



# Optimized Network Monitoring

Four ways matrix switching streamlines data center operation, reduces costs and positions IT for growth

WHITE PAPER  
MARCH 2008

APCON, Inc.  
T 503.682.4050  
800.624.6808  
F 503.682.4059  
[www.apcon.com](http://www.apcon.com)

## OPTIMIZED NETWORK MONITORING



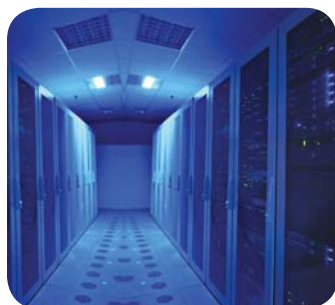
### INTRODUCTION

Companies rely on their networks more than ever to serve customers and stay competitive in the marketplace. From banking and investment to travel and entertainment, IT infrastructure has become the keystone upon which business is conducted.

Thus the “holy grail” for today’s savvy IT organization is not only resolving network issues quickly, it’s in preventing them from occurring at all. A robust network monitoring program enables your IT group to stay a step ahead – scrutinizing the network and addressing issues before they become meltdowns.

But with the budget cutbacks and corporate downsizing affecting corporate America today, how does the intrepid IT manager keep up?

## OPTIMIZED NETWORK MONITORING



### **SIMPLIFY INFRASTRUCTURE & PROVIDE SECURE, REMOTE ACCESS**

Adding a highly engineered matrix switch, or an array of switches, to a data center infrastructure is a significant step in the right direction. Its four key enablers are outlined below. But from the perspective of overall value, the benefits of a matrix switch are that it will:

- Simplify network structure
- Fully utilize available monitoring devices and reduce the cost of expanding network monitoring capabilities
- Provide remote access for multiple users
- Increase physical security of the network

There are numerous matrix switches available in the market today. But not all can or will address the “pain points” an IT manager has to deal with, especially in a complex environment. To this, we submit that if a particular switch speaks to the following four key factors, it is well worth considering.

### **1. Connectivity**

In this area, a top notch switch offers such functionality as:

**Embedded Firmware** – Specifically an embedded web GUI, so there is no software to install and maintain. This saves staff time and eliminates the need to upgrade each client with every new bug fix and product enhancement. By simply upgrading the embedded software, every user who accesses the switch will be working with the latest firmware build.

**Web Browser Access** – Staff can simply launch their favorite web browser and enter a customer-defined IP address to the switch to be granted secure, remote access. In a case where the IP network is down, the switch also offers a console port by which users can still securely and remotely access the switch with an SSH connection.

## OPTIMIZED NETWORK MONITORING



**Signal Regeneration** – Networks can experience signal degradation due to the length of connections, dirty connectors, old cable infrastructure and other hardware issues. If the incoming signal (copper or fiber) has low signal strength, a well engineered switch will fully regenerate each connection to full signal strength, making sure that the two end devices can talk to each other.

**Digital Diagnostics** – Optimally, switches should enable users to see the digital diagnostics for each optical port via an embedded web GUI. Look for a switch that can pull optical characteristics. These would include Tx and Rx signal strength, current bias, temperature, voltage, data rates and protocols supported, fiber type, part numbers, and serial numbers on a per-optical-port basis.

**Cable Test** – It's best to have a cable test feature embedded in firmware that enables clients to apply degradation to the receive side of each optical transceiver by .05dbm, so they can see a color-coded change as the signal gets worse. Allowing quick checks for any bad optical cables more than pays for itself when there are hundreds of optical connections involved and staff is trying to pinpoint an issue that may be related to a \$25 cable.

## 2. Scalability

True scalability is defined in these terms:

**Platform for Expansion** – A switch should allow for partial population of its chassis, thereby leaving room for future expansion. By installing a larger density switch and partially populating it, customers can reduce the number of chassis to manage – and pay for at one time – and allow for future growth.

