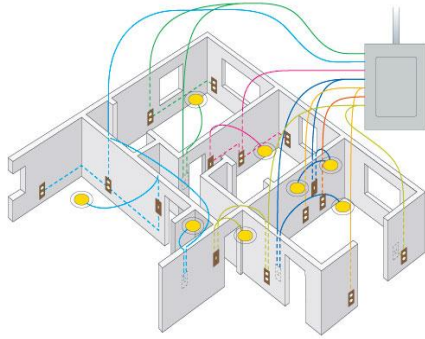


Pre-Instrumentation

An Application and Networking Monitoring Imperative

Can you imagine having a house designed and built without first specifying the location of each electrical outlet? A situation where, each time an electrical outlet was required, an electrician would have to be called out. If the outlet was to be added to an existing circuit, the circuit would have to be turned off at the circuit breaker panel and, consequently, any appliances or lights plugged into that circuit would be powered off. The process would be quite disruptive, expensive, time-consuming and labor-intensive.



Now imagine a similar situation when installing enterprise, service provider or government agency 10G networks or datacenters. The omission of business critical security, application performance and troubleshooting monitoring tools would be exponentially more disruptive, expensive, time-consuming and labor-intensive. Disruptions in 10G networks and datacenters result in diminished employee productivity, dissatisfied customers and lost revenue.

Pre-Instrumentation Explained

Pre-Instrumentation is the process by which 10G networks and data centers are designed and installed with traffic access points and gateways in order to provide access to monitoring tools (instruments) without disrupting application or network traffic. Pre-Instrumentation is not a replacement for monitoring tools. On the contrary, pre-instrumentation allows for the placement and use of monitoring tools anywhere in the network without impacting applications or the network itself.

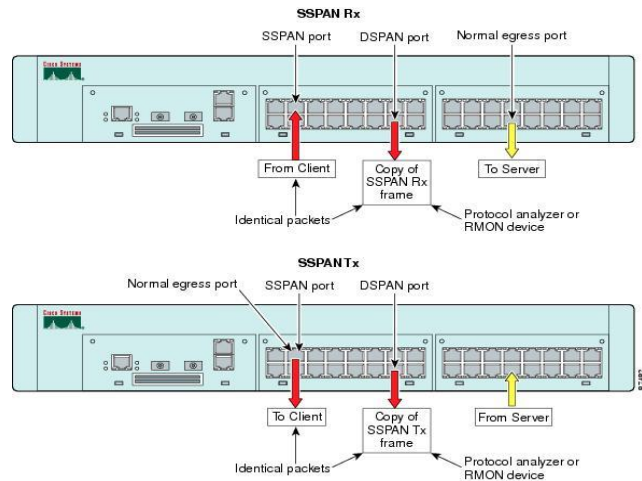
There are 4 basic ways of pre-instrumenting a network:

- 1) *SPAN ports* on Ethernet switches
- 2) *Passive Traffic Access Points* or TAPs
- 3) *Enhanced Traffic Access Points* or Enhanced TAPs
- 4) *Traffic Access Gateways* or TAGs

SPAN Ports

SPAN ports, also known as mirror ports, provide the least expensive but most limited method for providing access to monitoring tools. Most Ethernet switches allow an unused Ethernet port to be configured at a SPAN port, which basically means that traffic from any other port can be replicated onto the SPAN port. Alternatively certain VLANs from all other ports can be replicated onto the SPAN port.

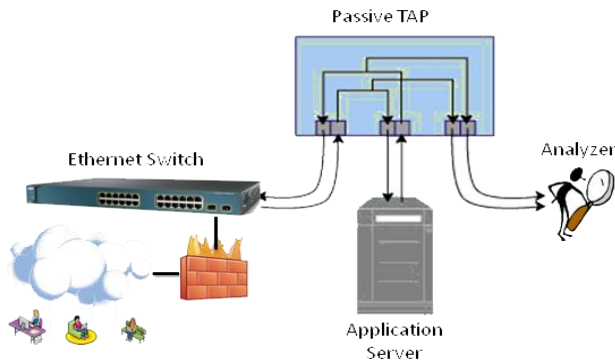
SPAN ports are a common way organizations gain access into the network for monitoring; however, SPAN ports have several shortcomings. The first is that SPAN ports are limited in performance due to the potential for bandwidth oversubscription. The second shortcoming is that heavily utilized SPAN ports can impact performance of the overall switch contributing to application or network issues. The third drawback is that a SPAN port does not see all the traffic – specifically runt (short) packets or packets containing errors, which are essential for troubleshooting.



