Application Note

Maximizing visibility for your OptiView™ Series III Integrated Network Analyzer

Network management and security departments have different network access requirements from the end user and server groups. Visibility into critical links and across meshed architectures is a requirement, but not always possible using plain switch ports or SPAN/mirror port configurations. Effective access for network management and security requires the latest generation of tapping technology that includes regeneration, filtering and aggregation. These capabilities provide a new standard for network teams looking to improve MTTR, decrease costs, enhance performance and increase ROI.

Fluke Networks provides a broad line of modern taps for network management, security and application analysis. Five categories of taps provide the flexibility to deploy a wide selection of analysis devices on any critical link, or extend the reach of a single monitoring device across numerous locations. In some situations, tapping provides the only means of gaining visibility to the network and its performance. Connectivity to taps eliminates the time needed to reconfigure, locate and negotiate access for test and measurement equipment on critical network segments. For OptiView analyzer owners, using taps enables visibility and effective troubleshooting capabilities in the OptiView analyzer which otherwise go untouched. This application note will outline different access strategies for the OptiView analyzer and how taps can greatly increase the value of this solution.

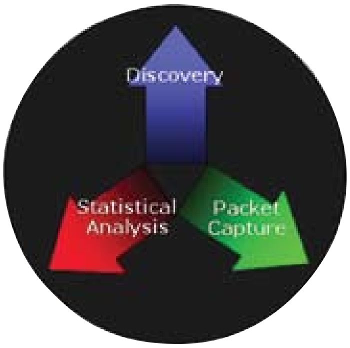
Integrated network analyzer overview

One of the most popular network analysis solutions offered by Fluke Networks is the OptiView Series III Integrated Network Analyzer. This portable network analyzer combines three major capabilities – discovery, monitoring and packet capture – to make it the most complete network troubleshooting solution on the market. The comprehensive design makes it a true workhorse for the busy network technician. However, many users do not fully leverage the capabilities of the OptiView analyzer when they simply plug it into a generic LAN connection. The following application note will help OptiView analyzer customers maximize visibility and troubleshooting capabilities. We will also review modern network architectures and the requirement for built-in data access points dedicated for monitoring, security and troubleshooting devices.

The OptiView analyzer integrates three major functions into a portable and powerful network analyzer.

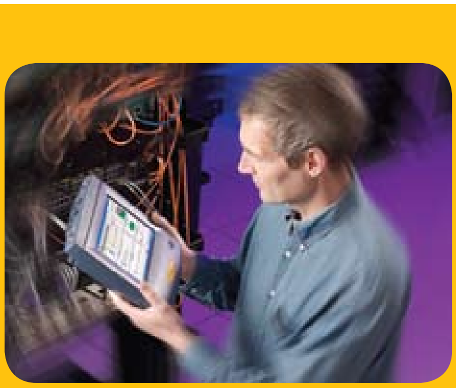
Network discovery

The OptiView analyzer uses many discovery techniques including ping sweeps, broadcast queries, SNMP queries, router solicitations, as well as passive monitoring to discover network devices within communication reach of the OptiView analyzer. By using these technologies, the OptiView analyzer can uncover a multitude of information about the network and devices attached to it.



The OptiView analyzer's unique three vector analysis combines discovery, real-time link monitoring, and packet capture analysis to provide the most powerful, portable network analyzer on the market.

A network inventory will show all the devices on a network within the broadcast domain, or beyond if so configured, and will categorize the devices by type: router, switch, server, host, managed hub or managed access points. On a network that utilizes switches with embedded MIB2 (management information base) and RMON (remote monitoring) counters, the OptiView analyzer will be able to display traffic levels by port, error counts by port, and graph these statistics over time. The discovery information is ideal when taking stock of devices attached to a network



OptiView™ Series III Integrated Network Analyzer

The only portable, integrated analyzer with enterprise-wide vision.

or when trying to understand how a network has changed over time. Rogue devices and servers are easily uncovered and identified for the user. Switch MIB information is collected through discovery and provides an inside look at the health and utilization levels for critical devices. Uncovering an over utilized or error congested switch port will help the user quickly isolate network segments that need immediate attention.

Network monitoring

The network monitoring capability within the OptiView analyzer shows detailed statistics about the level and composition of traffic on links of interest. These links usually include critical network uplinks, internet connections and server farm convergence points. Network monitoring statistics include utilization levels, error counts, protocol/application distribution, hosts by protocol and byte/packet counts for the users of those applications. This information is vital when trying to understand which protocols are using critical bandwidth. Malicious viruses or P2P applications can be uncovered and quickly shut down, leading to more network resources for true business users.