**Mix and Match Capability** – Users should be able to mix and match media in the same chassis, supporting interfaces from T1 to 10Gig both copper and fiber. On a per-port basis optically, clients can then mix and match different data rates and protocols.

For example, A01 could be GigE SM fiber running 1310nm while port A02 is GigE MM fiber running 850nm. The switch can logically patch those two ports together because they are the same data rates and protocols, and can thereby talk to each other.

Some switches offer even greater flexibility in that clients can have different protocols and data rates optically on the same blade. An example of this would be port A01 supporting GigE SM fiber, 850nm, while port A02 is SONET OC3, MM fiber running 1310nm. Port A03 could be Fibre channel 1,2, or 4 Gig and so on.

## OPTIMIZED NETWORK MONITORING

**Flexible Monitoring** – Customers using Fibre channel packet capturing tools for network monitoring should also be able to electronically rove these devices for SAN monitoring in the same chassis as the Ethernet for SPAN port monitoring. Where a switch supports interfaces from T1 to 10Gig, using the same monitoring type port on a networking device or network taps, clients can perform monitoring at any aspect of their network.

**Data-Rate Selection** – This allows both copper Ethernet and optical Ethernet ports to be set to different data rates (for example having the copper Ethernet blades set to data rates on a per-port basis of 10/100/1000 Mbps). If the appropriate optical transceivers are populated on the switch blades, the fiber Ethernet ports can also be independently configured for 100/1000 Mbps.

**Media Conversion** – The best switch products provide the ability to connect a copper port to a fiber port. They also provide the flexibility of connecting a single mode fiber port to a multi-mode fiber port. Neither of these connections requires a media conversion device, as this function can be performed internally with the appropriate blades resident on the switch.

### 3. Flexibility

It will be realized in switches with capabilities such as:

**Any-to-Any Matrix** – Switches should provide a significant monitor-ports-to-monitor-tools ratio in the matrix configuration. With switches offering up to 288-ports per chassis, packet capturing or network monitoring is simplified for all layers of the data center (core, distribution, access and DMZ).

**Port Naming** – A well engineered switch will allow users to customize the names of its ports, so they can identify connections by device name/type and location, or another naming convention that is meaningful to them. For example, a port might be named “datacenter-floor2” or “snifferdevice-rack2.” Having a field of up to 255 characters is the most helpful.

## OPTIMIZED NETWORK MONITORING

**Common Chassis Management** – Regardless of the chassis deployed, it's best if the management interface is exactly the same for each switch. It's even better if the switch offers a centralized management interface that provides secure, remote control of multiple switches from a single screen. This continuity will reduce training efforts and simplify user operation.

**Real-Time Current Patches** – A switch interface equipped with a “current patches” screen takes the guesswork out of determining which ports are connected. This screen shows, in real-time, the port numbers of the switch that are connected and the port number to which the monitoring tools are connected. If the same SPAN port is connected to multiple tools, the current patching screen will show this in real-time. User simplicity of viewing will be enhanced if both the ports and the port names are fields that can be sorted.

**Zoning** – An administrator will appreciate the ability to create zones, which offers the ability to divide the chassis up per port, per user. Therefore, if the administrator does not want other users to have access to certain ports (i.e., IDS), he/she could create a zone and add these ports to that zone so no other users would have access.

**Import/Exporting Chassis Configurations** – Firmware that allows clients to export the configuration of the chassis to store for backup is a good choice. It also allows clients to make minor edits to that XML file and import the XML file into new chassis deployments to simplify new installations.

**SNMP** – Switches supporting SNMP will give clients the ability to get SNMP traps such as temperature and power failure for example.

**Syslogs** – If members of the IT staff are using a Syslog server, they will have the ability to see time stamps per user on changes that occur within the switch.

### 4. Security

How best to achieve it?

