

# Any-to-any switching with aggregation and filtering reduces monitoring costs

## Summary

Physical Layer Switches can filter and forward packet data to one or many monitoring devices.

With intuitive graphical user interfaces the switch traffic can be configured to aggregate packet data and move it to a monitoring device. In addition, filtering this information improves monitoring tool performance as the tools do not need to process non-relevant packets. By using a physical layer switch the number of monitoring devices can be reduced.

## Problem

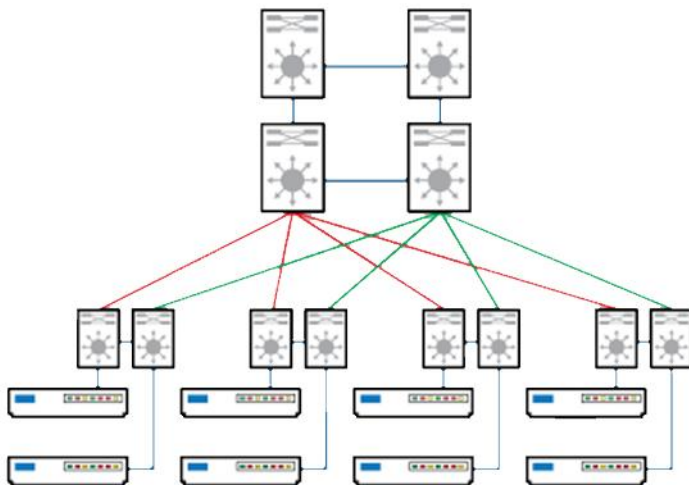
Too many network monitoring devices:

- Intrusion Detection\Prevention
- Sniffer or Network Analyzer
- Network Recorder
- Network Performance Monitor
- Compliance Reporting Systems
- Web Monitor
- VoIP Monitor

Too few capture points:

- Span or monitoring ports limited
- Too many TAP's required
- Unwieldy connection management

## SPAN/Monitoring Ports



A SPAN or monitoring port is a feature on a switch that copies the packets from ports or a VLAN to a port used for analysis. The monitoring function, typically allows, one destination port per SPAN session.

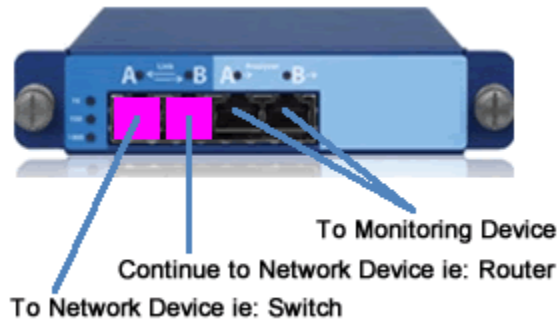
Many switches allow you only one monitoring port per switch. Large Chassis/Blade switches support a fixed number of monitoring ports.

The diagram illustrates an expensive worse case example where monitoring the red and green links each require a monitoring port and an attached monitoring device.

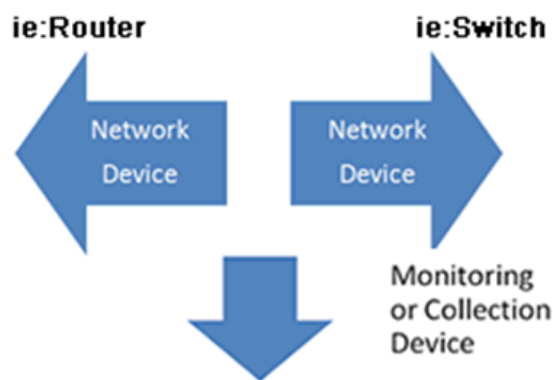
Oversubscription for these SPAN/monitoring ports frequently occurs when more than one packet monitoring device may need access.

An alternative to SPAN/monitoring ports is the full duplex or aggregation TAP.

## TAP's



A full-duplex TAP will guarantee that all of the network traffic, including error information, makes it to the analysis device without delay. It requires the analysis device to have two receive ports one for ingress and another for egress traffic. Taps are useful because they are non-obtrusive, non-detectable and will pass-through traffic even if the tap stops working or loses power.



An Aggregator TAP merges ingress and egress data into single streams for transmission to a single port analysis device with minimal delay. These are also designed to pass-through traffic even if the tap stops working or loses power. However Aggregation TAP's are quite a bit more expensive.

Although high end switch vendors will claim that SPAN/monitoring ports will not impact switch performance, TAP makers claim span ports are apt to consume switch resources, degrading its overall performance. A TAP may be a better solution for full-duplex monitoring devices as two SPAN/monitoring ports would be required.

performance. A TAP may be a better solution for full-duplex monitoring devices as two SPAN/monitoring ports would be required.

