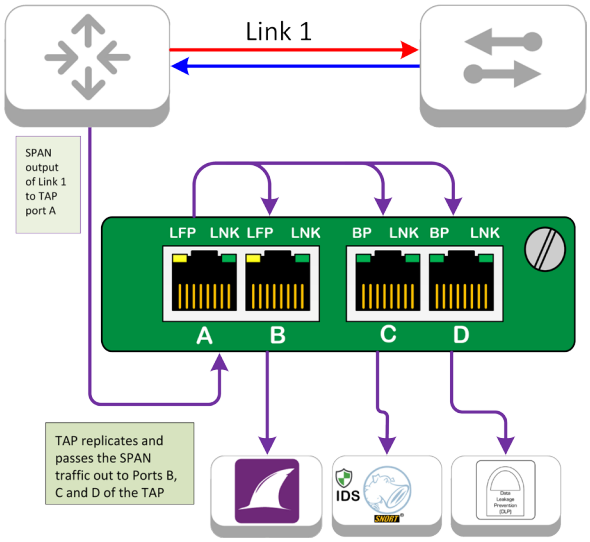

Figure 2: SPAN Mirrored Output regenerates traffic to send to appliances

There are many situations when there are not enough SPAN/Mirrored ports available on a router or switch to allow access to all of the monitoring tools that need to see the traffic of the Link, so introducing a SPAN Mode TAP provides a way to distribute a Link's traffic to up to three network tools as illustrated in Figure 2.

RSPAN (remote SPAN) is not a viable access technology especially if the packets are passed over the WAN as it will gobble up all your bandwidth passing frames back to your local switch that have already passed through the network.

RSPAN is not anywhere near an acceptable nor viable visualization access method.

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 consideration 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."

Please consider that a switch, thus a SPAN access is not fault tolerant and can be a major fault or failure point for your monitoring and management vision. A real TAP is not a failure point.

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 40 Gbps Full Duplex.
3. We have entered into the era of Data Security, Deep Capture, Legal and policy Compliance, network auditing and Lawful Intercept (CALEA) 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 (i.e. application performance monitoring).

These demands will continue to grow since we have become a very digitally focused society and are all connected via the Internet of Things (IoT) 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. These monitoring products are looking for low bandwidth application layer events like "conversation or connection analysis," "application flows," and applications where real time and knowing real delta times are not important.

These monitoring requirements utilize a small amount of bandwidth and grooming does not affect the quality of the reports and statistics. The reason for their success is that they keep within the parameters and capability of the SPAN ports capability and they do not need every frame for their successful reporting and analysis. In other words, SPAN port is a 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 from Gigabit to 40 Gigabit networks and with the demands of seeing all frames for Data Security and policy Compliance, deep capture and Lawful Intercept one must use "real" access (TAPs) technology to fulfill the demands of today's complex analysis and monitoring technologies.

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.
- TAP's are timeless. They never need to down load or be upgraded, they do not have access to anything except the LAN they are monitoring.
- VLAN tags are not 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 errored packets.
- Short or large frames are not filtered.
- Bad CRC frames are not filtered.
- The interframe gap is not dropped nor altered.
- TAPs do not drop packets regardless of the bandwidth.
- TAPs are not addressable network devices and therefore cannot be hacked – High Security.
- TAPs have no setups or command line issues so getting all the data is assured and saves users any setup time. -They are Plug and Monitor 100%
- TAPs are completely passive and do not cause any distortion even on FDX and full bandwidth networks.
- TAPs are fault tolerant.
- TAPs do not care if the traffic is IPv4 or IPv6, it passes all traffic through
- TAPs do not have any filter setup, that is a marketing name for a SPAN device called a TAP, but is not a "real" TAP.

Anyway you analyze it, TAPs are the only "Real 100% Network Access Technology."

Question: We purchase glasses so we can see clearly, why would we pay for glasses if they distorted our view?

Every network should have TAPs to access and pass on the data! TAPs pass ALL the data not just part of it.

If you cannot see it, then how can you fix it?

To learn more about TAPs and designing a suitable visibility plane for your network, **contact the experts at Garland Technology.**

Garland Technology is all about connections – connecting your network to your appliance, connecting your data to your IT team, and reconnecting you to your core business. It's all about better network design. Choose from a full line of access products: a network TAP that supports aggregation, regeneration, bypass and breakout modes; packet brokering products; and cables and pluggables. We want to help you avoid introducing additional software, points of failure and bulk into your network. Garland's hardware solutions let you **see every bit, byte, and packet®** in your network.

Contact

Sales, quotations, product inquiries:
sales@garlandtechnology.com

Garland Technology, LLC.
New York | Texas | Germany