# *Complexity is the Mortal Enemy of Reliability*

## Build an impenetrable hardware foundation of security, reliability and availability under your mission-critical enterprise network

Security, reliability and network availability are three fundamental concepts that network administrators strive relentlessly to deliver. They spend billions of dollars every year to acquire and install the latest software-based intrusion detection and firewall systems, state of the art intelligent network switches and innovative network management applications. As we approach the end of the first decade of the 21st century, all of this incredibly sophisticated *software* continues to fail its primary objective. Spectacular network hacks continue to be Page 1 News.

Hardware security appliances have been largely overlooked, yet hardware is inherently secure and its lower level of complexity (as compared to software solutions) makes hardware much more dependable. High performance hardware solutions support the next generation of higher speed networks with true plug'n'play installation. There is no software to be hacked, patched or regularly upgraded.

You may be wondering: isn't the physical layer composed of the cables, jacks and patch panels that reside at the bottom layer of the network pyramid? Those components are the obvious parts of Layer 1. The installation of secure, reliable hardware switches and switching systems adds real power to the physical layer of your network, where they control access and provide nearly instantaneous backup. Other important applications include air gap isolation in networks of mixed security classifications and bypass switching. Hardware switches are fundamental additions to crucial information networks – and what networks aren't crucial to their enterprises?

Network hardware switches are becoming the preferred means for adding an additional layer of security, reliability and network availability. Network architects of the most advanced commercial, government and military networks have specified Layer 1 communications hardware to maximize control and minimize downtime. Unauthorized users are physically locked out and maintenance is performed without shutting down the network. Before we address the power of Layer 1, let's take a look at the vulnerabilities that are embedded in software-driven network components of higher network layers by creating some hypothetical but very real world "what if" scenarios.

**Scenario A:** ***"You are the data-center manager of a large financial services company whose success is built directly on the network. Your network is responsible for thousands of critical client transactions and is also home to the VoIP 7x24x365 call center. At 9:00 AM you have a catastrophic failure in a high-density edge switch. Now what? The SNMP manager is down so it's useless for troubleshooting. Your help desk is unable to answer phone calls from angry users whose customers want to get that sell order in NOW. The IT Support Team has pinpointed the problem switch, but spare switches are stored in a different location.***

***Scrambling to swap out the failed switch, you've solved a critical problem in just under an hour – relatively quickly. It's now 10:00 AM and the market dropped 400 points while your net was down. Someone has to answer to customers for their losses due to a brief network outage. No good deed goes unpunished…"***

Complexity is the mortal enemy of reliability. Failures of complex network components occur frequently and the consequences range from simple inconvenience to heavy financial losses and compromised public safety. How can network downtime be minimized without adding complexity that further reduces reliability?

Providers and consumers of crucial commercial and military information have formerly relied on duplication in higher layers of their network infrastructure, increasing their exposure to failures of complex network components. The availability of high performance hardware-based Layer 1 switches from Market Central has led to revised network architectures that offer much higher network availability to users and dependability to information providers. Reduced overall complexity dramatically improves network reliability while also implementing simplified access control and ease of network maintenance. The exceptionally high data rates made possible by proprietary fiber optic switches and 10 Gigabit Ethernet switches serve next generation networks and make their addition to present networks even more economical to implement.

Market Central's SwitchMaster® Layer-1 ganged A/B switches enable a hot back-up network switch to be swapped almost instantly, maintaining workstation, server and IP-phone connections when a main switch fails. The swap can be controlled locally in the datacenter or from a remote location and downtime is measured in seconds, not hours. SwitchMaster® systems are scalable to thousands of users.

Figure 1 illustrates a typical SwitchMaster® ganged A/B switching solution.