Oversubscription can occur with both SPAN/monitoring ports and Aggregation TAP's. This can occur when SPAN ports have been configured in such a way that the traffic being sent to the monitoring port exceeds the ports capacity. Where traffic is aggregated, for example 100Mbps Ethernet port with 70% utilization in both directions, ingress and egress traffic is aggregated and sent to a single port, that port would be oversubscribed at 140Mbps.

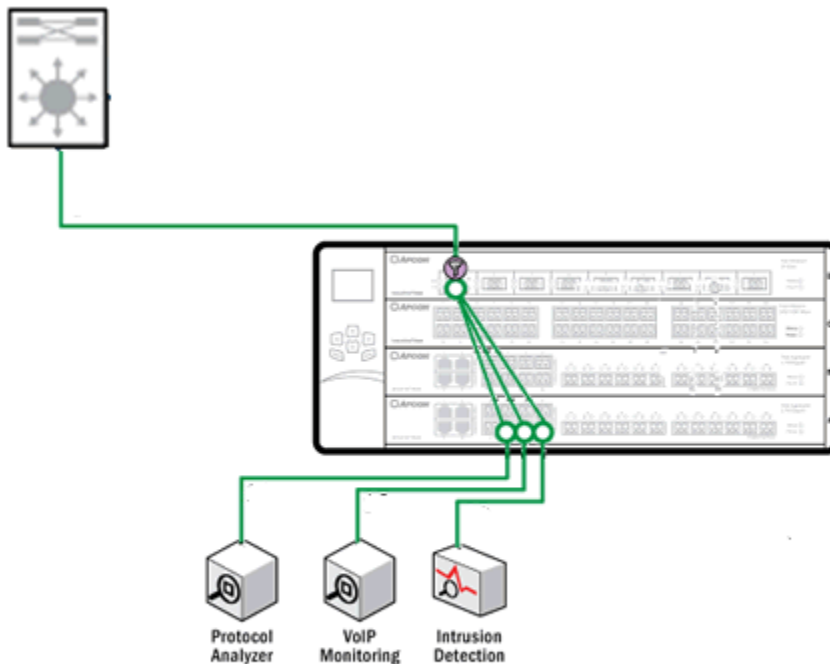
Switch ports and monitoring device may also not be able to perform at line rate, in the case above at 100Mbps. When that occurs it is possible to oversubscribe a monitoring device with a full-duplex TAP.

The problem is the same if you substitute 70% for 1 Gig and 10 Gig. Switches and monitoring devices have performance limits. Testing devices will provide you with answers to those limits.

## Physical Layer Switch

Physical layer, matrix or aggregation switches can be used with monitoring ports and TAP's to solve some common problems. Either there is contention for the same monitoring port by multiple monitoring devices or purchasing dedicated devices for all monitoring points on a network is cost prohibitive. These switches also are great for test labs as devices are wired once and then reconfigured via software.

### One to many



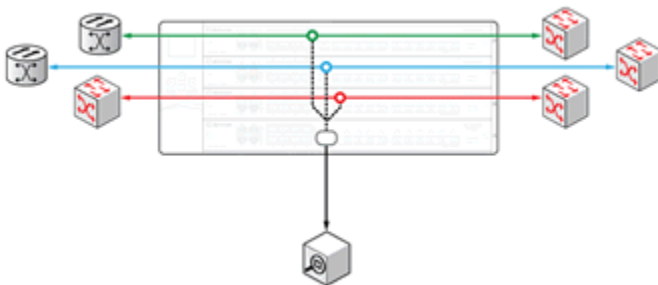
With a Physical Layer Switch the number of capture points is reduced, when a one to many relationship is established, it sends the packet information from a single capture point to different monitoring devices.

Enterprise versions of these switches come with high-availability and fault-tolerant features such as dual power supplies and controllers and hot-swappable components.

Expandable Chassis and Blade designs are available.

