Secure Switches for Today's Applications

Handling Traffic for Media-Rich, Data-Intensive Applications

Today's local area network (LAN) switches have tougher jobs than ever.

Convergence, or the merging of voice and multimedia traffic onto data networks, means LAN switches have to support Quality of Service (QoS) and other features, to ensure real-time applications get adequate service. Data-intensive applications also require proper handling, especially when they are extended over wide-area links, which applications like Microsoft Exchange were not originally architected for.

At the same time, the growing security challenges of today's network threats mean that IT has to provide security not only at the network perimeter (gateways to the Internet and private wide area networks) and on client and host computers, but also in the network itself.

"Security is one of the biggest concerns that medium-sized businesses have," states Sanjeev Aggarwal, senior analyst, small and medium business strategies, with the tech research firm Yankee Group. "Network-based on-demand applications like Salesforce.com and hosted applications like Microsoft Dynamics increase the need for security and performance, both inside the premises and overall in the communications layer."

Leading network vendors like Cisco, Enterasys, Foundry, Nortel and 3Com are addressing these challenges with the next generation of network switches — "secure switches," which embed security features like deep packet inspection (DPI) and intrusion detection directly into the switches' silicon. The result: cost-effective manageable security and appropriate performance.

"We're seeing a shift of customers from being concerned not so much about deploying technology for VoIP [Voice over Internet Protocol], convergence or other applications as deploying it while maintaining a secure environment for our existing applications and these new ones," says Steve Hargis, director of solutions architectures, Enterasys Networks, Inc. "Our customers are telling us that security is their top issue. Any business use of the network infrastructure poses a potential security risk. They have to factor that into any changes. So we have to make sure they can deploy not only network connectivity with QoS and other bandwidth requirements, but also do it in a way that locks down the availability of that service and maintains the security posture."

Regulatory compliance adds another reason for companies to embed security directly into their networks, notes Joel Conover, research director, Infrastructure & Security, with the tech research firm Current Analysis,, Inc., "There's a growing need for identity on the network, [to determine] what network user was connected to what port at what time."