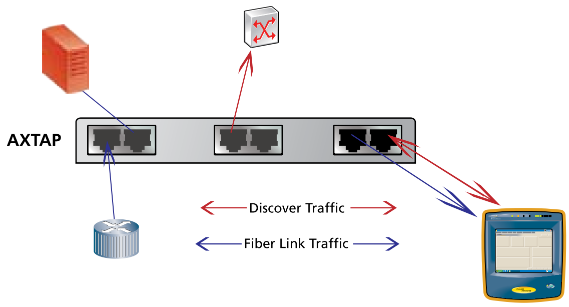
Packet capture and protocol analysis

Packet capture is the tool of choice after network health is confirmed and application or device degradation is suspected of causing performance problems. Packet capture and analysis (often referred to as protocol analysis) is one of the more difficult analysis methods to master, but yields the greatest understanding of how applications and packets are actually behaving on the network. Protocol analysis entails capturing a copy of the network traffic in the OptiView analyzer and then analyzing the data within the built-in protocol analysis software (integrated Protocol Expert). Trained users will employ capture filters to isolate only the necessary traffic under investigation – typically identified by IP addresses or TCP/UPD port number(s). Filtering only users and applications that are known to be of issue will eliminate "noise" from the packet capture and allow the user to quickly diagnose the root cause of application problems. Some examples of application problems uncovered by protocol analysis include:

- Too much data being transmitted by the application
- Too many small packets being transmitted
- Consistently large inter-packet gaps
- Inconsistent large inter-packet gaps
- Data retransmissions

When it is necessary to investigate device performance, such as a firewall, proxy server, switch or router, OptiView analyzer users will look at packets as they go through such equipment. Typically, the engineer will be looking for a change in inter-packet gaps (jitter), latency of the packets going through the device or even a change in the packet payload. For many organizations, packet captures also provide indisputable evidence about what is occurring on the network. This is very helpful when tackling device problems with vendors or application problems with development groups.

OptiView analyzer capability/use matrix	Use/benefit
Discovery	• Network inventory and change reports • Discovery of rouge network attached • SNMP data gathering for devices health and performance
Monitoring	• Provides useful link statistics that can determine if network is under stress from errors or utilization • Application traffic analysis can identify what's being used on the network, how much impact it is making and who is generating that application traffic, e.g., VoIP or Oracle traffic levels • Identify malicious applications and sources on network like viruses and P2P file sharing
Packet capture and analysis	• Application analysis and troubleshooting within the packets • VoIP analysis on call-by-call basis with QoS scores • Provides proof of application and device behavior to vendors and application developers



A combination tap (AXTAP) configuration will copy link information to an OptiView analyzer analysis port, while routing discovery packets to a switch port.

OptiView analyzer deployment scenarios

The above three capabilities – discovery, monitoring and packet capture, are available to OptiView analyzer users, but the value of the data gathered by each capability will vary depending on the data access options utilized to connect the OptiView analyzer with the network. There are three typical scenarios for connecting the OptiView analyzer with the network. Each one has its advantages and disadvantages depending on the task. The first option is to plug the OptiView analyzer into any available switch port. By their nature, switches take packets entering a port and forward them to a known destination address – which works great for the discovery engine inside the integrated OptiView. However, switch ports will only receive packets that are destined for the devices attached to that port. The only other traffic seen will be broadcast traffic, multicast traffic and discovery packets generated by the OptiView analyzer and its target devices. In addition, any error packets detected by a switch will not be forwarded to the OptiView analyzer or seen in the monitoring views since error packets are blocked by all switch ports. The nature of a typical switch port will limit the OptiView analyzer's information gathering capabilities to discovery, while link monitoring and packet capture will only show broadcast, multicast traffic of marginal usefulness when troubleshooting a network. The second alternative for connecting an OptiView analyzer to the network is to use a mirror port (also called a SPAN port by Cisco). Mirror ports are configurable on most enterprise class switches and routers. They are configured as a special port that will copy packets from the switch or router backplane and forward to the device attached to the mirror connection. Each switch/router manufacturer offers different mirror or SPAN configuration options, which can be powerful, or very limiting. Some of the most common limitations of mirror/SPAN port are:

- Only one or two mirror/SPAN ports can be configured per device. This can cause contention between different IT groups (engineering and security, typically) which need access to critical network segments
- Mirror/SPAN ports will not allow packet injection from monitoring devices back onto the network. This negates the OptiView analyzer's discovery capability
- Mirror/SPAN ports require configuration. This can delay Mean Time To Resolution (MTTR) when troubleshooting network problems
- Mirror/SPAN port configuration can take down the network. If a SPAN port is misconfigured, it can flood traffic onto critical links. For this reason, some companies don't even allow the use of mirror/SPAN ports
- Mirror/SPAN ports can be oversubscribed with traffic and will drop packets
- Mirror/SPAN ports will not forward network errors

Even with these limitations, mirror/SPAN ports are useful and can provide needed access for network test equipment with minimal extra investment.

