PROFITAP

WHITE PAPER:

THE REALITY OF MEETING YOUR DATA VISUALIZATION DEMANDS!

VISIT **WWW.PROFITAP.COM**

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

TAP, SPAN (rspan), VACL Reviewed for FULL Visibility Access! Just know the Devil or Angel you are dealing with!

► Authors Note: 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!

BASIC RULES FOR NETWORK DATA VISUALIZATION ACCESS

1. First Rule of Network Visualization – Any device or network structure that touches a frame has changed the frame – even if nothing more than changing its absolute timing reference to the network.

2. Second Rule of Network Visualization - It is essential to keep all changes by a device, linear. If the frame offset was 10ms than 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 port.

3. Third Rule of Network Visualization – All access devices can change the frame and its environment, Rule #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.

4. The Fourth Rule of Network Visualization – A TAP is the ONLY device that will pass every bit, byte, nibble and octet, including the interframe gap, bad, large, small and other errored 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 stand alone TAP, not an integrated one! **There is significant debate about the viability of passing bad packets for capture and post capture analysis. I feel the just counting the bad packets/types are acceptable for baselining analysis. Bad Packet analysis is usually for developers who wish to see if their hardware is problematic and not for the network engineer.

5. The Fifth Rule of Network Visualization - Before one deploys an access technology, one should do two things and know a lot more –
   - 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!
   - 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.
   - Always purchase one that has growth potential and that you do not have to purchase all the ports until needed.

There are many factors to consider before you choose a device – CLI or a real GUI for maximum usability. Can only one person use the device or can many, can there be layers of access, tiered secure access, a syslog of access and issues, can filters be shared or Not between access levels, how deep are the filters, can you easily test a filter and get ingress and egress statistics, can you reuse the packets in deep complex filters, including Boolean filtering, is there higher level filtering capability or is the filter restricted to a certain number of bytes and the most important does the device have Dynamic Filtering –WOW!

That is a lot to consider/swallow and there is even more for you to know and evaluate. I will explain more about filtering techniques in detail in Part 2 and what this means to help you get the very best solution, plus more. The higher level of the technology, the more questions that need to be asked and considered to make sure you are getting what you really need for today and tomorrow.

Do not forget that any access device might be called into question in cases of using the data captured for evidence in employee misuse or for CALEA type situations!

This is a lot to cover but some parts already have been covered in previous articles so I will refer to them for your reading pleasure and erudition. Later this year I will take all the old but still valid information and add it to all the latest and greatest information for a concise treatise on Network Data Access Methodologies – Know the Devils and Angels you are dealing with.

TAP versus SPAN was originally written in 2007 for the LoveMyTool.com readers, and is being used by several universities with my approval and has been stolen and changed by others without my permission. This article with comments from the industries best

analysts is still located in the LoveMyTool.com list at –

http://www.lovemytool.com/blog/2007/08/span-ports-or-t.html

I also did an article on RSPAN which is on the LoveMyTool.com site at –

http://www.lovemytool.com/blog/2007/11/rspan.html

I also wrote the article on how CALEA is enacted and how one can use advanced access technology to meet the needs and requirements of a CALEA warrant. This is another article that has been hijacked by a desperate company and changed to make them look good, without my permission. The original article is here –

http://www.lovemytool.com/blog/2007/09/calea-complianc.html

A VACL AS A MONITORING AND ANALYSIS ACCESS TOOL

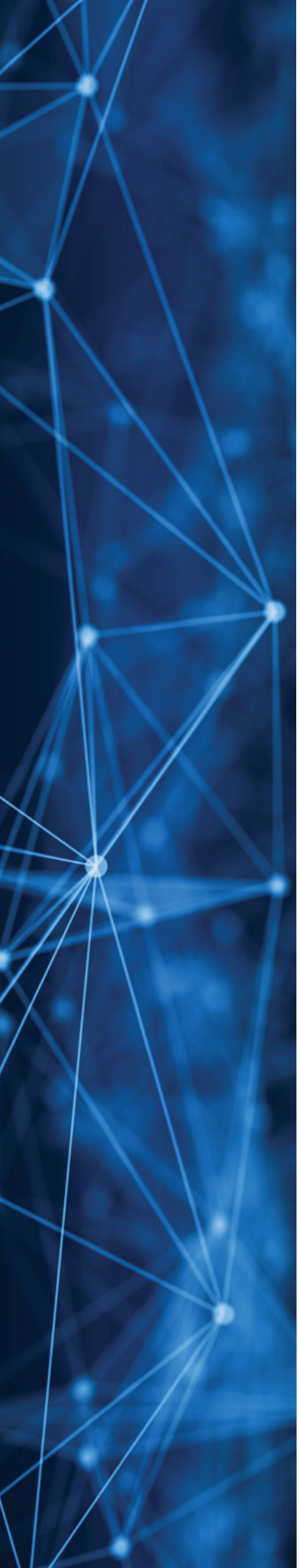
Since the above subjects have been covered in the referenced articles, I will now move on to explaining how the VACL from Cisco can be used, as an expensive, complex but limited data access technology.

VACL stands for VLAN Access Control List. The programming of a VACL is all line code and runs only on the latest models of Cisco Switches. I find this a very difficult and expensive application and quite aberrant to the actual design and network functionality of a core network device. None the less, some people think that it gives network milk to their analyzers. Most of the VACL followers still believe that SPAN access is acceptable for all network analysis and monitoring.