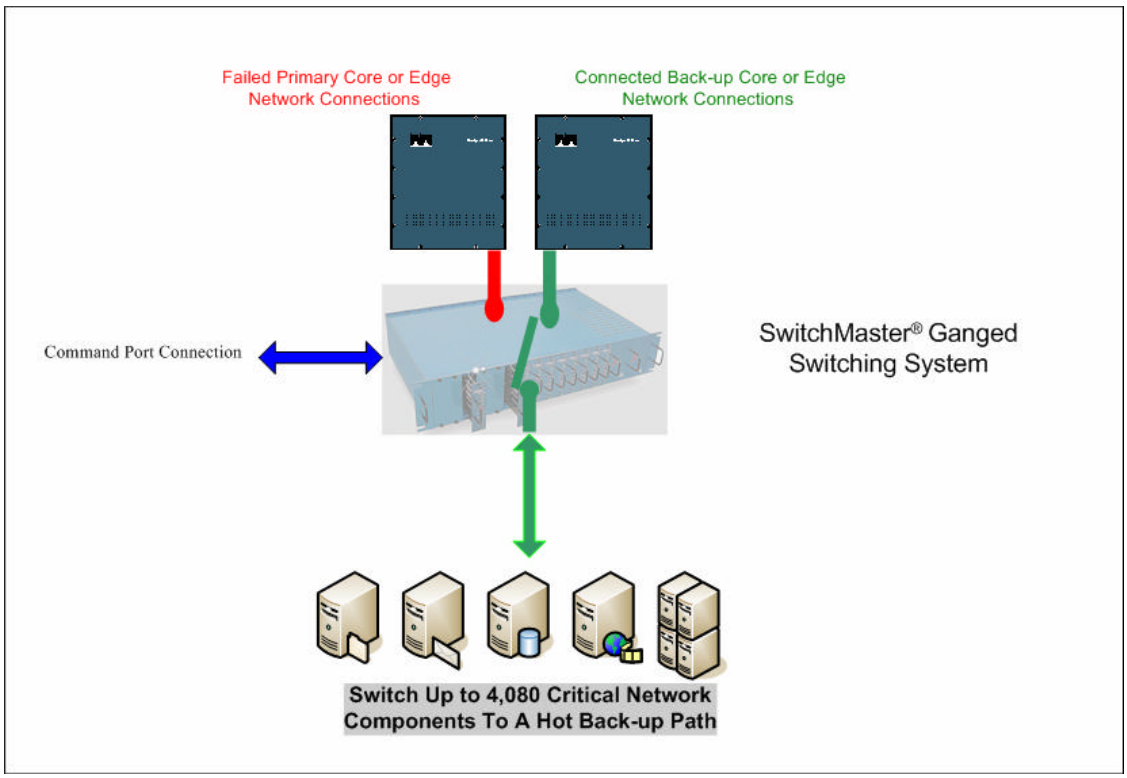


**Figure-1**

**Scenario B:** ***"You are the administrator of a sensitive data network at a Defense Department location. Your network is equipped with the best intrusion detection and firewall systems that money can buy. The network infrastructure is built from top-of-the-line hardware with all the best management and intelligence features. Operations run smoothly until traffic volume suddenly multiplies. The network is under cyber attack by a hostile agent in an offshore location. The IDS detects the hack and your remediation plan launches – a few seconds too late. A new worm moves virally through the network as you watch it spread. Data files are corrupted and sensitive information is being transmitted through the hacker's unexpected back door. Pulling the main fiber link is the fastest way to shut it down. Only a few minutes have elapsed. How much information was lost? How much was leaked? How long will it take to restore the corrupted files and to determine what got out? The magnitude of the required damage control will not be known for hours, maybe days, and there could be diplomatic consequences."***

Dramatic? You bet it is. Cyber terrorism is a fact of life in the Internet age. Civilization has come to depend on data networks and microprocessor-driven communications. Cell Phones, email, the electric power grid, ATM Machines, air traffic and even retail cash registers all incorporate network based technologies. Compromised networks can produce consequences far beyond mere inconvenience. Loss of life, compromised national security and financial ruin are well publicized consequences of network failures.

Cyber terrorists target the computers and networks that pervade modern civilization and maintain everyone's safety. Their attacks have come without warning and have destroyed and compromised critical information at Internet speed. The greatest challenges after an attack has begun can be to protect the network from continuing hacks while stopping the outflow of sensitive data. Often the best immediate response is to disconnect the critical network components including the WAN links as quickly as possible.

The damage in this case can be minimized by implementing a system for disconnecting the internal LAN from the WAN immediately upon detection of the hack.

The SwitchMaster® equipment deployed in this case is the same system as that of Scenario A but it's installed in a different manner. As illustrated in Figure 2, all network traffic passes through the SwitchMaster® System which also has connectivity to the intrusion detection system. Operation is elegantly simple: When the IDS detects a hostile event it issues a command to the SwitchMaster® system, isolating the paths to the affected equipment.

The system should also have conveniently located local control for managing individual blades and all blades in a system. The SwitchMaster system does this via toggle switches. Local terminal control is also standard in every SwitchMaster® system. Other control options are available, including remotely located manual switches and SNMP remote control.