OptiView analyzer access methods and implications	**Plain switch port**	**SPAN/mirror port**	**In-line tap**
Discovery	Excellent	Limited, some switch/router models do not allow SPAN/mirror ports to accept discovery packets from the OptiView analyzer	Excellent, fiber links require special tap
Monitoring	Limited, user will only see broadcasts, multicasts and discovery packets from the OptiView analyzer	Good, however SPAN/mirror ports block error packets and configuration will affect traffic seen by the OptiView analyzer	Excellent
Packet capture and analysis	Limited, user will only see broadcasts, multicasts and discovery packets from the OptiView analyzer	Yes, however SPAN/mirror configuration will affect traffic seen by the OptiView analyzer. Packet timing can also be impacted by switch buffering	Excellent

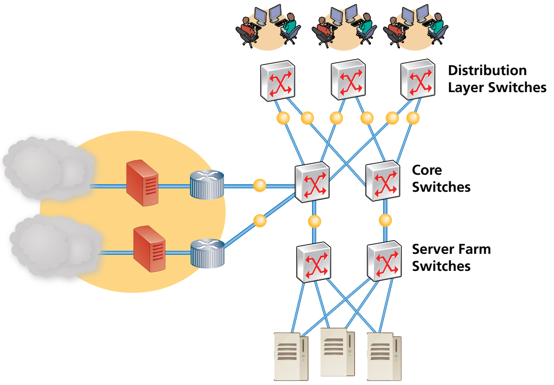
The final means of gaining data access on the network is with a network tap. In-line taps connect between two end-points on the network, typically a switch, router, firewall or server. Once installed, taps provide instant plug-and-play access to the network with full visibility into link traffic, errors and applications. Traditionally, an in-line tap would require a dual interface analyzer to support full duplex links. However, in-line taps can also support aggregation and allow the OptiView analyzer to connect to full duplex links using just a single monitoring port. Inserting your OptiView analyzer onto critical links with a tap provides visibility using all of the built-in capabilities. Additionally, the user gains plug-and-play simplicity since no configurations need to be made.

One consideration when tapping fiber links is the discovery mechanism. On copper links, the discovery packets (SNMP) are sent back through the tap directly onto the link. On a fiber link, a good tap utilizes a fiber splitter for fail-safe/passive operation. However, fiber splitters will not allow the transmission of packets back onto the network through the tapped connection. This means users need to consider a tap that can support the placement of packets back onto the network using a management port. Fluke Networks offers special taps for just this purpose. Combination taps provide configurable ports that will allow the OptiView analyzer to receive packets from the link and send packets back onto the network. This capability is useful for any other analysis device that needs to send packets back onto the network, but doesn't have a separate management port.

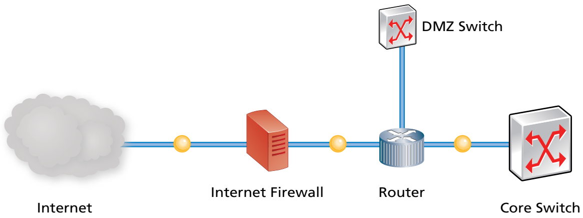
OptiView analyzer deployment strategies

Since the installation of in-line taps requires a link disruption for a short period, the best tapping strategy employs permanent tap installations that act as a window into the network at key locations. The installation of the taps can then occur during a planned network maintenance period or during network deployment and configuration.

There are several locations on a network where an IT department typically needs visibility for effective management. First is at the network edge, where an enterprise network has traffic entering from the internet and exiting from end users and servers. OptiView analyzer can investigate at this location on the network to ensure low bandwidth internet connections, that have a monthly cost associated with them, are not being flooded with non-business traffic. This location will also offer proximity to the WAN for throughput tests that can verify a carrier is providing bandwidth according to contract. The network edge is a location important to the network engineers who troubleshoot internet connectivity issues, as well as the IT security group that must ensure malicious traffic is not entering or leaving the enterprise domain. Because of its importance, extra tap access ports should be planned to accommodate both of these IT groups.