A VACL is defined by Cisco through many papers – for reference –

http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_example09186a0080883ca2.shtml

The VACL capability is available on 6000, 6500 and 7000 series Cisco switches
Cisco says "VACLs are primarily not designed to monitor traffic, but, with a wide range of capability to classify the traffic, the Capture Port feature was introduced so that network traffic analysis can become much simpler" Document ID: 89962 – This says it all. More from Cisco - VACLs support only IP, IPX, and MAC-Layer traffic. VACLs applied to WAN interfaces support only IP traffic for VACL capture. VACLs do not support any V6



traffic or higher layers over L2. In a VACL there is NO ingress or egress differentiation, so you do not know the direction of the frames, a serious limitation of using a VACL for monitoring and analysis! Also – A VACL can send a lot of traffic to your monitoring tool on one port and that can easily over load the monitoring device and over load the VACL port causing dropped packets, etc.

The VACL is only for VLAN traffic and duplicate packets are possible.

When you configure a VACL and apply it to a VLAN, all packets that enter the VLAN are checked against this VACL. If you apply a VACL to the VLAN and an ACL to a routed interface in the VLAN, a packet that comes into the VLAN is first checked against the VACL and, if permitted, is then checked against the input ACL before it is handled by the routed interface. When the packet is routed to another VLAN, it is first checked against the output ACL that is applied to the routed interface, and, if permitted, the VACL configured for the destination VLAN is applied. If a VACL is configured for a packet type and a packet of that type does not match the VACL, the default action is deny. These are the guidelines for the capture option in VACL.

- The capture port cannot be an ATM port.
- The capture port needs to be in the spanning-tree forwarding state for the VLAN.
- The switch has no restriction on the number of capture ports.
- The capture port captures only packets permitted by the configured ACL.
- Capture ports only transmit traffic that belongs to the capture port VLAN. Configure the capture port as a trunk that carries the required VLANs in order to capture traffic that goes to many VLANs.

► *Caution:* Incorrect combination of ACLs (Access Control List) can disrupt the traffic flow. Exercise extra caution while you configure the ACLs in your device.

► Note: There are several limitations of VSPAN usage for traffic analysis:

- All layer 2 traffic that flows in a VLAN is captured. This increases the amount of data to be analyzed.
- The number of SPAN sessions that can be configured on the Catalyst 6000 & 6500 Series Switches is limited. Refer to Local SPAN and RSPAN Session Limits for more information.
- A destination port receives copies of sent and received traffic for all monitored source ports. If a destination port is oversubscribed, it can become congested. This congestion can affect traffic forwarding on one or more of the source ports.

All of this checking and handing off, plus any congestion will certainly lead to incorrect timing and possibly lost or duplicated packets. Plus remember, this is just for VLANs and no bad frames will be counted or passed on to the analysis/monitoring tool. You cannot disperse the filtering to accommodate lower bandwidth monitoring and analysis tools. The filtering is only for the lower layers and has very limited capability when compared to the entire new filter based data access devices.

So a VACL can be used to monitor VLANs but has limitations and to me the biggest limitation is getting it scripted correctly and this even lacks any verification capability. Another big issue for me is that a 6500 or 7000 switch, which is designed to get the proper data to the proper IP/Mac address costs from 40K to around $100K+ or more depending on the configuration. Is this the best use of your slim network dollars? With this level of $'s one could buy 2+, top of the line fully configured/loaded10G access solutions and 3-4 of the lesser versions. All this including complex CLI scripts with no debugging to make your switch a poor monitoring access technology? Please also consider that in high security environments a VACL may not be allowed as the VLAN lists are subject to DDoS/DoS, Flood and miscellaneous Jumping attacks and other layer 2 attacks. A VACL would not be allowed as the access technology for a CALEA warrant, in most cases.

People bring this up to me all the time as if they MUST support SPAN and thus VACL's as acceptable access technology. I will no longer hear arguments on the virtues of RSPAN! A switch is for getting packets to your users, like a router is part for your infrastructure and I find it difficult to use a device made for one application to try to fulfill another and at the same time –It makes No Sense! It cannot be done as the NEED is for a method for real visualization – Total Visibility – you have to be the judge of this and responsible for using variable technology.

As long as one can afford this and live within the limitations and complexity, I say go for it. As long as you know the devil you are dealing with and you can live with what you are NOT getting/seeing is OK with you and your monitoring, security and analysis strategy.

Let's hope your boss doesn't know that money is being wasted with such limited access and visibility. Do Not Lie to yourself or your company if you do not know the effects on the accuracy of your setup and devices – Test it! Testing and full accurate comparison is the ONLY way to know the devil or angel you are dealing with and to understand the value and or problems it can present in your successful visualization strategy. Hey, testing is fun that is what engineers do, we design, build, test and deploy! I strongly suggest that if one is a serious analyst and needs quality and accuracy in their Monitoring, Security, Compliance activities, one should use a TAP as the access technology so you can connect advanced filtering technology to get incredible and accurate visibility into your network, applications, etc.

Remember GIGO – Garbage In - Garbage out ! With today's requirements for data security, the ONLY REAL access technique must be a TAP or optical splitter. The new GDPR requirements are for full capture and total visibility thus SPAN, RSPAN, VACL's do NOT meet the requirements!

I WISH YOU ALL GREAT SUCCESS

IT ALL STARTS WITH VISIBILITY

PROFITAP

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

Profitap

@Profitap

profitap-international