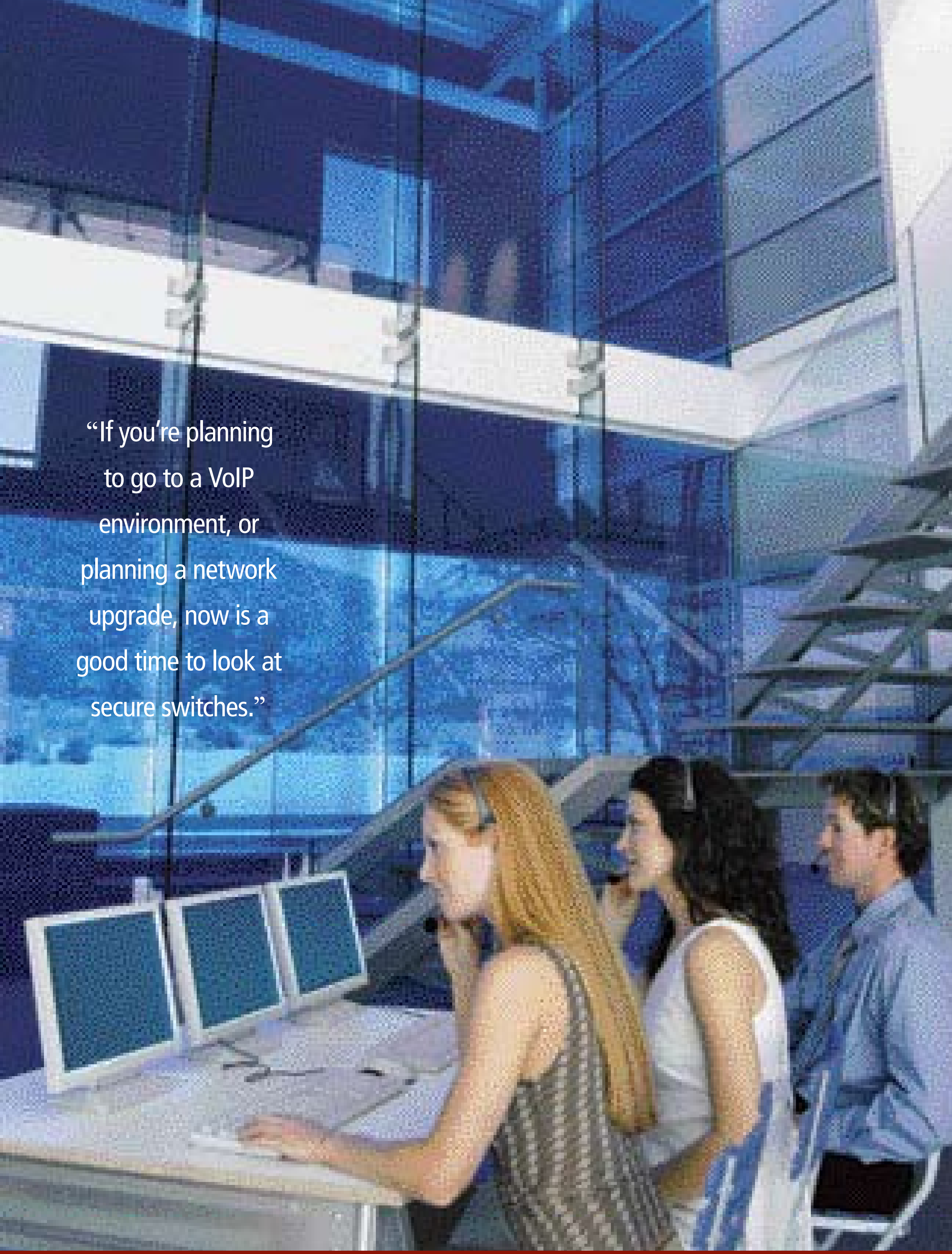
Switching Traffic

"Converging voice and data networks means your infrastructure has to do a number of things," says Nikos Koutsoukos, director, SMB Product Management, 3Com Corporation. "It needs to support QoS features to ensure adequate bandwidth so voice applications can run across the network." All of 3Com's switches can run and prioritize voice applications, Koutsoukos says.

"Voice as an application does funny things to your network. It can use unicast and multicast traffic, so your network has to be able to recognize these and handle them accordingly," he adds.

Adding more intelligence in the switch "lets it react," says Ed Kudey, senior manager of solutions development, Cisco Systems, Inc. "We support Layer 2 through Layer 4 QoS, and also Network-Based Application Recognition [NBAR], which lets the switch recognize applications and give them priority."

"If you look in a data center, applications need to be communicating in the multi-gigabit range, so you can need multiple secure 10 Gigabit Ethernet feeds," says Siva Subramanian, strategy leader, Security and Application Intelligence, Nortel. "And when you move into the network core, your bandwidth requirements are even greater, so your per-port firewall or intrusion prevention has to handle hundreds of gigabits per second of traffic. Doing full security on all that traffic may be too expensive, so we offer intelligent ways of optimizing what traffic gets inspected, using what filters and what functions get done. Many applications were designed to work inside the LAN, at LAN speeds, but not that well across the Internet, where there can be performance issues." »



“If you’re planning to go to a VoIP environment, or planning a network upgrade, now is a good time to look at secure switches.”

Security and Performance Features

However, as Dan Schrader, application switching product marketing manager with Nortel, points out, there are ways to accelerate application traffic, and these solutions can also provide security functions.

More than half of today's network security threats come from inside the network. "The model of there being a safe zone inside the network is no longer true," says Schrader. "Every endpoint has Internet access, so you can't just have a gateway and expect all relevant threats go through it and can be scanned. You need security in front of application servers, Web servers and other systems."

Putting security functions on the switches, versus deploying security appliances just outside each port, "gives you one less thing to control," says Current Analysis' Conover. "You'd have to funnel all that traffic through that device, which adds a bottleneck, or choose which traffic — or use it only for some mission critical act, like when a user logs in."

"Service and performance through in-the-switch intelligence complement each other," says Cisco's Kudey. "If we establish security through our switches, and have these secure switches in the wiring closets, where notebooks and wireless and desktops connect, the security decisions about traffic can be made there, rather than on the servers, or elsewhere in the network core. This reduces bad traffic before it gets onto the backbone — it's like deterring bad drivers before they get onto the highway."

"To assure service, you want a network with as few hops as possible, so that VoIP and multimedia experience will be seamless," says Nortel's Schrader. "Cables can't have security, so you put it into switches."

Another good reason to put security tasks inside switches, adds Schrader, is that many switches are already doing DPI. "Application switches — formerly known as load balancers — look at Layer 4 through Layer 7 information to make their routing decisions. If you're opening up packets and assembling packet fragments to do a Layer 7 inspection, you may as well look for threats." Nortel recently announced the addition of Symantec's Intrusion Detection and Prevention System, including Live Update capabilities, to its Application Switch.

"Security features are in our firmware, and can be key-activated," says Enterasys' Hargis. "For example, our Advanced Policy capability lets IT set and enforce permit/deny rules at ports of entry, such as 'this user can only talk to these applications.'" Access management will support methods including 802.1x and MAC-based access control. Other features include intrusion detection and prevention and class-of-service management.