**Secure, Remote Access** – Once logged in, customers can have the ability to secure remote access by forcing SSL or https, and forcing SSH for the CLI connections.

## OPTIMIZED NETWORK MONITORING

**Reduced Access To The Data Center** – Companies with a manual patching process that requires employees to access a data center with each patching change are open to user patching errors. The goal is to reduce the likelihood where users can accidentally pull the wrong cable and cause network outage.

The best switches increase security in customer data centers by eliminating the users' need to access the facility each time they want to change a patch from the monitoring tool to a different SPAN or Tap port. This also will significantly reduce the MTTR (Mean-Time-To-Repair) by eliminating the manual process of accessing the data center to change patches.

**User Authentication** – Switches that offer the ability to use existing RADIUS or TACACS+ servers to provide secure user authentication are preferable because they streamline user logins. As a results, users with multiple network devices will be able to use a single login for multi-switch access.

**Security Blade** – With the unique function of a security blade, users no longer have the option of accidentally making a full duplex connection when connecting a SPAN port to a monitoring tool. The security blade will force all simplex connections, eliminating user error and preventing traffic from accidentally being sent back in the direction of a monitoring tool.

**SPAN Port Safety Logic** – SPAN port safety logic prevents users from accidentally connecting SPAN ports and creating an infinite network loop leading to a catastrophic failure.

**Port Locking** – Port locking allows users to lock ports down while doing packet capturing between SPAN ports and monitoring tools so another user does not accidentally take down a connection.

This is helpful when multiple users are accessing the same SPAN ports at the same time. Users have the flexibility of locking down the SPAN port and the monitoring tool, or simply the monitoring tool, which would allow other users to take that same SPAN port and multicast the same traffic to another tool to further analyze the traffic patterns.

## OPTIMIZED NETWORK MONITORING

### SAVINGS

With top notch Layer 1 matrix switches come cost and time savings. Key examples include the following:



**Fewer Switches To Manage** – Switches that scale to 288 ports in a single chassis can significantly reduce the number of matrix switches and monitoring tools to manage. With other low-density matrix switches, customers need to purchase additional tools each time they exceed the port capacity of an existing matrix switch.

**Reduction in Monitoring Devices** – Customers are able to limit the number of monitoring tools required at any given time, rather than basing the requirement on the number of matrix switches available. The best matrix switches provide the ability to remotely move and share expensive monitoring devices across an entire network.

**Reduced Power Consumption** – Data centers nationwide are getting “greener” with close attention paid to power consumption and heating/cooling systems. Leading switch providers are helping companies utilize power more efficiently by optimizing use of network devices – reducing the number of devices necessary to achieve monitoring and testing goals and using them efficiently. Fewer matrix switches also means fewer power outlets are required for each rack.

### SUMMARY

Network monitoring systems in the data center industry are becoming increasingly complex, with multiple layers of technology needing to work hand-in-glove and increased security concerns making remote access a priority. With the deployment of a solution that offers both increased flexibility and connectivity, as well as scalability for future expansion, companies have the opportunity to experience an ROI in the hundreds of thousands of dollars, hundreds of hours of staff time and increased security.

## OPTIMIZED NETWORK MONITORING

### ABOUT APCON

APCON, Inc., a pioneer in the field of physical layer technology, is globally recognized as the leading provider of matrix switching solutions. APCON's customer list includes Fortune 500 companies, networking and computer OEMs, government and military organizations, telecommunication and service providers, financial services firms, and medical companies.

Being the total solution means that APCON provides both hardware and software for managing physical layer connections. In fact, APCON is the only company today that offers a single-sourced integrated solution.

With thousands of systems installed in over 30 countries, APCON is the leader with unique solutions for both test labs and production network environments.



APCON, Inc.  
9255 SW Pioneer Court  
Wilsonville, Oregon 97070  
T: 800.624.6808  
503.682.4050  
F: 503.682.4059  
[www.apcon.com](http://www.apcon.com)