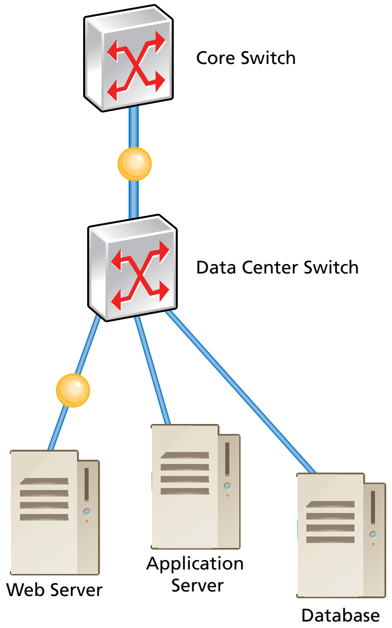


A successful strategy for monitoring, analysis and security devices will offer network tap access at the edge, data center and distribution layers of the network.



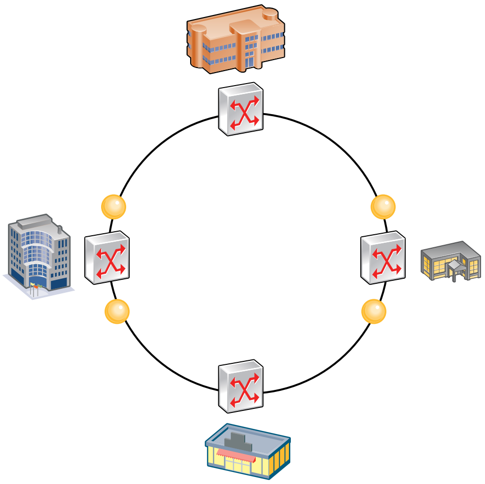
Three possible tap locations for visibility into traffic entering and leaving an enterprise network at the edge.

The second most important location on a network for permanent network test access is at the data center. Most escalated application problems are investigated by network engineers as close to the data center as possible. In most cases, the protocol analyzer built into the OptiView analyzer will be utilized as the primary tool in identifying an application degradation issue. By analyzing close to the server, latency issues associated with the network are eliminated and transactional timing between data requests and responses from the server are accurately depicted. A tap in front of the data center switch will provide immediate access to a converged location where all users and applications must pass into the data center. If managing multi-tiered applications, a tap between the front tier and the switch will enable transactional analysis between tiers, such as a web server and database.



Test access points within the data center help the OptiView analyze application performance and n-tier transactions.

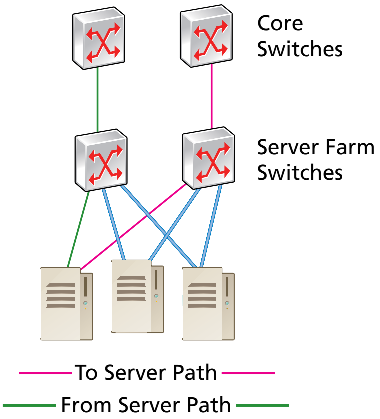
The final location that needs consideration for the deployment of permanent taps is at the distribution layer, between core switches and distribution layer switches. The architecture for distribution layer switches can vary. In some models, the distribution switches are all homed to the core switch, while campus environments often employ campus ring architecture. In either case, test access at the distribution layer allows OptiView analyzer users to isolate network issues that vary across different groups of end users. If there is a problem with network degradation, network engineers can use the OptiView analyzer to evaluate the critical links that support different user groups.



Campus rings require permanent taps for test and monitoring access when analysis is required at the distribution layer.

Visibility across redundant, meshed architectures

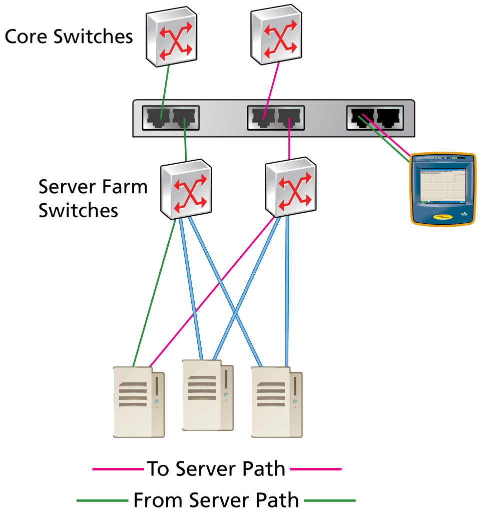
The requirement for high availability networks and limited downtime has resulted in a common network design that utilizes redundant switches and routers for fail-safe, load-balanced operation. While redundant equipment is valuable for network continuity for the end user and server groups, it provides a challenge for the network engineer in need of transaction analysis and switch configuration visibility across the multiple paths.