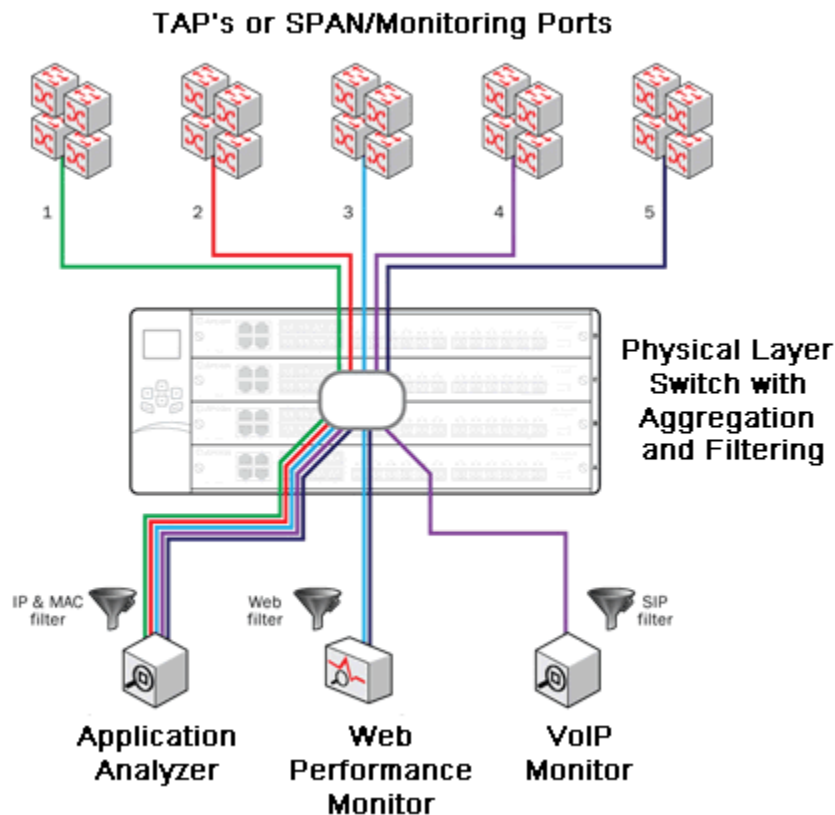
### Inline Tapping

Physical Layer Switches can be configured to serve as an in line TAP. Generally network TAP's are preferred and then connected to the physical layer switch, as they reduce possible points of failure on the network.



The diagram on the right illustrates how a physical layer switch can act as a TAP between multiple devices and send packet information to a monitoring device.

## Many to Many



Aggregating the capture point data and forwarding to a single monitoring device rather than having many devices at each capture point reduces costs.

In the diagram at the right TAP's or SPAN/Monitoring ports 1 through 5 are aggregated and sent to the application analyzer.

Physical Layer Switches that also filter and aggregate better facilitate critical monitoring and reduce the costs associated with acquiring monitoring solutions.

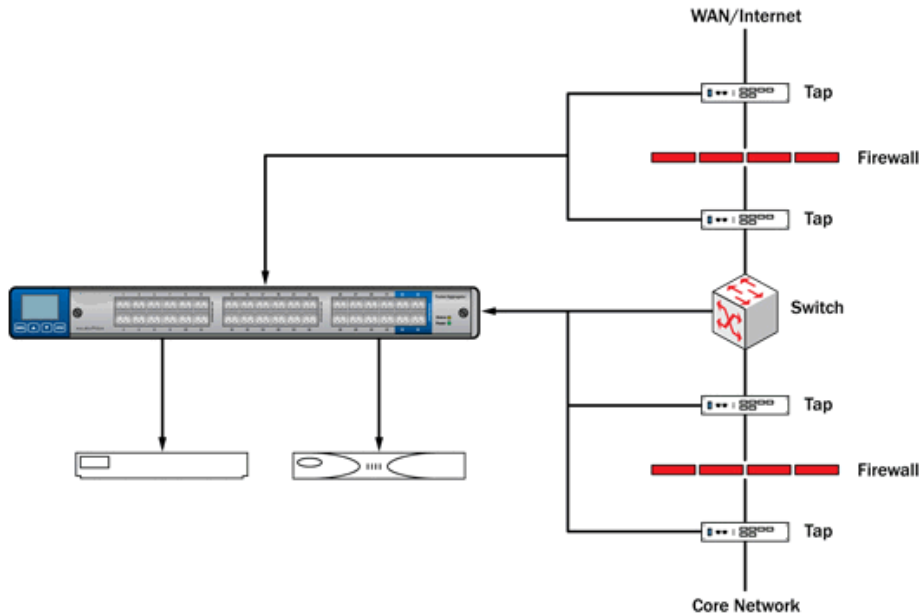
In the diagram Web traffic is filtered from the monitoring ports 3 and 5 and sent to the Web Performance Monitor. If VoIP traffic was all that was moving through port 4 it could be sent directly to the VoIP monitor. But a filter could also be applied to monitor specific VoIP traffic.

In addition, the use of filtering makes it possible to monitor 10 Gig links with 1 Gig tools.

Most network monitoring devices only need to see a small fraction of network traffic to do their jobs. In some cases, sending more data than is required actually degrades efficiency because tools must expend processing power to process and disregard the non-relevant packets.