Passive TAPs

Passive TAPs overcome the limitations of SPAN ports. All traffic is replicated out the TAP to the attached monitoring tool. Passive optical TAPs are essentially optical splitters, so the optical signal strength is split between the network port and the monitor port. As an example, passive optical TAPs can be ordered with a 50:50, 70:30 or 80:20 signal level split between network and monitor ports.

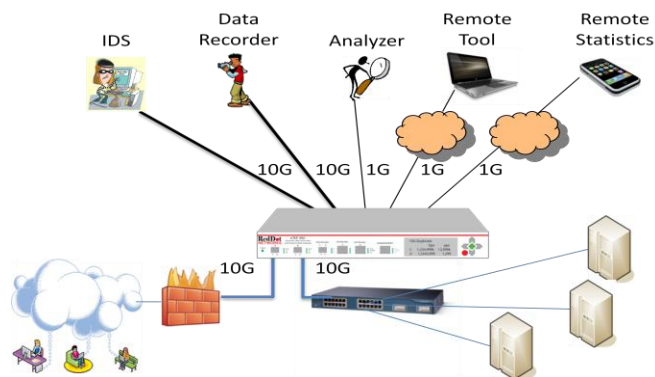
Passive optical TAPs are inherently failsafe, so there is no issue with network disruptions. That being said, there remain 3 challenges with Passive TAPs: 1) Passive TAPs typically connect to only one monitoring tool, 2) Passive TAPs do not provide any filtering of replicated traffic, so monitoring tools can be overwhelmed with traffic that is not of interest and 3) Passive TAPs do not allow 1G monitoring tools to monitor a 10G network.



Enhanced TAPs

To overcome the inherent challenges with existing TAPs, a new generation of Enhanced TAPs is proving their value. In addition to providing the capabilities of a passive TAP, Enhanced TAPs provide the following benefits:

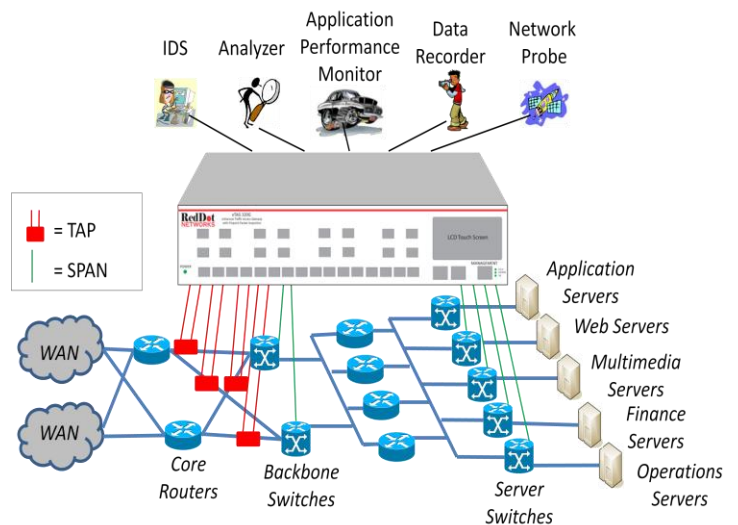
- Filtering (both fixed-offset and content-based) in order to prevent overwhelming of tools and to monitor a 10G network with a 1G monitoring tool
- Additional monitor ports in order to connect to more than one monitoring tool
- Add optional timestamp to replicated traffic to monitor latency
- Remote TAP so that replicated traffic can be sent to a remote monitoring tool



Traffic Access Gateway (TAG)

Traffic Access Gateways offer high 10G/1G port densities (e.g. 32 ports) and are used to pinpoint relevant traffic from SPAN ports, TAPs and Enhanced TAPs to monitoring tools. TAGs offer the following benefits:

- Selectively replicate and distribute traffic from any network port to many monitoring tools
- Aggregate many network ports to any monitoring tools
- Overcome shortages in access points (SPAN ports or TAPs)
- Pre-filter traffic (both fixed-offset and content-based) to monitoring tools to prevent the tools from being overwhelmed and to preserve 1G monitoring tool investments to monitor 10G networks
- Add optional timestamp to replicated traffic to monitor latency
- Limited local burst capture of selective traffic
- Real-time network and monitor port statistics



Conclusion

Pre-instrumentation is an application and network monitoring imperative in enterprise, service provider and government agency networks and data centers. The alternative exposes organizations to unnecessary and avoidable risk. Past solutions offered only limited scalability and flexibility. A new generation of products including Enhanced TAPs and TAGs are maximizing the value and efficiency of network and application monitoring tools.

What are you waiting for? Contact RedDot Networks today!