"Also, we offer user node and neighbor discovery, Enterasys' intelligent location services, which let IT use the infrastructure to locate users and devices," says Hargis. "This is important when you have a real-time threat entering the network, so you can identify not only the threat, but also its source. And our network surveillance feature lets customers engage analysis tools like flow and port mirroring, right at the switch, so you can see what's causing a concern."

Security is no longer a "point product," observes Cisco's Kudey. "It's how it fits into the network architecture that matters. For example, Cisco's Network Admission Control [NAC] helps secure desktop machines' connections to the network, so that viruses or other problems don't propagate over the backbone." Most of Cisco's switches already have firewall, intrusion prevention and antivirus/antispyware, he notes. "We can leverage our NAC appliance to provide even more security at the switch."

Similarly, Enterasys' integrated framework and architecture lets IT "command and control our advanced security and policy features in a meaningful way, versus having to manage every switch to configure the security parameters," says Enterasys' Hargis. "This lets users command and control those features in a meaningful manner, versus managing every switch to configure the security parameters. And secure switches are available across the full range of sizes. Our modular Matrix N-Series has the advanced security and optimization features that server farms, data hosting and storage need for application and bandwidth control to and from servers. This protects the data center from intrusions on a user and application flow basis."

Security Inside Simplifies Management

"There has been an influx of point security products, making the network very complex, in purchase as well as operational costs to manage and to scale," says Nortel's Schrader. "As a result, networking companies are integrating more and more of the security features into routing and switching lines, built into the DNA of the network."

For example, Foundry Networks' SecureIron Security Traffic Managers and SecureIronLS secure LAN switches are designed, according to the company, "to be deployed as a security value-added alternative to traditional LAN switches in the distribution layer as an internal firewall, or at the edge as a personal firewall with direct desktop and server connectivity."

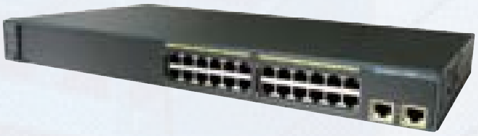
Foundry Networks' secure LAN switches protect against network and application-layer attacks, DoS (denial-of-service) attacks, intrusions, viruses, worms, spam and Web-based attacks, and also provide comprehensive admission, access and usage control for all traffic flowing to and from the edge of the network. "These switches look into the application layer, can string packets together to inspect more fully and apply security filters that IT has created, like 'Drop traffic belonging to a certain user,'" says Gopala Tumuluri, director of product management, Foundry Networks. "And if there is a virus or a worm, you can set up a signature or pattern match. Traditional Level 2/Level 3 switches don't make these kinds of security decisions."

3Com's switches offer a quarantine feature, says the firm's Koutsoukos, which works in conjunction with security devices like intrusion prevention systems and with policies set by IT to make sure that only authorized users are allowed to access the network.

Another management reason for in-switch security, says Foundry Networks' Tumuluri, is that "modular switches let you hot-swap and enhance modules. You can't do that with appliances." Marrying security features with the switch is a better approach than forcing organizations to deploy appliances that can't be scaled as easily. You need an appliance on each wire, but a switch can aggregate multiple links and switch traffic among them.

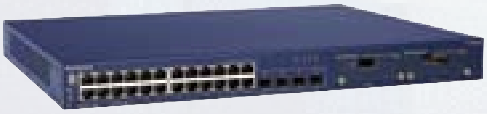
"Integrated security will absolutely be a trend," says Current Analysis' Joel Conover. "It's important look at this technology as part of an upgrade strategy. You have the opportunity to increase the security of your network. If you're planning to go to a VoIP environment, or planning a network upgrade, now is a good time to look at secure switches. Investment in them will let you cut down your troubleshooting."

Upgrading to secure switches also offers IT a chance to add Power over Ethernet (802.3af PoE), to provide power for VoIP, wireless access points, IP video security and other devices through LAN cabling, Conover points out. "This is a good time to add PoE as part of your upgrade. It will be much cheaper than a PoE midspan injector." ◊



Cisco® Catalyst® 2960 Series Intelligent Ethernet Switch
Integrated security includes NAC and advanced QoS
$822.99 CDW 850878
Page 4

3Com® Switch 4500 PWR
SSHv2 and SNMPv3 features ensure secure management access
$2319.99 CDW 875646
Page 7



NETGEAR® GSM7328S
Manage multiple switches securely via SNMPv3 and ProSafe™ software
$2023.99 CDW 867707
Page 8