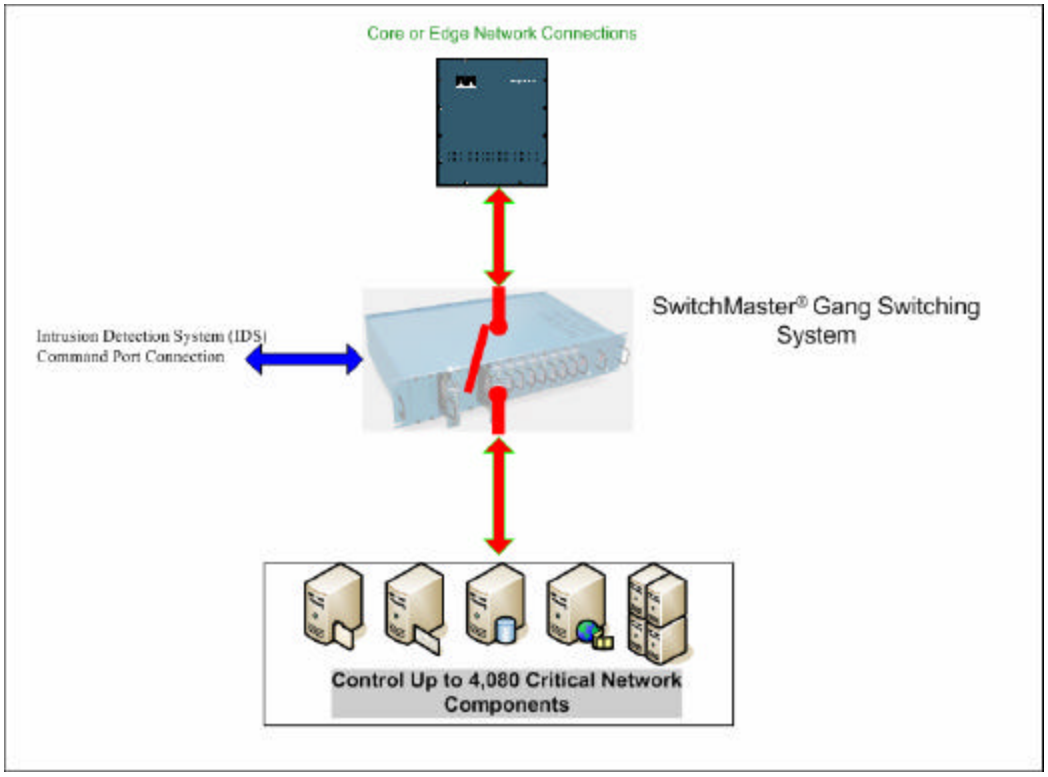


**Figure 2**

## About SwitchMaster® ganged A/B physical layer switching systems

SwitchMaster® Layer 1 switching solutions are scalable hardware systems used in disaster recovery, continuity of operations and network access control applications. They are conceptually similar to the manual desktop A/B switches that were commonly used to share a Personal Computer's communications port with a modem and a printer. In fact, we were the originators of those early switches and SwitchMaster® systems are their advanced evolutionary descendants. We have manufactured hundreds of thousands of switches, sharers and converters in Pittsburgh that have been shipped to users worldwide over several decades.

At the heart of the SwitchMaster® family is the 19" blade-based rack mount chassis which is built to accept up to 16 A/B switch cards. Cards are available to switch many different communications interfaces and include proprietary latching micro-mirror fiber optic switches and Category 6 Ethernet switches. Multiple chassis can be cascaded together easily and quickly to build switching systems capable of supporting thousands of switched ports, each controlled individually and all controlled by a single network administrator locally or remotely.

SwitchMaster® A/B switch interfaces include Category-6 RJ45 10GbE, latching and non-latching Fiber Optics, serial (DB9, DB15 and DB25), RF Video, Coax and more. Custom card designs and configurations are available. Most SwitchMaster® A/B switch cards employ latching relay or proprietary micro-mirror technology as the switching mechanism. There are many important key benefits associated with these techniques:

1. These relays and micro-mirrors maintain electrical and optical continuity through the connected path and provide true air gap isolation in the disconnected path.

2. The connected path appears as nothing more than an unimpeded cable connection and all switch cards pass data independently of data rates, formats/protocols, and signal levels. SwitchMaster® systems can be used in any communications environment including data, voice and video applications.

3. The air gap in the disconnected path provides high isolation that enforces security. Although network switches in higher network layers can deactivate or disable network ports via software or logic, their continuing physical connection enables potential back doors to information flow. Back doors are locked shut by SwitchMaster® systems.

4. Latching relay circuitry was developed long ago and has an established record of utmost reliability in telephone networks. The technologies employed in SwitchMaster® systems have service lives measured in millions of cycles. Similar to the telephone systems in which they were first used, Market Central's switches maintain their connections even when power fails or is removed.

5. SwitchMaster® solutions are energy efficient. Each SwitchMaster® switch card is typically idle and draws insignificant power. Peak power consumption only occurs when the system is actually changing connection states, and then this peak time is measured in milliseconds before the unit returns to the idle state.

6. For additional efficiency, "*Zero Power Mode*" can be established by simply removing power from the system once the desired port connections have been made. Power is re-applied to the system when port connection states must be changed. Again, the latching circuits ensure that data will pass through the system when power has been removed from it. There is no power consumed when a SwitchMaster® system is operated in Zero Power Mode.

7. SwitchMaster® solutions add no significant burden on data center cooling systems.

SwitchMaster® solutions are the most flexible, reliable and secure systems available and are widely deployed by well known financial service providers, in transportation signaling systems, process industries and within many government agencies including the United States Department of Defense. They provide security and enhance network availability in mission-critical systems worldwide. To learn more about SwitchMaster® solutions and the inherent reliability and security of hardware please contact our sales engineers now.

## About Market Central, Inc.

We have been providing advanced communications switching hardware to customers around the world for decades. Our solutions add reliability, security and network availability to critical data, voice and video networks. All of our products are designed, manufactured and quality-assured in Pittsburgh, Pennsylvania. Market Central is owned and operated by the engineers who design them. Many of our customers have purchased our products under the private labels of internationally recognized distributors.

SwitchMaster® Solutions =