An OptiView analyzer can only look at one link at a time. However, redundant paths across the mesh can make it nearly impossible to get full visibility. A typical scenario is to use protocol analysis in order to understand application transaction performance. Without dual link visibility, it might take numerous captures in order to get a transaction that starts and finishes on the same link. Another typical scenario is understanding the volume and make-up of traffic between end users and servers using the monitoring capability in the OptiView analyzer. Once again, the user will only be able to see one link at time that might or might not be representative of the whole picture.

Dual link taps can solve this problem by aggregating full duplex traffic from two links into a single data stream for OptiView analyzer analysis. Dual link taps come in multiple configurations and allow filtering of traffic before aggregation in order to minimize the possibility of oversubscription.

Tap models for redundant link analysis	Description
ATAP-2000-BT-BT	Dual 10/100/1000 aggregating tap, dual 10/100/1000 copper monitor ports
ATAP-2000-SX-SX	Dual-port LX fiber aggregating tap, dual SX fiber monitor ports
ATAP-2000-LX-SX	Dual-port LX fiber aggregating tap, dual SX fiber monitor ports
FATAP-2000BT	Dual 10/100/1000 filtering aggregation tap with 4 10/100/1000 and SFP (SX or LX) monitor ports
FATAP-2000SX	Dual SX gigabit filtering aggregation tap with 4 10/100/1000 and SFP (SX or LX) monitor ports
FATAP-2000LX	Dual LX gigabit filtering aggregation tap with 4 10/100/1000 and SFP (SX or LX) monitor ports
AXTAP2210BT-BT/SFP	Dual link in line 10/100/1000 copper tap with 6 any-to-any ports (4 BT & 2 SFP)



A dual link aggregation tap collects network traffic from two links and outputs it as a single data stream to network analysis devices, like the OptiView analyzer. Simultaneous visibility across both links is otherwise impossible for a single device.

Conclusion

The OptiView™ Integrated Network Analyzer from Fluke Networks is one the most advanced portable network analyzers on the market. The combination of active discovery, network monitoring, packet capture and analysis provide multiple lenses through which you can effectively manage your network. However, to leverage these capabilities, network architects and engineers must ensure proper network data access and connectivity. By combining the OptiView analyzer with the flexibility and visibility of in-line taps, users gain greater insight into network behavior and application performance on critical links. Using the power of link aggregation and regeneration, this visibility extends to the OptiView analyzer, and any other monitoring devices used by IT departments. For more information visit **www.flukenetworks.com/taps**

Tap model types		
Type	**Fluke Networks model prefix**	**Description**
In-line taps	**TAP** (copper products) **FTAP** (fiber products)	Provide fault tolerant in-line visibility to full duplex, line rate network traffic between two network devices.
Aggregating in-line taps	**ATAP**	Install in-line on a network link and aggregate full-duplex traffic into a single data stream. These devices are necessary for in-line analysis with single port monitoring devices and can output copies of the network traffic to numerous analysis devices.
Aggregating and switching SPAN taps	**ASTAP** (aggregating SPAN taps) **STAP** (SPAN switch)	Allow analysis devices to see aggregated traffic from multiple SPAN ports in a single data stream, which is replicated for numerous analysis solutions. Switching taps allow analysis devices to be remotely switched across a broad number of SPAN ports for specific troubleshooting.

Tap model types

Type	Fluke Networks model prefix	Description
Filtering link aggregation taps	**FATAP** (filtering link aggregation in-line tap) **FASTAP** (filtering link aggregation SPAN tap)	Provide hardware based filtering within the tap to increase performance of analysis equipment, and prevent dropped packets when aggregating high bandwidth traffic. Filtering link aggregation taps work in line or with SPAN ports, aggregate multi-link traffic, and replicate onto four monitoring ports for use with multiple analysis devices.
Combination taps	**AXTAP** (combination in-line tap) **AXSTAP** (combination SPAN aggregation tap)	Install in-line or with SPAN ports. Port configurations can be set to aggregate, replicate or pass traffic at full line rate to any other port. Configuration sets ports for network side connectivity, or analysis device connectivity. These products offer the highest number of replication ports for critical link locations where numerous analysis devices are deployed.

Printed in U.S.A. 4/2007 3037687 D-EN-N Rev A