When working with SPAN/Monitoring ports and aggregation switches, care must be taken to not duplicate packets. For example, where multiple ports are being monitored, a packet travels through ports 1 and 2 and they have been configured to send data to the monitoring port then that packet will be sent to the monitoring port from both ports 1 and 2. Network Traffic analysis, the use of filtering; along with specific ingress and egress monitoring will prevent duplication.

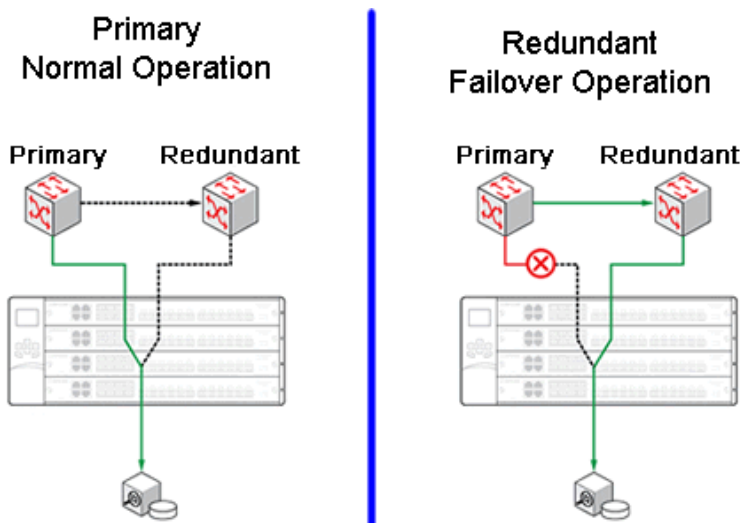
## DMZ Security



Many monitoring products are clustered around the firewall to monitor for suspicious traffic by analyzing protocol activity, unusual traffic flows, matching signatures and other security detection and prevention. In addition, Web Server monitoring may also be required. A physical layer switch can reduce the number of monitoring devices as well support a larger number of monitoring devices.

## Uninterrupted Monitoring

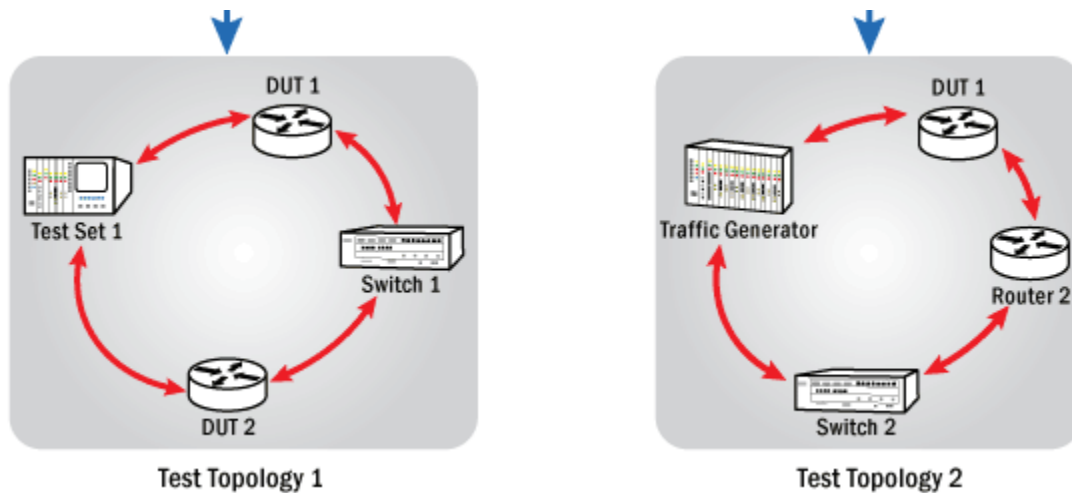
When network paths change due to failure and failover paths implement, monitoring can continue.



In the diagram on the right when the physical layer switch can send to the monitoring device packet data gather from either route. This is another advantage to an aggregation switch.

## Test Lab Flexibility

Physical Layer Switches are ideal for Test Labs as they can quickly automate the task of reconfiguring hardware for different test scenarios.



In addition they are ideal for Redundancy and Failover testing as they can be used to electronically break and reconnect links. The physical layer switch reduces test equipment costs, configuration labor and can provide for remote test lab access.

## Conclusion

Physical Layer switches make it possible for IT engineers to design a monitoring layer into the network infrastructure. By taking advantage of filtering and aggregation capabilities, improved monitoring can be accomplished with shared monitoring devices. Total monitoring costs can be reduced not only in the acquisition of monitoring devices but also the operational costs associated with administration, rack space, power, and cooling.

*Operative Software Products specializes in software and appliances that helps IT professionals test, troubleshoot, manage and monitor their applications and systems. We have solutions for small/medium business, corporate divisions and corporate enterprises.*

---